$\mathfrak{Sl}_3(\mathbb{F}_q)$ et $\mathrm{PGL}_2(\mathbb{F}_q)$

Étienne AFFALOU
ENS de Rennes - Année scolaire 2025-2026

Référence : Philippe Caldero. *L'isomorphisme exceptionnel entre* $\mathrm{PGL}_2(\mathbb{F}_p)$ *et* $\mathrm{SO}_3(\mathbb{F}_p)$. https://www.youtube.com/watch?v=PB0ItBFah9s.
Recasages : Leçons 101, 103, 104, 106, 149, 170 et 190.

> Théorème Soit q un puissance d'un nombre premier impair avec $q \neq 3$.
> Alors, le groupe $\mathrm{SO}_3(\mathbb{F}_q)$ est isomorphe au groupe $\mathrm{PGL}_2(\mathbb{F}_q)$.

☞ **Étape 1 :** *Le groupe* $\mathrm{GL}_2(\mathbb{F}_q)$ *agit linéairement par conjugaison sur* $\mathfrak{sl}_2(\mathbb{F}_q) = \{M \in \mathcal{M}_2(\mathbb{F}_q) \mid \mathrm{Tr}(M) = 0\}$.
En effet, l'application associée $\begin{array}{rccc} \varphi & : & \mathrm{GL}_2(\mathbb{F}_q) & \longrightarrow & \mathrm{GL}(\mathfrak{sl}_2(\mathbb{F}_q)) \\ & & g & \longmapsto & (M \mapsto gMg^{-1}) \end{array}$ est bien définie (la conjugaison préserve la trace, et on a bien des applications linéaires inversibles à l'arrivée) et donne bien un morphisme de groupes.

☞ **Étape 2 :** *Le* det *sur* $\mathfrak{sl}_2(\mathbb{F}_q)$ *est une forme quadratique, congruente à la forme quadratique canonique de* $(\mathbb{F}_q)^3$.
Une matrice $M \in \mathfrak{sl}_2(\mathbb{F}_q)$ s'écrit $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ et son déterminant vaut alors $-a^2 - bc$, donc det est bien une forme quadratique sur $\mathfrak{sl}_2(\mathbb{F}_q)$. L'identité de polarisation ($2 \neq 0$) nous permet alors d'obtenir la matrice de notre forme quadratique det dans la base (E, F, H) avec $E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $F = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et $H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. On obtient la matrice $J = \mathrm{Mat}_{(E,F,H)}(\det) = \begin{pmatrix} 0 & -1/2 & 0 \\ -1/2 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. Le déterminant de J vaut $1/4 = (1/2)^2$, donc par la classification des formes quadratiques sur $\mathbb{F}_q$, det sur $\mathfrak{sl}_2(\mathbb{F}_q)$ est congruente à $Q(x, y, z) = x^2 + y^2 + z^2$.

☞ **Étape 3 :** *On a un morphisme injectif* $\mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow \mathrm{SO}_3(\mathbb{F}_q)$.
La conjugaison préservant la forme quadratique det, l'image du morphisme φ défini à l'étape 1 est dans $\mathrm{O}(\mathfrak{sl}_2(\mathbb{F}_q), \det)$. L'étape 2 assure que $\mathrm{O}(\mathfrak{sl}_2(\mathbb{F}_q), \det)$ est isomorphe à $\mathrm{O}_3(\mathbb{F}_q)$ donc on peut voir $\varphi : \mathrm{GL}_2(\mathbb{F}_q) \to \mathrm{O}_3(\mathbb{F}_q)$.
Une matrice dans le noyau de φ commute avec les éléments de $\mathfrak{sl}_2(\mathbb{F}_q)$, donc comme $\mathcal{M}_2(\mathbb{F}_q) = \mathfrak{sl}_2(\mathbb{F}_q) \oplus \mathbb{F}_q I_2$ ($\mathrm{Tr}(I_2) \neq 0$), le noyau de φ est égal au centre de $\mathrm{GL}_2(\mathbb{F}_q)$, d'où un morphisme injectif $\tilde{\varphi} : \mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow \mathrm{O}_3(\mathbb{F}_q)$.
Il reste à montrer que $\det(\varphi(g)) = 1$ pour tout $g \in \mathrm{GL}_2(\mathbb{F}_q)$. Mais si $g \in \mathrm{GL}_2(\mathbb{F}_q)$, on peut toujours écrire $g = \begin{pmatrix} \det(g) & 0 \\ 0 & 1 \end{pmatrix} g'$ avec $g' \in \mathrm{SL}_2(\mathbb{F}_q)$. Il suffit donc de montrer le résultat pour les matrices de $\mathrm{SL}_2(\mathbb{F}_q)$ et pour les matrices de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$ avec $\lambda \in (\mathbb{F}_q)^*$. Vu notre choix pour la valeur de q, $\mathrm{SL}_2(\mathbb{F}_q) = D(\mathrm{SL}_2(\mathbb{F}_q))$ donc comme $(\mathbb{F}_q)^*$ est abélien, les commutateurs puis les éléments de $\mathrm{SL}_2(\mathbb{F}_q)$ sont bien envoyés sur 1. Si $\lambda \in (\mathbb{F}_q)^*$,

$$\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \lambda a & \lambda b \\ c & -a \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \lambda b \\ \lambda^{-1} c & -a \end{pmatrix}$$

donc dans la base (E, F, H), l'image de notre matrice diagonale par φ est une matrice diagonale avec λ, λ^{-1} et 1 sur la diagonale : c'est bien une matrice de déterminant 1.

