Problème A : localisation de racines

1) *Étude d'une fonction auxiliaire f*

a) La fonction f est polynomiale, donc $\mathcal{C}^\infty$ sur $\mathbb{R}$ et j'ai, puisque $p>0$,

$$\forall r\geq 0 \quad f'(r)=(p+1)\,r^p-p\,(M+1)\,r^{p-1}=(p+1)\,r^{p-1}\,(r-r_0) \quad \text{où} \quad r_0=\frac{p\,(M+1)}{p+1}=\frac{M+1}{\dfrac{1}{p}+1}$$

Il en résulte que

$$\boxed{\text{L'unique zéro strictement positif } r_0 \text{ de } f' \text{ est } \frac{M+1}{\dfrac{1}{p}+1} \text{ ; si } M\leq\frac{1}{p},\ r_0\leq 1 \text{ ; si } M>\frac{1}{p},\ r_0>1.}$$

Notons que f est strictement décroissante sur $[0,r_0]$ et strictement croissante sur $[r_0,+\infty[$; par ailleurs $f(1)=0$.

b) On suppose $M\leq\dfrac{1}{p}$. Alors d'après les résultats précédents, $r_0\leq 1$ et f est en particulier strictement croissante sur $[1,+\infty[$. Donc, comme $f(1)=0$,

$$\boxed{f \text{ est strictement positive sur }]1,+\infty[.}$$

c) On suppose $M>\dfrac{1}{p}$. Ici $r_0>1$ donc $f(r_0)<0$; mais $r_0=\dfrac{M+1}{\dfrac{1}{p}+1}<M+1$, donc f est en particulier strictement croissante sur $[M+1,+\infty[$or

$$f(M+1)=(M+1)^{p+1}-(M+1)\,(M+1)^p+M=M>0$$

puisque par hypothèse $M>\dfrac{1}{p}$! Par conséquent,

$$\boxed{f \text{ est strictement positive sur } [M+1,+\infty[.}$$

2) *Localisation des racines du polynôme P*

a) Soit z complexe tel que $|z|\neq 1$ et $P(z)=0$. J'ai donc

$$z^p=-\sum_{k=0}^{p-1}a_k z^k,$$

d'où, grâce à l'inégalité triangulaire, la définition de M et

$$|z|^p\leq\sum_{k=0}^{p-1}|a_k|\cdot|z|^k\leq M\cdot\sum_{k=0}^{p-1}|z|^k$$

donc par la formule donnant la somme de termes consécutifs d'une suite géométrique de raison différente de 1 :

$$\boxed{|z|^p\leq M\cdot\frac{|z|^p-1}{|z|-1}.}$$

En supposant $|z|>1$, je peux multiplier l'inégalité précédente par $|z|-1$, ce qui donne en développant

$$|z|^{p+1}-|z|^p\leq M\cdot|z|^p-M$$

et j'ai donc établi

$$\boxed{\text{Si } z \text{ est une racine de } P \text{ telle que } |z|>1, \text{ alors } f(|z|)\leq 0.}$$

b) Si $M\leq\dfrac{1}{p}$, **1)b)** et **2)a)** donneraient une contradiction si P admettait une racine de module strictement supérieur à 1, donc

$$\boxed{\text{Les racines de } P \text{ sont de module inférieur ou égal à 1.}}$$

c) De même, si $M>\dfrac{1}{p}$, **1)c)** et **2)a)** donneraient une contradiction si P admettait une racine de module supérieur ou égal à $M+1$ (donc *a fortiori* à 1 !). Ainsi

$$\boxed{\text{Les racines de } P \text{ sont de module strictement inférieur à } M+1.}$$

3) *Premier exemple*

Ici $M = \dfrac{1}{p}$, donc le **2)b)** s'applique :

$$\boxed{\text{Les racines de } P \text{ sont de module inférieur ou égal à 1.}}$$

Comme la somme dans la définition de P comporte p termes, j'ai $P(1) = 0$. Je vérifie alors que $P'(1) \neq 0$:

$$P'(1) = p - \frac{1}{p} \cdot \sum_{k=1}^{p-1} k = p - \frac{1}{p} \cdot \frac{(p-1)\,p}{2} = \frac{p+1}{2}.$$

En conclusion

$$\boxed{1 \text{ est racine simple de } P.}$$

Rappelons qu'en cas de question floue ou mal posée, il s'agit de trouver malgré tout une réponse "intéressante"... Dans ce cas de figure, le **2)b)** a fourni 1 comme majorant des modules des racines de P. Cet exemple montre que l'on ne peut pas remplacer (dans le cas général !) 1 par une valeur plus petite.

