Notations et définitions

Selon l'usage, les corps sont supposés commutatifs. Dans tout le problème, n est un élément de $\mathbb{N}^*$, $\mathbb{K}$ est un corps.

Si $\mathbb{A}$ est un sous-anneau d'un corps, si p et q sont des éléments de $\mathbb{N}^*$, on note $\mathcal{M}_{p,q}(\mathbb{A})$ l'ensemble des matrices à p lignes et q colonnes à coefficients dans $\mathbb{A}$. On abrège $\mathcal{M}_{p,p}(\mathbb{A})$ en $\mathcal{M}_p(\mathbb{A})$; la matrice identité de $\mathcal{M}_p(\mathbb{A})$ est notée I_p. Le groupe des inversibles de l'anneau $\mathcal{M}_p(\mathbb{A})$ est noté $GL_p(\mathbb{A})$. Pour m dans $\mathbb{N}$, on note $U_m(\mathbb{A})$ l'ensemble des polynômes unitaires de $\mathbb{A}[X]$.

Deux matrices M et N de $\mathcal{M}_n(\mathbb{A})$ sont dites semblables sur $\mathbb{A}$ si, et seulement si, il existe P dans $GL_n(\mathbb{A})$ telle que :

$$N = PMP^{-1}$$

La relation de similitude sur $\mathcal{M}_n(\mathbb{A})$ est une relation d'équivalence. Les classes de cette relation sont appelées classes de similitude sur $\mathbb{A}$; pour $\mathbb{A} = \mathbb{Z}$, on les appellera également classes de similitude entière.

Pour M dans $\mathcal{M}_n(\mathbb{K})$, soit χ_M le polynôme caractéristique (unitaire) de M :

$$\chi_M(X) = \det(XI_n - M)$$

Pour P dans $U_n(\mathbb{K})$, soit $\mathcal{E}_{\mathbb{K}}(P)$ l'ensemble des matrices M de $\mathcal{M}_n(\mathbb{K})$ telles que $\chi_M = P$. Puisque deux matrices semblables dans $\mathcal{M}_n(\mathbb{K})$ ont même polynôme caractéristique, $\mathcal{E}_{\mathbb{K}}(P)$ est une réunion de classes de similitude sur $\mathbb{K}$.

Il est clair que si M est dans $\mathcal{M}_n(\mathbb{Z})$, χ_M est dans $U_n(\mathbb{Z})$. Si P est dans $U_n(\mathbb{Z})$, on note $\mathcal{E}_{\mathbb{Z}}(P)$ l'ensemble des matrices M de $\mathcal{M}_n(\mathbb{Z})$ telles que $\chi_M = P$; cet ensemble est une réunion de classes de similitude entière. On note $\mathcal{D}_{\mathbb{Z}}(P)$ l'ensemble des matrices de $\mathcal{E}_{\mathbb{Z}}(P)$ diagonalisables sur $\mathbb{C}$.

Si P est le polynôme $X^n - a_{n-1}X^{n-1} - \cdots - a_1X - a_0$ de $\mathbb{K}[X]$, on note $C(P)$ la matrice compagnon de P, c'est-à-dire :

$$C(P) = \begin{pmatrix} 0 & \cdots & 0 & a_0 \\ 1 & \ddots & \vdots & a_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & a_{p-1} \end{pmatrix} \text{ si } n \geq 2 \text{ et } (a_0) \text{ si } n = 1$$

– I – Préliminaires

– A – Matrices à coefficients dans $\mathbb{K}$

1.

(a) Pour quels (a, b, c) de $\mathbb{K}^3$, la matrice $M = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ est-elle diagonalisable sur $\mathbb{K}$?

(b) Si $a \neq c$ et b quelconque dans $\mathbb{K}$, la matrice M est alors triangulaire supérieure dans $\mathcal{M}_2(\mathbb{K})$ avec deux valeurs propres distinctes, elle est donc diagonalisable.
Si $a = c$, elle est diagonalisable si, et seulement si, $b = 0$. En effet, pour $b = 0$, elle est diagonale et pour $b \neq 0$, a est valeur propre double de M et l'équation $MX = X$ équivaut à $by = 0$, soit à $y = 0$. L'espace propre associé à l'unique valeur propre a de M est donc la droite $D = R\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et M n'est pas diagonalisable.

