Dans leurs copies, les candidats se lancent trop souvent dans des calculs longs et inadaptés ; il serait préférable de privilégier la recherche de méthodes adaptées à la résolution des questions. Plus généralement, une lecture attentive du sujet serait sans doute utile aux candidats.
Comme cela était rappelé dans le sujet, les premières questions du sujet nécessitent un soin particulier et les calculs doivent être détaillés.

Dans la suite, on donne des remarques détaillées pour certaines questions. Le plus souvent, on mentionne les erreurs les plus courantes et les écueils de rédaction.

Vrai ou faux ?

1a. Certains candidats se contentent de ne traiter que le cas $n = 2$. Plus généralement, il est préférable d'éviter de maladroitement nommer $m_{i,j}$ les coefficients d'une matrice notée A.

1b. Ici, on ne peut pas se contenter de l'affirmation $\chi_M(X) = X^2 - \mathrm{Tr}\,(M)X + \det(M)$. Cette égalité doit être démontrée et l'équivalence demandée doit être correctement justifiée.

1c. Le théorème spectral n'est pas valable sur le corps $\mathbf{C}$. Un contre-exemple était attendu et contrairement à ce que certains candidats pensent, le fait que le polynôme caractéristique d'une matrice soit scindé ne suffit pas à affirmer que cette matrice est diagonalisable.

1d. Très peu de candidats ont su donner un contre-exemple.

Exercice préliminaire

2. La rédaction de la récurrence qui était demandée est presque systématiquement approximative. Très souvent, l'hypothèse de récurrence est mal formulée ou alors l'initialisation n'est pas faite pour $d = 1$; la conclusion du raisonnement n'est pas toujours donnée.

3a-i L'utilisation du théorème de la base incomplète nécessite de bien préciser dans quel espace vectoriel on se place.

3a-ii Alors que cette égalité n'a pas de sens, dans trop de copies on peut lire que $P(M)Q(M)x = P(M)x.Q(M)x$ où P et Q sont des polynômes, M une matrice carrée et x un vecteur.

3b. Le but de la question et de l'exercice est de donner une démonstration du théorème de Cayley Hamilton. Il n'est pas possible d'utiliser ce théorème pour justifier la réponse à la question.
Le fait que pour un vecteur x non-nul on ait $\chi_M(M)x = 0$ ne suffit pas pour conclure et dans cette égalité on ne peut évidemment pas simplifier par x.

Problème, I

4. Il n'est pas suffisant d'affirmer que la symétrie de la matrice implique la symétrie de l'endomorphisme sans plus de précisions.

5 Dans cette question, certains candidats confondent les notions " être diagonalisable" et "être diagonale" pour les matrices carrées.

6. Trop de candidats oublient que la matrice $S + T$ est symétrique et n'utilisent pas la question précédente.

7. Bien que cette question corresponde à un résultat classique, il est étonnant de constater qu'elle n'à que très rarement été abordée.

8a. On a noté des confusions entre u et u^n. De plus les candidats oublient la définition d'un endomorphisme symétrique rappelée en préambule.

8c. L'unicité de u_i est rarement démontrée.

9. Les candidats peinent à donner explicitement le lien entre les matrices carrées et les endomorphismes.

10. Il ne faut pas oublier de vérifier que l'application ensembliste est bien définie. Puisque cette application n'est pas linéaire, on ne peut pas parler de son noyau.
Trop de candidats ne maîtrisent pas la notion de bijection.

Problème, II

11. La majorité des candidats s'est lancée dans un calcul direct très pénible et fastidieux. Afin d'être facilement traitée, cette question nécessitait un temps de réflexion avant de se lancer directement dans des calculs.

12. Dans l'ensemble, les différents cas sont bien traités. Cependant, certains candidats se lancent dans des calculs sans strtatégie ni réflexion.

14. Trop peu de candidats prennent le temps de vérifier que si $X \in SL_2(\mathbf{Z})$ alors $X^k \in SL_2(\mathbf{Z})$.

Problème, III

15. Il est à noter que beaucoup de candidats manquent de rigueur dans la rédaction de cette question. Les notions d'espaces vectoriels et de sous-espaces vectoriels sont approximatives. Le calcul de la dimension a rarement été abordé.

16.-17. Les définitions de sous-corps et de morphisme de corps ne sont pas connues de tous les candidats ; de nombreuses confusions ont été constatées avec les applications linéaires.

18a.-18b. La rédaction de ces questions à été très approximative et manquait de rigueur.

Problème, IV

19. Certains candidats ont confondu la notation $\overline{M}$ avec la conjugaison complexe des coefficients de la matrice M, d'autres oublient d'utiliser le fait que φ est un morphisme de corps.

20. Les candidats qui utilisent le déterminant pour résoudre cette question ne pensent pas tous à montrer que l'on a $\det(\overline{F}) = \overline{\det(F)}$.

21. De nombreux candidats utilisent l'indice n au lieu de p. Les commutativités des produits matriciels sont rarement justifiées.

23. Question souvent abordée, mais peu de candidats prennent le temps de justifier que $\delta \neq 0$.

24. Trop de candidats pensent que si les matrices ont le même polynôme caractéristique alors elles sont semblables.

2.1.3 Quelques éléments de correction

Le sujet s'inspire de l'article de Alex Khazanov intitulé *Fermat's equation in matrices.* Il a été publié dans la revue *Serdica Mathematical Journal* 21 (1995), no. 1, pp. 19 – 40.

Les éléments de correction donnent les grandes lignes de résolution des questions ; ils ne correspondent pas à la rédaction attendue par le jury. Dans leurs copies, les candidats doivent rédiger soigneusement et apporter une attention particulière aux justifications de leurs affirmations et de leurs calculs. Les rappels, les définitions des objets mathématiques et les énoncés des résultats utilisés sont indispensables ; par ailleurs, avant d'appliquer un résultat que l'on vient d'énoncer il est indispensable d'en vérifier les hypothèses.

Notations.
· *Dans tout le problème, n désignera un entier naturel non nul et* **L** *désignera le corps des nombres réels* **R** *ou le corps des nombres complexes* **C**.
· *Si p désigne un entier naturel non nul et* **L** *un corps, on note* $\mathcal{M}_p(\mathbf{L})$ *l'ensemble des matrices carrées de taille* $p \times p$ *à coefficients dans* **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* **A** *un sous-anneau de* **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* **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* **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** $\mathrm{Tr}\,(MN) \neq \mathrm{Tr}\,(NM)$**."**
   L'affirmation est fausse. En effet, pour tout couple de matrices M et N dans $\mathcal{M}_n(\mathbf{C})$, on a
   $$\mathrm{Tr}\,(MN) = \sum_{k=1}^{n} \sum_{j=1}^{n} m_{kj} n_{jk} = \sum_{j=1}^{n} \sum_{k=1}^{n} n_{jk} m_{kj} = \mathrm{Tr}\,(NM)$$
   (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."**

Tournez la page S.V.P.

Cette affirmation est vraie, car si $M \in \mathcal{M}_2(\mathbf{C})$, son polynôme caractéristique est donné par $\chi_M = X^2 - \mathrm{Tr}\,(M)X + \det(M)$, et deux polynômes sont égaux si et seulement s'ils ont les mêmes coefficients. Il faut aussi noter que deux matrices semblables ont la même trace et même déterminant.

(c) Affirmation : "Les matrices carrées et symétriques à coefficients dans C sont diagonalisables."

Cette affirmation est fausse. La matrice $\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$ a pour polynôme caractéristique X^2, et donc sa seule valeur propre est nulle. Or, la seule matrice semblable à la matrice nulle est la matrice nulle, et puisque cette matrice est non nulle, elle n'est pas diagonalisable.

(d) Soit $\varphi : A \to B$ un morphisme d'anneaux.

Affirmation : "Si $\varphi(a)$ est inversible dans B, alors a est inversible dans A."

Cette affirmation est fausse. La surjection canonique de $\mathbf{Z}$ dans $\mathbf{Z}/2\mathbf{Z}$ est un morphisme d'anneaux, mais l'entier naturel 3 n'est pas inversible dans $\mathbf{Z}$ mais son image l'est dans $\mathbf{Z}/2\mathbf{Z}$.

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 $\chi_{C_P}(X) = P(X)$.

On raisonne par récurrence sur la taille de la matrice, la propriété au rang $d \in \mathbf{N}^*$ s'écrit avec les notations de l'énoncé : $\forall (a_j)_{j \in [\![0, d-1]\!]} \in \mathbf{C}^d$, $\chi_{C_P}(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0$.

- ▷ **Initialisation :** le cas $d = 1$ est clair.
- ▷ **Hérédité :** soit d un entier naturel supérieur ou égal à 2, supposons la propriété vraie au rang $d-1$. Le développement de $\det(X I_d - C_P)$ par rapport à la première ligne comme indiqué dans l'énoncé donne $\det(X I_d - C_P) = (-1)^{1+1} X \det(X I_{d-1} - C_Q) + (-1)^{d+1} a_0 \det(T)$ où la matrice $T \in \mathcal{M}_{d-1}(\mathbf{C})$ est triangulaire supérieure à coefficients diagonaux égaux à -1, donc de déterminant $(-1)^{d-1}$, et le polynôme Q est donné par $Q(X) = X^{d-1} + a_{d-1}X^{d-2} + \ldots + a_1$. Ainsi, par hypothèse de récurrence, $\det(X I_d - C_P) = XQ(X) + a_0 = P(X)$, ce qui achève la récurrence.