4) *Second exemple*

a) Ici $M = 1 > \dfrac{1}{p}$, donc le **2)c)** s'applique :

$$\boxed{\text{Les racines de } P \text{ sont de module strictement inférieur à 2.}}$$

b) Soit z racine de P, j'ai donc

$$z^p = z^{p-1} + \cdots + 1$$

d'où, en multipliant par $z-1$ et en simplifiant,

$$z^{p+1} - z^p = z^p - 1 \quad \text{soit} \quad z^{p+1} - 2z^p + 1 = 0.$$

Ainsi,

$$\boxed{\text{Si } z \text{ est racine de } P, \text{ alors } z \text{ est racine de } X^{p+1} - 2X^p + 1.}$$

c) Soit la fonction polynomiale $g : r \mapsto r^{p+1} - 2r^p + 1$. Elle est $\mathcal{C}^\infty$ sur $\mathbb{R}$ et

$$\forall r \geq 0 \quad g'(r) = (p+1)\,r^p - 2pr^{p-1} = (p+1)\,r^{p-1}(r-\alpha) \quad \text{où} \quad \alpha = \frac{2p}{p+1}.$$

Ainsi g décroît strictement sur $[0,\alpha]$ et croît strictement sur $[\alpha,+\infty[$. Or

$$\alpha - 1 = \frac{p-1}{p+1} \quad \text{donc} \quad \alpha > 1 \quad \text{car} \quad p \geq 2.$$

Par ailleurs $g(1) = 0$ donc $g(\alpha) < 0$. Comme $g(2) = 1$, le théorème de la bijection montre que g s'annule en un unique point x_p de $[\alpha, 2]$.

N.B. : on peut aussi remarquer que g n'est autre que la fonction f du **1)** dans le cas $M = 1$...

Le **b)** montre que x_p est la seule racine possible de P dans $[\alpha, 2]$, mais il ne faut pas omettre de vérifier qu'elle est bien racine ! Heureusement c'est immédiat, du fait que $x_p \neq 1$ (car $\alpha > 1$), ce qui permet de diviser par $(x_p - 1)$ l'égalité

$$x_p^{p+1} - x_p^p = x_p^p - 1$$

pour "remonter" le calcul du **b)**. En conclusion

$$\boxed{\text{Le polynôme } P \text{ admet une racine réelle } x_p \text{ telle que } \frac{2p}{p+1} \leq x_p \leq 2.}$$

Là encore, puisque $x_p \underset{p\to\infty}{\longrightarrow} 2$ (théorème d'encadrement), j'en déduis que le majorant 2 fourni par le **2)c)** est optimal (au sens où l'on ne peut le remplacer par une valeur inférieure valable pour tout p).

d) On pose $\varepsilon_p = 2 - x_p$. La relation $g(x_p) = 0$ s'écrit

$$2x_p^p - x_p^{p+1} = 1 \quad \text{soit} \quad \varepsilon_p x_p^p = 1 \quad \text{donc} \quad \varepsilon_p = x_p^{-p}.$$

Or $x_p = 2 - \varepsilon_p$ d'où finalement

$$\boxed{\varepsilon_p = (2-\varepsilon_p)^{-p}.}$$

J'ai vu au **c)** que $\varepsilon_p \underset{p\to\infty}{\longrightarrow} 0$. Et $x_p < 2$ donc $\varepsilon_p > 0$ et à partir d'un certain rang $\varepsilon_p \leq \dfrac{1}{2}$, soit $2 - \varepsilon_p \geq \dfrac{3}{2}$, d'où

$$\varepsilon_p \leq \left(\frac{2}{3}\right)^p.$$

J'en déduis par croissances comparées que

$$\boxed{p\varepsilon_p \underset{p\to\infty}{\longrightarrow} 0.}$$

Or

$$\varepsilon_p = \frac{1}{2^p}\left(1 - \frac{\varepsilon_p}{2}\right)^{-p} = \frac{1}{2^p}\exp\left(-p\ln\left(1 - \frac{\varepsilon_p}{2}\right)\right).$$