(c) Trouver deux matrices de $\mathcal{M}_2(\mathbb{K})$ non semblables sur $\mathbb{K}$ et ayant même polynôme caractéristique.

(d) Pour a, b dans $\mathbb{K}$, avec $b \neq 0$, les matrices $M = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ et $N = aI_2$ ont le même polynôme caractéristique, $\chi_M(X) = (X-a)^2$ et ne peuvent être semblables puisque N est diagonalisable et M ne l'est pas (ou bien le polynôme minimal de M est $(X-a)^2$ et celui de N, $X-a$).

(e) Soient M et M' deux éléments de $\mathcal{M}_n(\mathbb{K})$ diagonalisables sur $\mathbb{K}$ et telles que $\chi_M = \chi_{M'}$. Montrer que M et M' sont semblables sur $\mathbb{K}$.

(f) Une matrice $M \in \mathcal{M}_n(\mathbb{K})$ diagonalisable a un polynôme caractéristique scindé, $\chi_M(X) = \prod_{k=1}^{p} (X-\lambda_k)^{\alpha_k}$, où les λ_k sont deux à deux distincts dans $\mathbb{K}$ et les α_k sont des entiers naturels non nuls, le polynôme minimal étant $\pi_M(X) = \prod_{k=1}^{p} (X-\lambda_k)$. L'égalité $\chi_M = \chi_{M'}$ avec M, M' diagonalisables sur $\mathbb{K}$, nous dit alors que $\pi_M = \pi_{M'}$, ces deux polynômes étant scindés à racines simples. Il en résulte que M et M' sont diagonalisables avec les mêmes valeurs propres, elles sont donc semblables à une même matrice diagonale et conséquence semblables entre elles.

2. Soit P dans $U_n(\mathbb{K})$.

(a) Montrer que $\chi_{C(P)} = P$.

(b) En notant $P_{(a_0,\cdots,a_{n-1})}(X) = \det(XI_n - C(P))$ le polynôme caractéristique de $C(P)$ et en le développant par rapport à la première ligne, on a :

$$P_{(a_0,\cdots,a_{n-1})}(X) = \begin{vmatrix} X & \cdots & 0 & -a_0 \\ -1 & \ddots & \vdots & -a_1 \\ \vdots & \ddots & X & \vdots \\ 0 & \cdots & -1 & X-a_{n-1} \end{vmatrix} = X \cdot P_{(a_1,\cdots,a_{n-1})}(X) - a_0$$

et par récurrence $P_{(a_0,\cdots,a_{n-1})}(X) = X^p - \sum_{k=0}^{n-1} a_k X^k = P(X)$.

b. bis On peut en fait vérifier que P est le polynôme caractéristique et aussi le polynôme minimal de $C(P)$.

On désigne par E l'espace vectoriel quotient $\dfrac{\mathbb{K}[X]}{(P)}$, où $(P) = \mathbb{K}[X] \cdot P$ est l'idéal engendré par P et $u \in \mathcal{L}(E)$ est défini par :

$$\forall \overline{A} \in E,\ u\left(\overline{A}\right) = \overline{XA}$$

i. Par division euclidienne, tout polynôme $A \in \mathbb{K}[X]$ s'écrit $A = PQ + R$ avec $R \in \mathbb{K}_{n-1}[X]$ et $\overline{P} = \overline{R} = \sum_{k=0}^{n-1} \alpha_k \overline{X^k}$, donc $\left(\overline{X^k}\right)_{0 \leq k \leq n-1}$ est une famille génératrice de E.

Dire que $\sum_{k=0}^{n-1} \alpha_k \overline{X^k} = \overline{0}$ dans E équivaut à dire que $R = \sum_{k=0}^{n-1} \alpha_k X^k$ est multiple

de P, donc nul à cause des degré, ce qui revient à dire que tous les α_k sont nuls. La famille $\mathcal{B} = \left(\overline{X^k}\right)_{0\leq k\leq n-1}$ est donc une base de E et $\dim(E) = n = \deg(P)$.
On notons $e_k = \overline{X^{k-1}}$ pour k compris entre 1 et n.

ii. Avec $u(e_k) = u\left(\overline{X^{k-1}}\right) = \overline{X^k} = e_{k+1}$ pour $1 \leq k \leq n-1$ et :

$$u(e_n) = u\left(\overline{X^{n-1}}\right) = \overline{X^n} = \sum_{k=0}^{n-1} a_k \overline{X^k} = \sum_{k=1}^{n} a_{k-1} e_k$$

