

$\mathbf{SL}_2(\mathbf{F}_3)$

OLIVIER SERMAN

Théorème. *Le groupe $\mathbf{SL}_2(\mathbf{F}_3)$ est un produit semi-direct $\mathbf{H}_8 \rtimes \mathbf{Z}/3\mathbf{Z}$ du groupe des quaternions \mathbf{H}_8 et de $\mathbf{Z}/3\mathbf{Z}$.*

Le groupe $\mathbf{SL}_2(\mathbf{F}_3)$ est d'ordre 24. Il est donc naturel de se demander si ce groupe est isomorphe à \mathfrak{S}_4 . Ce ne peut être le cas, puisque le centre $Z(\mathbf{SL}_2(\mathbf{F}_3))$ de $\mathbf{SL}_2(\mathbf{F}_3)$ est le groupe à deux éléments $\{\pm \text{id}\}$, tandis que celui du groupe symétrique est trivial.

On a donc un groupe non abélien d'ordre 24 qui n'est pas isomorphe à \mathfrak{S}_4 , dont on veut comprendre la structure¹.

On donne ici deux façons de parvenir à ce résultat. La première repose sur la compréhension du sous-groupe dérivé de $\mathbf{SL}_2(\mathbf{F}_3)$. La seconde, plus directe et plus explicite, ne demande qu'un peu d'algèbre linéaire.

1. PREMIÈRE MÉTHODE : CONSIDÉRATION DU GROUPE DÉRIVÉ

On montre que le groupe dérivé $D(\mathbf{SL}_2(\mathbf{F}_3))$ de $\mathbf{SL}_2(\mathbf{F}_3)$ est le groupe des quaternions \mathbf{H}_8 , en commençant par étudier la structure de $\mathbf{PSL}_2(\mathbf{F}_3)$.

Étape 1 : $\mathbf{PSL}_2(\mathbf{F}_3) \simeq A_4$

Le point de départ est l'isomorphisme

$$\mathbf{PGL}_2(\mathbf{F}_3) \simeq \mathfrak{S}_4$$

qu'on obtient ainsi (cf. Perrin pour les détails) : on fait opérer $\mathbf{GL}_2(\mathbf{F}_3)$ sur l'espace projectif $\mathbf{P}^1(\mathbf{F}_3)$ des droites vectorielles du plan \mathbf{F}_3^2 , une transformation $g \in \mathbf{GL}_2(\mathbf{F}_3)$ envoyant la droite engendrée par un vecteur u sur la droite engendrée par le vecteur $g(u)$. On a donc un morphisme $\mathbf{GL}_2(\mathbf{F}_3) \rightarrow \mathfrak{S}_{\mathbf{P}^1(\mathbf{F}_3)}$, dont le noyau est exactement le sous-groupe des homothéties. Comme $\mathbf{P}^1(\mathbf{F}_3)$ contient 4 éléments, on a donc une injection $\mathbf{PGL}_2(\mathbf{F}_3) \hookrightarrow \mathfrak{S}_4$. Ces groupes ayant même cardinal, cette injection est un isomorphisme.

On a alors que $\mathbf{PSL}_2(\mathbf{F}_3)$ est un sous-groupe d'indice 2 dans $\mathbf{PGL}_2(\mathbf{F}_3) \simeq \mathfrak{S}_4$. C'est donc le groupe alterné A_4 .

Étape 2 : détermination du groupe dérivé $D(\mathbf{SL}_2(\mathbf{F}_3))$

On connaît le sous-groupe dérivé de A_4 , qui est le groupe de Klein

$$D(A_4) = V_4 \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

(rappelons que ce groupe apparaît comme le sous-groupe H constitué des double-transpositions : on « voit » que c'est le sous-groupe dérivé $D(A_4)$ en notant que ce sous-groupe est distingué, d'indice 3, de sorte que le quotient A_4/H est $\mathbf{Z}/3\mathbf{Z}$, qui est abélien. Mais, comme H n'a aucun sous-groupe distingué non trivial, H est le sous-groupe dérivé).

On a donc une suite exacte

$$1 \rightarrow D(\mathbf{PSL}_2(\mathbf{F}_3)) \rightarrow \mathbf{PSL}_2(\mathbf{F}_3) \rightarrow \mathbf{Z}/3\mathbf{Z} \rightarrow 0.$$

Date: 4 janvier 2011.

¹Rappelons qu'il y a 15 groupes de cardinal 24, à isomorphisme près (cf. Perrin, exercice I.E.5).