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

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

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

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

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

Notons que l'entier μ est bien défini et appartient à l'ensemble $[\![1, p]\!]$ puisque x est non nul et que la famille $\{x, Mx, \dots, M^p x\}$ est liée en tant que famille de $p+1$ éléments dans un espace vectoriel de dimension p.

Par définition, la famille $\{x, Mx, \dots, M^{\mu-1} x\}$ est libre. On complète cette famille libre en une base notée $\mathcal{B}$ de $\mathbf{C}^p$, de la forme $\{x, Mx, \dots, M^{\mu-1}x, e_{\mu+1}, \dots, e_p\}$, ce qui est licite d'après le théorème de la base incomplète.

Par abus de notation, on note toujours M l'endomorphisme de $\mathcal{M}_{p,1}(\mathbf{C})$ (que l'on identifie à $\mathbf{C}^p$) canoniquement associé à M. Par construction, les $\mu-1$ premières colonnes de la matrice de M dans la base $\mathcal{B}$ ont la forme voulue.

Enfin, la famille $\{x, Mx, \dots, M^\mu x\}$ est liée, donc il existe $(a_j)_{j\in[\![1,\mu]\!]} \in \mathbf{C}^p \setminus \{0\}$ tel que $\sum_{j=0}^{\mu} a_j M^j x = 0$. Nécessairement, $a_\mu \neq 0$, sinon cela contredirait la liberté de la famille $\{x, Mx, \dots, M^{\mu-1}x\}$. Ainsi, après division par a_μ, on obtient l'existence de $(\alpha_0, \dots, \alpha_{\mu-1}) \in \mathbf{C}^\mu$ tels que $M^\mu x + \sum_{j=0}^{\mu-1} \alpha_j M^j x = 0$. Cela donne la forme voulue pour la colonne d'indice μ de la matrice de M dans $\mathcal{B}$, et donc pour l'existence d'une matrice M' semblable à M de la forme souhaitée.

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

Puisque M et M' sont semblables, $\chi_M = \chi_{M'}$. La matrice M' est triangulaire supérieure par blocs, donc en notant $P = X^\mu + \sum_{j=0}^{\mu-1} \alpha_j X^j$, la question 2 donne $\chi_M = \chi_N \chi_{C_P} = \chi_N P$. Enfin, $\chi_M(M)x = \chi_N(M)P(M)x$, et par construction $P(M)x = 0$ d'après la question précédente.

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

Le raisonnement de la question précédente assure que pour tout x de $\mathbf{C}^p$, $\chi_M(M)x = 0$. Il suffit de choisir des vecteurs de x parcourant une base de $\mathbf{C}^p$ pour en déduire que la matrice $\chi_M(M)$ est nulle, ce qui termine la preuve.

Problème.

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

Soient n et p deux entiers strictement positifs.

Tournez la page S.V.P.

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 $\mathbf{R}^p$.**
Soit $\mathcal{B}$ la base canonique de $\mathbf{R}^p$ qui est orthonormée pour le produit scalaire usuel. Pour $x, y \in \mathbf{R}^p$, en notant X et Y les matrices colonnes correspondantes dans la base $\mathcal{B}$, on a :

$$\langle a(x)|y\rangle = {}^t(AX)Y = {}^tX{}^tAY = {}^tX(AY) = \langle x|a(y)\rangle$$

Affirmer que a est représenté matriciellement par une matrice symétrique A **en base orthonormée** est un argument valable.

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**

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

   - ▷ Sens direct : le théorème spectral assure l'existence de $P \in O_p(\mathbf{R})$ telle que $S = {}^tPDP$ avec $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_p)$ où les λ_i sont des réels positifs.
   Pour $Y \in \mathcal{M}_{p,1}(\mathbf{R})$, ${}^tYSY = {}^t(PY)D(PY)$, d'où en notant $(x_i)_{1\leqslant i\leqslant p}$ les coordonnées de PY, cela donne ${}^tYSY = \sum_{i=1}^p \lambda_i x_i^2 \geqslant 0$.
   - ▷ Sens réciproque : si Y est un vecteur propre de S associé à la valeur propre λ, alors ${}^tYSY = \lambda\|Y\|^2 \geqslant 0$ puis $\lambda \geqslant 0$, car Y est non nul, donc : $\|Y\|^2 > 0$.

6. **Démontrer que pour toutes les matrices S et T de $\mathcal{S}_p^+(\mathbf{R})$, la matrice $S+T$ appartient à $\mathcal{S}_p^+(\mathbf{R})$.**
Tout d'abord $S+T$ est une matrice symétrique.
Il suffit d'écrire ensuite : $\forall Y \in \mathcal{M}_{p,1}(\mathbf{R})$, ${}^tY(S+T)Y = {}^tYSY + {}^tYTY \geqslant 0$ et d'appliquer la question précédente.

7. **Soit $S \in \mathcal{S}_p^+(\mathbf{R})$. Montrer qu'il existe une matrice R de $\mathcal{S}_p^+(\mathbf{R})$ telle que $R^n = S$.**
On diagonalise S comme à la question 5, puis la matrice $R = {}^tP\mathrm{diag}(\lambda_i^{1/n})P$ convient (ceci a un sens car tous les λ_i sont positifs).

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.
   Les puissances de u commutent entre elles, donc u et s commutent. Ainsi, les espaces propres de s sont stables par u, ce qui légitime l'existence de l'endomorphisme u_i induit par u sur $E_{\lambda_i}(s)$. Enfin, la relation $\forall x, y \in \mathbf{R}^p$, $\langle u(x)|y\rangle = \langle x|u(y)\rangle$ reste vraie sur $E_{\lambda_i}(s)$, ce qui prouve que u_i est symétrique.

   (b) Soit $i \in [\![1, q]\!]$. Démontrer que $\sqrt[n]{\lambda_i}$ est la seule valeur propre possible de u_i.
   Soit μ une valeur propre de u_i, soit x un vecteur propre associé. Il vient $s(x) = u_i^n(x) = \mu^n x$ et puisque $x \in E_{\lambda_i}(s)$, $s(x) = \lambda_i x$. Comme x est non nul, on tire $\mu^n = \lambda_i$, et puisque ces réels sont positifs par hypothèse, $\mu = \sqrt[n]{\lambda_i}$

   (c) Démontrer que l'endomorphisme u est unique.
   L'endomorphisme u_i est symétrique, donc admet une base orthonormée de vecteurs propres $(f_1 \ldots, f_k)$. D'après la question précédente, $u(f_i) = u_i(f_i) = \sqrt[n]{\lambda_i} f_i$ pour tout indice i, ce qui signifie que $u_i = \sqrt[n]{\lambda_i} id_{E_{\lambda_i}(s)}$. Enfin, $s(f_i) = u^n(f_i) = \lambda_i f_i$ par construction. Ainsi, puisque $\oplus_{i=1}^q E_{\lambda_i}(s) = \mathbf{R}^p$, cela définit u et donc U de façon 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 $R^n = S$.**
La question 7 prouve l'existence d'une telle matrice R.
L'ensemble des endomorphismes sur $\mathbf{R}^p$ est naturellement en bijection avec l'ensemble $\mathcal{M}_p(\mathbf{R})$ via l'application qui à un endomorphisme associe sa matrice dans la base canonique.
La question 8c prouve l'unicité d'un endomorphisme r de $\mathbf{R}^p$ tel que $r^n = s$. Puisque r est un endomorphisme symétrique positif dans la base canonique qui est orthonormée, alors R est symétrique à valeurs propres positives, et est donc bien dans $\mathcal{S}_p^+(\mathbf{R})$.
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**

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

est une bijection.
Pour prouver la bonne définition de ψ, on note que si U et V sont deux matrices symétriques positives il en est de même pour $U+V$ d'après la question 6. Ainsi, pour un tel couple (U,V), $\sqrt[n]{U+V}$ existe. Par ailleurs, $\sqrt[n]{U}^n + \sqrt[n]{V}^n = U + V = \left(\sqrt[n]{U+V}\right)^n$, ce qui assure que ψ est bien à valeurs dans $\{(X,Y,Z) \in (\mathcal{S}_p^+(\mathbf{R}))^3 / \; X^n + Y^n = Z^n\} = \mathcal{F}$
Soit

$$\varphi : \left\{ \begin{array}{lll} \mathcal{F} & \to & (\mathcal{S}_p^+(\mathbf{R}))^2 \\ (X,Y,Z) & \mapsto & (X^n, Y^n) \end{array} \right.$$

