Annexe A

Etude de $\mathrm{SL}_2(\mathbb{Z})$

Voici un chapitre, totalement lié à une leçon d'agrégation. Cependant, il m'est impossible de ne me limiter qu'aux seules leçons du concours qui, de toute façon, évoluent chaque année. Je souhaite toujours élargir les perspectives.
Pour ce chapitre, j'ai utilisé les leçons d'agrégation réalisées par des préparationnaires ou des collègues *(plus ou moins bien faites)* ; je me suis surtout inspiré du papier de Keith Conrad et d'un article de la RMS de Novembre-Décembre 1995 *(106-ième année N° 3-4 pp 282-287)*

Introduction

⇒ On rappelle que $\mathrm{SL}_2(\mathbb{Z})$ est l'ensemble des matrices carrées d'ordre 2 à coefficients dans $\mathbb{Z}$ et de déterminant 1, c'est à dire :

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ avec } a \in \mathbb{Z}, b \in \mathbb{Z}, c \in \mathbb{Z}, d \in \mathbb{Z} \text{ et } ad - bc = 1 \right\}$$

⇒ $\mathrm{SL}_2(\mathbb{R})$ est l'ensemble des matrices carrées d'ordre 2 à coefficients dans $\mathbb{R}$ et de déterminant 1 ; bien entendu $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R})$
⇒ $\mathrm{SL}_2(\mathbb{Z})$ est à $\mathrm{SL}_2(\mathbb{R})$, ce que $\mathbb{Z}$ est à $\mathbb{R}$
⇒ C'est l'exemple le plus basique de groupe discret non abélien

A.1 Génération du groupe $\mathrm{SL}_2(\mathbb{Z})$: étude algébrique

A.1.1 Proposition

$\mathrm{SL}_2(\mathbb{Z})$ est un groupe non commutatif

Démonstration

La démonstration est simple et élémentaire

1. Tout d'abord $\mathrm{SL}_2(\mathbb{Z})$ est non vide puisque $\mathrm{Id}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$
2. La multiplication est une loi interne : il suffit d'utiliser les déterminants *(le déterminant d'un produit de matrices est le produit des déterminants des matrices)*
3. Si $A \in \mathrm{SL}_2(\mathbb{Z})$ avec $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, alors $A^{-1} \in \mathrm{SL}_2(\mathbb{Z})$ puisque $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
4. Ensuite, si $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, alors

$$ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \text{ et } TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

Nous avons $ST \neq TS$, ce qui montre la non commutativité

A.1.2 Théorème

Les matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ engendrent $\mathrm{SL}_2(\mathbb{Z})$

