Notations.

· *Dans tout le problème, n désignera un entier naturel non nul et* $\mathbf{L}$ *désignera le corps des nombres réels* $\mathbf{R}$ *ou le corps des nombres complexes* $\mathbf{C}$.

· *Si p désigne un entier naturel non nul et* $\mathbf{L}$ *un corps, on note* $\mathcal{M}_p(\mathbf{L})$ *l'ensemble des matrices carrées de taille* $p \times p$ *à coefficients dans* $\mathbf{L}$ *; on notera* $\mathrm{Tr}\,(M)$ *la trace d'une matrice carrée M.*

· *On appelle I_p la matrice identité de* $\mathcal{M}_p(\mathbf{L})$, *qui est la matrice diagonale constituée uniquement de* 1 *sur la diagonale.*

· *L'ensemble des matrices inversibles de* $\mathcal{M}_p(\mathbf{L})$ *est noté* $GL_p(\mathbf{L})$ *et l'ensemble des matrices de* $GL_p(\mathbf{L})$ *de déterminant* 1 *est noté* $SL_p(\mathbf{L})$.

· *Soit* $\mathbf{A}$ *un sous-anneau de* $\mathbf{L}$. *On note* $\mathcal{M}_p(\mathbf{A})$ *(respectivement* $GL_p(\mathbf{A})$ *et* $SL_p(\mathbf{A})$*) l'ensemble des matrices de* $\mathcal{M}_p(\mathbf{L})$ *(respectivement de* $GL_p(\mathbf{L})$ *et* $SL_p(\mathbf{L})$*) à coefficients dans* $\mathbf{A}$.

· *Soit* $M \in \mathcal{M}_p(\mathbf{L})$, *on note* χ_M *le polynôme caractéristique de M défini par* $\chi_M(X) = \det(X I_p - M)$.

· *Soit* $\delta \in \mathbf{C} \setminus \mathbf{Q}$ *tel que* $D = \delta^2 \in \mathbf{Q}$. *Dans tout le problème, on posera* $\mathbf{K} = \mathbf{Q}[\delta] = \left\{a + b\delta \mid a, b \in \mathbf{Q}\right\}$.

· *Pour tout a, b de* $\mathbf{Q}$, *on pose* $\overline{a + \delta b} = a - \delta b$.

· *Pour* $x \in \mathbf{K}$, *on pose* $N(x) = x\overline{x}$.

· *Pour* $M = [a_{i,j}]_{1 \leqslant i,j \leqslant p}$ *une matrice de* $\mathcal{M}_p(\mathbf{K})$, *on définit la matrice* $\overline{M} = [\overline{a_{i,j}}]_{1 \leqslant i,j \leqslant p}$.

· *On note* $\mathcal{S}_p(\mathbf{R})$ *l'ensemble des matrices carrées symétriques réelles de taille* $p \times p$ *et* $\mathcal{S}_p^+(\mathbf{R})$ *l'ensemble des matrices carrées symétriques réelles de taille* $p \times p$ *ayant des valeurs propres positives ou nulles.*

· *Soit E un espace euclidien muni d'un produit scalaire* $\langle \cdot, \cdot \rangle$. *Un endomorphisme u de E est dit symétrique si :* $\forall x, y \in E,\ \langle u(x), y \rangle = \langle x, u(y) \rangle$.

· *Pour* $m, n \in \mathbf{Z}$, *tel que* $m \leqslant n$, *on note* $[\![m, n]\!]$ *l'intervalle d'entiers relatifs constitué des éléments de l'ensemble* $\{m, m+1, ..., n-1, n\}$.

Objectifs du problème.

Après un questionnaire "vrai ou faux" et un exercice préliminaire, les parties du problème portent sur la recherche de solutions non nulles de l'équation matricielle $X^n + Y^n = Z^n$, avec n un entier strictement positif.

· La partie **I** traite de la résolution du problème dans $\mathcal{S}_p^+(\mathbf{R})$.

· Les parties **II** à **VII** visent à discuter de l'existence de solutions dans $SL_2(\mathbf{Z})$, suivant les valeurs de n.

· Dans les parties **VIII** et **IX**, à partir d'une solution (X, Y, Z) dans $(SL_2(\mathbf{Q}))^3$, nous montrons comment construire une solution (X_1, Y_1, Z_1) dans $(SL_2(\mathbf{Q}))^3$ telle que (X_1^n, Y_1^n, Z_1^n) soit dans $(SL_2(\mathbf{Z}))^3$.