On vérifie directement que la puissance n-ième d'une matrice symétrique positive l'est également (le spectre élévé à la puissance n reste dans $\mathbf{R}_+$). En outre,

$$\forall (X,Y,Z) \in \mathcal{F}, \; \psi \circ \varphi(X,Y,Z) = \psi(X^n, Y^n) = \left(\sqrt[n]{X^n}, \sqrt[n]{Y^n}, \sqrt[n]{X^n + Y^n} \right)$$

Or, $\sqrt[n]{X^n} = X$, $\sqrt[n]{Y^n} = Y$ et $\sqrt[n]{X^n + Y^n} = Z$ par unicité de la solution et puisque ces matrices sont symétriques positives,
Enfin,

$$\forall (U,V) \in (\mathcal{S}_p^+(\mathbf{R}))^2, \; \varphi \circ \psi(U,V) = \varphi \left(\sqrt[n]{U}, \sqrt[n]{V}, \sqrt[n]{U+V} \right) = (U,V)$$

car par définition de $\sqrt[n]{U}$, on a $\left(\sqrt[n]{U}\right)^n = U$.
Ainsi, φ et ψ sont réciproques l'une de l'autres, donc ψ 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 $\mathrm{Tr}\,(M^4) = \mathrm{Tr}\,(M)^4 - 4\,\mathrm{Tr}\,(M)^2 + 2$.**
▷ Première méthode : d'après le théorème de Cayley-Hamilton, $M^2 - \mathrm{Tr}\,(M)M + I_2 = 0$, donc par élévation au carré, puisque les puissances de M commutent entre elles,

$$M^4 = \mathrm{Tr}\,(M)^2 M^2 - 2\,\mathrm{Tr}\,(M)M + I_2 = \mathrm{Tr}\,(M)^2(\mathrm{Tr}\,(M)M - I_2) - 2\,\mathrm{Tr}\,(M)M + I_2$$

d'où

$$M^4 = (\mathrm{Tr}\,(M)^3 - 2\,\mathrm{Tr}\,(M))M + (1 - \mathrm{Tr}\,(M)^2)I_2.$$

On passe à la trace et la relation s'obtient par linéarité.

Tournez la page S.V.P.

▷ Seconde méthode : trigonaliser dans $\mathbf{C}$, élever à la puissance 4, et constater que

$$\mathrm{Tr}\,(M^4) = \lambda_1^4 + \lambda_2^4 = (\lambda_1^2 + \lambda_2^2)^2 - 2\lambda_1^2\lambda_2^2 = \left((\lambda_1 + \lambda_2)^2 - 2\lambda_1\lambda_2\right)^2 - 2\lambda_1^2\lambda_2^2 = (\mathrm{Tr}\,(M)^2 - 2)^2 - 2$$

puisque $\det(M) = \lambda_1\lambda_2 = 1$.

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

Grâce à la question précédente, on a $\mathrm{Tr}\,(M^4) = (\mathrm{Tr}\,(M)^2 - 2)^2 - 2$.

▷ Premier cas : $\mathrm{Tr}\,(M) = 2k + 1$ est un entier impair. On obtient alors

$$\mathrm{Tr}\,(M^4) = ((2k+1)^2 - 2)^2 - 2 = (4k^2 + 4k - 1)^2 - 2 = (4k^2 + 4k)^2 - 2(4k^2 + 4k) + 1 - 2 \equiv -1[8]$$

▷ Second cas : $\mathrm{Tr}\,(M) = 2k$ est un entier pair. On obtient alors

$$\mathrm{Tr}\,(M^4) = ((2k)^2 - 2)^2 - 2 = 16k^4 - 16k^2 + 2 \equiv 2[8]$$

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

Supposons l'existence d'une solution (X, Y, Z) dans le cas où $n = 4$. En distinguant selon les valeurs prises par $\mathrm{Tr}\,(X)$ et $\mathrm{Tr}\,(Y)$, le résultat de la question précédente prouve que $\mathrm{Tr}\,(X^4+Y^4) \equiv -2,\ 1,$ ou $4[8]$. Ainsi, on ne peut pas avoir $\mathrm{Tr}\,(Z^4) \equiv -1, 2[8]$, ce qui fournit une contradiction.

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 $SL_2(\mathbf{Z})$.

Supposons n divisible par 4. On écrit $n = 4k$ pour un entier naturel k. Si cette équation admettait une solution (X, Y, Z), le triplet (X^k, Y^k, Z^k) de matrices à coefficients entiers de déterminant 1 fournirait une solution à l'équation de la question précédente, ce qui est absurde.

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

On pose

$$\varphi : \left\{ \begin{array}{ccc} \mathbf{K} & \to & \mathbf{K} \\ x & \mapsto & \overline{x} \end{array} \right.$$

15. Démontrer que K est un Q-espace vectoriel dont on précisera la dimension.

D'une part, $\mathbf{K} = \mathrm{vect}_{\mathbf{Q}}(1, \delta)$ donc $\mathbf{K}$ est un sous-espace vectoriel du $\mathbf{Q}$-espace vectoriel $\mathbf{C}$. D'autre part, si $a, b \in \mathbf{Q}$ vérifient $a + b\delta = 0$, nécessairement $b = 0$ sans quoi $\delta = -\frac{b}{a} \in \mathbf{Q}$, donc $a = 0$, ce qui prouve la $\mathbf{Q}$-liberté de la famille $(1, \delta)$. Ainsi, $\mathbf{K}$ est un $\mathbf{Q}$-espace vectoriel de dimension 2.

16. Démontrer que K est un sous-corps de C.

D'après ce qui précède, $\mathbf{K}$ est un sous-groupe additif de $\mathbf{C}$, et $1 \in \mathbf{K}$.

Si $a + b\delta$ et $c + d\delta$ sont deux éléments de $\mathbf{K}$, leur produit vaut $ac + Dbd + \delta(ad + bc)$ qui est bien dans $\mathbf{K}$ car $D \in \mathbf{Q}$. Cela prouve que $\mathbf{K}$ est un sous-anneau de $(\mathbf{C}, +, \times)$.

Enfin, si $x = a + b\delta \in \mathbf{K}^*$, on note que $(a, b) \neq (0, 0)$ et donc $a - b\delta \neq 0$ par liberté sur $\mathbf{Q}$ de $(1, \delta)$. Par conséquent,

$$\frac{1}{a + b\delta} = \frac{a - b\delta}{(a + b\delta)(a - b\delta)} = \frac{a}{a^2 - b^2D} - \frac{b}{a^2 - b^2D}\delta \in \mathbf{K}$$

ce qui prouve que $\mathbf{K}$ est un sous-corps de $\mathbf{C}$.

17. Démontrer que φ est un isomorphisme de corps.

On constate que φ est involutive donc bijective. Reste à vérifier que φ est un morphisme de corps. On utilise dans tous les calculs qui suivent l'unicité de l'écriture d'un élément de $\mathbf{K}$ sous la forme $a + b\delta$ avec $a, b \in \mathbf{Q}$:

- $\varphi(1) = \varphi(1 + 0\delta) = 1$
- $\forall (a,b,c,d) \in \mathbf{Q}^4,\ \varphi(a+b\delta+c+d\delta) = \varphi(a+c+(b+d)\delta) = a+c-(b+d)\delta = \varphi(a+b\delta)+\varphi(c+d\delta)$
- $\forall (a,b,c,d) \in \mathbf{Q}^4,\ \varphi((a+b\delta)(c+d\delta)) = \varphi(ac+Dbd+\delta(ad+bc)) = ac+Dbd-\delta(ad+bc) = (a-b\delta)(c-d\delta)$ d'où $\forall (a,b,c,d) \in \mathbf{Q}^4,\ \varphi((a+b\delta)(c+d\delta)) = \varphi(a+b\delta)\varphi(c+d\delta)$ ce qui termine la preuve.

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

Soient $x, y \in \mathbf{Q}$ tels que $\psi(x) = \psi(y)$. On a $\frac{x+\delta}{x-\delta} = \frac{y+\delta}{y-\delta}$ d'où $xy+(y-x)\delta-D = xy+(x-y)\delta-D$ et par $\mathbf{Q}$-liberté de $(1,\delta)$ cela donne $y-x = x-y$, donc $x = y$, donc ψ est injective.

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

L'image d'un ensemble infini par une application injective est un ensemble infini, donc grâce à la question précédente, l'ensemble $\left\{ \frac{x+\delta}{x-\delta},\ x \in \mathbf{Q} \right\}$ est infini et cet ensemble est inclus dans $\left\{ \frac{\theta}{\overline{\theta}},\ \theta \in \mathbf{K} \setminus \{0\} \right\}$ qui est donc un ensemble infini.

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 $\overline{AB} = \overline{A}\ \overline{B}$.

Avec des notations usuelles, si $C = AB$, on a grâce au fait que φ est un morphisme de corps $\forall i, j \in [\![1,p]\!],\ \overline{c_{i,j}} = \overline{\sum_{k=1}^{p} a_{ik}b_{kj}} = \sum_{k=1}^{p} \overline{a_{ik}}\,\overline{b_{kj}}$ où l'on reconnaît le coefficient d'indice (i,j) du produit $\overline{A} \cdot \overline{B}$. Ainsi, $\forall A, B \in \mathcal{M}_p(\mathbf{K}),\ \overline{AB} = \overline{A} \cdot \overline{B}$.