(qui résulte de $\overline{P} = \overline{0}$), on voit que $C(P)$ est la matrice de u dans la base $\mathcal{B}$.

iii. On a $e_k = u^{k-1}(e_1)$ pour $1 \leq k \leq n$ et :

$$\left(u^n - \sum_{k=1}^{n} a_{k-1} u^{k-1}\right)(e_1) = 0$$

$$\left(u^n - \sum_{k=1}^{n} a_{k-1} u^{k-1}\right)(e_j) = u^{j-1}\left(\left(u^n - \sum_{k=1}^{n} a_{k-1} u^{k-1}\right)(e_1)\right) = 0$$

pour $1 \leq j \leq n$, ce qui signifie que u est annulé par P. Le polynôme minimal $\pi_{C(P)} = \pi_u$ divise donc P. Si π_u est de degré $p < n$, u^p est alors combinaison linéaire de $Id, u, \cdots, u^{p-1}$, donc $e_{p+1} = u^p(e_1)$ est combinaison linéaire de $e_1, e_2, \cdots, e_p$, ce qui n'est pas. On a donc $p = n$ et $\pi_{C(P)} = \pi_u = P$.

iv. Le théorème de Cayley-Hamilton nous dit $\pi_{C(P)}$ est unitaire de degré n divisant le polynôme caractéristique lui aussi unitaire de degré n, donc ces polynômes sont égaux.
En définitive, $\chi_{C(P)} = \pi_{C(P)} = P$.

(c) Si λ est dans $\mathbb{K}$, montrer que le rang de $C(P) - \lambda I_n$ est supérieur ou égal à $n-1$.

(d) Pour $n \geq 2$, on a :

$$C(P) = \begin{pmatrix} 0_{1,n-1} & a_0 \\ I_{n-1} & \beta \end{pmatrix}$$

où $0_{1,n-1}$ est le vecteur nul de $\mathcal{M}_{1,n-1}(\mathbb{K})$ et $\beta \in \mathcal{M}_{n-1,1}(\mathbb{K})$, donc pour tout $\lambda \in \mathbb{K}$:

$$C(P) - \lambda I_n = \begin{pmatrix} \alpha_\lambda & a_0 \\ T_{n-1}(\lambda) & \beta_\lambda \end{pmatrix}$$

où $\alpha_\lambda = (-\lambda, 0_{1,n-2}) \in \mathcal{M}_{1,n-1}(\mathbb{K})$, $\beta_\lambda \in \mathcal{M}_{n-1,1}(\mathbb{K})$ et $T_{n-1}(\lambda) \in \mathcal{M}_{n-1}(\mathbb{K})$ est triangulaire supérieure avec la diagonale formée de 1. On a donc $\det(T_{n-1}(\lambda)) = 1 \neq 0$ et la matrice $C(P)$ est de rang au moins égal à $n-1$. Précisément, ce rang est $n-1$ si λ est valeur propre de $C(P)$ et n sinon.
Pour $n = 1$, $C(P) - \lambda I_1 = (a_0 - \lambda)$ est de rang 0 ou 1.

(e) Montrer l'équivalence entre les trois assertions suivantes :

i. le polynôme P est scindé sur $\mathbb{K}$ à racines simples ;

ii. toutes les matrices de $\mathcal{E}_{\mathbb{K}}(P)$ sont diagonalisables sur $\mathbb{K}$;

iii. $C(P)$ est diagonalisable sur $\mathbb{K}$.

(f)

$(i) \Rightarrow (ii)$ Si P est scindé sur $\mathbb{K}$ à racines simples, il en est de même de $\chi_M = P$ pour toute matrice $M \in \mathcal{E}_{\mathbb{K}}(P)$ et M est diagonalisable sur $\mathbb{K}$.

$(ii) \Rightarrow (iii)$ Si toutes les matrices de $\mathcal{E}_{\mathbb{K}}(P)$ sont diagonalisables sur $\mathbb{K}$, la matrice $C(P)$ qui est dans $\mathcal{E}_{\mathbb{K}}(P)$ (puisque $\chi_{C(P)} = P$) est diagonalisable.