Les parties **I**, **II**, **III** et **VIII** peuvent se traiter indépendamment des autres, tout comme la partie **VII** en dehors de la dernière question.

Vrai ou faux ?

1. Les affirmations suivantes sont-elles vraies ou fausses ? On justifiera soigneusement les réponses.

(a) Soit n un entier strictement positif.
Affirmation : "Il existe des matrices M et N de $\mathcal{M}_n(\mathbf{C})$ telles que $\mathrm{Tr}\,(MN) \neq \mathrm{Tr}\,(NM)$."

(b) Affirmation : "Deux matrices de $\mathcal{M}_2(\mathbf{C})$ ont le même polynôme caractéristique si et seulement si elles ont la même trace et le même déterminant."

(c) Affirmation : "Les matrices carrées et symétriques à coefficients dans $\mathbf{C}$ sont diagonalisables."

(d) Soit $\varphi : A \to B$ un morphisme d'anneaux.
Affirmation : "Si $\varphi(a)$ est inversible dans B, alors a est inversible dans A."

Exercice préliminaire.

2. Soit d un entier strictement positif. Soit $P(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0$ un polynôme de $\mathbf{C}[X]$ à coefficients complexes. On appelle *matrice compagnon* du polynôme P la matrice C_P de $\mathcal{M}_d(\mathbf{C})$ suivante

$$C_P = \begin{pmatrix} 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & 0 & & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-2} \\ 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix}$$

En développant le déterminant $\chi_{C_P}(X) = \det(X\,I_d - C_P)$ par rapport à sa première ligne et à l'aide d'une récurrence, montrer que $\chi_{C_P}(X) = P(X)$.

3. Soit p un entier strictement positif et soit M une matrice de $\mathcal{M}_p(\mathbf{C})$.

(a) Étant donné un élément x quelconque non nul de $\mathbf{C}^p$ on pose

$$\mu = \min\left\{ r \geqslant 1 \mid \text{la famille } \{x, M\,x, \ldots, M^r\,x\} \text{ est liée dans } \mathbf{C}^p \right\}.$$

i) Montrer qu'il existe un élément $(\alpha_0, \ldots, \alpha_{\mu-1})$ de $\mathbf{C}^\mu$ et une matrice N de $\mathcal{M}_{p-\mu}(\mathbf{C})$ tels que la matrice M soit semblable à une matrice M' de la forme suivante

$$M' = \begin{pmatrix} 0 & \ldots & \ldots & 0 & -\alpha_0 & * \\ 1 & 0 & & \vdots & -\alpha_1 & * \\ 0 & 1 & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -\alpha_{\mu-2} & * \\ 0 & \ldots & 0 & 1 & -\alpha_{\mu-1} & * \\ O & & \ldots & & O & N \end{pmatrix}$$

où les $*$ représentent des lignes d'éléments de $\mathbf{C}$ et les O représentent des colonnes nulles.

ii) Montrer que $\chi_M(M)\,x = 0$.

(b) Montrer que χ_M est un polynôme annulateur de M.

Problème.

I. Exemple dans $\mathcal{S}_p^+(\mathbf{R})$.

Soient n et p deux entiers strictement positifs.

4. Soit A une matrice de $\mathcal{S}_p(\mathbf{R})$ et soit a l'endomorphisme de $\mathbf{R}^p$ dont la matrice relativement à la base canonique de $\mathbf{R}^p$ est A. Montrer que a est un endomorphisme symétrique de $\mathbf{R}^p$.

5. Soit $S \in \mathcal{S}_p(\mathbf{R})$. Démontrer que S est une matrice de $\mathcal{S}_p^+(\mathbf{R})$ si et seulement si

$$\forall Y \in \mathcal{M}_{p,1}(\mathbf{R}),\ {}^tYSY \geqslant 0.$$

6. Démontrer que pour toutes les matrices S et T de $\mathcal{S}_p^+(\mathbf{R})$, la matrice $S+T$ appartient à $\mathcal{S}_p^+(\mathbf{R})$.

7. Soit $S \in \mathcal{S}_p^+(\mathbf{R})$. Montrer qu'il existe une matrice R de $\mathcal{S}_p^+(\mathbf{R})$ telle que $R^n = S$.

8. Soient $S \in \mathcal{S}_p^+(\mathbf{R})$ et $U \in \mathcal{S}_p^+(\mathbf{R})$ telles que $U^n = S$. On note s et u les endomorphismes de $\mathbf{R}^p$ dont les matrices relativement à la base canonique de $\mathbf{R}^p$ sont respectivement S et U. Soit $\{\lambda_1, ..., \lambda_q\}$ le spectre de s ; pour i élément de $[\![1,q]\!]$, on note $E_{\lambda_i}(s)$ le sous-espace propre associé à la valeur propre λ_i.

