Sous-groupes d'ordre 8 de $\mathrm{SL}_2(\mathbb{F}_p)$

Étienne AFFALOU

05/11/2024

Dans tout ce document, p est un nombre premier impair. Compter le nombre de bases de $\mathbb{F}_p^2$ nous permet de connaître l'ordre du groupe linéaire $\mathrm{GL}_2(\mathbb{F}_p)$ des matrices de taille 2 à coefficients dans le corps $\mathbb{F}_p$ (voir [**1**]). On trouve

$$|\,\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p).$$

Maintenant, le morphisme det : $\mathrm{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^*$ est surjectif, car tout élément $k \in \mathbb{F}_p^*$ est l'image de la matrice diagonale $\mathrm{diag}(1,k)$ par le morphisme det. Par le premier théorème d'isomorphisme, le noyau de det que l'on note dans la suite $\mathrm{SL}_2(\mathbb{F}_p)$ a un ordre égal à

$$|\,\mathrm{SL}_2(\mathbb{F}_p)| = \frac{(p^2-1)(p^2-p)}{p-1} = \frac{(p^2-1)p(p-1)}{p-1} = (p^2-1)p = (p-1)p(p+1).$$

Remarquons que p étant premier impair, $p-1$ et $p+1$ sont pairs. Mais sur deux nombres pairs consécutifs, au moins l'un des deux est multiple de 4. Ainsi, $(p-1)(p+1)$ est multiple de 8, et donc $|\,\mathrm{SL}_2(\mathbb{F}_p)|$ est multiple de 8. Le théorème de Lagrange assure alors qu'il est légitime de se demander si $\mathrm{SL}_2(\mathbb{F}_p)$ a des sous-groupes d'ordre 8.

À isomorphisme près, il n'y a que 5 groupes d'ordre 8 : le groupe cyclique $\mathbb{Z}/8\mathbb{Z}$, le produit direct du groupe cyclique d'ordre 4 par le groupe cyclique d'ordre 2 noté $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, le produit du groupe de Klein par le groupe cyclique d'ordre deux $(\mathbb{Z}/2\mathbb{Z})^3$, le groupe diédral D_4 et le groupe quaternionique Q_8 (la preuve est faite dans [**2**]).
La question est donc la suivante : $\mathrm{SL}_2(\mathbb{F}_p)$ contient-il une copie de l'un des groupes d'ordre 8 listés ci-dessus ?
On commence nos recherches en se posant la question suivante : $\mathrm{SL}_2(\mathbb{F}_p)$ contient-il des éléments d'ordre 2 ?

Lemme 1 La seule matrice d'ordre 2 de $\mathrm{SL}_2(\mathbb{F}_p)$ est $-I_2$.

Preuve : Soit $A \in \mathrm{SL}_2(\mathbb{F}_p)$ une matrice d'ordre 2. La matrice A s'écrit sous la forme

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

avec $(a,b,c,d) \in (\mathbb{F}_p)^4$ et $ad-bc=1$ dans $\mathbb{F}_p$. Or A est d'ordre 2 donc $A^2 = I_2$. Ainsi,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix}.$$

Ainsi, $a^2+bc=1$ mais comme $ad-1=bc$, on obtient $a^2+ad-1=1$ soit $a(a+d)=2$. En particulier, $a \neq -d$ et comme $b(a+d)=c(a+d)=0$, on a $b=c=0$.
Mais $A \in \mathrm{SL}_2(\mathbb{F}_p)$, donc $ad=1$ et comme $a^2+bc=1$, $a^2=1$ d'où $a=\pm 1$. Si $a=1$, alors $d=ad=1$ et $A=I_2$, ce qui contredit le fait que A est d'ordre 2. Donc, a vaut nécessairement -1, et $-d=1$ puis $d=-1$. Ainsi, $A=-I_2$. Inversement, $-I_2$ est bien dans $\mathrm{SL}_2(\mathbb{F}_p)$, et est d'ordre 2.

