A.2 Sous-groupe de congruence de $\mathrm{SL}_2(\mathbb{Z})$

Zoologie

« Zoologie », dans un cours de mathématiques, est un mot qui a une forme d'extra-territorialité ; c'est pourtant le mot qu'utilisait l'un de mes maîtres pour expliquer l'environnement dans lequel la théorie que nous allons étudier s'inscrit, en bref, l'écosystème de ce que nous allons étudier.

1. Nous avons étudié $\mathcal{M}_2(\mathbb{C})$, $\mathcal{M}_2(\mathbb{R})$, $\mathcal{M}_2(\mathbb{Z})$. Pourquoi ne pas étudier $\mathcal{M}_2(\mathbb{Z}/n\mathbb{Z})$ pour $n \in \mathbb{N}$ et $n \geqslant 2$
2. Par exemple, dans $\mathcal{M}_2(\mathbb{Z}/6\mathbb{Z})$, la matrice $A = \begin{pmatrix} \dot{1} & \dot{2} \\ \dot{3} & \dot{4} \end{pmatrix}$ est-elle inversible ?
   - ▷ L'un des premiers réflexes est d'en calculer le déterminant qui sera un élément de $\mathbb{Z}/6\mathbb{Z}$. Nous avons $\det A = \dot{1} \times \dot{4} - \dot{2} \times \dot{6} = -\dot{2} = \dot{4}$. Le déterminant est donc non nul et il nous est loisible de penser que A soit inversible.
     Si A est inversible, alors $A^{-1} = \dfrac{1}{\det A}\begin{pmatrix} \dot{4} & -\dot{2} \\ -\dot{3} & \dot{1} \end{pmatrix} = \dfrac{1}{\det A}\begin{pmatrix} \dot{4} & \dot{4} \\ \dot{3} & \dot{1} \end{pmatrix}$
   - ▷ Seulement, l'inverse de $\dot{4}$ n'existe pas dans $\mathbb{Z}/6\mathbb{Z}$ puisque 4 et 6 ne sont pas premiers entre eux et donc, même si le téterminant est non nul, l'inverse de A n'existe pas dans $\mathcal{M}_2(\mathbb{Z}/6\mathbb{Z})$
     En fait, il est assez facile, par calcul, de voir que la matrice $A = \begin{pmatrix} \dot{1} & \dot{2} \\ \dot{3} & \dot{4} \end{pmatrix}$ n'est pas inversible dans $\mathcal{M}_2(\mathbb{Z}/6\mathbb{Z})$
     Soit $M = \begin{pmatrix} \dot{a} & \dot{b} \\ \dot{c} & \dot{d} \end{pmatrix}$ une matrice telle que $AM = \mathrm{Id}_{\mathbb{Z}/6\mathbb{Z}}$.
     Nous avons alors : $AM = \begin{pmatrix} \dot{a} + \dot{2}\dot{c} & \dot{b} + \dot{2}\dot{d} \\ \dot{3}\dot{a} + \dot{4}\dot{c} & \dot{3}\dot{b} + \dot{4}\dot{d} \end{pmatrix}$
     Ce qui nous conduit à écrire $\dot{a} + \dot{2}\dot{c} = \dot{1}$ et $\dot{3}\dot{a} + \dot{4}\dot{c} = \dot{0}$.
     En additionnant, nous obtenons : $\dot{4}\dot{a} + \dot{6}\dot{c} = \dot{1} \Longrightarrow \dot{4}\dot{a} = \dot{1}$ ou encore $4a + 6u = 1 + 6v$.
     Or, $1 + 6v$ est un entier impair alors que $4a + 6u$ est un nombre pair ; l'égalité est donc impossible. Il n'existe donc pas, dans $\mathcal{M}_2(\mathbb{Z}/6\mathbb{Z})$, d'inverse à la matrice A
3. Ainsi, rien que $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ est-il difficile à trouver ; il faut que pour $A \in \mathcal{M}_2(\mathbb{Z}/6\mathbb{Z})$, $\det A$ soit inversible dans $\mathbb{Z}/6\mathbb{Z}$, et là, nous n'avons que 2 possibilités : $\det A = \dot{1}$ ou $\det A = \dot{5} = -\dot{1}$
   - ▷ Ainsi $X = \begin{pmatrix} \dot{5} & \dot{2} \\ \dot{1} & \dot{4} \end{pmatrix}$ est telle que $\det A = \dot{2} - \dot{2} = 0$ et X n'est donc pas inversible dans $\mathcal{M}_2(\mathbb{Z}/6\mathbb{Z})$.
     Il suffit de remarquer que $4 \times \begin{pmatrix} \dot{5} \\ \dot{1} \end{pmatrix} = \begin{pmatrix} \dot{2} \\ \dot{4} \end{pmatrix}$; les 2 colonnes de la matrice sont donc liées.
   - ▷ $Y = \begin{pmatrix} \dot{5} & \dot{2} \\ \dot{1} & \dot{3} \end{pmatrix}$ est telle que $\det A = \dot{1}$ et Y est donc inversible dans $\mathcal{M}_2(\mathbb{Z}/6\mathbb{Z})$.
     Par calcul, nous avons $Y^{-1} = \begin{pmatrix} \dot{3} & \dot{4} \\ \dot{5} & \dot{5} \end{pmatrix}$
4. Par contre, pourquoi ne pas s'intéresser à $\mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z}) = \left\{A \in \mathcal{M}_2(\mathbb{Z}/6\mathbb{Z}) \text{ telle que } \det A = \dot{1}\right\}$.
   D'ores et déjà, nous savons que $\mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z}) \neq \emptyset$ puisque $\mathrm{Id}_{\mathbb{Z}/6\mathbb{Z}} \in \mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z})$ et $Y = \begin{pmatrix} \dot{5} & \dot{2} \\ \dot{1} & \dot{3} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z})$
5. N'y aurait-il pas des $\mathbb{Z}/n\mathbb{Z}$ particuliers où tout serait facile ? Rapidement, nous nous tournons vers les nombres premiers où, si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps.
6. Prenons l'exemple de $\mathbb{Z}/7\mathbb{Z}$; 7 étant un nombre premier, $(\mathbb{Z}/7\mathbb{Z}, +, \times)$ est un corps commutatif.
   - ▷ Tout nombre de $\mathbb{Z}/7\mathbb{Z}$ non nul est inversible. Soit $A \in \mathcal{M}_2(\mathbb{Z}/7\mathbb{Z})$, alors si $\det A$ n'est pas congru à 0 modulo 7, alors la matrice A est inversible.
   - ▷ Soit donc $A = \begin{pmatrix} \dot{1} & \dot{2} \\ \dot{3} & \dot{4} \end{pmatrix}$ une matrice de $\mathcal{M}_2(\mathbb{Z}/7\mathbb{Z})$