   (a) Soit $i \in [\![1,q]\!]$. Démontrer que u induit un endomorphisme symétrique sur $E_{\lambda_i}(s)$. On notera cet endomorphisme u_i.

   (b) Soit $i \in [\![1,q]\!]$. Démontrer que $\sqrt[n]{\lambda_i}$ est la seule valeur propre possible de u_i.

   (c) Démontrer que l'endomorphisme u est unique.

9. Soit $S \in \mathcal{S}_p^+(\mathbf{R})$. Montrer qu'il existe une unique matrice R de $\mathcal{S}_p^+(\mathbf{R})$ telle que $R^n = S$.

   Étant donnée une matrice S de $\mathcal{S}_p^+(\mathbf{R})$, on notera $R = \sqrt[n]{S}$, l'unique matrice de $\mathcal{S}_p^+(\mathbf{R})$ telle que $R^n = S$.

10. Démontrer que l'application

$$\psi : \begin{cases} (\mathcal{S}_p^+(\mathbf{R}))^2 & \to \quad \left\{(X,Y,Z) \in (\mathcal{S}_p^+(\mathbf{R}))^3 \;\middle|\; X^n + Y^n = Z^n\right\} \\ (U,V) & \mapsto \quad \left(\sqrt[n]{U}, \sqrt[n]{V}, \sqrt[n]{U+V}\right) \end{cases}$$

   est une bijection.

II. Si $n \equiv 0[4]$, l'équation $X^n + Y^n = Z^n$ n'admet pas de solutions dans $SL_2(\mathbf{Z})$.

11. Soit $M \in SL_2(\mathbf{Z})$. Démontrer que $\mathrm{Tr}\,(M^4) = \mathrm{Tr}\,(M)^4 - 4\,\mathrm{Tr}\,(M)^2 + 2$.

12. En déduire que l'on a $\mathrm{Tr}\,(M^4) \equiv 2[8]$ ou $\mathrm{Tr}\,(M^4) \equiv -1[8]$.

13. Démontrer que l'équation $X^4 + Y^4 = Z^4$ d'inconnues X, Y et Z n'admet pas de solutions dans $SL_2(\mathbf{Z})$.

14. En déduire que si 4 divise n, alors l'équation $X^n + Y^n = Z^n$ d'inconnues X, Y et Z n'admet pas de solutions dans $SL_2(\mathbf{Z})$.

III. Le corps $\mathbf{K} = \mathbf{Q}[\delta]$.

On pose

$$\varphi : \begin{cases} \mathbf{K} & \to & \mathbf{K} \\ x & \mapsto & \overline{x} \end{cases}$$

15. Démontrer que $\mathbf{K}$ est un $\mathbf{Q}$-espace vectoriel dont on précisera la dimension.

16. Démontrer que $\mathbf{K}$ est un sous-corps de $\mathbf{C}$.

17. Démontrer que φ est un isomorphisme de corps.

18. **(a)** Démontrer que l'application $\psi : \begin{cases} \mathbf{Q} & \to & \mathbf{C} \\ x & \mapsto & \dfrac{x+\delta}{x-\delta} \end{cases}$ est injective.

    (b) Démontrer que $\left\{\dfrac{\theta}{\overline{\theta}},\ \theta \in \mathbf{K} \setminus \{0\}\right\}$ est un ensemble infini.

Tournez la page S.V.P.

IV. Matrices de $\mathcal{M}_p(\mathbf{K})$ conjuguées à une matrice de $\mathcal{M}_p(\mathbf{Q})$.

Soit p un entier strictement positif.

19. Démontrer que si A et B sont des matrices quelconques de $\mathcal{M}_p(\mathbf{K})$, alors on a la relation $\overline{AB} = \overline{A}\,\overline{B}$.

20. Soit $F \in \mathcal{M}_p(\mathbf{K})$. Démontrer que F appartient à $GL_p(\mathbf{K})$ si et seulement si $\overline{F}$ appartient à $GL_p(\mathbf{K})$. Dans ce cas, démontrer que l'on a $\left(\overline{F}\right)^{-1} = \overline{F^{-1}}$.

21. Soit $X \in GL_p(\mathbf{K})$.

(a) On suppose qu'il existe une matrice F de $GL_p(\mathbf{K})$ tel que $X = F\left(\overline{F}\right)^{-1}$. Déterminer la matrice $X\overline{X}$.

