Proposition 1. *On a les isomorphismes suivant :*

$$\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathcal{A}_4 \text{ et } \mathrm{SL}_2(\mathbb{F}_3) \simeq Q_8 \rtimes_\rho \mathbb{Z}/3\mathbb{Z}$$

pour un certain $\rho \in \mathrm{Hom}(\mathbb{Z}/3\mathbb{Z}, \mathrm{Aut}(Q_8))$.

Résumé de la preuve :

1 On prouve le premier isomorphisme en faisant agir $\mathrm{SL}_2(\mathbb{F}_3)$ sur l'ensemble des droites de $\mathbb{F}_3^2$ (ou $\mathbb{P}^1(\mathbb{F}_3)$ de son petit nom) pour obtenir le premier isomorphisme.

2 Le morphisme $\mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow \mathcal{A}_4$ permet de tirer en arrière $V_4 \lhd \mathcal{A}_4$ en un sous-groupe $H \lhd \mathrm{SL}_2(\mathbb{F}_3)$ de cardinal égal à 8. On obtient alors presque gratuitement $\mathrm{SL}_2(\mathbb{F}_3) \simeq H \rtimes_\rho \mathbb{Z}/3\mathbb{Z}$.

3 On étudie H et on montre $H \simeq Q_8$ à partir d'une présentation de Q_8.

Démonstration. **Étape 1 :** On note $\mathbb{P}^1(\mathbb{F}_3)$ l'ensemble des droites du plan $\mathbb{F}_3^2$. Cet ensemble est fini et on peut le dénombrer facilement : les droites correspondent (en enlevant 0) aux orbites de l'action par multiplication externe de $\mathbb{F}_3^\times$ sur $\mathbb{F}_3^2 \setminus \{0\}$. Cette action est libre ($\lambda \cdot x = x \Rightarrow x = 0$ ou $\lambda = 1$) donc [1]

$$|\mathbb{P}^1(\mathbb{F}_3)| = \frac{|\mathbb{F}_3^2 \setminus \{0\}|}{|\mathbb{F}_3^\times|} = \frac{3^2 - 1}{3 - 1} = 3 + 1 = 4.$$

On obtient alors un morphisme $\mathrm{SL}_2(\mathbb{F}_3) \to \mathcal{S}_4$. Le noyau de ce morphisme correspond aux endomorphismes du plan de déterminant 1 stabilisant toutes les droites. On sait qu'un endomorphisme stabilise toutes les droites si et seulement si c'est une homothétie [2] et elle est de déterminant 1 si et seulement si son rapport est une racine carré de l'unité. Or, $\mathbb{F}_3$ admet exactement deux racines carrés de l'unité : $\{\pm 1\}$. De plus, le quotient de $\mathrm{SL}_2(\mathbb{F}_3)$ par ce noyau est $\mathrm{PSL}_2(\mathbb{F}_3)$ [3]. Ainsi, on obtient un morphisme injectif

$$\mathrm{SL}_2(\mathbb{F}_3)/\{\pm I_2\} = \mathrm{PSL}_2(\mathbb{F}_3) \hookrightarrow \mathcal{S}_4.$$

Enfin, on a

$$|\mathrm{SL}_2(\mathbb{F}_3)| = \frac{|\mathrm{GL}_2(\mathbb{F}_3)|}{|\mathbb{F}_3^\times|} = \frac{3(3^2 - 1)(3 - 1)}{3 - 1} = (3 - 1) \cdot 3 \cdot (3 + 1) = 4!$$

donc l'indice de $\mathrm{PSL}_2(\mathbb{F}_3)$ dans $\mathcal{S}_4$ est 2 d'où [4] :

$$\boxed{\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathcal{A}_4.}$$

Étape 2 : Notons $\pi : \mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow \mathcal{A}_4$ le morphisme surjectif ainsi obtenu. Le groupe $\mathcal{A}_4$ admet un sous-groupe propre distingué engendré par les doubles transpositions

$$V_4 = \{\mathrm{id}, a, b, c\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

que l'on peut tirer en arrière en un sous-groupe $H := \pi^{-1}(V_4) \lhd \mathrm{SL}_2(\mathbb{F}_3)$ qui est de cardinal (théorème de Lagrange) $|\{\pm I_2\}| \cdot |V_4| = 8$.

1. Le fait que G agit librement sur X revient à dire que les stabilisateurs sont tous triviaux et donc par relation orbite-stabilisateur, que les orbites sont toutes de cardinal $|G|$. Ainsi si on note X/G l'ensemble des G-orbites de X, on a $|X| = |X/G| \cdot |G|$ si bien que

$$|X/G| = \frac{|X|}{|G|}$$

2. Poser λ_x le scalaire tel que $u(x) = \lambda_x \cdot x$ et vérifier que si $x \neq y$ on a $\lambda_x = \lambda_y$ dans le cas où x et y sont alignés et vérifier $\lambda_x = \lambda_{x+y} = \lambda_y$ dans l'autre.