On veut maintenant déterminer le groupe dérivé $D(\mathbf{SL}_2(\mathbf{F}_3))$ de $\mathbf{SL}_2(\mathbf{F}_3)$. On commence par remarquer que la composée des projections $\mathbf{SL}_2(\mathbf{F}_3) \rightarrow \mathbf{PSL}_2(\mathbf{F}_3)$ et $\mathbf{PSL}_2(\mathbf{F}_3) \rightarrow \mathbf{Z}/3\mathbf{Z}$ donne une application surjective

$$\mathbf{SL}_2(\mathbf{F}_3) \twoheadrightarrow \mathbf{Z}/3\mathbf{Z}.$$

Le sous-groupe dérivé $D(\mathbf{PSL}_2(\mathbf{F}_3))$ est contenu dans le noyau de ce morphisme, qui est d'ordre $24/3 = 8$. On va montrer que le groupe dérivé est exactement égal au noyau de ce morphisme. Il suffit de montrer qu'il est d'ordre 8.

Pour cela on remarque que la projection $\mathbf{SL}_2(\mathbf{F}_3) \twoheadrightarrow \mathbf{PSL}_2(\mathbf{F}_3)$ induit une projection

$$D(\mathbf{SL}_2(\mathbf{F}_3)) \twoheadrightarrow D(\mathbf{PSL}_2(\mathbf{F}_3))$$

(de manière générale, tout morphisme de groupes $G \twoheadrightarrow G'$ surjectif induit une surjection $D(G) \twoheadrightarrow D(G')$: en effet, l'image d'un commutateur de G est un commutateur, et tout commutateur de G' est image d'un commutateur de G ...).

Puisque $D(\mathbf{PSL}_2(\mathbf{F}_3)) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ est d'ordre 4, l'ordre du groupe $D(\mathbf{SL}_2(\mathbf{F}_3))$ est au moins égal à 4. Comme il divise 8, il vaut 4 ou 8. Supposons qu'il soit d'ordre 4². La surjection $D(\mathbf{SL}_2(\mathbf{F}_3)) \twoheadrightarrow D(\mathbf{PSL}_2(\mathbf{F}_3))$ serait alors un isomorphisme, et le groupe dérivé $D(\mathbf{SL}_2(\mathbf{F}_3))$ serait un sous-groupe de $\mathbf{SL}_2(\mathbf{F}_3)$ isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. En particulier, $\mathbf{SL}_2(\mathbf{F}_3)$ contiendrait au moins 3 éléments d'ordre 2, ce qui est faux en vertu du lemme d'algèbre linéaire suivant :

Lemme. *Les seules involutions contenues dans $\mathbf{SL}_2(\mathbf{F}_3)$ sont $\pm \text{id}$.*

Démonstration. Le polynôme minimal d'un tel élément g divise $X^2 - 1$: g est donc diagonalisable. Son déterminant étant égal à 1, g est une homothétie. \square

Conclusion : on a montré que $D(\mathbf{SL}_2(\mathbf{F}_3))$ est d'ordre 8, et qu'il ne contient qu'un seul élément d'ordre 2. Mais on connaît les groupes d'ordre 8 : comme $D(\mathbf{SL}_2(\mathbf{F}_3))$ ne contient qu'un seul élément d'ordre 2, il est isomorphe ou bien à \mathbf{H}_8 , ou bien au groupe cyclique $\mathbf{Z}/8\mathbf{Z}$. Ce second cas est impossible, car $D(\mathbf{SL}_2(\mathbf{F}_3))$ se projette sur $D(\mathbf{PSL}_2(\mathbf{F}_3)) = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ qui n'est pas cyclique (on peut aussi retrouver la structure du groupe des quaternions en considérant la suite exacte $0 \rightarrow \mathbf{Z}/2\mathbf{Z} \rightarrow D(\mathbf{SL}_2(\mathbf{F}_3)) \rightarrow \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \rightarrow 0$ et le lemme précédent).

On a donc établi le résultat suivant

Proposition. *Il existe un isomorphisme*

$$D(\mathbf{SL}_2(\mathbf{F}_3)) \simeq \mathbf{H}_8.$$

Conclusion

On a montré que $D(\mathbf{SL}_2(\mathbf{F}_3))$ est un sous-groupe distingué d'indice 3 dans $\mathbf{SL}_2(\mathbf{F}_3)$. Autrement dit, on a une suite exacte

$$1 \rightarrow \mathbf{H}_8 \rightarrow \mathbf{SL}_2(\mathbf{F}_3) \rightarrow \mathbf{Z}/3\mathbf{Z} \rightarrow 0.$$

On en déduit (grâce à l'existence des 3-Sylow) que $\mathbf{SL}_2(\mathbf{F}_3)$ est produit semi-direct de \mathbf{H}_8 et $\mathbf{Z}/3\mathbf{Z}$.