$(iii) \Rightarrow (i)$ Si $C(P)$ est diagonalisable, son polynôme caractéristique $\chi_{C(P)} = P$ est scindé sur $\mathbb{K}$. Si $\lambda \in \mathbb{K}$ est une valeur propre de $C(P)$, le rang de $C(P) - \lambda I_n$ vaut $n-1$, donc l'espace propre associé est de dimension 1. Les valeurs propres de $C(P)$ sont donc toutes simples. En définitive $P = \chi_{C(P)}$ est scindé sur $\mathbb{K}$ à racines simples.

3. Soient r et s dans $\mathbb{N}^*$, A dans $\mathcal{M}_r(\mathbb{K})$, A' dans $\mathcal{M}_s(\mathbb{K})$, $M = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}$.
   Montrer que M est diagonalisable sur $\mathbb{K}$ si, et seulement si, A et A' sont diagonalisables sur $\mathbb{K}$.

4. Si M est diagonalisable sur $\mathbb{K}$, son polynôme minimal π_M est scindé sur $\mathbb{K}$ à racines simples et avec :
$$0 = \pi_M(M) = \begin{pmatrix} \pi_M(A) & 0 \\ 0 & \pi_M(A') \end{pmatrix}$$
   on déduit que A et A' sont annulées par un polynôme scindé sur $\mathbb{K}$ à racines simples, elles sont donc diagonalisables.
   Réciproquement si A, A' sont diagonalisables sur $\mathbb{K}$, il existe alors $P \in GL_r(\mathbb{K})$, $Q \in GL_s(\mathbb{K})$ telles que $P^{-1}AP$ et $Q^{-1}A'Q$ soient diagonales. La matrice $R = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}$ est alors inversible et :
$$R^{-1}MR = \begin{pmatrix} P^{-1} & 0 \\ 0 & Q^{-1} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix} = \begin{pmatrix} P^{-1}AP & 0 \\ 0 & Q^{-1}A'Q \end{pmatrix}$$
   est diagonale.
   Ce résultat est en fait valable pour une matrice diagonale à r blocs, c'est-à-dire qu'une matrice diagonale par blocs $M = \operatorname{diag}(A_1, \cdots, A_r)$, où $A_k \in \mathcal{M}_{r_k}(\mathbb{K})$ pour tout k, est diagonalisable sur $\mathbb{K}$ si, et seulement si, toutes les matrices A_k sont diagonalisables sur $\mathbb{K}$.

5. Montrer que, pour tout P de $U_n(\mathbb{K})$, l'ensemble $\mathcal{E}_{\mathbb{K}}(P)$ est une réunion finie de classes de similitude sur $\mathbb{K}$. On pourra admettre et utiliser le résultat suivant [1].
   « Si M est dans $\mathcal{M}_n(\mathbb{K})$, il existe r dans $\mathbb{N}^*$ et r polynômes unitaires non constants $P_1, \cdots, P_r$ de $\mathbb{K}[X]$ tels que M soit semblable sur $\mathbb{K}$ à une matrice diagonale par blocs dont les blocs diagonaux sont $C(P_1), \cdots, C(P_r)$. »

6. Le théorème de Frobénius nous dit qu'une matrice $M \in \mathcal{E}_{\mathbb{K}}(P)$ est semblable à une matrice de la forme :
$$F = \begin{pmatrix} C(P_1) & 0 & \cdots & 0 \\ 0 & C(P_2) & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & C(P_r) \end{pmatrix}$$

1. c'est la décomposition de Frobénius

elle est donc dans la classe de similitude de F. Le polynôme caractéristique de F est :

$$P = \chi_F = \prod_{k=1}^{r} \chi_{C(P_k)} = \prod_{k=1}^{r} P_k$$

Dans l'anneau factoriel $\mathbb{K}[X]$, il n'y a qu'un nombre fini de polynômes unitaires P_k tels que $P = \prod_{k=1}^{r} P_k$, ce qui ne laisse qu'un nombre fini de possibilités pour F.
L'ensemble $\mathcal{E}_{\mathbb{K}}(P)$ est donc une réunion finie de classes de similitude sur $\mathbb{K}$.