3. On pourrait très bien définir $\mathrm{PSL}_n(K)$ comme le quotient de $\mathrm{SL}_n(K)$ par le noyau de l'action de ce dernier sur les droites de K^n mais ce n'est pas classique. Si on souhaite montrer que ce noyau coïncide avec le centre de $\mathrm{SL}_n(K)$ on utilise la commutation avec les transvections (qui sont de déterminant 1). De manière générale, si τ est une transvection de droite D, *i.e* il existe $\varphi \in E^* \setminus \{0\}$ et $a \in D \setminus \{0\} \subset \mathrm{Ker}(\varphi)$ tels que $\tau(x) = x + \varphi(x)a$, alors pour tout endomorphisme u, le conjugué $u\tau u^{-1}$ est une transvection de droite $u(D)$. Ainsi, un endomorphisme commutant avec toutes les transvection stabilise toutes les droites et réciproquement, un endomorphisme stabilisant toutes les droites et une homothétie et donc commute avec tout ce que l'on souhaite. On peut aussi faire ça matriciellement en regardant la commutation avec les transvections élémentaires $T_{i,j} := I_n + E_{i,j}$ avec $i \neq j$.

4. Un sous-groupe d'indice 2 est forcément distingué et $\mathcal{S}_n$ n'admet qu'un seul sous-groupe distingué d'indice 2 puisqu'il n'existe qu'un seul morphisme non trivial de $\mathcal{S}_n$ vers $\mathbb{Z}/2\mathbb{Z}$.

Comme tous les groupes d'ordre 3 sont cycliques, on a une suite exacte :

$$H \hookrightarrow \mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}$$

qui est alors scindée à droite [5]. En effet, pour la scinder, il suffit de trouver un élément α d'ordre 3 dans $\mathrm{SL}_2(\mathbb{F}_3)$ dont on peut montrer l'existence de deux manières. On peut évoquer l'existence des 3-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$ qui sont d'ordre 3. Ou bien, on peut trouver directement un élément d'ordre 3 comme $\alpha = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Le sous-groupe de $\mathrm{SL}_2(\mathbb{F}_3)$ d'ordre 3 alors exhibé agit par conjugaison sur H et on a $\boxed{\mathrm{SL}_2(\mathbb{F}_3) \simeq H \rtimes \langle \alpha \rangle}$.

Étape 3 : Pour trouver la structure de H, on part de la suites exacte

$$\{\pm I_2\} \hookrightarrow H \xrightarrow{\pi} \!\!\!\!\twoheadrightarrow V_4$$

et on va montrer qu'alors H est isomorphe à $Q_8 = \langle -1, i, j, k \,|\, (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$. En faisant agir $\{\pm I_2\}$ sur H par multiplication à gauche, on sait qu'il existe des matrices $A, B, C \in H$ telles que $H = \{\pm I_2, \pm A, \pm B, \pm C\}$. On sait que $(-I_2)^2 = I_2$ ce qui nous invite à montrer les relations

$$A^2 = B^2 = C^2 = ABC = -I_2.$$

Soit $M \in \{A, B, C\}$. On a $\pi(M^2) = \pi(M)^2 = \mathrm{id}$ car les doubles transpositions sont d'ordre 2. Ainsi, $M^2 \in \{\pm I_2\}$. Or, les seules matrices vérifiant $M^2 = I_2$ sont $\pm I_2$. En effet, si $M^2 = I_2$, alors le polynôme $X^2 - 1 = (X-1)(X+1)$ annule M. Ce polynôme étant scindé à racines simples, M est diagonalisable avec pour valeurs propres $\lambda_1, \lambda_2 \in \{\pm 1\}$. Comme $\lambda_1 \lambda_2 = \det(M) = 1$ on a $\lambda_1 = \lambda_2$ et $M = \pm I_2$. Finalement, comme $M \neq \pm I_2$ par hypothèse, on a forcément d'après ce qui précède $\boxed{M^2 = -I_2}$.

Pour la dernière relation, même stratégie. On a $\pi(ABC) = \pi(A)\pi(B)\pi(C) = \mathrm{id}$. En effet, comme π est surjectif, il induit un isomorphisme entre $H/\{\pm I_2\}$ et V_4 si bien que $\pi(A)\pi(B)\pi(C) = abc = 1$. Ainsi, on a bien $ABC \in \{\pm I_2\}$. S'il s'avère que $ABC = I_2$, on peut toujours remplacer A par $-A$: ça ne change pas les relations précédentes puisque $(-A)^2 = A^2$ et on aura alors $\boxed{ABC = -I_2}$. Finalement, on a

$$\boxed{H = \langle -I_2, A, B, C \,|\, (-I_2)^2 = 1, A^2 = B^2 = C^2 = ABC = -I_2 \rangle \simeq Q_8}.$$