Il semblerait que cette question fasse souvent l'objet d'exercices

Démonstration

1. Pour commencer, remarquons que $S^2 = -\mathrm{Id}_2$, $S^3 = -S$ et donc $S^4 = \mathrm{Id}_2$.
   S est un élément d'ordre 4. En particulier, $S^{-1} = S^3 = -S$
   De même, remarquons que $T^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$
   Les deux points qui suivent sont élémentaires, mais fondamentaux pour la suite de la démonstration, notamment pour démontrer la génération de $\mathrm{SL}_2(\mathbb{Z})$
2. **Démontrons que, pour tout $n \in \mathbb{Z}$, $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$**
   $\Rightarrow$ Démontrons, par une récurrence sur $n \in \mathbb{N}$ que $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
   $\star$ C'est vrai pour $n = 0$ puisque $T^0 = \mathrm{Id}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $n = 1$ puisque $T^1 = T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
   $\star$ Supposons que pour $n \in \mathbb{N}$, $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
   $\star$ Alors, $T^{n+1} = T^n \times T = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$
   Ce qui montre effectivement que, pour tout $n \in \mathbb{N}$, $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
   $\Rightarrow$ Soit $n \in \mathbb{Z}^-$, c'est à dire $n \in \mathbb{Z}$ tel que $n \leqslant -1$.
   Il existe alors $n' \in \mathbb{N}^*$ tel que $n = -n'$. Alors :
   $$T^n = T^{-n'} = \left(T^{n'}\right)^{-1} = \left[\begin{pmatrix} 1 & n' \\ 0 & 1 \end{pmatrix}\right]^{-1} = \begin{pmatrix} 1 & -n' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$
   Nous venons donc de montrer que, pour tout $n \in \mathbb{Z}$, $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
3. Pour toute matrice $M \in \mathcal{M}_2(\mathbb{Z})$ où $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, nous avons :
   $$SM = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \text{ et } T^n M = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$$
4. Nous appelons $\Gamma(S,T)$ le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ engendré par S et T.[1]
   Toutes les matrices $M \in \Gamma(S,T)$ s'écrivent $M = S^{\alpha_1} T^{\beta_1} S^{\alpha_2} T^{\beta_2} \cdots S^{\alpha_p} T^{\beta_p}$ où $0 \leqslant \alpha_i \leqslant 3$ et $\beta_i \in \mathbb{Z}$.
   Nous avons donc $\Gamma(S,T) \subset \mathrm{SL}_2(\mathbb{Z})$
   Il faut montrer que $\Gamma(S,T) = \mathrm{SL}_2(\mathbb{Z})$ et il nous reste donc à montrer que $\mathrm{SL}_2(\mathbb{Z}) \subset \Gamma(S,T)$
5. **Montrons que $\mathrm{SL}_2(\mathbb{Z}) \subset \Gamma(S,T)$**
   Soit $M \in \mathrm{SL}_2(\mathbb{Z})$ c'est à dire $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc = 1$
   $\Rightarrow$ Si $c = 0$, alors $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ et $ad = 1$; a et d sont donc inversibles dans $\mathbb{Z}$. Donc

1. Une autre notation possible et souvent utilisée est $\langle S,T \rangle$

▷ Soit $a=d=1$ et alors $M=\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$ est du type $M=T^b=S^0T^b$

▷ Soit $a=d=-1$ et alors $M=\begin{pmatrix}-1 & b\\ 0 & -1\end{pmatrix}=-\begin{pmatrix}1 & -b\\ 0 & 1\end{pmatrix}=-T^{-b}=S^2T^{-b}$

M est donc du type $M=S^2T^{-b}$

Dans ces deux cas, $M\in\Gamma(S,T)$

$\Rightarrow$ Si $c\neq 0$

▷ Supposons $|a|\geqslant|c|$

⋆ Nous effectuons la division euclidienne de a par c.
Il existe donc un unique couple d'entiers (q,r) avec $0\leqslant r<|c|$ tel que $a=cq+r$

⋆ La matrice $M_1=T^{-q}M=\begin{pmatrix}a-qc & b-qd\\ c & d\end{pmatrix}$.

Comme $a-cq=r$, nous avons $M_1=T^{-q}M=\begin{pmatrix}r & b-qd\\ c & d\end{pmatrix}$.

Par construction,nous avons $0\leqslant r<|c|$ et donc $SM_1=\begin{pmatrix}-c & -d\\ r & b-qd\end{pmatrix}$

⋆ Si $r=0$, alors $SM_1=\begin{pmatrix}-c & -d\\ 0 & b-qd\end{pmatrix}$ et comme $SM_1\in\mathrm{SL}_2(\mathbb{Z})$, nous avons

$$(-c)(b-qd)=-bc+(cq)d=-bc+ad=1$$

Et donc

$$SM_1=\begin{pmatrix}1 & -d\\ 0 & 1\end{pmatrix}\text{ ou bien }SM_1=\begin{pmatrix}-1 & -d\\ 0 & -1\end{pmatrix}$$

◇ Si $SM_1=\begin{pmatrix}1 & -d\\ 0 & 1\end{pmatrix}$, alors $SM_1=T^{-d}$ et donc $ST^{-q}M=T^{-d}\Longleftrightarrow M=T^qS^3T^{-d}$ et donc $M\in\Gamma(S,T)$