Nous avons $\det A = -\dot{2} = \dot{5}$. A est donc inversible et sa matrice inverse est

$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} \dot{4} & -\dot{2} \\ -\dot{3} & \dot{1} \end{pmatrix} = \dot{3}\begin{pmatrix} \dot{4} & \dot{5} \\ \dot{4} & \dot{1} \end{pmatrix} = \begin{pmatrix} \dot{5} & \dot{1} \\ \dot{5} & \dot{3} \end{pmatrix}$$

▷ Bien sûr qu'il est aussi possible de s'intéresser à $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$, c'est à dire l'ensemble des matrices de $\mathcal{M}_2(\mathbb{Z}/7\mathbb{Z})$ de déterminant non nul qui, bien entendu est un sous-groupe de $\mathcal{M}_2(\mathbb{Z}/7\mathbb{Z})$. De même, $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$, l'ensemble des matrices de $\mathcal{M}_2(\mathbb{Z}/7\mathbb{Z})$ de déterminant 1 est un sous-groupe de $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$.
Par exemples :
⋆ $A = \begin{pmatrix} \dot{1} & \dot{2} \\ \dot{3} & \dot{4} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$
⋆ Et $B = \begin{pmatrix} \dot{2} & \dot{3} \\ \dot{5} & \dot{1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$

A.2.1 Théorème

Soit $n \in \mathbb{N}$, avec $n \geqslant 2$.
Considérons l'application $\Phi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ définie par :

$$\left\{ \begin{array}{ccc} \Phi : \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \\ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \Phi(A) = A = \begin{pmatrix} \dot{a} & \dot{b} \\ \dot{c} & \dot{d} \end{pmatrix} \end{array} \right.$$

Où $\dot{a}$, $\dot{b}$, $\dot{c}$ et $\dot{d}$ désignent les classes de a, b, c et d modulo n. On pourrait appeler cet homomorphisme, « l'homomorphisme naturel »
⇒ C'est clairement un homomorphisme de groupe multiplicatif
⇒ Le noyau de Φ est donné par

$$\ker\Phi = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ tel que } \Phi(M) = \begin{pmatrix} \dot{1} & \dot{0} \\ \dot{0} & \dot{1} \end{pmatrix} \right\}$$