Ce lemme permet d'éliminer les trois groupes suivants car ils contiennent trop d'éléments d'ordre 2.

1. Le groupe $(\mathbb{Z}/2\mathbb{Z})^3$ qui contient 7 éléments d'ordre 2.
2. Le groupe D_4 qui contient 5 éléments d'ordre 2.
3. Le groupe $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ qui contient 3 éléments d'ordre 2.

Les candidats qui restent dans la course sont Q_8 et $\mathbb{Z}/8\mathbb{Z}$. Nous allons d'abord montrer que $\mathrm{SL}_2(\mathbb{F}_p)$ contient une copie de Q_8 pour tout nombre premier impair p. Pour cela, on a besoin du lemme ci-dessous.

LEMME 2 Il existe $(a,b) \in (\mathbb{F}_p)^2$ tel que $a^2+b^2=-1$ dans $\mathbb{F}_p$.

PREUVE : Comptons les carrés de $\mathbb{F}_p$.
On commence par remarquer que l'application $\varphi : (\mathbb{F}_p)^* \to (\mathbb{F}_p)^*$ définie par $\forall x \in (\mathbb{F}_p)^*$, $\varphi(x) = x^2$ est bien définie, et est un morphisme de groupes multiplicatifs ($\mathbb{F}_p$ est un corps).
Un élément x du noyau de φ vérifie alors $x^2=1$ soit $x^2-1=0$ ou encore $(x-1)(x+1)=0$. Donc $x \in \{1,-1\}$, en gardant en tête que comme $p \neq 2$, on a $-1 \neq 1$. Inversement, $\{-1,1\} \subset \ker(\varphi)$ et on a donc $\ker(\varphi)=\{1,-1\}$.
Ainsi, le premier théorème d'isomorphisme fournit un isomorphisme entre l'image de φ et l'ensemble $(\mathbb{F}_p)^*/\{1,-1\}$, dont le cardinal vaut $(p-1)/2$ étant donné que $-1 \neq 1$.
Le nombre de carrés dans $\mathbb{F}_p$ vaut $1+|\mathrm{Im}(\varphi)|$ étant donné que 0 est également un carré. Donc ce nombre vaut $1+((p-1)/2)=(p+1)/2$ en vertu de ce qui précède.
On a donc $(p+1)/2$ éléments de la forme $-a^2$ dans $\mathbb{F}_p$, et $(p+1)/2$ éléments de la forme $1+b^2$ dans $\mathbb{F}_p$ (on peut construire des bijections entre l'ensemble des carrés de $\mathbb{F}_p$ et l'ensemble des éléments de la forme $-a^2$ ou $1+b^2$).
Mais $((p+1)/2)+((p+1)/2)=p+1$ donc comme $|\mathbb{F}_p|=p$, on est assurés de l'existence d'au moins un élément qui s'écrit sous la forme $-a^2$ et aussi de la forme $1+b^2$.
Cet élément fournit une égalité du type $1+b^2=-a^2$, ou encore $a^2+b^2=-1$.

PROPOSITION 1 Le groupe $\mathrm{SL}_2(\mathbb{F}_p)$ contient une copie de Q_8.

L'idée de la preuve provient de **[3]** (10.2.3 page 159).

PREUVE : On va donner trois matrices distinctes I,J,K de $\mathrm{SL}_2(\mathbb{F}_p)$ qui vérifient $I^2=J^2=K^2=IJK=-I_2$.
Une définition de Q_8 est souvent donnée par trois matrices de déterminant 1, mais deux d'entre elles sont à coefficients complexes. On garde quand même

$$J=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

qui est bien définie dans les matrices à coefficients dans $\mathbb{F}_p$, et dont le déterminant vaut bien 1. On cherche ensuite une matrice de $\mathrm{SL}_2(\mathbb{F}_p)$ dont le carré vaut $-I_2$. L'écriture explicite des équations amène à une égalité du type $a^2+bc=-1$ dans $\mathbb{F}_p$. On utilise alors le lemme 2, et on pose