– B – Polynômes

1. Soient P dans $\mathbb{K}[X]$, a dans $\mathbb{K}$ une racine de P. Montrer que a est racine simple de P si, et seulement si, $P'(a) \neq 0$.
2. Dire que a est racine de P signifie qu'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)Q(X)$ et cette racine est simple si, et seulement si, $Q(a) \neq 0$, ce qui équivaut encore à $P'(a) \neq 0$, puisque $P'(X) = Q(X) + (X-a)Q'(X)$ et $P'(a) = Q(a)$.
3. Soit P un élément irréductible de $\mathbb{Q}[X]$. Montrer que les racines de P dans $\mathbb{C}$ sont simples.
4. Si P est irréductible dans $\mathbb{Q}[X]$, on a alors $P \wedge P' = 1$ dans $\mathbb{Q}[X]$ (de manière générale $P \wedge Q = 1$ pour Q non nul de degré strictement inférieur à n) et le théorème de Bézout nous dit qu'il existe deux polynômes U, V dans $\mathbb{Q}[X]$ tels que $UP + VP' = 1$. Si $a \in \mathbb{C}$ est une racine de P, on a alors $V(a)P'(a) = 1$, donc $P'(a) \neq 0$ et a est racine simple de P.
5. Soient P et Q dans $\mathbb{Q}[X]$, unitaires, tels que P appartienne à $\mathbb{Z}[X]$ et que Q divise P dans $\mathbb{Q}[X]$. Montre que Q appartient à $\mathbb{Z}[X]$. On pourra admettre et utiliser le lemme de Gauss suivant.
« Si U est dans $\mathbb{Z}[X] \setminus \{0\}$, soit $c(U)$ le pgcd des coefficients de U.[2] Alors pour tout couple (U, V) d'éléments de $\mathbb{Z}[X] \setminus \{0\}$: $c(UV) = c(U)c(V)$. »
6. On a $P = QR$ unitaire $\mathbb{Z}[X]$ avec Q, R unitaires dans $\mathbb{Q}[X]$.
Après réduction au même dénominateur des coefficients de Q et R, on peut écrire que $Q = \frac{1}{m}Q_1$, $R = \frac{1}{m}R_1$, avec m dans $\mathbb{N}^*$ et Q_1, R_1 dans $\mathbb{Z}[X]$ de coefficient dominant égal à m (Q et R sont unitaires). On a alors $m^2QR = Q_1R_1$ dans $\mathbb{Z}[X]$ et on peut écrire :

$$c\left(m^2QR\right) = m^2c(QR) = c(Q_1)c(R_1)$$

avec $c(QR) = 1$ puisque $P = QR$ est unitaire dans $\mathbb{Z}[X]$. On a donc $m^2 = c(Q_1)c(R_1)$ avec $c(Q_1)$ et $c(R_1)$ qui divisent m (m est le coefficient dominant des polynômes Q_1 et R_1), ce qui implique que $c(Q_1) = c(R_1) = m$, c'est-à-dire que m divise tous les coefficients de Q_1 et R_1 et donc $Q = \frac{1}{m}Q_1$, $R = \frac{1}{m}R_1$ sont dans $\mathbb{Z}[X]$.
Par récurrence, on en déduit que si $P = \prod_{k=1}^{r} P_k$ est unitaire $\mathbb{Z}[X]$, les P_k étant unitaires dans $\mathbb{Q}[X]$, alors tous les P_k sont dans $\mathbb{Z}[X]$.
7. Soit P dans $U_n(\mathbb{Z})$. Montrer que $\mathcal{D}_{\mathbb{Z}}(P)$ n'est pas vide.

2. $c(U)$ est le contenu de U

8. Dans l'anneaux factoriel $\mathbb{Q}[X]$, le polynôme $P \in U_n(\mathbb{Z})$ est produit de polynômes irréductibles, soit $P = \prod_{k=1}^{r} P_k$, les P_k étant unitaires dans $\mathbb{Q}[X]$.
La question précédente nous dit que les P_k sont nécessairement dans $\mathbb{Z}[X]$.
Comme les P_k sont irréductibles dans $\mathbb{Q}[X]$, la question **I.B.2.** nous dit qu'ils sont scindés à racines simples dans $\mathbb{C}$, et **I.A.2.c.** nous dit que les $C(P_k)$ sont diagonalisables sur $\mathbb{C}$.
De **I.A.3.** on déduit que la matrice $M = \text{diag}(C(P_1), \cdots, C(P_r))$ est diagonalisable sur $\mathbb{C}$. Cette matrice est dans $\mathcal{M}_n(\mathbb{Z})$ avec $\chi_M = \prod_{k=1}^{r} \chi_{C(P_k)} = \prod_{k=1}^{r} P_k = P$, elle est donc dans $\mathcal{E}_{\mathbb{Z}}(P)$ et dans $\mathcal{D}_{\mathbb{Z}}(P)$. Cet ensemble est donc non vide.