✿

Remarque 2. Le sous-groupe H est en fait le groupé dérivé $D(\mathrm{SL}_2(\mathbb{F}_3))$. C'est une pathologie du corps à 3 éléments car au delà de 3, on a toujours $D(\mathrm{SL}_2(\mathbb{F}_q)) = \mathrm{SL}_2(\mathbb{F}_q)$ par simplicité de $\mathrm{PSL}_2(\mathbb{F}_q)$. Par ailleurs, cette pathologie se comprend bien par l'action mise en évidence : $D(\mathcal{A}_4) = V_4$ donc $D(\mathrm{SL}_2(\mathbb{F}_3)) \subset \pi^{-1}(V_4) \subsetneq \mathrm{SL}_2(\mathbb{F}_3)$.
Remarque 3. Le groupe $\mathrm{SO}_2(\mathbb{F}_3)$ est un groupes cyclique d'ordre 4 (car -1 n'est pas un carré modulo 3). Il est engendré par exemple par la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Ainsi, ses éléments sont d'ordres 1, 2 ou 4 et leurs images par π dans $\mathcal{A}_4$ sont donc forcément dans V_4. On a alors $\mathrm{SO}_2(\mathbb{F}_3) \subset H$ et on peut identifier $i \in Q_8$ à une rotation du plan sur $\mathbb{F}_3$.
Remarque 4. On peut montrer que $\mathrm{SL}_2(\mathbb{F}_3)$ n'est pas isomorphe à $Q_8 \times \mathbb{Z}/3\mathbb{Z}$. En effet, en considérant la matrice $i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in H$ et $\alpha = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, on a $i\alpha i^{-1} = -i\alpha i = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \notin \{I_2, \alpha, \alpha^{-1}\} = \langle \alpha \rangle$. Donc, $\mathrm{SL}_2(\mathbb{F}_3)$ ne peut pas admettre un unique 3-Sylow puisqu'il y en a un non distingué (il en contient exactement 4) contrairement à $Q_8 \times \mathbb{Z}/3\mathbb{Z}$ qui n'en contient bien qu'un seul.
Remarque 5. On n'a pas cherché à détailler la nature du morphisme $\rho : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(Q_8)$ en se contentant de dire que l'on fait juste agir n'importe quel 3-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$ sur H par conjugaison. En fait, on peut montrer que tous les produits semi-directs non triviaux de Q_8 par $\mathbb{Z}/3\mathbb{Z}$ sont isomorphes mais c'est loin d'être évident. On part de la propriété suivante dont la démonstration ne pose aucun problème.

5. On dit qu'une suite exacte de morphisme surjectif $\pi : E \twoheadrightarrow Q$ est scindée à droite si π admet une section *i.e* un morphisme de groupe $s : Q \to E$ tel que $\pi \circ s = \mathrm{id}_Q$. On peut montrer qu'une suite exacte est scindée à droite si et seulement si elle est équivalente à la suite exacte d'un produit semi-direct. On peut bien-sûr ignorer tout ce vocabulaire et simplement chercher un 3-Sylow et vérifier les axiomes du produit semi-direct interne à la main.

Proposition 6. *Soit N et Q deux groupes. L'action de* $\mathrm{Aut}(\mathrm{Aut}(N))$ *sur* $\mathrm{Hom}(Q, \mathrm{Aut}(N))$ *par post-composition induit par restriction à* $\mathrm{Int}(\mathrm{Aut}(N))$ *une action de* $\mathrm{Aut}(N)$ *sur* $\mathrm{Hom}(Q, \mathrm{Aut}(N))$*. Si deux morphismes $\rho, \rho' : Q \to \mathrm{Aut}(N)$ sont dans la même orbite pour cette action* i.e *il existe $\alpha \in \mathrm{Aut}(N)$ tel que pour tout $x \in Q$, $\rho'(x) = \alpha \circ \rho(x) \circ \alpha^{-1}$, alors on a un isomorphisme :*

$$N \rtimes_{\rho} Q \xrightarrow{\sim} N \rtimes_{\rho'} Q$$

$$(n, x) \longmapsto (\alpha(n), x)$$

Dans notre cas on peut montrer (pas évident) que $\mathrm{Aut}(Q_8) \simeq \mathcal{S}_4$. L'ensemble $\mathrm{Hom}(\mathbb{Z}/3\mathbb{Z}, \mathrm{Aut}(Q_8))$ s'identifie alors à l'ensemble $X = \{\mathrm{id}\} \cup \{\text{3-cycles}\} \subset \mathcal{S}_4$ et l'action de $\mathrm{Aut}(Q_8)$ sur cet ensemble correspond à l'action de $\mathcal{S}_4$ sur X par conjugaison. Or, cet ensemble admet exactement deux classes de conjugaison :

— $\{\mathrm{id}\}$ correspondant à l'action triviale et donc au produit direct $Q_8 \times \mathbb{Z}/3\mathbb{Z}$.

— L'ensemble des 3-cycles de $\mathcal{S}_4$ correspondant à la classe des produits semi-directs non triviaux alors tous isomorphes à $\mathrm{SL}_2(\mathbb{F}_3)$.