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

où $(a,b) \in (\mathbb{F}_p)^2$ vérifie $a^2+b^2=-1$, de sorte que $\det(I)=-a^2-b^2=1$. De plus,

$$I^2=\begin{pmatrix}a & b\\ b & -a\end{pmatrix}\begin{pmatrix}a & b\\ b & -a\end{pmatrix}=\begin{pmatrix}a^2+b^2 & ab-ba\\ ba-ab & b^2+a^2\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}.$$

Vu la forme de I, on a bien $I \neq J$ ($-1 \neq 1$). L'égalité $IJK=-I_2$ impose alors la forme de K. Posons donc

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

Là encore, $\det(K)=-b^2-a^2=1$ et

$$K^2=\begin{pmatrix}-b & a\\ a & b\end{pmatrix}\begin{pmatrix}-b & a\\ a & b\end{pmatrix}=\begin{pmatrix}b^2+a^2 & -ba+ab\\ -ab+ba & a^2+b^2\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}.$$

Toujours sachant que $-1 \neq 1$, on a $K \neq J$. De plus, $I \neq K$. En effet, si on avait $I=K$, on aurait $a=-b$ et $a=b$ d'où $2b=0$ puis $(2 \neq 0)$ $b=0$ et $a=0$. Mais $0^2+0^2 \neq -1$ donc on a bien $I \neq K$.
On a donc trouvé trois matrices distinctes I,J et K qui sont toutes les trois dans $\mathrm{SL}_2(\mathbb{F}_p)$, et donc le carré vaut -1 dans $\mathrm{SL}_2(\mathbb{F}_p)$. Reste à vérifier que $IJK=-I_2$. Pour cela, il suffit de remarquer que

$$IJ=\begin{pmatrix}a & b\\ b & -a\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}=\begin{pmatrix}-b & a\\ a & b\end{pmatrix}=K$$

ce qui prouve que $IJK=(IJ)K=K^2=-I_2$. Finalement, le sous-groupe de $\mathrm{SL}_2(\mathbb{F}_p)$ engendré par les trois matrices I,J et K est effectivement une copie de Q_8.

Il ne reste plus que le cas de $\mathbb{Z}/8\mathbb{Z}$. On voit facilement que le groupe $\mathrm{SL}_2(\mathbb{F}_p)$ contient une copie de $\mathbb{Z}/8\mathbb{Z}$ si et seulement si ce groupe possède un élément d'ordre 8. Donnons d'abord une condition nécessaire sur notre nombre premier impair p pour que $\mathrm{SL}_2(\mathbb{F}_p)$ contienne une copie de $\mathbb{Z}/8\mathbb{Z}$.

PROPOSITION 2 Si $\mathrm{SL}_2(\mathbb{F}_p)$ possède une matrice d'ordre 8, alors p est congru à ± 1 modulo 8.

PREUVE : Soit $A \in \mathrm{SL}_2(\mathbb{F}_p)$ une matrice d'ordre 8.
On remarque que $(A^4)^2 = I_2$ donc A^4 est d'ordre 2 ($A^4 \neq I_2$ car A est d'ordre 8).
Par le lemme 1, on a nécessairement $A^4 = -I_2$. Ainsi, si A^2 s'écrit

$$A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

avec $(a, b, c, d) \in (\mathbb{F}_p)^4$ tels que $ad - bc = 1$, on a

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 = A^4 = A^2 A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{pmatrix}.$$

Ainsi, $a^2 + bc = -1$ mais comme $bc = ad - 1$, $a^2 + ad = 0$ ou encore $a(a + d) = 0$. De même, on montre que $d(a + d) = 0$. Mais $b(a + d) = 0$ et $c(a + d) = 0$ donc comme $A^2 \neq 0_2$, $d = -a$ et A^2 s'écrit

$$A^2 = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

avec $-a^2 - bc = 1$, c'est-à-dire $a^2 + bc = -1$. Mais A est elle-même une matrice de $\mathrm{SL}_2(\mathbb{F}_p)$ donc A s'écrit

$$A = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

où $(x, y, z, t) \in (\mathbb{F}_p)^4$ vérifie $xt - yz = 1$. Mais $A^2 = AA$ donc