D'après ce qui précède,

$$-p\ln\left(1 - \frac{\varepsilon_p}{2}\right) \underset{p\to\infty}{\sim} \frac{p\varepsilon_p}{2} \underset{p\to\infty}{\longrightarrow} 0$$

et donc $\left(1 - \dfrac{\varepsilon_p}{2}\right)^{-p} \underset{p\to\infty}{\longrightarrow} 1$ d'où finalement

$$\boxed{\varepsilon_p \underset{p\to\infty}{\sim} \frac{1}{2^p}.}$$

Ainsi $\varepsilon_p \underset{p\to\infty}{=} \dfrac{1}{2^p} + o\left(\dfrac{1}{2^p}\right)$ or $x_p = 2 - \varepsilon_p$:

$$\boxed{x_p \underset{p\to\infty}{=} 2 - \frac{1}{2^p} + o\left(\frac{1}{2^p}\right).}$$

5) Pour cette dernière question, il suffit de remarquer qu'un réel positif est plus grand que 1/2 si et seulement si son inverse est plus petit que 2… Soit donc z une racine de P ; $P(0) = -1$ donc $z \neq 0$. De plus $P(z) = 0$, d'où en divisant par z^p

$$1 - \frac{1}{z} - \frac{1}{z^2} - \cdots - \frac{1}{z^p} = 0$$

donc, en changeant les signes, $\dfrac{1}{z}$ est racine du polynôme

$$Q(X) = X^p + \cdots + X^2 + X - 1.$$

Le **3)c)** s'applique à ce polynôme (avec $M = 1$) et donc $0 < \left|\dfrac{1}{z}\right| < 2$, d'où $|z| > \dfrac{1}{2}$.

$$\boxed{\text{Toutes les racines de } P \text{ sont de module compris strictement entre } \frac{1}{2} \text{ et } 2.}$$

Problème B : irrationalité de π

1) En vertu des théorèmes opératoires classiques, G est de classe $\mathcal{C}^\infty$. Soit x réel ; calculons :

$$G'(x) = F''(x)\sin x + F'(x)\cos x - \left(F'(x)\cos x - F(x)\sin x\right),$$

soit : $G'(x) = \left(F''(x) + F(x)\right)\cdot\sin x$.

Or, en réindexant et en tenant compte de $P^{(2n+2)} = 0$ (puisque P est de degré $2n$) :

$$F''(x) = \sum_{k=0}^{n}(-1)^k P^{(2k+2)}(x) = \sum_{k=1}^{n}(-1)^{k-1}P^{(2k)}(x) \quad \text{d'où} \quad F''(x) + F(x) = P(x).$$

Par conséquent :

$$\boxed{\forall x\in\mathbb{R} \quad G'(x) = P(x)\cdot\sin x.}$$

J'ai donc : $\displaystyle\int_0^\pi P(x)\sin x\mathrm{d}x = \int_0^\pi G'(x)\,\mathrm{d}x = G(\pi) - G(0)$, soit, par définition de G :

$$\boxed{\int_0^\pi P(x)\sin x\mathrm{d}x = F(0) + F(\pi).}$$

2) a) Par définition, 0 est racine d'ordre n de P donc, d'après la caractérisation de l'ordre de multiplicité d'une racine :

$$\boxed{\forall j \in [\![0, n-1]\!] \quad P^{(j)}(0) = 0.}$$

En développant par la formule du binôme (a et $-bx$ commutent !) :

$$P(x) = \frac{1}{n!} x^n \sum_{j=0}^{n} \binom{n}{j} a^{n-j} (-bx)^j = \frac{1}{n!} \sum_{j=0}^{n} (-1)^j \binom{n}{j} a^{n-j} b^j x^{n+j},$$

ainsi,

$$\boxed{\text{Pour } j \in [\![0, n]\!], \text{ le coefficient de } x^{n+j} \text{ de } P(x) \text{ est } \frac{1}{n!} (-1)^j \binom{n}{j} a^{n-j} b^j.}$$