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 $\left(\overline{F}\right)^{-1} = \overline{F^{-1}}$.

- Si $F \in GL_p(\mathbf{K})$, on écrit $FF^{-1} = I_p$ et grâce à la question précédente, $\overline{F}\,\overline{F^{-1}} = \overline{I_p} = I_p$, donc $\overline{F} \in GL_p(\mathbf{K})$ et $\overline{F}^{-1} = \overline{F^{-1}}$.
- Si $\overline{F} \in GL_p(\mathbf{K})$, on procède de même car $\overline{\overline{F}} = F$.

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 $X\overline{X}$.

Un petit calcul qui résulte directement de la question précédente donne

$X\overline{X} = F(\overline{F})^{-1}\overline{F(\overline{F})^{-1}} = F(\overline{F})^{-1}\overline{F}(\overline{\overline{F}})^{-1} = FF^{-1} = I_p$

(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.**

Si $\theta \neq 0$, on écrit $F(\theta) = \overline{\theta}\left(\frac{\theta}{\overline{\theta}}I_p + X\right)$ et puisque $\overline{\theta} \neq 0$, cette matrice n'est pas inversible si et seulement si $\frac{\theta}{\overline{\theta}}I_p + X$ n'est pas inversible si et seulement si $-\frac{\theta}{\overline{\theta}} \in Sp(X)$. Or, X admet

au plus p valeurs propres distinctes, et $\left\{ \frac{\theta}{\overline{\theta}},\ \theta \in \mathbf{K} \setminus \{0\} \right\}$ est un ensemble infini, d'où l'existence d'un θ_0 convenable.

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

$$X\overline{F(\theta_0)} = X\left(\overline{\theta_0}I_p + \theta_0\overline{X}\right) = \overline{\theta_0}X + \theta_0 X\overline{X} = \overline{\theta_0}X + \theta_0 I_p = F(\theta_0)$$

(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 :** $\begin{cases} X^{-1}AX = \overline{A} \\ X^{-1}BX = \overline{B} \\ X\overline{X} = I_p \end{cases}$

Supposons (i) vraie. Soit $X = F(\overline{F})^{-1}$. On a $\overline{F^{-1}AF} = F^{-1}AF$ puisque cette matrice est à coefficients rationnels. Ainsi, en utilisant la question 19, $\overline{F^{-1}} \cdot \overline{A} \cdot \overline{F} = F^{-1}AF$, puis cela s'écrit $\overline{A} = \overline{F}F^{-1}AF\overline{F}^{-1} = X^{-1}AX$. On procède de même pour établir $X^{-1}BX = \overline{B}$ et $X\overline{X} = I_p$ résulte de 20, d'où la preuve de (ii).
Réciproquement, soit θ_0 choisi comme à la question 21b. D'après les calculs précédents, on a : $\overline{F(\theta_0)^{-1}AF(\theta_0)} = F(\theta_0)^{-1}AF(\theta_0)$, donc $F(\theta_0)^{-1}AF(\theta_0) \in \mathcal{M}_p(\mathbf{Q})$. On procède de même pour $F(\theta_0)^{-1}BF(\theta_0)$.

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 K. On suppose que λ n'est pas élément de Q.

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

Soit $X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.
On a les équivalences suivantes :

$$\begin{cases} X^{-1}AX = \overline{A} \\ X\overline{X} = I_2 \end{cases} \iff \begin{cases} AX = X\overline{A} \\ X\overline{X} = I_2 \end{cases} \iff \begin{cases} \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \overline{\lambda} & 0 \\ 0 & \lambda \end{pmatrix} \\ X\overline{X} = I_2 \end{cases}$$

Ainsi,

$$AX = X\overline{A} \iff \begin{cases} \lambda\alpha = \overline{\lambda}\alpha \\ \lambda\beta = \lambda\beta \\ \overline{\lambda}\gamma = \overline{\lambda}\gamma \\ \overline{\lambda}\delta = \lambda\delta \end{cases} \iff \begin{cases} (\lambda - \overline{\lambda})\alpha = 0 \\ (\lambda - \overline{\lambda})\delta = 0 \end{cases} \iff \alpha = \delta = 0$$

car $\lambda \notin \mathbf{Q} \iff \lambda \neq \overline{\lambda}$, ce qui donne pour conclure

$$X^{-1}AX = \overline{A} \iff \exists(\beta, \gamma) \in \mathbf{K}^2,\ X = \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}$$

Enfin, si X est de la forme précédente, on a

$$X\overline{X} = I_2 \iff \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}\begin{pmatrix} 0 & \overline{\beta} \\ \overline{\gamma} & 0 \end{pmatrix} = I_2 \iff \begin{cases} \beta\overline{\gamma} = 1 \\ \overline{\beta}\gamma = 1 \end{cases} \iff \gamma = \frac{1}{\overline{\beta}}$$

en notant que nécessairement, $\beta \neq 0$ car $X \in GL_2(\mathbf{K})$.

(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 K tel que l'on a $N(a) - 1 = N(x)$ (c'est-à-dire $a\overline{a} - 1 = x\overline{x}$).

▷ Deux matrices semblables ayant même déterminant, on a $\det(A) = \det(B)$.

▷ D'après la question 21c, il existe $X \in GL_2(\mathbf{K})$ tel que $\begin{cases} X^{-1}AX = \overline{A} \\ X^{-1}BX = \overline{B} \\ X\overline{X} = I_n \end{cases}$. D'après la question 22a, il existe $u \in \mathbf{K}^*$ tel que $X = \begin{pmatrix} 0 & u \\ \frac{1}{\overline{u}} & 0 \end{pmatrix}$. La relation $X^{-1}BX = \overline{B}$ donne $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & u \\ \frac{1}{\overline{u}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & u \\ \frac{1}{\overline{u}} & 0 \end{pmatrix}\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ et le calcul matriciel donne $\begin{cases} au = \overline{d}u \\ b = \overline{c}u\overline{u} \end{cases}$ d'où $a = \overline{d}$ car $u \neq 0$.

Or, $1 = \det(B) = ad - bc$ donc $a\overline{a} - 1 = bc = c\overline{c}u\overline{u}$. Ainsi, $N(a) - 1 = N(x)$ avec $x = cu$.

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

Soient α un élément de 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 $a - d = \dfrac{2\alpha m_1 + 1}{\delta}$.

D'une part, $1 = \det(B_1) = ad - bc$. D'autre part,

$$\begin{aligned} \det(A_1 + B_1) &= (a + \alpha + \delta)(d + \alpha - \delta) - bc \\ &= ad - bc + (\alpha + \delta)d + (\alpha - \delta)a + \alpha^2 - \delta^2 \\ &= 1 + \alpha\,\mathrm{Tr}\,(B) - \delta(a - d) + \alpha^2 - D \\ &= 2 + 2\alpha m_1 - \delta(a - d) \end{aligned}$$

donc $\delta(a - d) = 1 + 2\alpha m_1$ d'où $a - d = \frac{1+2\alpha m_1}{\delta}$, en notant que $\delta \neq 0$ car $\delta \notin \mathbf{Q}$.

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 $A_1 = \begin{pmatrix} \alpha + \delta & 0 \\ 0 & \alpha - \delta \end{pmatrix}$.

Le polynôme caractéristique de A s'écrit $\chi_A = X^2 - (\mathrm{Tr}\,A)X + \det(A) = X^2 - 2\alpha X + 1$ car $\begin{cases} (\alpha + \delta) + (\alpha - \delta) = 2\alpha \\ (\alpha + \delta)(\alpha - \delta) = \alpha^2 - \delta^2 = \alpha^2 - D = 1 \end{cases}$ donc $\alpha + \delta$ et $\alpha - \delta$ sont les racines de χ_A. Puisque $\delta \neq 0$ en tant qu'irrationnel, on en déduit que les valeurs propres de A sont distinctes, ce que prouve que A est diagonalisable dans le corps $\mathbf{K}$: il existe $P \in GL_2(\mathbf{K})$ tel que $A = PA_1P^{-1}$.

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

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

On conserve les notations de la question précédente, notons $B_1 = P^{-1}BP = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a $\det(A_1) = \det(B_1) = \det(A_1 + B_1) = 1$ car $A_1 + B_1 = P^{-1}(A + B)P$. On reprend les notations de la question 23, on a $a - d = \frac{2\alpha m+1}{\delta}$ car $2m = \text{Tr } B_1 = \text{Tr } B$ car la trace est un invariant de similitude. En prenant $F = P^{-1}$, la question 22b nous assure que $d = \overline{a}$ et qu'il existe $x \in \mathbf{K}$ tel que $N(a) - 1 = N(x)$. On a enfin $\text{Tr } B = a + d$, donc $\begin{cases} a + d = 2m \\ a - d = \frac{2\alpha m+1}{\delta} \end{cases}$ donc $\begin{cases} a = m + \frac{\alpha m+1/2}{\delta} \\ d = m - \frac{\alpha m+1/2}{\delta} \end{cases}$ et puisque $d = \overline{a}$, cela donne

$$N(x) = N(a) - 1 = a\overline{a} - 1 = \left(m + \frac{\alpha m + 1/2}{\delta}\right)\left(m - \frac{\alpha m + 1/2}{\delta}\right) - 1$$

d'où

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

car $\delta^2 = D = \alpha^2 - 1$.