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} x^2 + yz & y(x+t) \\ z(x+t) & t^2 + yz \end{pmatrix}.$$

En particulier, $x^2 + yz = a$ et $t^2 + yz = -a$. Mais $yz = xt - 1$ donc $x^2 + xt = 1 + a$ et $t^2 + xt = 1 - a$.
Ainsi, $x(x + t) = 1 + a$ et $t(x + t) = 1 - a$. Ajouter ces deux égalité fournit

$$(x+t)^2 = (x+t)(x+t) = x(x+t) + t(x+t) = 1 + a + 1 - a = 2.$$

Mais $x + t \in \mathbb{F}_p$, donc 2 est un carré modulo p. Par la deuxième loi complémentaire, p est congru à ± 1 modulo 8.

Nous allons montrer en deux temps que la réciproque est vraie. Le cas où p est congru à 1 modulo 8 est le cas facile.

PROPOSITION 3 Si p est congru à 1 modulo 8, alors $\mathrm{SL}_2(\mathbb{F}_p)$ contient une matrice d'ordre 8.

PREUVE : On sait que le groupe $\mathbb{F}_p^*$ est cyclique, isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.
Donc, $p - 1$ étant multiple de 8, $\mathbb{F}_p^*$ contient un élément d'ordre 8, que nous noterons α.
On remarque que $\alpha^{-1} \neq \alpha$ (sinon, $\alpha^2 = 1$) et que α^{-1} est aussi d'ordre 8. Il suffit alors de poser

$$A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}.$$

Ainsi, $\det(A) = 1$ et A est d'ordre 8 (diagonale avec des éléments d'ordre 8 dans $\mathbb{F}_p^*$ sur la diagonale).

Pour le cas où p est congru à -1 modulo 8, l'idée est de procéder comme dans la proposition 2.8 de [**4**]. Il s'agit de considérer le groupe spécial orthogonal $\mathrm{SO}_2(\mathbb{F}_p)$ et de montrer que $\mathrm{SO}_2(\mathbb{F}_p)$ est cyclique d'ordre $p + 1$. On ramène ensuite un élément d'ordre $p + 1$ dans $\mathrm{SL}_2(\mathbb{F}_p)$ pour conclure.

PROPOSITION 4 Si p est congru à -1 modulo 8, alors $\mathrm{SL}_2(\mathbb{F}_p)$ contient une matrice d'ordre 8.

PREUVE : Notre nombre premier p étant congru à -1 modulo 8, il s'écrit $p = 8k+7$ où $k \in \mathbb{N}$.
On introduit l'ensemble G des matrices de $\mathrm{SL}_2(\mathbb{F}_p)$ de la forme suivante

$$G = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x^2 + y^2 = 1 \right\}.$$

On peut montrer que $G = \mathrm{SO}_2(\mathbb{F}_p)$, mais montrons seulement que G est un sous-groupe de $\mathrm{SL}_2(\mathbb{F}_p)$.

1. La matrice I_2 est dans G en prenant $x = 1$ et $y = 0$ qui vérifient bien $1^2 + 0^2 = 1$.
2. Soient $X, Y \in G$ qui s'écrivent donc

$$X = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \text{ et } Y = \begin{pmatrix} x' & y' \\ -y' & x' \end{pmatrix}$$

avec $x^2 + y^2 = (x')^2 + (y')^2 = 1$. On remarque que

$$XY = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} x' & y' \\ -y' & x' \end{pmatrix} = \begin{pmatrix} xx' - yy' & xy' + x'y \\ -(xy' + x'y) & xx' - yy' \end{pmatrix}$$

avec

$$\begin{aligned} (xx' - yy')^2 + (xy' + x'y)^2 &= x^2(x')^2 - 2xx'yy' + y^2(y')^2 + x^2(y')^2 + 2xx'yy' + (x')^2y^2 \\ &= (x')^2(x^2 + y^2) + (y')^2(x^2 + y^2) \\ &= (x')^2 + (y')^2 \\ &= 1. \end{aligned}$$

Ainsi, $XY \in G$.