C'est à dire que $b \equiv c \equiv 0\,[n]$ et $a \equiv d \equiv 1\,[n]$

Enoncé du théorème

L'homomorphisme naturel $\Phi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ est surjectif

Démonstration

Soit $\begin{pmatrix} \dot{a} & \dot{b} \\ \dot{c} & \dot{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$

▷ L'objet de la démonstration de ce théorème est de trouver une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ telle que

$$\Phi(M) = \Phi\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = \begin{pmatrix} \dot{a} & \dot{b} \\ \dot{c} & \dot{d} \end{pmatrix}$$

C'est à dire que nous devons rechercher une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telle que

$$\Phi(M) = \begin{pmatrix} \dot{a} & \dot{b} \\ \dot{c} & \dot{d} \end{pmatrix}$$

Avec $ad - bc = 1$
▷ Ce n'est pas si facile que cela ! La difficulté réside dans le fait que nous soyons dans $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$

Revenons, par exemple, dans $\mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z})$

La matrice $\begin{pmatrix} \dot{3} & \dot{-1} \\ \dot{7} & \dot{4} \end{pmatrix}$ est une matrice de $\mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z})$ puisque son déterminant Δ est tel que

$$\Delta = \dot{4} \times \dot{3} - \dot{-1} \times \dot{7} = \dot{7} = \dot{1}$$

Par contre, la matrice $\begin{pmatrix} 3 & -1 \\ 7 & 4 \end{pmatrix}$ est bien une matrice de $\mathcal{M}_2(\mathbb{Z})$.

Mais, comme son déterminant est 19, c'est une matrice de $\mathrm{GL}_2(\mathbb{Z})$, sans être une matrice de $\mathrm{SL}_2(\mathbb{Z})$

▷ Pour commencer, si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice de $\mathrm{SL}_2(\mathbb{Z})$, c'est à dire $\det M = 1$, alors M vérifie $\Phi(M) = \begin{pmatrix} \dot{a} & \dot{b} \\ \dot{c} & \dot{d} \end{pmatrix}$

▷ Dans $\mathbb{Z}$, si $a = 0$, c'est à dire si $\dot{a} = 0$, il est possible de remplacer a par $a + n$, puisque

$$\dot{\overline{a+n}} = \dot{a} + \dot{n} = \dot{a}$$

▷ Nous supposons, maintenant, $a \in \mathbb{Z}$ et $a \neq 0$, c'est à dire $a \in \mathbb{Z}^*$

▷ Nous avons $\dot{a} \times \dot{d} - \dot{b} \times \dot{c} = 1$, c'est à dire $ad - bc \equiv 1\,[n]$; autrement dit :

$$ad - bc + kn = 1 \text{ avec } k \in \mathbb{Z}$$

▷ **Nous avons** $\mathrm{pgcd}(a, b, n) = 1$
Supposons le contraire, c'est à dire $\mathrm{pgcd}(a, b, n) = p$ avec $p > 1$
Alors, $a = a'p$, $b = b'p$ et $c = c'p$, c'est à dire $a \equiv 0\,[p]$, $b \equiv 0\,[p]$ et $n \equiv 0\,[p]$.
Si $ad - bc + kn = 1$ avec $k \in \mathbb{Z}$, alors $ad - bc + kn \equiv 1\,[p]$.
Comme nous avons supposé $\mathrm{pgcd}(a, b, n) = p$ avec $p > 1$, alors

$$ad - bc + kn = a'pd - b'pc + kn'p = p(a'p - b'd + kn') \equiv 0\,[p]$$

Il y a donc une contradiction, et il est impossible que $\mathrm{pgcd}(a, b, n) = p$ avec $p > 1$, et donc nous avons $\mathrm{pgcd}(a, b, n) = 1$

▷ **Nous allons chercher** $b' \in \mathbb{Z}$ **tel que** $b' \equiv b\,[n]$ **et tel que** $\mathrm{pgcd}(a, b') = 1$

⋆ Si $b' \equiv b\,[n]$, alors il existe $k \in \mathbb{Z}$ tel que $b' - b = kn \iff b' = b + kn$. Nous allons donc recherche un $k \in \mathbb{Z}$ particulier tel que $\mathrm{pgcd}(b, b + kn) = 1$, c'est à dire $\mathrm{pgcd}(b, b') = 1$