Or, d'après la formule de Taylor, ce coefficient n'est autre que $\dfrac{P^{(n+j)}(0)}{(n+j)!}$, d'où

$$\boxed{P^{(n+j)}(0) = \frac{(n+j)!}{n!} (-1)^j \binom{n}{j} a^{n-j} b^j.}$$

Puisque $\binom{n}{j}, a, b$ sont entiers et que $n!$ divise $(n+j)!$, il en résulte que les $P^{(n+j)}(0)$ sont dans $\mathbb{Z}$, cela pour tout j de $[\![0, n]\!]$. Finalement, les $P^{(j)}(0)$ sont dans $\mathbb{Z}$, pour tout j dans $[\![0, 2n]\!]$; donc, d'après l'expression de $F(0)$:

$$\boxed{F(0) \text{ est un entier relatif.}}$$

b) Soit $x \in \mathbb{R}$; par définition de P et du fait que $\pi = \dfrac{a}{b}$:

$$P(\pi - x) = \frac{1}{n!} (\pi - x)^n \left(a - b(\pi - x)\right)^n = \frac{1}{n!} \left(\frac{a}{b} - x\right)^n (bx)^n,$$

ainsi

$$\boxed{\forall x \in \mathbb{R} \quad P(\pi - x) = P(x).}$$

J'en déduis, pour x fixé dans $\mathbb{R}$, par une récurrence immédiate sur j, que

$$\forall j \in \mathbb{N} \quad P^{(j)}(\pi - x) = (-1)^j P^{(j)}(x), \quad \text{d'où} \quad \forall k \in \mathbb{N} \quad P^{(2k)}(\pi - x) = P^{(2k)}(x)$$

donc, par combinaison linéaire :

$$F(\pi - x) = F(x).$$

En particulier, pour $x = 0$, j'obtiens $F(\pi) = F(0)$, donc, d'après la question précédente :

$$\boxed{F(\pi) \text{ est un entier relatif.}}$$

c) En tant qu'intégrale d'une fonction continue sur $[0, \pi]$, strictement positive sur $]0, \pi[$, I_n est strictement positif, cela pour tout n.

De plus, d'après les questions précédentes, $I_n = F(0) + F(\pi)$ est un entier relatif, donc finalement

$$\boxed{(I_n) \text{ est une suite d'entiers strictement positifs.}}$$

d) Majorons I_n, pour $n \in \mathbb{N}$. La fonction $x \mapsto x(\pi - x)$ atteint son maximum en $\pi/2$, d'où

$$\forall x \in [0, \pi] \quad x(\pi - x) \leq \frac{\pi^2}{4} \quad \text{donc} \quad P(x) \leq \frac{b^n}{n!} \left(\frac{\pi^2}{4}\right)^n = \frac{B^n}{n!}$$

en posant $B = \dfrac{b\pi^2}{4}$; j'en déduis que $0 \leq I_n \leq \pi \dfrac{B^n}{n!}$. Or, d'après les croissances comparées des suites classiques, $B^n = o(n!)$, d'où finalement :

$$\boxed{\text{La suite } (I_n) \text{ converge vers 0.}}$$

e) Les deux résultats précédents apportent bien sûr une contradiction : tout entier strictement positifs est au moins égal à 1 (!), donc la suite (I_n) ne peut converger vers 0. En conclusion,

$$\boxed{\pi \text{ n'est pas un nombre rationnel.}}$$

Problème C : dénombrement de surjections

1) a) Pour $P = \sum_{k=0}^{n} \lambda_k X^k \in \mathbb{R}_n[X]$, $T_a P = \sum_{k=0}^{n} \lambda_k (X+a)^k$ est bien encore élément de $\mathbb{R}_n[X]$; T_a est donc une application de $\mathbb{R}_n[X]$ dans lui-même, sa linéarité est banale :

$$\boxed{T_a \text{ est un endomorphisme de } \mathbb{R}_n[X].}$$

Les colonnes de sa matrice M_a dans la base canonique $\mathcal{B}$ contiennent les coordonnées dans $\mathcal{B}$ des images des vecteurs de $\mathcal{B}$ par T_a ; par commodité, je numérote les $n+1$ lignes et colonnes de 0 à n et je développe par la formule du binôme :

$$\forall j \in [\![0,n]\!] \quad T_a e_j = (X+a)^j = \sum_{i=0}^{j} \tbinom{j}{i} a^{j-i} X^i.$$