(b) On suppose que $X\overline{X} = I_p$.
Pour tout élément θ de $\mathbf{K}$, on pose $F(\theta) = \theta I_p + \overline{\theta}X$.

i) Montrer qu'il existe un élément θ_0 de $\mathbf{K}$ tel que $F(\theta_0)$ soit inversible.

ii) En déduire, pour ce θ_0, que $X = F(\theta_0)\left(\overline{F(\theta_0)}\right)^{-1}$.

(c) Soient $A, B \in \mathcal{M}_p(\mathbf{K})$. Démontrer que les deux propositions suivantes sont équivalentes :

i) Il existe une matrice F de $GL_p(\mathbf{K})$ telle que les matrices $F^{-1}AF$ et $F^{-1}BF$ appartiennent à $\mathcal{M}_p(\mathbf{Q})$.

ii) Il existe une matrice X de $GL_p(\mathbf{K})$ tel que : $\left\{\begin{array}{c} X^{-1}AX = \overline{A} \\ X^{-1}BX = \overline{B} \\ X\overline{X} = I_p \end{array}\right.$

22. Soient $A = \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}$ et $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ deux matrices à coefficients dans $\mathbf{K}$. On suppose que λ n'est pas élément de $\mathbf{Q}$.

(a) Soit $X \in GL_2(\mathbf{K})$. Démontrer que X vérifie les relations $\left\{\begin{array}{c} X^{-1}AX = \overline{A} \\ X\overline{X} = I_2 \end{array}\right.$ si et seulement s'il existe un élément u de $\mathbf{K} \setminus \{0\}$ tel que $X = \begin{pmatrix} 0 & u \\ \frac{1}{\overline{u}} & 0 \end{pmatrix}$.

(b) On suppose qu'il existe une matrice F de $GL_2(\mathbf{K})$ telle que les matrices $F^{-1}AF$ et $F^{-1}BF$ appartiennent à $SL_2(\mathbf{Q})$.
Montrer que l'on a $\det(A) = \det(B) = 1$ et $d = \overline{a}$ et en déduire qu'il existe un élément x de $\mathbf{K}$ tel que l'on a $N(a) - 1 = N(x)$ (c'est-à-dire $a\overline{a} - 1 = x\overline{x}$).

V. Conditions pour qu'une somme de matrices de $SL_2(\mathbf{Q})$ soit dans $SL_2(\mathbf{Q})$.

Soient α un élément de $\mathbf{Q}$ et δ un élément de $\mathbf{C} \setminus \mathbf{Q}$ tels que $\alpha^2 - 1 = \delta^2$.

23. Soient $A_1 = \begin{pmatrix} \alpha + \delta & 0 \\ 0 & \alpha - \delta \end{pmatrix}$ et $B_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ deux matrice de $\mathcal{M}_2(\mathbf{K})$, posons $m_1 = \dfrac{\mathrm{Tr}\,(B_1)}{2}$.
On suppose que $\det(B_1) = \det(A_1 + B_1) = 1$. Démontrer l'égalité $a - d = \dfrac{2\alpha m_1 + 1}{\delta}$.

24. On suppose qu'il existe deux matrices A et B de $SL_2(\mathbf{Q})$ telles que $\mathrm{Tr}\,(A) = 2\alpha$ et $\det(A + B) = 1$.
Posons $m = \dfrac{\mathrm{Tr}\,(B)}{2}$.

(a) Démontrer que dans $\mathcal{M}_2(\mathbf{K})$, la matrice A est semblable à la matrice $A_1 = \begin{pmatrix} \alpha+\delta & 0 \\ 0 & \alpha-\delta \end{pmatrix}$.

(b) En utilisant la question **23.** et la question **22b.**, montrer qu'il existe un élément x de $\mathbf{K}$ tel que l'on ait

$$\frac{\left(\alpha m + \frac{1}{2}\right)^2 - (\alpha^2-1)(m^2-1)}{1-\alpha^2} = N(x) = x\overline{x}.$$

(c) Démontrer que le résultat de la question précédente est équivalent à l'existence d'un élément y de $\mathbf{K}$ tel que

$$\left(\alpha m + \frac{1}{2}\right)^2 - (\alpha^2-1)(m^2-1) = N(y) = y\overline{y}.$$