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

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

Puisque $1 - \alpha^2 = -\delta^2 = \overline{\delta}\delta$, il suffit de poser $y = \delta x$.

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* $\text{Tr}\,(A) = 2\alpha$ *et* $\det(A + B) = 1$*, alors si $m = \frac{\text{Tr}\,(B)}{2}$ 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.

Posons $x = 3k + \ell$ avec $\ell \in [\![0, 2]\!]$. Il suffit d'écrire

$$u = x^3 - 3x = 27k^3 + 27k^2\ell + 9k\ell + \ell^3 - 9k - 3\ell \equiv \ell^3 - 3\ell[9]$$

Ainsi, $\begin{cases} u \equiv \ \ 0[9] \text{ si } \ell = 0, \\ u \equiv -2[9] \text{ si } \ell = 1, \\ u \equiv \ \ 2[9] \text{ si } \ell = 2 \end{cases}$

(b) Soit M une matrice de $SL_2(\mathbf{Z})$, démontrer que l'on a $\mathrm{Tr}\,(M^3) = (\mathrm{Tr}\,(M))^3 - 3\,\mathrm{Tr}\,(M)$.
La matrice M est trigonalisable vue comme matrice à coefficients complexes : il existe $P \in GL_2(\mathbf{C})$ tel que $M = P\begin{pmatrix}\lambda_1 & \star \\ 0 & \lambda_2\end{pmatrix}P^{-1}$ d'où $M^3 = P\begin{pmatrix}\lambda_1^3 & \star \\ 0 & \lambda_2^3\end{pmatrix}P^{-1}$. Ainsi,

$$\mathrm{Tr}\ M^3 = \lambda_1^3 + \lambda_2^3 = (\lambda_1+\lambda_2)^3 - 3\lambda_1^2\lambda_2 - 3\lambda_1\lambda_2^2 = \mathrm{Tr}\ M^3 - 3\lambda_1\lambda_2(\lambda_1+\lambda_2)$$

et donc, $\mathrm{Tr}\ M^3 = \mathrm{Tr}\ M^3 - 3\det(M)\,\mathrm{Tr}\ M = \mathrm{Tr}\ M^3 - 3\,\mathrm{Tr}\ M$

(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 $\mathrm{Tr}\,(C_1^3) \equiv 2[9]$.**

- ▷ Si $\mathrm{Tr}\ A^3 \equiv 0[9]$: on pose $A_1 = A$ alors $\mathrm{Tr}\ B^3 = \mathrm{Tr}\ C^3$ est congru à 2 ou -2 modulo 9 par hypothèse et d'après les questions 25a et 25b.
  - — Si $\mathrm{Tr}\ B^3 = -2$, on choisit alors $B_1 = -B$ et $C_1 = -C$ et (A_1, B_1, C_1) convient. En effet, $\det(-B) = (-1)^2\det(B) = 1$ et de même pour C.
  - — Sinon, le triplet (A, B, C) convient.
- ▷ Si $\mathrm{Tr}\ A^3 \equiv 2[9]$: grâce aux questions 25a et 25b, $\mathrm{Tr}\ A^3 + \mathrm{Tr}\ B^3 \equiv 0, 2, 4[9]$. Les cas $\mathrm{Tr}\ A^3 + \mathrm{Tr}\ B^3 \equiv 4[9]$ sont exclus.
  - — Si $\mathrm{Tr}\ B^3 \equiv 0[9]$, on prend $(A_1, B_1, C_1) = (B, A, C)$.
  - — Si $\mathrm{Tr}\ B^3 \equiv -2[9]$, dans ce cas $\mathrm{Tr}\ C^3 \equiv 0[9]$ et $A^3 + (-C)^3 \equiv (-B)^3$, on prend donc $(A_1, B_1, C_1) = (-C, A, -B)$.
- ▷ Si $\mathrm{Tr}\ A^3 \equiv -2[9]$, on se ramène au cas précédent via la relation $(-A)^3 + (-B)^3 = (-C)^3$.

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 $(X-1)^2$.**
Comme $\mathrm{Tr}\ B_1^3 = (\mathrm{Tr}\ B_1)^3 - 3\,\mathrm{Tr}\ B_1$, le raisonnement de la question 25a nous assure que $\mathrm{Tr}\ B_1 \equiv 2[3]$ (ce qui correspond au cas $\ell = 2$). Ainsi, dans le corps $\mathbf{Z}/3\mathbf{Z}$,

$$\chi_{\dot{B}_1} = X^2 - (\mathrm{Tr}\ \dot{B}_1)X + \det\dot{B}_1 = X^2 - 2X + 1 = (X-1)^2$$

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 $\mathbf{Z}/3\mathbf{Z}$.**

Le polynôme caractéristique de la matrice $\dot{B}_1$ est scindé dans le corps $\mathbf{Z}/3\mathbf{Z}$ et admet pour seule racine 1, donc B_1 est trigonalisable dans $\mathcal{M}_2(\mathbf{Z}/3\mathbf{Z})$ et est semblable à une matrice de la forme $\begin{pmatrix}1 & k \\ 0 & 1\end{pmatrix}$, avec k dans $\mathbf{Z}/3\mathbf{Z}$. On raisonne de même pour $\dot{C}_1$.

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.**

On note P une matrice inversible de $\mathcal{M}_2(\mathbf{Z}/3\mathbf{Z})$ telle que $\overset{\bullet}{B}_1 = P\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}P^{-1}$ dont l'existence a été établie à la question précédente. Remarquons alors que

$$\overset{\bullet}{B}_1^{\,3} = P\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}^3 P^{-1} = P\begin{pmatrix}1 & 3k\\ 0 & 1\end{pmatrix}P^{-1} = I_2$$

et de même $\overset{\bullet}{C}_1^{\,3} = I_2$, la relation $A_1^3 + B_1^3 = C_1^3$ entraîne donc $\overset{\bullet}{A}_1^3 = 0$.
Enfin, $\det\left(\overset{\bullet}{A}_1^3\right) = \left(\det(\overset{\bullet}{A}_1)\right)^3 = 0$, donc $\det(\overset{\bullet}{A}_1) = 0$ puisque $\mathbf{Z}/3\mathbf{Z}$ est un corps, ce qui fournit la contradiction espérée.

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 Q tels que 2α et $2m$ appartiennent à 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 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 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

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

Calculons les restes modulo 9 des quantités mises en jeu : $(4\alpha m + 2)^2 \equiv 2^2[9]$ et $((2\alpha)^2 - 4)((2m)^2 - 4) \equiv (-4)^2[9]$. On obtient ainsi

$$(4\alpha m + 2)^2 - ((2\alpha)^2 - 4)((2m)^2 - 4) \equiv 4 - 16[9] \equiv 6[9]$$

On a $4xd \in \mathbf{Z}$ et $2yd \in \mathbf{Z}$, car d est un dénominateur commun aux fractions x et y.
Notons $P = (4xd)^2 - \left((2\alpha)^2 - 4\right)(2yd)^2$. Puisque $2\alpha \equiv 0[9]$, on a directement $P \equiv (4xd)^2 + 4(2yd)^2[3] \equiv (4xd)^2 + (2yd)^2[3]$.
Grâce à la relation fournie, on tire $P = 6d^2 + 9k$ avec $k \in \mathbf{Z}$, donc $(4xd)^2 + (2yd)^2 \equiv 0[3]$.

(b) Montrer que l'on a $4xd \equiv 0[3]$ et $2yd \equiv 0[3]$.
On pose $a = 4xd \in \mathbf{Z}$ et $b = 2yd$. Les quantités a^2 et b^2 sont congrus à 0 ou 1 modulo 3 et $a^2 \equiv 0[3]$ si et seulement si $a \equiv 0[3]$. Ainsi, $a^2 + b^2 \equiv 0[3]$ implique que $a^2 \equiv 0[3]$ et $b^2 \equiv 0[3]$, donc $a \equiv 0[3]$ et $b \equiv 0[3]$.

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

On a $4xd = 3p$ et $2yd = 3q$, donc $(4xd)^2 - \left((2\alpha)^2 - 4\right)(2yd)^2 \equiv 0[9]$.

Or, $\left[(4\alpha m + 2)^2 - \left((2\alpha)^2 - 4\right)\left((2m)^2 - 4\right)\right] \equiv 6[9]$, donc $6d^2 \equiv 0[9]$, ou encore $2d^2 \equiv 0[3]$. Ainsi, $3|2d^2$, puis d'après le lemme de Gauss $3|d^2$, et toujours d'après le lemme de Gauss, $3|d$.