Il convient d'accompagner cette démonstration du diagramme suivant que l'on complète au fur et à mesure

$$\begin{array}{ccccccc} 1 & \longrightarrow & D(\mathbf{SL}_2(\mathbf{F}_3)) & \hookrightarrow & \mathbf{SL}_2(\mathbf{F}_3) & & \\ & & \downarrow & & \downarrow & \searrow & \\ 1 & \longrightarrow & D(\mathbf{PSL}_2(\mathbf{F}_3)) & \hookrightarrow & \mathbf{PSL}_2(\mathbf{F}_3) & \twoheadrightarrow & \mathbf{Z}/3\mathbf{Z} \longrightarrow 0 \end{array}$$

²Il est sans doute plus élégant de montrer directement que le noyau de la projection $D(\mathbf{SL}_2(\mathbf{F}_3)) \twoheadrightarrow D(\mathbf{PSL}_2(\mathbf{F}_3))$ est $Z(\mathbf{SL}_2(\mathbf{F}_3)) \cap D(\mathbf{SL}_2(\mathbf{F}_3))$, qui est égal à $Z(\mathbf{SL}_2(\mathbf{F}_3)) = \{\pm 1\}$ puisque $D(\mathbf{SL}_2(\mathbf{F}_3))$ contient, en tant que sous-groupe d'ordre une puissance de 2, un élément d'ordre 2, qui ne peut être que $-\text{id}$ vu le lemme. Le sous-groupe dérivé s'insère donc dans une suite exacte $1 \rightarrow Z(\mathbf{SL}_2(\mathbf{F}_3)) \rightarrow D(\mathbf{SL}_2(\mathbf{F}_3)) \rightarrow D(\mathbf{PSL}_2(\mathbf{F}_3)) \rightarrow 1$.

Pour aller plus loin, explicitons la structure de ce produit semi-direct.

Il s'agit de comprendre l'opération d'un 3-Sylow de $\mathbf{SL}_2(\mathbf{F}_3)$ sur le 2-Sylow. Pour cela, il suffit d'exhiber les éléments de $\mathbf{SL}_2(\mathbf{F}_3)$ d'ordre (divisant) 4 et un élément η d'ordre 3, et d'expliciter l'opération de η sur les éléments d'ordre (divisant) 4.

On peut aussi chercher les éléments d'ordre 3 dans $\text{Aut}(\mathbf{H}_8)$. Il faut se rappeler que $\text{Aut}(\mathbf{H}_8)$ est isomorphe au groupe symétrique \mathfrak{S}_4 . Dans ce groupe les éléments d'ordre 3 sont 2 à 2 conjugués, de sorte qu'il n'y a à isomorphisme près qu'un seul produit semi-direct de \mathbf{H}_8 et $\mathbf{Z}/3\mathbf{Z}$ non isomorphe à un produit direct. Il reste donc à vérifier que $\mathbf{SL}_2(\mathbf{F}_3)$ n'est pas isomorphe à un produit direct. On peut par exemple noter qu'il ne peut y avoir un seul 3-Sylow dans $\mathbf{SL}_2(\mathbf{F}_3)$, car on sait qu'il y a 4 3-Sylow dans $\mathbf{PSL}_2(\mathbf{F}_3)$.

En conclusion, on a montré que $\mathbf{SL}_2(\mathbf{F}_3)$ est l'unique produit semi-direct non trivial de \mathbf{H}_8 et $\mathbf{Z}/3\mathbf{Z}$.

2. SECONDE MÉTHODE : UN PEU D'ALGÈBRE LINÉAIRE

Le groupe $\mathbf{SL}_2(\mathbf{F}_3)$ est d'ordre $24 = 2^3 \cdot 3$. Il résulte du théorème de Sylow que $\mathbf{SL}_2(\mathbf{F}_3)$ contient 1 ou 3 2-Sylow. On va montrer qu'il n'y en a qu'un, en comptant les éléments d'ordre divisant 8.

Éléments d'ordre 2 dans $\mathbf{SL}_2(\mathbf{F}_3)$: le polynôme minimal d'un élément $g \in \mathbf{SL}_2(\mathbf{F}_3)$ d'ordre 2 divise $X^2 - 1 = (X - 1)(X + 1)$, et est donc égal à $X + 1$ ou à $X^2 - 1$. Le second cas est exclu, car $X^2 - 1$ serait le polynôme caractéristique de g , et son déterminant serait égal à -1 . On a donc³ :

Lemme. *$g = -\text{id}$ est le seul élément d'ordre 2 dans $\mathbf{SL}_2(\mathbf{F}_3)$.*

Remarquons que puisque tout 2-Sylow contient (au moins) un élément d'ordre 2, tout 2-Sylow de $\mathbf{SL}_2(\mathbf{F}_3)$ contient $-\text{id}$. De plus, un 2-Sylow ne contient aucun autre élément d'ordre 2. Il doit donc contenir des éléments d'ordre 4.