Dans la suite du problème, on admettra que ce résultat reste valable si δ appartient à $\mathbf{Q}$. C'est-à-dire qu'étant donné un élément α de $\mathbf{Q}$ et des matrices A et B de $SL_2(\mathbf{Q})$ qui vérifient $\mathrm{Tr}\,(A) = 2\alpha$ *et* $\det(A+B) = 1$, *alors si* $m = \frac{\mathrm{Tr}\,(B)}{2}$ *il existe deux éléments u et v de $\mathbf{Q}$ tels que*

$$\left(\alpha m + \frac{1}{2}\right)^2 - (\alpha^2-1)(m^2-1) = u^2 - (\alpha^2-1)v^2.$$

VI. Si $n \equiv 0[3]$, l'équation $X^n + Y^n = Z^n$ n'admet pas de solutions dans $SL_2(\mathbf{Z})$.

25. (a) Soit $x \in \mathbf{Z}$. Déterminer les classes de congruence de $x^3 - 3x$ modulo 9. Pour chaque classe, on explicitera un représentant.

(b) Soit M une matrice de $SL_2(\mathbf{Z})$, démontrer que l'on a $\mathrm{Tr}\,(M^3) = (\mathrm{Tr}\,(M))^3 - 3\,\mathrm{Tr}\,(M)$.

(c) Soient A, B et C trois matrices de $SL_2(\mathbf{Z})$ qui vérifient la relation $A^3 + B^3 = C^3$.
On suppose que parmi les nombres $\mathrm{Tr}\,(A^3), \mathrm{Tr}\,(B^3)$ et $\mathrm{Tr}\,(C^3)$, au moins l'un d'entre eux n'est pas divisible par 9.

i) Montrer qu'il existe trois matrices A_1, B_1 et C_1 de $SL_2(\mathbf{Z})$ telles que $A_1^3 + B_1^3 = C_1^3$, $\mathrm{Tr}\,(A_1^3) \equiv 0[9]$, $\mathrm{Tr}\,(B_1^3) \equiv 2[9]$ et $\mathrm{Tr}\,(C_1^3) \equiv 2[9]$.

Étant donnée une matrice $M = [a_{i,j}]_{1\leqslant 2, j\leqslant 2}$ de $\mathcal{M}_2(\mathbf{Z})$, on note $\dot{M} = [\dot{a}_{i,j}]_{1\leqslant 2, j\leqslant 2}$ la matrice de $\mathcal{M}_2(\mathbf{Z}/3\mathbf{Z})$ où $\dot{a}_{i,j}$ est la classe de $a_{i,j}$ dans $\mathbf{Z}/3\mathbf{Z}$.

ii) Dans $\mathbf{Z}/3\mathbf{Z}[X]$, démontrer que les polynômes caractéristiques de $\dot{B}_1$ et de $\dot{C}_1$ sont égaux à $(X-1)^2$.

iii) Dans $\mathcal{M}_2(\mathbf{Z}/3\mathbf{Z})$, démontrer que chacune des matrices $\dot{B}_1$ et $\dot{C}_1$ est semblable à une matrice de la forme $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, avec k un élément de $\mathbf{Z}/3\mathbf{Z}$.

iv) Montrer que $(\dot{A}_1)^3$ est égale à $\dot{0}$ la matrice nulle de $\mathcal{M}_2(\mathbf{Z}/3\mathbf{Z})$, en déduire une contradiction.

Nous venons de démontrer que si trois matrices A, B et C de $SL_2(\mathbf{Z})$ vérifient $A^3 + B^3 = C^3$, alors on a $\mathrm{Tr}\,(A^3) \equiv 0[9]$, $\mathrm{Tr}\,(B^3) \equiv 0[9]$ *et* $\mathrm{Tr}\,(C^3) \equiv 0[9]$.

26. Soient α et m deux éléments de $\mathbf{Q}$ tels que 2α et $2m$ appartiennent à $\mathbf{Z}$ et qui vérifient les relations $2\alpha \equiv 0[9]$ et $2m \equiv 0[9]$.
On suppose qu'il existe deux éléments x et y de $\mathbf{Q}$ tels que

$$\left(\alpha m + \frac{1}{2}\right)^2 - (\alpha^2 - 1)(m^2 - 1) = x^2 - (\alpha^2 - 1)y^2 \quad (*).$$

On note alors d le plus petit entier naturel non nul tel que $x = \frac{r}{d}$ et $y = \frac{s}{d}$, avec r et s des éléments de $\mathbf{Z}$; on admet alors que

$$d^2\left[(4\alpha m + 2)^2 - \left((2\alpha)^2 - 4\right)\left((2m)^2 - 4\right)\right] = (4xd)^2 - \left((2\alpha)^2 - 4\right)(2yd)^2 \quad (**).$$

(a) Démontrer que l'on a

$$\left[(4\alpha m + 2)^2 - \left((2\alpha)^2 - 4\right)\left((2m)^2 - 4\right)\right] \equiv 6[9]$$

et

$$(4xd)^2 + (2yd)^2 \equiv 0[3].$$

(b) Montrer que l'on a $4xd \equiv 0[3]$ et $2yd \equiv 0[3]$.