Ainsi :

$$\boxed{M_a = (m_{i,j})_{0\leq i,j\leq n} \quad \text{où} \quad m_{i,j} = \begin{cases} 0 & \text{si } i > j \\ \binom{j}{i} a^{j-i} & \text{si } i \leq j \end{cases}.}$$

b) Soit $(a,b) \in \mathbb{R}^2$; pour tout P de $\mathbb{R}_n[X]$,

$$\begin{aligned} (T_a \circ T_b) P(X) &= T_a Q(X) \quad \text{où} \quad Q(X) = P(X+b) \\ &= Q(X+a) = P(X+a+b) = T_{a+b} P(X) \end{aligned}$$

Par conséquent :

$$\boxed{\forall (a,b) \in \mathbb{R}^2 \quad T_a \circ T_b = T_{a+b}.}$$

c) Comme $T_0 = \mathrm{Id}_{\mathbb{R}_n[X]}$, le résultat précédent montre que $M_1^{-1} = M_{-1}$; donc d'après **a)**, en convenant que $\binom{j}{i} = 0$ pour $i > j$:

$$\boxed{M_1 = \left(\tbinom{j}{i}\right)_{0\leq i,j\leq n} \quad \text{et} \quad M_1^{-1} = \left((-1)^{j-i}\tbinom{j}{i}\right)_{0\leq i,j\leq n}.}$$

2) $s(p,0) = 0$ pour $p > 0$ est naturel (il n'y a aucune application d'un ensemble non vide vers $\emptyset$, *a fortiori* pas de surjection !), $s(0,n) = 0$ pour $n > 0$ et $s(0,0) = 1$ sont un peu moins naturels intuitivement, mais se comprennent bien si l'on réalise qu'il y a une unique application de $\emptyset$ dans n'importe quel ensemble F, dont le graphe est vide ("à rien, on n'associe rien"). C'est bien une application (tout élément de $\emptyset$ a une image et une seule dans F, essayez de dire le contraire...). Si F est non vide, ce n'est pas une surjection ! Si F est également vide, c'est une bijection !! (Essayez de dire le contraire !!!). Assez ri...

a) Je considère un ensemble E à p éléments (ici $p > 0$ par hypothèse).

- L'unique application de E dans un singleton $\{y\}$ est surjective : y admet tous les éléments de E pour antécédents, il y en a au moins 1 puisque j'ai supposé $p > 0$. Donc $s(p,1) = 1$.
- Parmi les 2^p applications de E dans une paire $\{y_1, y_2\}$, deux et deux seulement ne sont pas surjectives : les applications constantes $x \mapsto y_1$ et $x \mapsto y_2$. Donc $s(p,2) = 2^p - 2$.
- Parmi les applications entre deux ensembles finis de même cardinal p, les surjections sont exactement les bijections, au nombre de $p!$. Ainsi $s(p,p) = p!$.
- Lorsque $n > p$, il n'y a aucune surjection de e dans un ensemble de cardinal n, puisque l'image de E par une application contient au plus p éléments : $s(p,n) = 0$ lorsque $n > p$.

b) Soient deux ensembles, E de cardinal p et F de cardinal n. L'ensemble F^E des applications de E dans F a pour cardinal n^p. Pour $k \in [\![0,n]\!]$, je note $\mathcal{F}_k$ l'ensemble des applications f de E dans F dont l'image $f(E)$ a pour cardinal k (noter que $\mathcal{F}_0$ est vide, puisque $p > 0$!). Les $\mathcal{F}_k$ sont clairement disjoints deux à deux et leur réunion est F^E tout entier, j'ai donc