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

D'après la question 26b, il existe $u, v \in \mathbf{Z}$ tels que $\begin{cases} xd = 3u \\ 2yd = 3v \end{cases}$ car $4xd \equiv xd[3]$.

Par ailleurs, la question précédente nous assure de l'existence de $d' \in \mathbf{N}^*$ tel que $d = 3d'$.

Ainsi, $\begin{cases} xd' = u \\ 2yd' = v \end{cases}$ donc $\begin{cases} 2xd' \in \mathbf{Z} \\ 2yd' \in \mathbf{Z} \end{cases}$. Or, $2d' < 3d' = d$, ce qui contredit la minimalité de d.

27. Soient α et m deux éléments de Q tels que 2α et $2m$ appartiennent à 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

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

Supposons que de tels U et V existent. La conclusion de la partie **V** nous assure de l'existence de rationnels x et y tels que

$$\left(\alpha m + \frac{1}{2}\right)^2 - (\alpha^2 - 1)(m^2 - 1) = x^2 - Dy^2 \qquad (\star)$$

La relation $(\star)$ est impossible, grâce à la contradiction de la question précédente.

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 $SL_2(\mathbf{Z})$.

La conclusion de la question 25 nous assure que s'il existe $X, Y, Z \in SL_2(\mathbf{Z})$ telles que $X^3 + Y^3 = Z^3$, alors $\mathrm{Tr}\ X^3 \equiv 0[9]$, ainsi que $\mathrm{Tr}\ Y^3 \equiv 0[9]$ et $\mathrm{Tr}\ Z^3 \equiv 0[9]$.

On pose $U = X^3$ et $V = Y^3$. Puisque $\det(U) = 1$ et $\det(V) = 1$, et $\det(U+V) = \det(Z^3) = 1$, ainsi que $\mathrm{Tr}\ U \equiv 0[9]$ et $\mathrm{Tr}\ V \equiv 0[9]$, cela est en contradiction avec la question 27. Par conséquent, l'équation $X^3 + Y^3 = Z^3$ n'a pas de solutions dans $SL_2(\mathbf{Z})$. De même, si $n = 3\ell$ est divisible par 3, un triplet $(X, Y, Z) \in SL_2(\mathbf{Z})^3$ solution de $X^n + Y^n = Z^n$ fournirait une solution (X^ℓ, Y^ℓ, Z^ℓ) de l'équation de degré trois, ce qui est absurde.

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 $\mathcal{M}_p(\mathbf{C})$.

Soit M une matrice k-périodique de $\mathcal{M}_p(\mathbf{C})$, avec $k \in \mathbf{N}^*$. Le polynôme $X^k - 1 = \prod_{l=0}^{k-1}(X - \mathrm{e}^{\frac{2il\pi}{k}})$ est scindé à racines simples sur $\mathbf{C}$ et annule M, donc M 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,

Grâce au théorème de Cayley-Hamilton, on a $X^2 - \mathrm{Tr}\,(X)X + \det(X)I_2 = 0$, ce qui permet d'obtenir $X = -X^2 - I_2 = -A - I_2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} = B$. Une seule matrice X est donc candidate.

On vérifie enfin que $X^{12} = A^6 = B^3 = I_2$, ce qui prouve bien la 12-périodicité de X.

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

D'après la question précédente, $Y = A$ convient.

(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 $X^2 + Y^2 = Z^2$.

Rappelons que $C = A + B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2$. Ainsi, $X = B$, $Y = A$ et $Z = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ conviennent. On vérifie au passage que $Z^{12} = (Z^2)^6 = (-I_2)^6 = I_2$, donc Z est 12-périodique. On remarque bien que X, Y et Z sont dans $SL_2(\mathbf{Z})$.

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 $X^n + Y^n = Z^n$.

Soit $k \in \mathbf{Z}$. D'une part, on a $X^{2+12k} = X^2X^{12k} = X^2$, sachant que par inversibilité de la matrice X, le cas où $k < 0$ est licite. On procède de même pour Y et Z, ce qui donne $X^{2+12k} + Y^{2+12k} = Z^{2+12k}$ et fournit un triplet (X, Y, Z) solution. On remarque bien que X, Y et Z sont dans $SL_2(\mathbf{Z})$.

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 $X^n + Y^n = Z^n$.

On reprend un triplet (X, Y, Z) de matrices 12-périodiques, solution de $X^2 + Y^2 = Z^2$. On a donc $(X^{-1})^{-2} + (Y^{-1})^{-2} = (Z^{-1})^{-2}$. Comme dans la question précédente, on montre que le triplet (X^{-1}, Y^{-1}, Z^{-1}) est solution de $X^n + Y^n = Z^n$, pour $n \equiv -2[12]$. On remarque bien que X^{-1}, Y^{-1} et Z^{-1} sont dans $SL_2(\mathbf{Z})$, car par exemple $X^{-1} = \frac{1}{\det(X)}{}^t(Com(X)) = {}^t(Com(X))$ est à coefficients entiers et de déterminant 1.

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 $X^n + Y^n = Z^n$.

Puisque $A^1 + B^1 = C^1$, la 6-périodicité des matrices A, B et C permet de construire des solutions pour $n \equiv 1[6]$. Si $n \equiv 5[6]$, on procède de même avec (A^{-1}, B^{-1}, C^{-1}) puisque $A^6 = I_2$ et l'inversibilité de A donnent $A^5 = A^{-1}$. Pour les mêmes raisons que la question précédente, A^{-1}, B^{-1} et C^{-1} sont dans $SL_2(\mathbf{Z})$.

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 $X^n + Y^n = Z^n$.

Le bilan des résultat précédents donne :

- ▷ Pour $n \equiv 2, 10[12]$, l'équation admet des solutions,
- ▷ pour $n \equiv 1, 5, 7, 11[12]$, l'équation admet des solutions,
- ▷ pour $n \equiv 0, 3, 6, 9[12]$, l'équation n'admet pas de solutions d'après la conclusion de la partie **VI**.
- ▷ pour $n \equiv 0, 4, 8[12]$, l'équation n'admet pas de solutions d'après la conclusion de la partie **II**.

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

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

Si $n \geqslant 2$, on note

$$\mathbf{Q}^{n-1} \times \{0\} = \Big\{ (x_1, ..., x_{n-1}, 0) \;\Big|\; x_1, ..., x_{n-1} \in \mathbf{Q} \Big\}.$$

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

L'application $\varphi : \left\{ \begin{array}{ccc} (\mathbf{Z}^m, +) & \to & (\mathbf{Q}^n, +) \\ (k_1, ..., k_m) & \mapsto & \sum_{i=1}^m k_i v_i \end{array} \right.$.
est un morphisme de groupes d'image $\mathcal{R}$, donc $\mathcal{R}$ 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

$$\mathcal{R} = r\mathbf{Z} = \big\{ rk \;\big|\; k \in \mathbf{Z} \big\}.$$

Ce r est-il unique ?

Par définition, $\mathcal{R} = \left\{ \sum_{i=1}^n k_i v_i, (k_i)_{1 \leqslant i \leqslant m} \in \mathbf{Z}^m \right\}$ avec $(v_i)_{1 \leqslant i \leqslant m} \in \mathbf{Q}^m$. On note $v_i = \frac{p_i}{q_i}$ avec $(p_i)_{1 \leqslant i \leqslant n} \in \mathbf{Z}^m$, $(q_i)_{1 \leqslant i \leqslant n} \in (\mathbf{N}^*)^m$ sous forme fractionnaire. On pose enfin $q = \prod_{i=1}^m q_i$. Ainsi, $\mathcal{R} = \left\{ \frac{1}{q} \sum_{i=1}^n k_i p_i \left(\prod_{j \neq i} q_j \right), (k_i)_{1 \leqslant i \leqslant m} \in \mathbf{Z}^m \right\}$. On pose alors $m_i = p_i \left(\prod_{j \neq i} q_j \right) \in \mathbf{Z}$, et $\mathcal{R}' = \left\{ \sum_{i=1}^m k_i m_i, (k_i)_{1 \leqslant i \leqslant m} \in \mathbf{Z}^m \right\}$ est un sous-groupe additif de $\mathbf{Z}$, d'où l'existence de $m \in \mathbf{Z}$ tel que $\mathcal{R}' = m\mathbf{Z}$. Enfin, $\mathcal{R} = \frac{1}{q}\mathcal{R}' = \frac{m}{q}\mathbf{Z}$.

Dans le cadre de l'énoncé, on a : $\mathcal{R} \neq \{0\}$ auquel cas un rationnel r tel que $\mathcal{R} = r\mathbf{Z}$ est non nul et son opposé donnent deux solutions distinctes. On peut facilement prouver l'unicité de r en le supposant positif.

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

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

L'application π est un morphisme de groupes additifs, donc $\pi(\mathcal{R}) = \left\{ \sum_{i=1}^m k_i \pi(v_i),\ (k_i)_{1 \leqslant i \leqslant m} \in \mathbf{Z}^m \right\}$. D'après la question 36, puisque $\pi(\mathcal{R}) \subset \mathbf{Q}$, il existe $r \in \mathbf{Q}$ tel que $\pi(\mathcal{R}) = r\mathbf{Z}$. Ainsi, $r = r \times 1 \in \pi(\mathcal{R})$, donc il existe $\omega \in \mathcal{R}$ tel que $r = \pi(\omega)$, ce qui donne finalement $\pi(\mathcal{R}) = \pi(\omega)\mathbf{Z}$.