3. Soit $X \in G$. La matrice X s'écrit

$$X = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

où $x^2 + y^2 = 1$. Or, l'inverse de X est

$$X^{-1} = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

avec $x^2 + (-y)^2 = x^2 + y^2 = 1$ et donc X^{-1} est encore un élément de G.

Ainsi, G est un sous-groupe de $\mathrm{SL}_2(\mathbb{F}_p)$. Notre objectif est de montrer que G contient une matrice d'ordre $p+1$. Pour cela, on commence par remarquer que -1 n'est pas un carré modulo p par la première loi complémentaire, car p n'est pas congru à 1 modulo 4. En effet, si on avait $k' \in \mathbb{N}$ tel que $p = 4k' + 1$, on aurait $8k + 7 = 4k' + 1$ donc $8k + 6 = 4k'$ et donc $4k + 3 = 2k'$ ce qui est impossible car $2k'$ est pair alors que $4k + 3$ est impair.
Cela prouve que le polynôme $X^2 + 1$ est irréductible sur $\mathbb{F}_p[X]$. Ainsi, $\langle X^2 + 1 \rangle$ est maximal, et le quotient $\mathbb{F}_p[X]/\langle X^2 + 1 \rangle$ est un corps à p^2 éléments (voir **[1]**). Notant $i = \overline{X}$ l'image de X dans ce quotient, les éléments de $\mathbb{F}_p[X]/\langle X^2 + 1 \rangle$ s'écrivent donc sous la forme $x + iy$ avec $(x, y) \in \mathbb{F}_p$ et $i^2 = -1$.
On introduit l'application $\varphi : G \to (\mathbb{F}_p[X]/\langle X^2 + 1 \rangle)^*$ (où $(\mathbb{F}_p[X]/\langle X^2 + 1 \rangle)^*$ désigne l'ensemble des éléments inversibles de $\mathbb{F}_p[X]/\langle X^2 + 1 \rangle$) définie de la façon suivante :

$$\text{si } X = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in G, \quad \varphi(X) = x + iy.$$

L'application φ est bien définie, car si $X \in G$ s'écrit comme ci-dessus, $\varphi(X)$ est inversible, d'inverse $x - iy$. En effet, $(x + iy)(x - iy) = x^2 + y^2 = 1$. De plus, φ est un morphisme de groupes.
Effectivement, si $(x, y, x', y') \in (\mathbb{F}_p)^4$ sont tels que $x^2 + y^2 = (x')^2 + (y')^2 = 1$,

$$\varphi\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} x' & y' \\ -y' & x' \end{pmatrix} \right) = \varphi\left(\begin{pmatrix} xx' - yy' & xy' + x'y \\ -(xy' + x'y) & xx' - yy' \end{pmatrix} \right) = xx' - yy' + i(xy' + x'y) = (x + iy)(x' + iy')$$

et donc φ est bien un morphisme de groupes. Si $X \in \ker(\varphi)$, alors on a directement $X = I_2$ et φ est injectif.
Mais $\mathbb{F}_p[X]/\langle X^2 + 1 \rangle$ est un corps fini à p^2 éléments, donc $(\mathbb{F}_p[X]/\langle X^2 + 1 \rangle)^*$ est cyclique d'ordre $p^2 - 1 =$