(c) À l'aide de l'égalité $(**)$ montrer que 3 divise d.

(d) En déduire une contradiction sur la définition de d.

27. Soient α et m deux éléments de $\mathbf{Q}$ tels que 2α et $2m$ appartiennent à $\mathbf{Z}$ et qui vérifient les relations $2\alpha \equiv 0[9]$ et $2m \equiv 0[9]$.
Montrer qu'il n'existe pas de matrices U et V de $SL_2(\mathbf{Z})$ vérifiant

$$\mathrm{Tr}\,(U) = 2\alpha, \mathrm{Tr}\,(V) = 2m \text{ et } \det(U + V) = 1.$$

28. Montrer si 3 divise n, alors l'équation $X^n + Y^n = Z^n$ d'inconnues X, Y et Z n'admet pas de solutions dans $SL_2(\mathbf{Z})$.

VII. Recherche de solutions de $X^n + Y^n = Z^n$ dans $SL_2(\mathbf{Z})$ si n n'est pas divisible par 3 ou 4.

Soit $k \in \mathbf{N}^*$ et soit $p \in \mathbf{N}^*$. On dit qu'une matrice M de $\mathcal{M}_p(\mathbf{R})$ est k-périodique si $M^k = I_p$.
Soient $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ et $C = -I_2$ trois matrices de $SL_2(\mathbf{Z})$ qui vérifient la relation $A + B = C$.

29. Montrer qu'une matrice k-périodique est diagonalisable dans $\mathcal{M}_p(\mathbf{C})$.

30. (a) Déterminer toutes les matrices X de $SL_2(\mathbf{Z})$ qui vérifient $\mathrm{Tr}\,(X) = -1$ et $X^2 = A$.
Montrer que ces matrices sont 12-périodiques,

(b) Déterminer une matrice Y de $SL_2(\mathbf{Z})$ qui est 12-périodique et qui vérifie la relation $Y^2 = B$.

(c) En déduire au moins un triplet (X, Y, Z) de matrices de $(SL_2(\mathbf{Z}))^3$, constitué de matrices 12-périodiques, tel que $X^2 + Y^2 = Z^2$.

31. Soit $n \equiv 2[12]$, montrer qu'il existe au moins un triplet (X, Y, Z) de matrices de $(SL_2(\mathbf{Z}))^3$ tel que $X^n + Y^n = Z^n$.

32. En déduire, lorsque $n \equiv -2[12]$, qu'il existe au moins un triplet (X, Y, Z) de matrices de $(SL_2(\mathbf{Z}))^3$ tel que $X^n + Y^n = Z^n$.

33. Lorsque $n \equiv 1[6]$ ou $n \equiv 5[6]$, à l'aide des matrices A et B déterminer des matrices X, Y et Z de $SL_2(\mathbf{Z})$ qui vérifient la relation $X^n + Y^n = Z^n$.

34. Suivant les valeurs de l'entier strictement positif n, discuter l'existence de matrices X, Y et Z de $SL_2(\mathbf{Z})$ qui vérifient la relation $X^n + Y^n = Z^n$.

VIII. Réseaux de $\mathbf{Q}^n$.

Dans cette partie, n et m désignent deux entiers naturels non nuls. Soient $v_1, ..., v_m$ des éléments non nuls de $\mathbf{Q}^n$, posons

$$\mathcal{R} = \mathbf{Z}v_1 + ... + \mathbf{Z}v_m = \left\{ \sum_{i=1}^{m} k_i v_i \mid k_1, ..., k_m \in \mathbf{Z} \right\}.$$

Si $n \geqslant 2$, on note

$$\mathbf{Q}^{n-1} \times \{0\} = \left\{ (x_1, ..., x_{n-1}, 0) \mid x_1, ..., x_{n-1} \in \mathbf{Q} \right\}.$$

35. Démontrer que $\mathcal{R}$ est un sous-groupe additif de $(\mathbf{Q}^n, +)$.

36. Si $n = 1$, montrer qu'il existe un élément r de $\mathbf{Q}$ tel que

$$\mathcal{R} = r\mathbf{Z} = \left\{ rk \mid k \in \mathbf{Z} \right\}.$$

Ce r est-il unique ?