☞ **Étape 4 :** *On a* $|\mathrm{SO}_3(\mathbb{F}_q)| \leqslant |\mathrm{PGL}_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)/(q-1) = q(q^2-1)$.
Pour démontrer ce résultat, on introduit $N^* = \{M \in \mathfrak{sl}_2(\mathbb{F}_q) \mid \det(M) = 0 \text{ et } M \neq 0\}$. Le théorème de Cayley-Hamilton assure alors que $N^* = \{PEP^{-1}, P \in \mathrm{GL}_2(\mathbb{F}_q)\}$ (une matrice M de N^* est non nulle de carré nul, donc on peut construire une famille libre (MX, X) en prenant $X \notin \ker(M)$). Ainsi, N^* est l'orbite de E sous l'action de $\mathrm{GL}_2(\mathbb{F}_q)$ par conjugaison, donc $|N^*| = |\mathrm{GL}_2(\mathbb{F}_q)|/|\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_q)}(E)|$. Or une matrice $P \in \mathrm{GL}_2(\mathbb{F}_q)$ qui vérifie $PEP^{-1} = E$ s'écrit nécessairement sous la forme $P = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ (polynômes en E car on calcule en fait l'intersection du commutant de la matrice cyclique E avec $\mathrm{GL}_2(\mathbb{F}_q)$) donc $|\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_q)}(E)| = (q-1)q$, puis $|N^*| = (q^2-1)(q^2-q)/(q(q-1)) = q^2 - 1$. Maintenant, $\mathrm{SO}(\mathfrak{sl}_2(\mathbb{F}_q), \det)$ agit sur N^*, et l'orbite de E est dans N^*. Ainsi, $|\mathrm{SO}(\mathfrak{sl}_2(\mathbb{F}_q), \det)| = |\mathrm{Orb}(E)||\mathrm{Stab}(E)| \leqslant (q^2-1)|\mathrm{Stab}(E)|$. Il reste à montrer que $|\mathrm{Stab}(E)| = q$.

Dans la base (E,F,H), une matrice de $\mathrm{Stab}(E)$ s'écrit $P=\begin{pmatrix}1&a&d\\0&b&e\\0&c&f\end{pmatrix}$, avec $P^TJP=J$ et $\det(P)=1$. Mais

$$P^TJP=-\begin{pmatrix}1&0&0\\a&b&c\\d&e&f\end{pmatrix}\begin{pmatrix}0&1/2&0\\1/2&0&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&a&d\\0&b&e\\0&c&f\end{pmatrix}=-\begin{pmatrix}0&1/2&0\\b/2&a/2&c\\e/2&d/2&f\end{pmatrix}\begin{pmatrix}1&a&d\\0&b&e\\0&c&f\end{pmatrix}$$

donc

$$\begin{pmatrix}0&1/2&0\\1/2&0&0\\0&0&1\end{pmatrix}=-P^TJP=\begin{pmatrix}0&b/2&e/2\\b/2&ab+c^2&(bd+ae)/2+cf\\e/2&(bd+ae)/2+cf&ed+f^2\end{pmatrix}.$$

La première ligne donne $b=1$ et $e=0$. Comme $\det(P)=1$, on a $bf-ce=1$ donc $f=1$. Sur la deuxième ligne, on trouve $ab+c^2=0$ puis $a=-c^2$, et $bd+ae=-2cf$ soit $d=-2c$. Ainsi, notre matrice P s'écrit

$$P=\begin{pmatrix}1&-c^2&-2c\\0&1&0\\0&c&1\end{pmatrix}\text{ avec } c\in\mathbb{F}_q.$$

On vérifie que les matrices de cette forme sont effectivement dans $\mathrm{Stab}(E)$, et donc que $|\mathrm{Stab}(E)|=q$.

☞ **Étape 5 :** *Conclusion.* On a trouvé un morphisme injectif $\tilde{\varphi}:\mathrm{PGL}_2(\mathbb{F}_q)\hookrightarrow\mathrm{SO}_3(\mathbb{F}_q)$ donc $|\mathrm{PGL}_2(\mathbb{F}_q)|\leqslant|\mathrm{SO}_3(\mathbb{F}_q)|$, et on a montré à l'étape 4 que $|\mathrm{PGL}_2(\mathbb{F}_q)|\geqslant|\mathrm{SO}_3(\mathbb{F}_q)|$. On a donc égalité des cardinaux, et notre morphisme est bien bijectif comme voulu.

Remarques sur le développement :
- Il faut savoir donner les grandes lignes de la preuve de la classification des formes quadratiques sur les corps finis.
- Pour démontrer que $\mathrm{SL}_2(\mathbb{F}_q)$ est un groupe parfait, savoir comment une transvection s'écrit comme un commutateur.
- Le résultat annoncé tient toujours pour $q=3$, comme on le voit en faisant les calculs à la main par exemple.
- Pour des valeurs de q petites, les groupes projectifs linéaires sont des groupes symétriques ! Exemple : $\mathrm{SO}_3(\mathbb{F}_5)\simeq\mathfrak{S}_5$.
- La situation est ici plus compliquée que pour les groupes $\mathrm{SO}_2(\mathbb{F}_q)$, ces derniers étant toujours cycliques.