$$n^p = \sum_{k=0}^{n} \mathrm{card}\, \mathcal{F}_k \ .$$

Pour k fixé, reste à dénombrer les éléments de $\mathcal{F}_k$: F contient $\binom{n}{k}$ parties à k éléments et, pour chaque partie B de F à k éléments, le nombre d'applications f de E dans F telles que $f(E) = B$ n'est autre que le nombre de surjections de E dans B, il y en a $s(p,k)$, d'où en conclusion :

$$\boxed{n^p = \sum_{k=0}^{n} \tbinom{n}{k} \cdot s(p,k).}$$

c) Par définition du produit matriciel,

$$\left[s\left(p,0\right)\ s\left(p,1\right)\ \ldots\ s\left(p,n\right)\right]\times M_1=\left[c_0\ c_1\ \ldots\ c_n\right]$$

où, d'après l'expression de M_1 et grâce à la question précédente :

$$\forall j\in[\![0,n]\!]\quad c_j=\sum_{i=0}^{n}s\left(p,i\right)\cdot\binom{j}{i}=\sum_{i=0}^{j}s\left(p,i\right)\cdot\binom{j}{i}=j^p.$$

Ainsi,

$$\boxed{\left[s\left(p,0\right)\ s\left(p,1\right)\ \ldots\ s\left(p,n\right)\right]\times M_1=\left[0^p\ 1^p\ 2^p\ \ldots\ n^p\right].}$$

En multipliant à droite par $M_1^{-1}=M_{-1}$, j'en déduis, dans la dernière colonne :

$$\boxed{s\left(p,n\right)=\sum_{i=0}^{n}i^p\left(-1\right)^{n-i}\binom{n}{i}.}$$

Noter que le terme pour $i=0$ n'a d'intérêt que pour $p=0\ldots$

3) a) C'est bien banal, puisque e^x et 1 commutent dans $\mathbb{R}\ldots$

$$\boxed{f_n\left(x\right)=\left(e^x-1\right)^n=\sum_{k=0}^{n}\binom{n}{k}\left(-1\right)^{n-k}e^{kx}.}$$

b) Soit p dans $\mathbb{N}$. En dérivant p fois, j'obtiens par linéarité :

$$f_n^{(p)}\left(x\right)=\sum_{k=0}^{n}\binom{n}{k}\left(-1\right)^{n-k}k^pe^{kx}$$

d'où, d'après le **2)** *in fine* :

$$\boxed{f_n^{(p)}\left(0\right)=s\left(p,n\right).}$$

c) D'après la formule de Taylor en 0 :

$$\boxed{e^x-1=x+\frac{x^2}{2}+\frac{x^3}{6}+o\left(x^3\right)=x\cdot\left(1+\frac{x}{2}+\frac{x^2}{6}+o\left(x^2\right)\right)}$$

d'où, par composition avec le développement limité de $\left(1+u\right)^n$:

$$\begin{aligned}f_n\left(x\right)&=x^n\cdot\left(1+\frac{x}{2}+\frac{x^2}{6}+o\left(x^2\right)\right)^n\\&=x^n\cdot\left(1+n\cdot\left(\frac{x}{2}+\frac{x^2}{6}\right)+\frac{n\left(n-1\right)}{2}\cdot\left(\frac{x}{2}+\frac{x^2}{6}\right)^2+o\left(x^2\right)\right)\\&=x^n\cdot\left(1+\frac{n}{2}\cdot x+\left(\frac{n}{6}+\frac{n\left(n-1\right)}{2}\cdot\frac{1}{4}\right)\cdot x^2+o\left(x^2\right)\right)\end{aligned}$$

soit

$$\boxed{f_n\left(x\right)=x^n+\frac{n}{2}\cdot x^{n+1}+\frac{n\left(3n+1\right)}{24}\cdot x^{n+2}+o\left(x^{n+2}\right).}$$

d) f étant de classe $\mathcal{C}^\infty$, elle admet aussi un développement limité en vertu de la formule de Taylor, d'où, par unicité des coefficients de ce développement limité :

$$f_n^{(p)}\left(0\right)=0\text{ pour }0\leq p<n\ ,\ \frac{f_n^{(n)}\left(0\right)}{n!}=1\ ,\ \frac{f_n^{(n+1)}\left(0\right)}{(n+1)!}=\frac{n}{2}\ ,\ \frac{f_n^{(n+2)}\left(0\right)}{(n+2)!}=\frac{n\left(3n+1\right)}{24}.$$