37. On suppose $n \geqslant 2$, posons $\pi : \left\{ \begin{array}{ccc} \mathbf{Q}^n & \to & \mathbf{Q} \\ (x_1, ..., x_n) & \mapsto & x_n \end{array} \right.$. Montrer qu'il existe un élément w de $\mathcal{R}$ tel que

$$\pi(\mathcal{R}) = \pi(w)\mathbf{Z} = \{\pi(w)k \mid k \in \mathbf{Z}\}.$$

Dans la suite de cette partie, si $\pi(\mathcal{R}) = \{0\}$, on prendra $w = (0, ..., 0)$.

38. Soit x un élément de $\mathcal{R}$ et w un élément de $\mathcal{R}$ défini comme dans la question précédente.

(a) Montrer qu'il existe un couple $(q, \widetilde{x})$ de $\mathbf{Z} \times \left(\mathcal{R} \cap (\mathbf{Q}^{n-1} \times \{0\})\right)$ tel que $x = qw + \widetilde{x}$.

(b) Démontrer que $\widetilde{x}$ est unique. L'entier q est-il toujours unique ?

39. Démontrer que l'on a

$$\mathcal{R} \cap (\mathbf{Q}^{n-1} \times \{0\}) = \mathbf{Z}\widetilde{v_1} + ... + \mathbf{Z}\widetilde{v_m} = \left\{ \sum_{i=1}^{m} k_i \widetilde{v_i} \mid k_1, ..., k_m \in \mathbf{Z} \right\}$$

où les éléments $\widetilde{v_1}, ..., \widetilde{v_m}$ de $\mathcal{R}$ sont définis comme dans la question précédente.

40. Montrer par récurrence sur la dimension de $\mathbf{Q}^n$, qu'il existe des éléments $u_1, ..., u_p$ de $\mathcal{R}$ tels que pour tout x de $\mathcal{R}$ il existe un unique p-uplet $(k_1, ..., k_p)$ de $\mathbf{Z}^p$ vérifiant $x = \sum_{i=1}^{p} k_i u_i$.

Une telle famille $(u_1, ..., u_p)$ de $\mathcal{R}$ est appelée $\mathbf{Z}$-base *de $\mathcal{R}$, on notera alors $\mathcal{R} = \bigoplus_{i=1}^{p} \mathbf{Z}u_i$.*

41. Supposons que $vect_{\mathbf{Q}}(v_1, ..., v_m) = \mathbf{Q}^n$. Si $(u_1, ..., u_p)$ est une $\mathbf{Z}$-base de $\mathcal{R}$ démontrer que $(u_1, ..., u_p)$ est une base de $\mathbf{Q}^n$ et que $p = n$.

IX. Condition pour que certains sous-groupes de $SL_2(\mathbf{Q})$ soient semblables à un sous-groupe de $SL_2(\mathbf{Z})$.

Soit p un entier strictement positif. Dans cette partie, on identifie $\mathcal{M}_{p,1}(\mathbf{Q})$ et $\mathbf{Q}^p$. On note $(e_1, \dots, e_p)$ la base canonique de $\mathbf{Q}^p$ et on admet que $(SL_p(\mathbf{Q}), .)$ est un groupe.

42. Soit G un sous-groupe multiplicatif de $(SL_p(\mathbf{Q}), .)$ tel qu'il existe un entier strictement positif d vérifiant

$$\forall M \in G,\ dM \in \mathcal{M}_p(\mathbf{Z}).$$

Soit H le sous-groupe additif de $(\mathbf{Q}^p, +)$ engendré par les éléments Me_i, avec M une matrice de G et i un élément de $[\![1, p]\!]$; c'est le plus petit sous-groupe de $(\mathbf{Q}^p, +)$ contenant l'ensemble $\left\{Me_i \mid M \in G,\ i \in [\![1, p]\!]\right\}$ et il peut s'écrire sous la forme suivante

$$H = \left\{y_1 + y_2 + \dots + y_q \mid q \in \mathbf{N}^*,\ y_1, y_2, \dots, y_q \in \mathcal{M}\right\}$$

où

$$\mathcal{M} = \left\{Me_i \mid M \in G,\ i \in [\![1, p]\!]\right\} \cup \left\{-Me_i \mid M \in G,\ i \in [\![1, p]\!]\right\} \cup \{0\}.$$

(a) Démontrer que les vecteurs $e_1, \dots, e_p$ appartiennent à H.