⋆ a ayant été choisi non nul, a se décompose de manière unique en un produit de facteurs premiers $a = p_1 \times \cdots \times p_j \times q_1 \times \cdots \times q_l$.
De même, b peut se décomposer en un produits de facteurs premiers, communs avec d'éventuels facteurs premiers divisant a, c'est à dire que nous pouvons écrire $b = p_1 \times \cdots \times p_j \times \varpi_1 \times \cdots \times \varpi_{l_1}$.
Nous appelons k le produit des entiers premiers qui divisent a, mais qui ne divisent pas b, c'est à dire $k = q_1 \times \cdots \times q_l$.
Remarquons que $\mathrm{pgcd}(b, k) = 1$ et que chaque entier premier divisant a divise b ou k, et, dans ce cas, c'est un « ou » exclusif.
Si tous les entiers premiers divisant a divisent aussi b, on prend $k = 1$ [2]

⋆ **Nous allons démontrer que, pour le k que nous venons de choisir,** $\mathrm{pgcd}(a, b + kn) = 1$**, par l'absurde**
Supposons $\mathrm{pgcd}(a, b + kn) = u$ où $u > 1$.
Alors, il existe un entier premier p qui divise a et $b + kn$
→ Si u est un nombre premier, alors u divise a et $b + kn$ et le problème est terminé
→ Si u n'est pas un nombre premier, alors u peut se décomposer en un produit de facteurs premiers et ces facteurs premiers divisent tous a et $b + kn$

2. Attention, ce n'est pas pour cela que a divise b ou que b divise a ; prendre, par exemple $a = 2 \times 3^2 \times 5 = 90$ et $b = 2 \times 3 \times 5 \times 7 = 210$: a ne divise pas b, b ne divise pas a, par contre, les entiers premiers entrant dans la décomposition de a divisent b

Il existe donc un entier premier p qui divise a et $b+kn$
Comme p divise a et p divise $b+kn$, nous pouvons écrire $a=p\alpha'$ et $b+kn=p\alpha$.
p étant premier, si p ne divise ni b ni kn, alors, p ne divise pas $b+kn$.
Donc p divise ou bien k ou bien kn
→ Supposons que p divise k,
Alors, $k=k_1p$ et donc $kn=k_1pn$, d'où

$$b+kn=p\alpha\Longleftrightarrow b=p\alpha-kn\Longleftrightarrow b=p\alpha-k_1pn\Longleftrightarrow b=p(\alpha-k_1n)$$

Et donc p divise b
p divisant k et b divise aussi $\mathrm{pgcd}(k,b)$; il y a contradiction puisque $\mathrm{pgcd}(k,b)=1$
→ Donc p divise b et ne divise pas k
→ Par construction, p divisant $b+kn$, c'est à dire $b+kn=p\alpha$, nous avons $kn=p\alpha-b=p\alpha-pb_1=p(\alpha-b_1)$.
Donc, p divise kn et, ne divisant pas k, p divise n
→ Donc, p divise a, b et n et donc, p divise $\mathrm{pgcd}(a,b,n)$ et comme $\mathrm{pgcd}(a,b,n)=1$, nous avons $p=1$ et donc $\mathrm{pgcd}(a,b+kn)=1$.
En posant $b'=b+kn$, nous avons trouvé un b' tel que $\mathrm{pgcd}(a,b')=1$

▷ Nous devons avoir $ad-bc=1$
⋆ Comme $b'=b+kn$, nous pouvons écrire $b=b'-kn$ et donc

$$ad-bc=ad-(b'-kn)c=1\Longleftrightarrow ad-b'c=1-kn$$

Il nous est donc possible d'écrire $ad-b'c=1+mn$ où $m\in\mathbb{Z}$
⋆ Toutes les matrices du type $\begin{pmatrix}a & b'\\ c+xn & d+yn\end{pmatrix}$ avec $x\in\mathbb{Z}$ et $y\in\mathbb{Z}$ sont telles que

$$\Phi\left[\begin{pmatrix}a & b'\\ c+xn & d+yn\end{pmatrix}\right]=\begin{pmatrix}\dot{a} & \dot{b}\\ \dot{c} & \dot{d}\end{pmatrix}$$

puisque $\dot{b'}=\dot{b}$.
⋆ Calculons le déterminant de $\begin{pmatrix}a & b'\\ c+xn & d+yn\end{pmatrix}$

$$\begin{aligned}\det\begin{pmatrix}a & b'\\ c+xn & d+yn\end{pmatrix}=\begin{vmatrix}a & b'\\ c+xn & d+yn\end{vmatrix} &= a(d+yn)-b'(c+xn)\\ &= (ad-b'c)+(ay-b'x)n\\ &= 1+mn+(ay-b'x)n\\ &= 1+(m+ay-b'x)n\end{aligned}$$