– C – Similitude sur $\mathbb{K}$ de matrices blocs

Pour U et V dans $\mathcal{M}_n(\mathbb{K})$, on note $\Phi_{U,V}$ l'endomorphisme de $\mathcal{M}_n(\mathbb{K})$ défini par :

$$\forall X \in \mathcal{M}_n(\mathbb{K}),\ \Phi_{U,V}(X) = UX - XV$$

1. Soient U dans $\mathcal{M}_n(\mathbb{K})$, Q dans $GL_n(\mathbb{K})$ et $V = QUQ^{-1}$. Déterminer un automorphisme du $\mathbb{K}$-espace vectoriel $\mathcal{M}_n(\mathbb{K})$ envoyant le noyau de $\Phi_{U,V}$ sur celui de $\Phi_{U,U}$.
Dans la suite, m est un entier tel que $0 < m < n$, A un élément de $\mathcal{M}_m(\mathbb{K})$, A' un élément de $\mathcal{M}_{n-m}(\mathbb{K})$, B un élément de $\mathcal{M}_{m,n-m}(\mathbb{K})$.
On note :
$$M = \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix},\ N = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}$$
2. On a, pour $Q \in GL_n(\mathbb{K})$:
$$\begin{aligned} \Phi_{U,V}(X) &= UX - XV = UX - XQUQ^{-1} = (UXQ - XQU)Q^{-1} \\ &= \Phi_{U,U}(XQ)Q^{-1} \end{aligned}$$
donc :
$$\Phi_{U,V}(X) = 0 \Leftrightarrow \Phi_{U,U}(XQ) = 0$$
soit :
$$X \in \ker(\Phi_{U,V}) \Leftrightarrow XQ \in \ker(\Phi_{U,U})$$
L'automorphisme $X \in \mathcal{M}_n(\mathbb{K}) \mapsto XQ$ envoie donc $\ker(\Phi_{U,V})$ sur $\ker(\Phi_{U,U})$.
3. Soient Y dans $\mathcal{M}_{m,n-m}(\mathbb{K})$ et $P = \begin{pmatrix} I_m & Y \\ 0 & I_{n-m} \end{pmatrix}$.
Vérifier que P appartient à $GL_n(\mathbb{K})$; déterminer P^{-1} et $P^{-1}NP$. En déduire que s'il existe Y dans $\mathcal{M}_{m,n-m}(\mathbb{K})$ tel que $B = AY - YA'$, alors M et N sont semblables.
4. De $\det(P) = 1$, on déduit que $P \in GL_n(\mathbb{K})$. Plus précisément, avec :
$$\begin{pmatrix} I_m & Y \\ 0 & I_{n-m} \end{pmatrix}\begin{pmatrix} I_m & Z \\ 0 & I_{n-m} \end{pmatrix} = \begin{pmatrix} I_m & Z+Y \\ 0 & I_{n-m} \end{pmatrix}$$
on déduit que $P \in GL_n(\mathbb{K})$ avec $P^{-1} = \begin{pmatrix} I_m & -Y \\ 0 & I_{n-m} \end{pmatrix}$ et :
$$\begin{aligned} P^{-1}NP &= \begin{pmatrix} I_m & -Y \\ 0 & I_{n-m} \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}\begin{pmatrix} I_m & Y \\ 0 & I_{n-m} \end{pmatrix} \\ &= \begin{pmatrix} A & AY - YA' \\ 0 & A' \end{pmatrix} \end{aligned}$$

Il en résulte que $M = \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix}$ est semblable à N pour $B = \Phi_{A,A'}(Y) = AY - YA'$.

5. Le but de cette question est de montrer que si M et N sont semblables sur $\mathbb{K}$, alors il existe Y dans $\mathcal{M}_{m,n-m}(\mathbb{K})$ tel que $B = AY - YA'$.
Si X est dans $\mathcal{M}_n(\mathbb{K})$, on pose :

$$X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix}$$

avec $X_{1,1} \in \mathcal{M}_m(\mathbb{K})$, $X_{1,2} \in \mathcal{M}_{m,n-m}(\mathbb{K})$, $X_{2,1} \in \mathcal{M}_{n-m,m}(\mathbb{K})$ et $X_{2,2} \in \mathcal{M}_{n-m}(\mathbb{K})$. On note alors :

$$\tau(X) = (X_{2,1}, X_{2,2})$$

Il est clair que τ est une application linéaire de $\mathcal{M}_n(\mathbb{K})$ dans $\mathcal{M}_{n-m,n}(\mathbb{K})$.