(b) Démontrer que H est stable par G, c'est-à-dire que l'on a

$$\forall M \in G, \forall h \in H,\ Mh \in H.$$

(c) Soient $M \in G$ et $j \in [\![1, p]\!]$. Montrer qu'il existe des éléments $r_1, \dots, r_p$ de $[\![0, d-1]\!]$ et des éléments $q_1, \dots, q_p$ de $\mathbf{Z}$ tels que

$$Me_j = \sum_{i=1}^{p} q_i e_i + \frac{1}{d} \sum_{i=1}^{p} r_i e_i.$$

(d) Montrer qu'il existe une famille génératrice $(v_1, \dots, v_m)$ de $\mathbf{Q}^p$ telle que

$$H = \mathbf{Z}v_1 + \dots + \mathbf{Z}v_m = \left\{\sum_{i=1}^{m} k_i v_i \mid k_1, \dots, k_m \in \mathbf{Z}\right\}.$$

(e) En déduire qu'il existe une base $(u_1, \dots, u_p)$ de $\mathbf{Q}^p$ telle que

$$\forall M \in G,\ Mu_i \in \mathbf{Z}u_1 + \dots + \mathbf{Z}u_p = \left\{\sum_{i=1}^{p} k_i u_i \mid k_1, \dots, k_p \in \mathbf{Z}\right\}.$$

(f) En déduire qu'il existe une matrice F de $GL_p(\mathbf{Q})$ telle que

$$\forall M \in G,\ F^{-1}MF \in SL_p(\mathbf{Z}).$$

Jusqu'à la fin du problème, on se place dans le cas particulier $p = 2$.

43. Soient A et B deux éléments de $SL_2(\mathbf{Q})$ et soit G le sous-groupe (multiplicatif) de $(SL_2(\mathbf{Q}), .)$ engendré par A et B. C'est le plus petit sous-groupe de $(SL_2(\mathbf{Q}), .)$ contenant A et B, il peut s'écrire

$$G = \left\{Q_1 Q_2 \dots Q_p \mid p \in \mathbf{N}^*,\ Q_1, Q_2, \dots, Q_p \in \{I_2, A, B, A^{-1}, B^{-1}\}\right\}.$$

On considère K le sous-groupe additif de $(\mathcal{M}_2(\mathbf{Q}), +)$ suivant

$$K = \mathbf{Z}I_2 + \mathbf{Z}A + \mathbf{Z}B + \mathbf{Z}AB + \mathbf{Z}BA + \mathbf{Z}ABA + \mathbf{Z}BAB$$

que l'on peut écrire

$$K = \left\{ k_1 I_2 + k_2 A + k_3 B + k_4 AB + k_5 BA + k_6 ABA + k_7 BAB \;\middle|\; k_1, \ldots, k_7 \in \mathbf{Z} \right\}.$$

On suppose de plus que $\mathrm{Tr}\,(A)$, $\mathrm{Tr}\,(B)$ et $\mathrm{Tr}\,(AB)$ appartiennent à $\mathbf{Z}$.

(a) Démontrer que A^{-1} et B^{-1} appartiennent à K.

(b) Démontrer que $G \subset K$.

(c) En déduire qu'il existe un entier strictement positif d tel que

$$\forall M \in G,\ dM \in \mathcal{M}_2(\mathbf{Z}).$$

44. Soient $A, B \in SL_2(\mathbf{Q})$.

(a) Montrer l'équivalence entre les deux propositions suivantes :

i) Il existe une matrice F de $GL_2(\mathbf{Q})$ telle que $F^{-1}AF$ et $F^{-1}BF$ appartiennent à $SL_2(\mathbf{Z})$.

ii) $\mathrm{Tr}\,(A), \mathrm{Tr}\,(B)$ et $\det(A + B)$ appartiennent à $\mathbf{Z}$.

(b) Soit n un entier strictement positif. Soient X, Y et Z des matrices de $SL_2(\mathbf{Q})$ telles que $\mathrm{Tr}\,(X)$ et $\mathrm{Tr}\,(Y)$ appartiennent à $\mathbf{Z}$ et qui satisfont la relation $X^n + Y^n = Z^n$.
Montrer qu'il existe une matrice F de $GL_2(\mathbf{Q})$ telle que $X_1 = F^{-1}XF$, $Y_1 = F^{-1}YF$ et $Z_1 = F^{-1}ZF$, avec X_1^n, Y_1^n et Z_1^n qui appartiennent à $SL_2(\mathbf{Z})$ et $X_1^n + Y_1^n = Z_1^n$.

FIN DU SUJET