Il en résulte, grâce à **a)** :

$$\boxed{s\left(p,n\right)=0\text{ pour }0\leq p<n,\ s\left(n,n\right)=n!,\ s\left(n+1,n\right)=\frac{n\cdot(n+1)!}{2}\text{ et }s\left(n+2,n\right)=\frac{n\left(3n+1\right)\cdot(n+2)!}{24}.}$$

Problème D : génération de $SL_2(\mathbb{Z})$

1) Je constate que $SL_2(\mathbb{Z})$ est un sous-groupe de $(GL_2(\mathbb{R}), \times)$: c'en est une partie (toute matrice de déterminant 1 est inversible !), non vide (contenant I), stable par $\times$ (le produit de deux matrices de $SL_2(\mathbb{Z})$ est bien à coefficients entiers et de déterminant $1 \times 1 = 1$), stable enfin par passage à l'inverse ; en effet, pour $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $\det M = 1$ et donc, tous calculs faits, $M^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ qui est bien dans $SL_2(\mathbb{Z})$.

Je remarque aussi que $(AB)_{1,1} = 0$ tandis que $(BA)_{1,1} = 1$, donc $AB \neq BA$ alors que A et B sont dans $SL_2(\mathbb{Z})$. En conclusion

$$\boxed{(SL_2(\mathbb{Z}), \times) \text{ est un groupe, non commutatif.}}$$

2) a) D'après ce qui précède, $B^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$; soit $\varepsilon = \pm 1$ et $N = \begin{pmatrix} 0 & \varepsilon \\ 0 & 0 \end{pmatrix}$; j'ai $N^2 = 0$ et donc toutes les puissances suivantes de N sont nulles. De plus I et N commutent, je peux appliquer la formule du binôme :

$$\forall k \in \mathbb{N} \quad (I+N)^k = I + kN,$$

tous les termes suivants étant nuls d'après la remarque précédente. Pour $\varepsilon = 1$, j'obtiens B^k et, pour $\varepsilon = -1$, $\left(B^{-1}\right)^k$ c'est-à-dire B^{-k}. Les deux résultats se regroupent :

$$\boxed{\forall k \in \mathbb{Z} \quad B^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.}$$

Ensuite il n'y a qu'à effectuer les produits.

$$\boxed{\forall k \in \mathbb{Z} \quad B^k A = \begin{pmatrix} k & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad PB^kA = \begin{pmatrix} c & 0 \\ bk+d & -b \end{pmatrix}.}$$

b) Notons que $bc = -1$ (puisque $P \in SL_2(\mathbb{Z})$) et donc, comme b et c sont entiers, $b = -c \in \{-1, 1\}$. Ainsi $k = -d/b$ est-il entier et pour cette valeur de k j'ai $PB^kA = cI$ donc

$$\boxed{\text{Il existe } k \text{ dans } \mathbb{Z} \text{ tel que } PB^kA \in \{-I, I\}.}$$

c) Avec k tel que dans la question précédente, $P = cIA^{-1}B^{-k}$, or $-I = A^2$ donc, que c vaille -1 ou 1, j'ai bien écrit P comme produit fini d'éléments de $\mathcal{E}$. Autrement dit

$$\boxed{P \in G.}$$

3) Je remarque (habilement) que $QA = \begin{pmatrix} 0 & -a \\ d & -b \end{pmatrix}$; or a, b et d sont entiers et $ad = 1$, donc $QA \in G$ d'après **2)**. Or une matrice de G multipliée par A^{-1} est encore dans G !

$$\boxed{Q \in G.}$$

4) <u>*Division euclidienne dans* $\mathbb{Z}$</u> : le théorème de la division euclidienne dans $\mathbb{N}$ me fournit q_1 et r_1 dans $\mathbb{N}$ tels que

$$|c| = |a|\, q_1 + r_1 \quad \text{et} \quad 0 \leq r_1 < |a|\,.$$

Il est alors aisé de trouver un couple (q, r) d'entiers relatifs vérifiant les conditions, dans chacun des cas suivants (qui recouvrent toutes les possibilités !) :

