

Corrigé colle S19
MPI/MPI* du lycée Faidherbe
Exercices 15, 20 et 21

Léane Parent

2 février 2026

Exercice 15

Soit p un nombre premier. On pose $q = (p^2 - p)(p^2 - 1)$. Soit $A \in M_2(\mathbb{Z}/p\mathbb{Z})$.

1) Donner le cardinal de $GL_2(\mathbb{Z}/p\mathbb{Z})$.

Une matrice est inversible ssi la famille de ses coefficients est libre.

On a donc $p^2 - 1$ choix pour la première colonne (les vecteurs non nuls), et $p^2 - p$ choix pour la seconde (les vecteurs non colinéaires au premier)

Soit, par principe multiplicatif : $\#GL_2(\mathbb{Z}/p\mathbb{Z}) = (p^2 - p)(p^2 - 1) = q$.

2) Montrer que $A^{q+2} = A^2$

D'après la question précédente, $GL_2(\mathbb{Z}/p\mathbb{Z})$ est un groupe d'ordre q . Ainsi, $o(A) \mid q$.

On a donc $A^{q+2} = A^q A^2 = A^2$.

3) Quel est le cardinal de $GL_n(\mathbb{Z}/p\mathbb{Z})$, pour $n \geq 1$?

On montre de même qu'en question (1) que :

$$\#GL_n(\mathbb{Z}/p\mathbb{Z}) = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$$

4) Quel est le cardinal de $SL_n(\mathbb{Z}/p\mathbb{Z})$?

$$GL_n(\mathbb{Z}/p\mathbb{Z}) = \bigcup_{i=0}^{p-1} \{M \mid \det M = i\}$$

Or, si M et M' ont même déterminant, $M^{-1}M' \in SL_n(\mathbb{Z}/p\mathbb{Z})$. On a donc, pour A de déterminant i :

$$A \cdot SL_n(\mathbb{Z}/p\mathbb{Z}) = \{M \mid \det M = i\}$$

On en déduit $\#GL_n(\mathbb{Z}/p\mathbb{Z}) = p \#SL_n(\mathbb{Z}/p\mathbb{Z})$, d'où :

$$\begin{aligned}\#SL_n(\mathbb{Z}/p\mathbb{Z}) &= \frac{1}{p}(p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) \\ &= (p^n - 1)(p^n - p) \dots (p^n - p^{n-2})(p^{n-1} - p^{n-2})\end{aligned}$$

Exercice 20

On définit $SL_2(\mathbb{Z})$ l'ensemble des matrices de taille 2×2 à coefficients entiers de déterminant 1. On définit également $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

1) Montrer que $SL_2(\mathbb{Z})$ est un groupe.

Montrons qu'il s'agit d'un sous-groupe de $GL_2(\mathbb{R})$. La stabilité par produit est immédiate.

De plus, si $M \in SL_2(\mathbb{Z})$, M est inversible, et $M^{-1} = \frac{1}{\det M} \text{Com } M = \text{Com } M \in SL_2(\mathbb{Z})$. (Où $\text{Com } M$ désigne la comatrice de M .)

Il s'agit bien d'un sous-groupe, donc d'un groupe.

2) Montrer que S et T engendrent $SL_2(\mathbb{Z})$.

D'une part, S et T appartiennent bien à $SL_2(\mathbb{Z})$

On vérifie par le calcul que, pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $k \in \mathbb{Z}$:

$$SM = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \quad \text{et} \quad T^k M = \begin{pmatrix} a + kc & b + kd \\ c & d \end{pmatrix}$$

On a alors, si $a = cq + r$ est la division euclidienne de a par c :

$$ST^{-q}M = \begin{pmatrix} -c & * \\ r & * \end{pmatrix}$$

On applique alors récursivement ce processus pour obtenir M' de la forme $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$ (algorithme d'Euclide).

Or, par produit, $M' \in SL_2(\mathbb{Z})$. Ainsi, elle est de déterminant 1 : on a $\alpha = \gamma = \pm 1$. Quitte à multiplier à gauche par $S^2 = -I_2$, on suppose $\alpha = \gamma = 1$.

Mézalor $M' = T^\beta$: en inversant les étapes de l'algorithme, on obtient une décomposition de M selon S et T .

On a bien $SL_2(\mathbb{Z}) = \langle S, T \rangle$.

3) Question posée pendant le temps restant : On admet que $A = \begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix}$ est dans $SL_2(\mathbb{Z})$. Déterminer sa décomposition avec les matrices S et T .

Peut-être que le candidat avait du temps restant, mais moi j'en ai pas avant d'aller me coucher.

Appliquez la démonstration de la question précédente.

Exercice 21

Montrer qu'un sous-groupe discret de \mathbb{R}^n admet une \mathbb{Z} -base.

Petit point vocabulaire :

- Un ensemble discret E , c'est un ensemble dont tous les points sont isolés, c'est-à-dire que pour tout $x \in E$, il existe ε tq $B_o(x, \varepsilon) \cap E = \{x\}$ (ie il n'existe pas de point arbitrairement proche de x). (La vraie définition est que toute intersection de E et d'un compact est finie, mais celle-ci est équivalente.)
- Parler de \mathbb{Z} -base, c'est considérer G comme un \mathbb{Z} -module : c'est comme un ev, sauf que les scalaires sont dans un anneau (ici \mathbb{Z}) et pas forcément dans un corps.
- Par souci de concision, on notera $\text{Vect } A = \text{Vect}_{\mathbb{R}} A$ le \mathbb{R} -espace engendré par A , et $\text{Vect}_{\mathbb{Z}} A$ le \mathbb{Z} -module engendré par A .

On note $G \leq \mathbb{R}^n$ discret.

Construisons notre base.

- On note $B_0 = \emptyset$
- Si $x \in G \setminus \text{Vect } B_i$ existe, ie si $G \not\subset \text{Vect } B_i$, $\text{Vect } x \cap G$ est discret, donc il existe $x' \in \text{Vect } x \cap G$ non nul de distance minimale (c'est à rédiger, je vous laisse le faire) à $\text{Vect } B_i$. On note $B_{i+1} = B_i \cup x'$.

Ce processus finit (car $\text{Vect } B_i$ est de dimension i dans un espace de dimension n) et donne donc une \mathbb{R} -base de $\text{Vect } G$. On note $B = (x_1, \dots, x_k)$ sa valeur finale.

Montrons que B est une \mathbb{Z} -base de G . Soit $x \in G$, $x = \lambda x_i + x'$, avec $x' \in \text{Vect } B_{k-1}$.

Si λ' est la partie fractionnaire de λ , et $x_k = p + h$ la décomposition de x_k selon $\text{Vect } B_i$ et son orthogonal, on a alors :

- $\|h\|$ est la distance de x_k à $\text{Vect } B_i$.
- $\lambda' x_k + x' \in G$ (car $x_i \in G$, d'où le résultat en soustrayant $x_i \lfloor \lambda \rfloor$ fois), de distance à $\text{Vect } B_i$ égale à $\lambda' \|h\|$

Or, $\lambda' \|h\| < \|h\|$, donc $\lambda' x_k + x' \in G$ est dans G de distance inférieure à la distance minimale : Ainsi, $\lambda' x_k + x' \notin G \setminus \text{Vect } B_i$, donc dans B_i : $\lambda' = 0$, soit $\lambda \in \mathbb{Z}$.

On applique ensuite récursivement à x' , en considérant $G \cap \text{Vect } B_i$ qui est bien un groupe : tous les coefficients sont entiers, donc B est une \mathbb{Z} -base de G .