◇ Si $SM_1=\begin{pmatrix}-1 & -d\\ 0 & -1\end{pmatrix}$, alors $S^2(SM_1)=\begin{pmatrix}1 & d\\ 0 & 1\end{pmatrix}$ et donc

$$S^3M_1=T^d\Longleftrightarrow S^3T^{-q}M=T^d\Longleftrightarrow M=T^qST^d$$

et donc $M\in\Gamma(S,T)$

⋆ Si $r\neq 0$, par la division euclidienne, nous avons $0\leqslant r<|c|$ et nous pouvons itérer une division euclidienne de $-c$ par r, cette fois-ci.
Il existe donc un unique couple d'entiers (q_1,r_1) avec $0\leqslant r_1<r$ tel que $-c=q_1r+r_1$ avec $0\leqslant r_1<r$
Nous faisons le même raisonnement que ci-dessus ($r_1=0$ ou $r_1\neq 0$)
◇ Si $r_1=0$ on démontre une nouvelle fois, et de la même manière, que $M\in\Gamma(S,T)$
◇ Si $r_1\neq 0$, nous itérons le processus

⋆ Nous avons ainsi créé une suite de nombres entiers positifs, décroissante. Il existe sûrement un entier $p\in\mathbb{N}$ *(une étape p)* pour lequel nous aurons $r_p=0$.
Nous pourrons ainsi conclure que $M\in\Gamma(S,T)$ avec $M=S^{\alpha_1}T^{\beta_1}\cdots S^{\alpha_q}T^{\beta_q}$ où, pour tout entier i tel que $1\leqslant i\leqslant q$, $0\leqslant\alpha_i$ et $\beta_i\in\mathbb{Z}$

▷ Et maintenant, si $|a|<|c|$

Nous multiplions la matrice $M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, à gauche, par S et nous avons :

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

Nous pouvons alors faire la division euclifienne de a par $-c$ et nous retombons alors dans le cas étudié ci-dessus. Nous démontrons alors, de la même manière que $M\in\Gamma(S,T)$

Nous venons de démontrer que toute matrice $M\in\mathrm{SL}_2(\mathbb{Z})$ et aussi une matrice de $\Gamma(S,T)$.
Nous avons donc $\mathrm{SL}_2(\mathbb{Z})\subset\Gamma(S,T)$

Ainsi, $\mathrm{SL}_2(\mathbb{Z})=\Gamma(S,T)$ et donc, nous avons bien les matrices $S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ et $T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ qui engendrent $\mathrm{SL}_2(\mathbb{Z})$

Exemple 1 :

Nous allons expliquer l'algorithme de décomposition d'une matrice de $\mathrm{SL}_2(\mathbb{Z})$ en produit de matrices S et T

Prenons $M = \begin{pmatrix} 19 & 8 \\ 7 & 3 \end{pmatrix}$

- ▷ Nous avons $19 = 7 \times 2 + 5$ et donc $T^{-2}M = \begin{pmatrix} 5 & 2 \\ 7 & 3 \end{pmatrix}$; d'où $ST^{-2}M = \begin{pmatrix} -7 & -2 \\ 5 & 1 \end{pmatrix}$
- ▷ Ensuite, nous avons $-7 = 5 \times -2 + 3$ et donc $T^2ST^{-2}M = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$; d'où $ST^2ST^{-2}M = \begin{pmatrix} -5 & -2 \\ 3 & 1 \end{pmatrix}$
- ▷ Nous itérons une division euclidienne et avons $-5 = 3 \times -2 + 1$ et donc $T^2ST^2ST^{-2}M = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$; d'où $ST^2ST^2ST^{-2}M = \begin{pmatrix} -3 & -1 \\ 1 & 0 \end{pmatrix}$
- ▷ Enfin $-3 = 1 \times -3 + 0$ et donc $T^3ST^2ST^2ST^{-2}M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = S$

Nous avons alors $T^3ST^2ST^2ST^{-2}M = S \Longleftrightarrow M = S^2T^2ST^{-2}ST^{-2}ST^3$

A.1.3 Proposition

Soient $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Alors, A et B engendrent aussi $\mathrm{SL}_2(\mathbb{Z})$