$(p-1)(p+1)$. Par injectivité de φ et par le premier théorème d'isomorphisme, on obtient que G est isomorphe à un sous-groupe du groupe cyclique $(\mathbb{F}_p[X]/\langle X^2+1\rangle)^*$. Donc, G est cyclique d'une part.
D'autre part, comme $p^2-1=(p-1)(p+1)$, $(\mathbb{F}_p[X]/\langle X^2+1\rangle)^*$ a un $x+iy$ élément d'ordre $p+1$ (par cyclicité). Gardant cette notation pour $x+iy$ d'ordre $p+1$, introduisons B la matrice

$$B=\begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

Tout d'abord, montrons que B est dans $\mathrm{SL}_2(\mathbb{F}_p)$. Pour cela, remarquons que

$$(x+iy)^p = x^p + i^p y^p = x + i^p y = x + i^{8k+7} y = x + i^3 y = x - iy$$

où on a utilisé les trois points suivants :

1. L'application qui à $x \in \mathbb{F}_p$ associe x^p est un morphisme d'anneaux.
2. Pour tout $a \in (\mathbb{F}_p)^*$, $a^{p-1}=1$ et donc $a^p = a$ et cette égalité reste vraie si $a=0$.
3. L'élément i de $(\mathbb{F}_p[X]/\langle X^2+1\rangle)^*$ est d'ordre 4 et $p=8k+7$.

Ainsi, le déterminant de B vaut

$$\det(B) = x^2+y^2 = (x+iy)(x-iy) = (x+iy)(x+iy)^p = (x+iy)^{p+1} = 1$$

étant donné que $x+iy$ est d'ordre $p+1$. Ainsi, $B \in \mathrm{SL}_2(\mathbb{F}_p)$.
Montrons que B est d'ordre $p+1$. Tout d'abord,

$$\varphi(B^{p+1}) = \varphi(B)^{p+1} = (x+iy)^{p+1} = 1$$

donc $B^{p+1} \in \ker(\varphi)$ et par injectivité, $B^{p+1} = I_2$.
Supposons un court instant qu'il existe $k \in \{1, \cdots, p\}$ tel que $B^k = I_2$. On aurait alors

$$1 = \varphi(I_2) = \varphi(B^k) = \varphi(B)^k = (x+iy)^k.$$

Cette égalité est impossible étant donné que $x+iy$ est d'ordre $p+1$. Ainsi, B est d'ordre $p+1$.
En se souvenant que $p+1 = 8k+8 = 8(k+1)$, posons $A = B^{k+1}$. Bien entendu, $A \in \mathrm{SL}_2(\mathbb{F}_p)$ et pour tout $j \in \{1, \cdots, 7\}$, $j(k+1) < p+1$, donc $A^j = B^{j(k+1)} \neq I_2$. De plus, $A^8 = B^{8(k+1)} = B^{p+1} = I_2$.
Pas de doute, $A \in \mathrm{SL}_2(\mathbb{F}_p)$, et A est d'ordre 8.

Le tableau suivant résume ce que nous avons montré.

Groupe d'ordre 8	S'injecte dans $\mathrm{SL}_2(\mathbb{F}_p)$?
Q_8	Oui
$\mathbb{Z}/8\mathbb{Z}$	Oui ssi $p \equiv \pm 1$ [8]
$(\mathbb{Z}/2\mathbb{Z})^3$	Non
$(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$	Non
D_4	Non

Les questions naturelles à se poser ensuite sont les suivantes.
Combien y a-t-il de copies de Q_8 dans $\mathrm{SL}_2(\mathbb{F}_p)$? Si $p \equiv \pm 1$ [8], combien y a-t-il de copies de $\mathbb{Z}/8\mathbb{Z}$ dans $\mathrm{SL}_2(\mathbb{F}_p)$?

Références :

— **[1]** Cours d'algèbre, *Daniel Perrin*
— **[2]** Groupes d'ordre p^3, classification, *Étienne Affalou*, `https://perso.eleves.ens-rennes.fr/~eaffa360/`
— **[3]** Finite Groups : An Introduction, *Jean-Pierre Serre*
— **[4]** Fuchs' problem for linear groups, *Keir Lockridge* et *Jacob Terkel*, `https://arxiv.org/abs/2401.11583`