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 $x = qw + \widetilde{x}$.

Grâce à la question 37, $\pi(x) \in \pi(\mathcal{R}) = \pi(\omega)\mathbf{Z}$. Ainsi, il existe $q \in \mathbf{Z}$ tel que $\pi(x) = \pi(\omega)q = \pi(q\omega)$ car π est un morphisme de groupes. Ainsi, $\pi(x - q\omega) = 0$, on pose donc $\widetilde{x} = x - qw$ qui est donc dans $\mathbf{Q}^{n-1} \times \{0\}$, mais aussi dans $\mathcal{R}$, car ce dernier ensemble est un groupe.

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

On conserve les notations de la question précédente.

▷ Premier cas : $\pi(\mathcal{R}) = \{0\}$, donc $\omega = 0$ puis $x = \widetilde{x}$ et $\widetilde{x}$ est unique. Dans ce cas, tout $q \in \mathbf{Z}$ convient dans la décomposition précédente donc q n'est pas unique.

▷ Second cas : $\pi(\mathcal{R}) \neq \{0\}$. Alors, $q = \frac{\pi(x)}{\pi(\omega)}$ est unique, puis $\widetilde{x} = x - \frac{\pi(x)}{\pi(\omega)}\omega$ est unique. Dans ce cas, soulignons que q est unique.

39. Démontrer que l'on a

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

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

Soit $x \in \mathcal{R} \cap (\mathbf{Q}^{n-1} \times \{0\})$. Par définition de $\mathcal{R}$, il existe $(k_i)_{1 \leqslant i \leqslant m} \in \mathbf{Z}^m$ que l'on fixe tels que $x = \sum_{i=1}^m k_i v_i$. On a ensuite : $\forall i \in [\![1, m]\!]$, $v_i = p_i\omega + \widetilde{v}_i$ avec $(p_i)_{1 \leqslant i \leqslant m} \in \mathbf{Z}^m$.
Ainsi, $x = \left(\sum_{i=1}^m k_i p_i\right)\omega + \sum_{i=1}^m k_i \widetilde{v}_i$, et $x = 0 \cdot \omega + x$, ainsi $x = \widetilde{x}$, et par unicité de $\widetilde{x}$, comme $\sum_{i=1}^m k_i \widetilde{v}_i \in \left(\mathbf{Q}^{n-1} \times \{0\}\right) \cap \mathcal{R}$ car cet ensemble est un groupe en tant qu'intersection de deux sous-groupes de $\mathbf{Q}^n$, on en déduit finalement $x = \widetilde{x} = \sum_{i=1}^m k_i \widetilde{v}_i$, d'où l'inclusion $\mathcal{R} \cap (\mathbf{Q}^{n-1} \times \{0\}) \subset \mathbf{Z}\widetilde{v_1} + ... + \mathbf{Z}\widetilde{v_m}$. L'autre inclusion est immédiate, car tous les $\widetilde{v}_i$ sont dans $\mathcal{R} \cap (\mathbf{Q}^{n-1} \times \{0\})$ et ce dernier ensemble est un groupe additif.

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 $x = \sum_{i=1}^{p} k_i u_i$.

▷ **Initialisation :** le cas $n = 1$ correspond au cas de la question 36 avec $u_1 = r$.
▷ **Hérédité :** supposons la propriété vraie à un rang n entier naturel non nul.
— **Premier cas :** si $\mathcal{R} \subset \mathbf{Q}^n \times \{0\}$, on peut utiliser l'hypothèse de récurrence pour $\mathbf{Q}^n$.
— **Second cas :** supposons $\mathcal{R} \not\subset \mathbf{Q}^n \times \{0\}$. En reprenant les notations des questions précédentes à partir de $\mathbf{Q}^{n+1}$, $\pi(\mathcal{R}) \neq \{0\}$. Il existe donc $\omega \in \mathcal{R} \setminus \{0\}$ tel que $\pi(\mathcal{R}) = \pi(\omega)\mathbf{Z}$ et $\pi(\omega) \neq 0$. En utilisant le second cas de la question 38b, la décomposition $x = p\omega + \widetilde{x}$ est unique pour $(p, \widetilde{x}) \in \mathbf{Z} \times ((\mathbf{Q}^n \times \{0\}) \cap \mathcal{R})$.
On applique l'hypothèse de récurrence à $(\mathbf{Q}^n \times \{0\}) \cap \mathcal{R} = \left\{\sum_{i=1}^m k_i \widetilde{v_i},\ k_1, ..., k_m \in \mathbf{Z}\right\}$ qui a bien la forme voulue, il existe $(u_j)_{2 \leqslant j \leqslant p}$ une $\mathbf{Z}$-base de $(\mathbf{Q}^n \times \{0\}) \cap \mathcal{R}$. Ainsi, on en déduit que $\widetilde{x}$ se décompose de manière unique sous la forme $\widetilde{x} = \sum_{i=2}^p \ell_i u_i$ avec $(\ell_i)_{2 \leqslant i \leqslant p} \in \mathbf{Z}^{p-1}$, et donc x se décompose de façon unique sous la forme $x = \sum_{i=2}^p \ell_i u_i + p\omega$. En posant $\omega = u_1$ on en déduit directement que $(u_i)_{1 \leqslant i \leqslant m}$ est une $\mathbf{Z}$-base de $\mathcal{R}$, ce qui achève la récurrence.

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

Démontrons que $(u_i)_{1 \leqslant i \leqslant p}$ est libre et génératrice dans $\mathbf{Q}^n$.

▷ Soit $(\lambda_i)_{1 \leqslant i \leqslant p} \in \mathbf{Q}^p$ tels que $\sum_{i=1}^p \lambda_i u_i = 0$. Soit K un dénominateur commun à tous les λ_i, on note $\forall i \in [\![1, p]\!]$, $\lambda_i = \frac{\mu_i}{K}$ avec $(\mu_i)_{1 \leqslant i \leqslant p} \in \mathbf{Z}^p$. Ainsi, $\sum_{i=1}^p \mu_i u_i = 0$. Or, $0 \in \mathcal{R}$, et par unicité de la décomposition établie à la question précédente, tous les μ_i sont nuls, ce qui termine la preuve de la liberté de la famille $(u_i)_{1 \leqslant i \leqslant p}$.
▷ Soit $x \in \mathbf{Q}^n$. Il existe par hypothèse $(\alpha_i)_{1 \leqslant i \leqslant m} \in \mathbf{Q}^m$ tels que $x = \sum_{i=1}^m \alpha_i v_i$. Or, pour tout $i \in [\![1, m]\!]$, il existe $(\gamma_{i,j})_{1 \leqslant j \leqslant p} \in \mathbf{Z}^p$ tel que $v_i = \sum_{j=1}^p \gamma_{i,j} u_j$. Ainsi, $x = \sum_{i=1}^m \alpha_i v_i = \sum_{i=1}^m \sum_{j=1}^p \alpha_i \gamma_{i,j} u_j = \sum_{j=1}^p \left(\sum_{i=1}^m \alpha_i \gamma_{i,j}\right) u_j$. Notons que pour tout $j \in [\![1, p]\!]$, $\sum_{i=1}^m \alpha_i \gamma_{i,j} \in \mathbf{Q}$, ce qui prouve que la famille $(u_i)_{1 \leqslant i \leqslant p}$ engendre $\mathbf{Q}^n$. En conclusion, $(u_i)_{1 \leqslant i \leqslant p}$ est une base du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}^n$, donc $n = p$.

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 $(e_1, ..., e_p)$ 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

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

où

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

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

Le sous-groupe G de $SL_p(\mathbf{Q})$ contient I_p, ainsi $\forall i \in [\![1, p]\!], I_p e_i = e_i \in H$.

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

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

Soit $A = \{Me_i,\ M \in G,\ i \in [\![1, p]\!]\}$. Par hypothèse, $< A >= H$.

Soit $N \in G$. Par structure de groupe de G, $\forall M \in G,\ \forall i \in [\![1, p]\!], NMe_i \in A$ car $NM \in G$. Ainsi, $NA \subset A$, puis $NA \subset H$. Soit $X \in H \setminus \{0\}$. Il existe $\ell \in \mathbf{N}^*$, $(A_i)_{1 \leqslant i \leqslant p} \in A^\ell$ et $(\varepsilon_i)_{1 \leqslant i \leqslant \ell} \in \{1, -1\}^\ell$ tels que $X = \sum_{i=1}^{\ell} \varepsilon_i A_i$. Par conséquent, $NX = \sum_{i=1}^{\ell} \varepsilon_i NA_i \in H$ car H est un groupe additif. Ainsi, $NH \subset H$, donc H est stable par N et donc par G.