Démonstration

En effet, il suffit de vérifier que $AB = T$ et que $A = -S = S^3$

Remarque 1 :

1. Nous avons aussi $A^2 = -\mathrm{Id}_2$ et $B^3 = -\mathrm{Id}_2$, donc $A^2 = B^3$, $A^4 = \mathrm{Id}_2$ et $A^2 = B^3$. $\mathrm{SL}_2(\mathbb{Z})$ est donc aussi engendré par 2 matrices d'ordre fini.
2. En fait, nous avons $A^4 = \mathrm{Id}_2$ et $B^6 = \mathrm{Id}_2$
3. On peut aussi démontrer que $\mathrm{SL}_2(\mathbb{Z})$ est engendré par les matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

   En effet,
   Nous avons $S = T^{-1}UT^{-1}$; donc $\Gamma(S,T) \subset \Gamma(U,T)$, c'est à dire $\mathrm{SL}_2(\mathbb{Z}) \subset \Gamma(U,T)$ et comme nous avons $\Gamma(U,T) \subset \mathrm{SL}_2(\mathbb{Z})$, nous avons donc $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(U,T)$

A.1.4 Proposition

Soit $\Psi : (\mathrm{SL}_2(\mathbb{Z}), \times) \longrightarrow (\mathbb{C}^*, \times)$ un homomorphisme de groupes.
Alors, $\mathrm{Im}\Psi$ est le groupe des racines 12° de l'unité

Démonstration

1. $\mathrm{SL}_2(\mathbb{Z})$ est un groupe engendré par $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.
   A est d'ordre 4 et B est d'ordre 6
2. Si $\Psi : (\mathrm{SL}_2(\mathbb{Z}), \times) \longrightarrow (\mathbb{C}^*, \times)$ un homomorphisme de groupes alors $\Psi(A^4) = \Psi(\mathrm{Id}_2) = 1$; de même, $\Psi(B^6) = 1$.
   Comme $\Psi(A^4) = \Psi(A)^4 = 1$, $\Psi(A)$ est une racine 4° de 1 ; de même $\Psi(B)$ est une racine 6° de 1
3. $\mathrm{Im}\Psi = \Gamma(\Psi(A), \Psi(b))$ et donc $\mathrm{Im}\Psi$ est le sous-groupe des racines 12° de 1

Remarque 2 :

Une remarque sur l'ordre des matrices.
Dans le groupe $\mathrm{SL}_2(\mathbb{Z})$, il existe des matrices qui ont un ordre fini. Par exemples :

- ▷ Id_2 est d'ordre 1 et $-\mathrm{Id}_2$ est d'ordre 2
- ▷ $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est d'ordre 4 et $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ est d'ordre 6
- ▷ $(ST)^2$ est d'ordre 3

Le théorème suivant répond à la question : quels sont les ordres des éléments d'ordre fini ?

A.1.5 Théorème

Une matrice de $\mathrm{SL}_2(\mathbb{Z})$ d'ordre fini a pour ordre 1, 2, 3, 4 ou 6

Démonstration

La démonstration de ce résultat, sans être difficile, prend réellement des chemins tortueux!! Il faut revenir sur les polynômes matriciels -et les polynômes classiques !- ainsi que la réduction des matrices

Soit donc $A \in \mathrm{SL}_2(\mathbb{Z})$ d'ordre fini n, c'est à dire telle que $A^n = \mathrm{Id}_2$. Nous souhaitons montrer que $n = 1, 2, 3, 4$ ou 6.