Éléments d'ordre 4 dans $\mathbf{SL}_2(\mathbf{F}_3)$: le polynôme minimal d'un élément d'ordre 4 divise $X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$. Comme $X^2 + 1$ est irréductible sur \mathbf{F}_3 (en tant que polynôme de degré 2 n'admettant aucune racine dans \mathbf{F}_3), ce polynôme minimal est égal à $X^2 + 1$. C'est aussi le polynôme caractéristique de g . Autrement dit, on a $\text{Tr}(g) = 0$ et $\det(g) = 1$. On peut alors faire la liste des éléments de $\mathbf{SL}_2(\mathbf{F}_3)$ vérifiant ces deux conditions :

Lemme. *Les éléments d'ordre 4 dans $\mathbf{SL}_2(\mathbf{F}_3)$ sont*

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

On a alors la bonne idée de noter $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ la première de ces matrices, $j = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$ la troisième, et $k = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$ la cinquième. On remarque alors avec satisfaction que les six matrices qu'on a trouvées sont, dans l'ordre,

$$i, i^3 = i^{-1} = -i, j, j^3 = j^{-1} = -j, k = ij = -ji, k^3 = k^{-1}.$$

On remarque alors que

$$H = \{\text{id}, -\text{id}, i, -i, j, -j, k, -k\}$$

³C'est exactement le lemme déjà utilisé dans la première méthode.

forme un sous-groupe d'ordre 8 de $\mathbf{SL}_2(\mathbf{F}_3)$: c'est donc un 2-Sylow⁴, **et c'est le seul**. En effet, H est exactement l'ensemble des éléments d'ordre divisant 4. Le conjugué d'un élément de H étant encore un élément d'ordre divisant 4, il appartient à H . Autrement dit, H est distingué. On a montré :

Proposition. *Le groupe H , qui est isomorphe au groupe des quaternions \mathbf{H}_8 , est l'unique 2-Sylow de $\mathbf{SL}_2(\mathbf{F}_3)$.*

Conclusion : H est sous-groupe distingué d'indice 3 dans $\mathbf{SL}_2(\mathbf{F}_3)$. L'existence d'un 3-Sylow assure que $\mathbf{SL}_2(\mathbf{F}_3)$ est un produit semi-direct de $H \simeq \mathbf{H}_8$ et $\mathbf{Z}/3\mathbf{Z}$.

Il faut ici donner explicitement un 3-Sylow et son opération sur le sous-groupe distingué H . Donner un 3-Sylow revient à choisir un élément d'ordre 3 de $\mathbf{SL}_2(\mathbf{F}_3)$.

Éléments d'ordre 3 dans $\mathbf{SL}_2(\mathbf{F}_3)$: le polynôme minimal d'un élément d'ordre 3 divise $X^3 - 1 = (X - 1)^3$. C'est donc le polynôme $(X - 1)^2 = X^2 + X + 1$. C'est donc aussi le polynôme caractéristique de g . On peut par exemple choisir⁵

$$\eta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Il ne reste maintenant plus qu'à écrire l'action de η sur \mathbf{H}_8 par conjugaison : on a, après calculs,

$$\begin{array}{lcl} \eta & : & -1 \mapsto -1 \\ & & i \mapsto -j \\ & & j \mapsto -k \\ & & k \mapsto i. \end{array}$$

⁴En particulier, puisque tous les 2-Sylow sont isomorphes, il n'y a pas d'élément d'ordre 8 dans $\mathbf{SL}_2(\mathbf{F}_3)$. On peut en profiter pour signaler l'argument direct suivant : le polynôme minimal d'un élément d'ordre 8 dans $\mathbf{SL}_2(\mathbf{F}_3)$ divise $X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$. On en déduit que le polynôme caractéristique de g est $X^2 + X - 1$ ou $X^2 - X - 1$ (pourquoi?), et donc que $\det(g) = -1$, ce qui est absurde.

⁵Remarquons tout de même qu'on peut d'une part montrer qu'il y a 8 éléments d'ordre 3 dans $\mathbf{SL}_2(\mathbf{F}_3)$, en remarquant qu'il y a 4 3-Sylow (pourquoi?), et que l'intersection de deux 3-Sylow distincts est triviale (pourquoi?), et d'autre part donner la liste de ces éléments :

$$\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$