- si a et c sont positifs, (q_1, r_1) convient
- si a et c sont négatifs, $(q_1, -r_1)$ convient
- si a est positif et c négatif, $(-q_1, -r_1)$ convient
- si a est négatif et c positif, $(-q_1, r_1)$ convient

Un tel couple (q, r) n'est pas toujours unique : par exemple $7 = 3 * 2 + 1 = 3 * 3 - 2$, donc avec $c = 7$ et $a = 3$, les deux couples $(2, 1)$ et $(3, -2)$ conviennent.

N.B. On vérifie facilement qu'il y a un unique couple (q, r) lorsque a divise c et deux sinon.

5) D'après **2)a)**, si $M_n = \begin{pmatrix} a_n & c_n \\ b_n & d_n \end{pmatrix}$, alors pour tout k dans $\mathbb{Z}$, $M_n B^k A = \begin{pmatrix} ka_n + c_n & -a_n \\ kb_n + d_n & -b_n \end{pmatrix}$.

Je construis alors les familles (k_n) et (M_n) selon l'algorithme suivant :

- $M_0 \leftarrow M$, $k_0 \leftarrow -q_0$ (où $c = aq_0 + r_0$ avec $|r_0| < |a|$ selon le **4)**
- $M_1 \leftarrow M_0 B^{k_0} A$ notée $\begin{pmatrix} a_1 & c_1 \\ b_1 & d_1 \end{pmatrix}$;
- $n \leftarrow 1$
- **tant que** $a_n \neq 0$

  $k_n \leftarrow -q_n$ (où $c_n = a_n q_n + r_n$ avec $|r_n| < |a_n|$ selon le **4)**

  $M_{n+1} \leftarrow M_n B^{k_n} A$ notée $\begin{pmatrix} a_{n+1} & c_{n+1} \\ b_{n+1} & d_{n+1} \end{pmatrix}$

  $n \leftarrow n + 1$

  fin tant que

Tant que l'on reste dans la boucle, $a_{n+1} = k_n a_n + c_n = r_n$ vérifie par construction $|a_{n+1}| < |a_n|$. Comme les a_n sont entiers, il en résulte que l'on ne passera qu'un nombre fini de fois dans la boucle. Autrement dit je dispose de p dans $\mathbb{N}^*$ tel que $a_n \neq 0$ pour $0 \leq n < p$ et $a_p = 0$.

La construction se termine et toutes les demandes de l'énoncé sont satisfaites.

6) Soit $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ une matrice de $SL_2(\mathbb{Z})$. Si $a = 0$ le **2)** a montré que $M \in G$. Si $a \neq 0$, le **4)** fournit une matrice

$$M_p = MB^{k_0} AB^{k_1} A \dots B^{k_{p-1}} A$$

qui appartient à G (toujours d'après **2)** puisque $a_p = 0$). Il en découle que

$$M = M_p A^{-1} B^{-k_{p-1}} \dots A^{-1} B^{-k_0}$$

appartient aussi à G. Je viens de montrer que $SL_2(\mathbb{Z}) \subset G$, or l'autre inclusion est banale, $SL_2(\mathbb{Z})$ étant un groupe contenant A et B, donc A^{-1} et B^{-1} et donc tous les produits finis d'éléments de $\mathcal{E}$ par stabilité !

$$\boxed{SL_2(\mathbb{Z}) = G.}$$

7) J'applique l'algorithme du **5)**... Ici $M = \begin{pmatrix} 5 & 4 \\ 11 & 9 \end{pmatrix}$, d'où

- $k_0 = -1$ et $M_1 = MB^{-1}A = \begin{pmatrix} -1 & -5 \\ -2 & -11 \end{pmatrix}$
- $k_1 = -5$ et $M_2 = M_1 B^{-5} A = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$

Alors d'après les calculs du **2)** $M_2 B^2 A = I$ d'où

$$MB^{-1}AB^{-5}AB^2A = I$$

et finalement

$$\boxed{M = A^{-1}B^{-2}A^{-1}B^5A^{-1}B.}$$