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

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

Soit $j \in [\![1, p]\!]$. Le vecteur Me_j est un élément de $\mathbf{Q}^p$ qui admet $(e_j)_{1 \leqslant j \leqslant p}$ comme base, donc il existe $(k_i)_{1 \leqslant i \leqslant p} \in \mathbf{Q}^p$ tels que $Me_j = \sum_{i=1}^{p} k_i e_i$.

Or, $dM \in M_p(\mathbf{Z})$, et dMe_j représente la j-ème colonne de dM ce qui s'écrit $dMe_j = \sum_{i=1}^{p} dk_i e_i$ avec $\forall i \in [\![1, p]\!], dk_i \in \mathbf{Z}$. On pose ensuite pour $i \in [\![1, p]\!]$, $dk_i = dq_i + r_i$ avec $r_i \in [\![0, d-1]\!]$ et $q_i \in \mathbf{Z}$ la division euclidienne de $dk_i \in \mathbf{Z}$ par d. Cela donne enfin $Me_j = \sum_{i=1}^{p} q_i e_i + \sum_{i=1}^{p} \frac{r_i}{d} e_i$

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

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

On conserve les notations de la question précédente. Soit $j \in [\![1,p]\!]$. Comme $(e_i)_{1\leqslant i\leqslant p} \in H$, et $Me_j \in H$, le fait que H soit un groupe et la question précédente donnent : $\sum_{i=1}^{p} \frac{r_i}{d} e_i \in H$.
Posons $B = \left\{e_1,\dots,e_p\right\} \cup \{\sum_{i=1}^{p} \frac{r_i}{d} e_i,\ \forall i \in [\![1,p]\!], r_i \in [\![0,d-1]\!] \text{ et } \sum_{i=1}^{p} \frac{r_i}{d} e_i \in H\}$. L'ensemble B est bien un ensemble fini car les r_i varient dans $[\![0,d-1]\!]$. De plus, $A \subset < B >$ grâce à la remarque initiale et à la question précédente. Ainsi, $< A > \subset < B >$ car $< A >$ est le plus petit sous-groupe additif de $\mathbf{Q}^p$ contenant A.
Par ailleurs, $(e_i)_{1\leqslant i\leqslant p} \in A$, et par définition de $\sum_{i=1}^{p} \frac{r_i}{d} e_i$ et de B, on a donc $B \subset H =< A >$. En conclusion, $< B > \subset < A >$ car $< B >$ est le plus petit sous-groupe de $\mathbf{Q}^n$ contenant B, ainsi $H =< A > =< B >$.
L'ensemble B contient la base canonique de $\mathbf{Q}^p$.
Ainsi, $\mathbf{Q}^p = \text{vect}_{\mathbf{Q}}(e_1,\dots,e_p) \subset \text{vect}_{\mathbf{Q}}(B) \subset \mathbf{Q}^p$, donc $\text{vect}_{\mathbf{Q}}(B) = \mathbf{Q}^p$.

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

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

On reprend les notations de la question précédente et on prend $\mathcal{R} = H =< B >$. En appliquant les résultats des questions 40 et 41 de la partie précédente (car $\text{vect}_{\mathbf{Q}}(B) = \mathbf{Q}^p$), il existe une $\mathbf{Z}$-base $(u_i)_{1\leqslant i\leqslant p}$ de H telle que $(u_i)_{1\leqslant i\leqslant p}$ soit une base de $\mathbf{Q}^p$.
Par ailleurs, : $\forall i \in [\![1,p]\!],\ u_i \in H = \oplus_{i=1}^{p} \mathbf{Z}u_i$, et comme H est stable par G d'après la question 42b, alors $\forall i \in [\![1,p]\!],\ \forall M \in G,\ Mu_i \in H = \oplus_{i=1}^{p} \mathbf{Z}u_i$.

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

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

Soit F la matrice de passage de la base $(e_i)_{1\leqslant i\leqslant p}$ à la base $(u_i)_{1\leqslant i\leqslant p}$. Soit $M \in G$. La matrice $F^{-1}MF$ est la matrice de l'endomorphisme canoniquement associé à M dans la base $(u_i)_{1\leqslant i\leqslant p}$ que l'on note f. Or, grâce à la question précédente, $\forall j \in [\![1,p]\!],\ \exists (m_{i,j})_{1\leqslant i\leqslant p} \in \mathbf{Z}^p,\ f(u_j) = \sum_{i=1}^{p} m_{i,j} u_i$. En conclusion, la matrice de f dans la base des (u_i) est à coefficients entiers, donc $F^{-1}MF \in M_p(\mathbf{Z})$. Or, $\det(M) = 1$, donc $\det(F^{-1}MF) = 1$, ce qui donne enfin $\forall M \in G,\ F^{-1}MF \in SL_p(\mathbf{Z})$.

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

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

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

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

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

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

Grâce au théorème de Cayley-Hamilton, on écrit $A^2 = \mathrm{Tr}\,(A)A - \det(A)I_2$. Par hypothèse, $\det(A) = 1$, et puisque A est inversible, cela donne $A^{-1} = \mathrm{Tr}\,(A)I_2 - A \in K$. On raisonne de même pour B.

(b) Démontrer que $G \subset K$.

L'ensemble G est constitué de toutes les multiplications possibles par A, B, A^{-1}, B^{-1}. Il suffit donc de démontrer que K est stable par multiplication par ces matrices.

- ▷ Pour la multiplication à gauche par A, il suffit de prouver que A^2B, A^2BA, A^2 et $ABAB$ restent dans K. Or, $A^2 = \mathrm{Tr}\,(A)A - I_2$ donc A^2B, A^2 et A^2BA restent dans K. De même $ABAB = (AB)^2 = \mathrm{Tr}\,(AB)AB - I_2$ montre que $ABAB$ est dans K.
- ▷ On procède de même pour la multiplication à droite par A, et à gauche et à droite par B.
- ▷ Puisque $A^{-1} = \mathrm{Tr}\,(A)I_2 - A$, on prouve de même que K est stable par la multiplication par A^{-1} à droite et à gauche, puis par B^{-1}.

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

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

Il existe $d \in \mathbf{N}^*$ tel que $dI_2, dA, dB, dAB, dBA, dABA, dBAB$ soient toutes à coefficients entiers en prenant un dénominateur commun de toutes les matrices I_2, A, B, AB, BA, ABA et BAB. Ainsi, $dK \subset M_2(\mathbf{Z})$, par suite $dG \subset M_2(\mathbf{Z})$.

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 $\mathbf{Z}$.**

- ▷ Supposons **i)** vérifiée. Alors, $\mathrm{Tr}\,(A) = \mathrm{Tr}\,(F^{-1}AF) \in \mathbf{Z}$ car $F^{-1}AF$ est à coefficients entiers. De même, $\mathrm{Tr}\,(B) \in \mathbf{Z}$. Par ailleurs, $\det(A+B) = \det\left(F^{-1}(A+B)F\right) = \det\left(F^{-1}AF + F^{-1}BF\right) \in \mathbf{Z}$ car $F^{-1}AF + F^{-1}BF$ est également à coefficients entiers, d'où **ii)**.
- ▷ Supposons **ii)**. Prouvons que $\mathrm{Tr}\,(AB) \in \mathbf{Z}$. Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} u & v \\ w & x \end{pmatrix}$, alors $AB = \begin{pmatrix} au+bw & * \\ * & cv+dx \end{pmatrix}$ alors $\det(A+B) = (a+u)(d+x) - (c+w)(b+u) = (ad-bc) + (ux - vw) + ax + ud - cv - bw$. Or $ad - bc = ux - vw = 1$, ce qui donne $\det(A+B) = 2 + ax + au + ud + dx - \mathrm{Tr}\,(AB) = 2 + \mathrm{Tr}\,(A)\,\mathrm{Tr}\,(B) - \mathrm{Tr}\,(AB)$, d'où $\mathrm{Tr}\,(AB) = 2 + \mathrm{Tr}\,(A)\,\mathrm{Tr}\,(B) - \det(A+B)$, d'où $\mathrm{Tr}\,(AB) \in \mathbf{Z}$. Or, par hypothèse, $\mathrm{Tr}\,(A), \mathrm{Tr}\,(B) \in \mathbf{Z}$, donc d'après la question 43c, il existe $d \in \mathbf{N}^*$ tel que $\forall M \in G,\ dM \in M_2(\mathbf{Z})$. La question 42f nous assure alors de l'existence de $F \in GL_2(\mathbf{Q})$ tel que : $\forall M \in G,\ F^{-1}MF \in SL_2(\mathbf{Z})$. En particulier, cela assure que $F^{-1}AF, F^{-1}BF \in SL_2(\mathbf{Z})$, ce qui prouve bien **i)** et termine la preuve de l'équivalence.

(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 $X_1^n + Y_1^n = Z_1^n$.

Le polynôme caractéristique de X s'écrit $\chi_X(T) = T^2 - \mathrm{Tr}\,(X)T + 1$. La division euclidienne de T^n par χ_X ne va faire intervenir qu'un quotient et un reste à coefficients entiers car T^n et