⋆ Comme nous voulons avoir $\det\begin{pmatrix}a & b'\\ c+xn & d+yn\end{pmatrix}=1$, nous devons trouver $x\in\mathbb{Z}$ et $y\in\mathbb{Z}$ tels que $ay-b'x=-m$.
a et b' étant premiers entre eux, il existe $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$ tels que $au+b'v=1$ et donc, nous avons $a(-mu)+b'(-mv)=-m$.
En posant $x=-um$ et $y=mv$, nous avons $ay-b'x=-m$

Ainsi, en choisissant ces tels x et y, nous avons donc $M=\begin{pmatrix}a & b'\\ c+xn & d+yn\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ qui est telle que $\Phi(M)=\begin{pmatrix}\dot{a} & \dot{b}\\ \dot{c} & \dot{d}\end{pmatrix}$

Φ est donc surjective

Exemple 2 :

Nous nous intéressons à $\mathrm{SL}_2(\mathbb{Z}/21\mathbb{Z})$.

Dans $\mathcal{M}_2(\mathbb{Z}/21\mathbb{Z})$, nous considérons la matrice $A=\begin{pmatrix}\dot{18} & \dot{14}\\ \dot{4} & \dot{2}\end{pmatrix}$; le calcul du déterminant nous donne $\det A=\dot{18}\times\dot{2}-\dot{4}\times\dot{14}=-\dot{20}=\dot{1}$. Donc $A\in\mathrm{SL}_2(\mathbb{Z}/21\mathbb{Z})$.
Cherchons maintenant une matrice $M\in\mathrm{SL}_2(\mathbb{Z})$ telle que $\Phi(M)=A$.

→ Les deux nombres 18 et 14 ne sont pas premiers entre eux, alors que 18 et $14+21=35$ le sont
→ Le déterminant de la matrice $\begin{pmatrix}18 & 35\\ 4 & 2\end{pmatrix}$ est $-104=1-105=1+21\times(-5)=1+21m$
→ Une solution à $18y-35x=-m=5$ est donnée par $x=5$ et $y=10$
→ Donc :

$$\begin{pmatrix}\dot{18} & \dot{14}\\ \dot{4} & \dot{2}\end{pmatrix}=\begin{pmatrix}\dot{18} & \dot{35}\\ \dot{4+5\times 21} & \dot{2+10\times 21}\end{pmatrix}=\begin{pmatrix}\dot{18} & \dot{35}\\ \dot{109} & \dot{212}\end{pmatrix}$$

Ainsi, la matrice $M=\begin{pmatrix}18 & 35\\ 109 & 212\end{pmatrix}$ est une matrice de $\mathrm{SL}_2(\mathbb{Z})$ telle que $\Phi(M)=A=\begin{pmatrix}\dot{18} & \dot{14}\\ \dot{4} & \dot{2}\end{pmatrix}$

Remarque 4 :

1. Nous avons $\ker\Phi=\left\{M\in\mathrm{SL}_2(\mathbb{Z}) \text{ telles que } \Phi(M)=\begin{pmatrix}\dot{1} & \dot{0}\\ \dot{0} & \dot{1}\end{pmatrix}\right\}$
   C'est évidemment un sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$
2. Par le théorème 12.7.6, nous avons $\mathrm{SL}_2(\mathbb{Z})/\ker\Phi$ isomorphe à $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$

A.2.2 Corollaire

Le groupe fini $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ est engendré par 2 éléments d'ordre n

Démonstration

Φ étant surjective, pour toute matrice $A\in\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, il existe $M\in\mathrm{SL}_2(\mathbb{Z})$ telle que $A=\Phi(M)$
Nous avons démontré en A.1.2 que $\mathrm{SL}_2(\mathbb{Z})$ était engendré par les matrices $S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ et $T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, ce qui veut dire que, pour tout $M\in\mathrm{SL}_2(\mathbb{Z})$, nous avons

$$M=S^{\alpha_1}T^{\beta_1}\cdots S^{\alpha_p}T^{\beta_p}$$

Et donc $\Phi(M)=[\Phi(S)]^{\alpha_1}[\Phi(T)]^{\beta_1}\cdots[\Phi(S)]^{\alpha_p}[\Phi(T)]^{\beta_p}$.
Or, $\Phi(S)$ et $\Phi(S)$ sont des éléments de $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ d'ordre n et donc $A=\Phi(M)$ est une matrice d'ordre n