1. De $A^n = \mathrm{Id}_2$, nous pouvons écrire $A^n - \mathrm{Id}_2 = \mathcal{O}_2$ où $\mathcal{O}_2$ est la matrice carrée nulle d'ordre 2.
   Le polynôme $X^n - 1$ est donc un polynôme annulateur de A
2. Ecrivons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc = 1$.
   Le polynôme caractéristique de A est donné par :
   $$\begin{aligned} P_A(X) = \quad & \det(A - X\mathrm{Id}_2) = \begin{vmatrix} a - X & b \\ c & d - X \end{vmatrix} \\ & = X^2 - (a+d)X + 1 = X^2 - \mathrm{tr}(A)X + 1 \end{aligned}$$
   où $\mathrm{tr}(A)$ est la trace de A
3. D'après le théorème de Cayley-Hamilton *(voir 13.6.15)*,$P_A(A) = \mathcal{O}_2$, c'est à dire sue
   $$A^2 - \mathrm{tr}(A)A + \mathrm{Id}_2 = \mathcal{O}_2$$
4. A étant annulé par les polynômes $X^n - 1$ et $X^2 - \mathrm{tr}(A)X + 1$, A est aussi annulé par le pgcd $\left(X^n - 1, X^2 - \mathrm{tr}(A)X + 1\right)$
   En effet, si $Q = \mathrm{pgcd}\left(X^n - 1, X^2 - \mathrm{tr}(A)X + 1\right)$, alors, par le théorème de Bezout, il existe 2 polynômes $P_1 \in \mathbb{C}[X]$ et $P_2 \in \mathbb{C}[X]$ tels que
   $$Q(X) = P_1(X)(X^n - 1) + P_2(X)(X^n - 1)$$
   Ainsi, si $A^n - \mathrm{Id}_2 = \mathcal{O}_2$ et $[A^2 - \mathrm{tr}(A)A + \mathrm{Id}_2 = \mathcal{O}_2$, alors $Q(A) = \mathcal{O}_2$
5. Soient λ_1 et λ_2 les valeurs propres de A.
   Alors, A est semblable à $\Lambda = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ et donc $A^n = P\lambda^n P^{-1} = \mathrm{Id}_2 \Longleftrightarrow \lambda^n = \mathrm{Id}_2$
   C'est à dire que λ_1 et λ_2 sont des racines n-ièmes de 1 et $\mathrm{tr}(A) = \lambda_1 + \lambda_2$
6. D'autre part, $|\mathrm{tr}(A)| = |\lambda_1 + \lambda_2| \leqslant |\lambda_1| + |\lambda_2| = 2$.
   Donc, de $|\mathrm{tr}(A)| \leqslant 2$ et de $\mathrm{tr}(A) \in \mathbb{Z}$, nous déduisons que nous n'avons qu'un nombre fini de possibilités.
7. De ci-dessus, nous tirons que $\mathrm{tr}(A) = \pm 2$, $\mathrm{tr}(A) = \pm 1$ et $\mathrm{tr}(A) = 0$
   (a) **Premier cas :** $\mathrm{tr}(A) = 2$
   - ▷ Alors $X^2 - \mathrm{tr}(A)X + 1 = X^2 - 2X + 1 = (X-1)^2$

▷ X^n-1 a n racines distinctes et nous avons $X^n-1=(X-1)\left(\sum_{k=0}^{n-1}X^k\right)$

▷ Le pgcd de X^n-1 et $(X-1)^2$ est donc $X-1$ et alors $A-\mathrm{Id}_2=\mathcal{O}_2$, c'est à dire $A=\mathrm{Id}_2$ et A est d'ordre 1

(b) **Second cas :** $\mathrm{tr}(A)=-2$

▷ Alors $X^2-\mathrm{tr}(A)X+1=X^2+2X+1=(X+1)^2$

▷ X^n-1 a toujours n racines distinctes

⋆ Si n est pair, c'est à dire que $X^n-1=X^{2k}-1$. Alors $X=-1$ est racine de $X^n-1=X^{2k}-1$ et alors le pgcd de X^n-1 et $(X+1)^2$ est donc $X+1$ et donc $A+\mathrm{Id}_2=\mathcal{O}_2$, c'est à dire $A=-\mathrm{Id}_2$ et A est d'ordre 1

⋆ Si n est impair, $X^n-1=X^{2k+1}-1$ et il n'y a pas de racines communes entre X^n-1 et $(X+1)^2$; ce sont des polynômes premiers entre eux

(c) **Troisième cas :** $\mathrm{tr}(A)=1$

▷ Alors $X^2-\mathrm{tr}(A)X+1=X^2-X+1$.
Or, X^2-X+1 est un facteur de X^3+1 puisque :

$$X^3+1=(X+1)\left(X^2-X+1\right)$$

▷ En passant aux polynômes matriciels, nous pouvons écrire :

$$A^3+\mathrm{Id}_2=(A+\mathrm{Id}_2)\left(A^2-A+\mathrm{Id}_2\right)=\mathcal{O}_2$$

Donc $A^3=-\mathrm{Id}_2$ et $A^6=\mathrm{Id}_2$. A est d'ordre 6

▷ A ne peut pas être d'ordre 2 puisque

$$A^2-A+\mathrm{Id}_2=\mathcal{O}_2\Longleftrightarrow A^2=A-\mathrm{Id}_2$$

Nous ne pouvons donc pas avoir $A=-\mathrm{Id}_2$, puisque ceci signifierait que A serait d'ordre 2

(d) **Quatrième cas :** $\mathrm{tr}(A)=-1$

L'étude de ce cas est semblable au précédent

▷ Alors $X^2-\mathrm{tr}(A)X+1=X^2+X+1$.
Or, X^2+X+1 est un facteur de X^3-1 puisque :

$$X^3-1=(X-1)\left(X^2+X+1\right)$$

▷ En passant aux polynômes matriciels, nous pouvons écrire :

$$A^3-\mathrm{Id}_2=(A-\mathrm{Id}_2)\left(A^2+A+\mathrm{Id}_2\right)=\mathcal{O}_2$$

Donc $A^3=\mathrm{Id}_2$ et A est d'ordre 3

▷ A ne peut pas être d'ordre 1 puisque

$$A^2+A+\mathrm{Id}_2=\mathcal{O}_2\Longleftrightarrow A^2=-A-\mathrm{Id}_2$$

Nous ne pouvons donc pas avoir $A=\mathrm{Id}_2$, puisque ceci signifierait que A serait d'ordre 1

(e) **Cinquième cas :** $\mathrm{tr}(A)=0$

Alors $X^2-\mathrm{tr}(A)X+1=X^2+1$.

En passant aux polynômes matriciels, nous pouvons écrire : $A^2+\mathrm{Id}_2=\mathcal{O}_2\Longleftrightarrow A^2=-\mathrm{Id}_2$ et donc $A^4=\mathrm{Id}_2$, ce qui montre que A est d'ordre 4

Ce que nous voulions

Remarque 3 :

1. Id_2 est donc la seule matrice de $\mathrm{SL}_2(\mathbb{Z})$ d'ordre 1
2. La démonstration ci-dessus montre que $-\mathrm{Id}_2$ est la seule matrice de $\mathrm{SL}_2(\mathbb{Z})$ d'ordre 2
3. Beaucoup de matrices de $\mathrm{GL}_2(\mathbb{Z})$ *[et non de* $\mathrm{SL}_2(\mathbb{Z})$*]* sont d'ordre 2

Exemples : Pour $n \in \mathbb{Z}$, les matrices $M_n = \begin{pmatrix} -1 & n \\ 0 & 1 \end{pmatrix}$ sont telles que $M_n^2 = \mathrm{Id}_2$ et sont donc d'ordre 2

Remarquons que $\det M_n = -1$ et que $M_n \notin \mathrm{SL}_2(\mathbb{Z})$

4. En nous intéressant à la conjugaison
   (a) La matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ est une matrice d'ordre 4. Toute matrice conjuguée à A est aussi d'ordre 4

   En effet, si $X = PAP^{-1}$, nous avons $X^4 = PA^4P^{-1} = P\mathrm{Id}_2P^{-1} = PP^{-1} = \mathrm{Id}_2$

   (b) De même, la matrice $B = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ et toutes ses conjuguées sont d'ordre 4

   (c) Les matrices $C = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ et $D = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ ainsi que leurs conjuguées sont d'ordre 6