(a) Montrer les relations :

$$\begin{cases} \ker(\tau) \cap \ker(\Phi_{N,N}) = \ker(\tau) \cap \ker(\Phi_{M,N}) \\ \tau(\ker(\Phi_{M,N})) \subset \tau(\ker(\Phi_{N,N})) \end{cases}$$

(b) Une matrice X dans $\ker(\tau)$ est de la forme $X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ 0 & 0 \end{pmatrix}$ et pour toute matrice B dans $\mathcal{M}_{m,n-m}(\mathbb{K})$, on a :

$$\begin{aligned} \Phi_{M,N}(X) &= MX - XN \\ &= \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix} \begin{pmatrix} X_{1,1} & X_{1,2} \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} X_{1,1} & X_{1,2} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} \\ &= \begin{pmatrix} AX_{1,1} - X_{1,1}A & AX_{1,2} - X_{1,2}A' \\ 0 & 0 \end{pmatrix} = \Phi_{N,N}(X) \end{aligned}$$

Il en résulte que $\ker(\tau) \cap \ker(\Phi_{N,N}) = \ker(\tau) \cap \ker(\Phi_{M,N})$.
Pour $X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} \in \ker(\Phi_{M,N})$, on a :

$$\begin{aligned} \Phi_{M,N}(X) &= MX - XN \\ &= \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix} \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} - \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} \\ &= \begin{pmatrix} AX_{1,1} + BX_{2,1} - X_{1,1}A & AX_{1,2} + BX_{2,2} - X_{1,2}A' \\ A'X_{2,1} - X_{2,1}A & A'X_{2,2} - X_{2,2}A' \end{pmatrix} = 0 \end{aligned}$$

donc :

$$\tau(\Phi_{M,N}(X)) = (A'X_{2,1} - X_{2,1}A, A'X_{2,2} - X_{2,2}A') = 0$$

En posant $X' = \begin{pmatrix} I_m & 0 \\ X_{2,1} & X_{2,2} \end{pmatrix}$, on a :

$$\begin{aligned} \Phi_{N,N}(X') &= NX' - X'N \\ &= \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} \begin{pmatrix} I_m & 0 \\ X_{2,1} & X_{2,2} \end{pmatrix} - \begin{pmatrix} I_m & 0 \\ X_{2,1} & X_{2,2} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ A'X_{2,1} - X_{2,1}A & A'X_{2,2} - X_{2,2}A' \end{pmatrix} = 0 \end{aligned}$$

donc, $\tau(X) = (X_{2,1}, X_{2,2}) = \tau(X')$ avec $X' \in \ker(\Phi_{N,N})$. On a donc montré que $\tau(\ker(\Phi_{M,N})) \subset \tau(\ker(\Phi_{N,N}))$.

(c) On suppose que M et N sont semblables sur $\mathbb{K}$. Montrer :

$$\tau(\ker(\Phi_{M,N})) = \tau(\ker(\Phi_{N,N}))$$

(d) En **I.C.1.** on a vu que, si M et N sont semblables sur $\mathbb{K}$, $\ker(\Phi_{M,N})$ est alors isomorphe à $\ker(\Phi_{N,N})$, donc ces espaces ont même dimension.
Le théorème du rang appliqué à la restriction de τ à $\ker(\Phi_{M,N})$ [resp. à $\ker(\Phi_{N,N})$] nous dit que :

$$\dim(\tau(\ker(\Phi_{M,N}))) = \dim(\ker(\Phi_{M,N})) - \dim(\ker(\tau) \cap \ker(\Phi_{M,N}))$$

$$[\text{resp. } \dim(\tau(\ker(\Phi_{N,N}))) = \dim(\ker(\Phi_{N,N})) - \dim(\ker(\tau) \cap \ker(\Phi_{N,N}))\,]$$

et de la première égalité de **I.C.3.a.** on déduit que $\ker(\tau) \cap \ker(\Phi_{M,N})$ et $\ker(\tau) \cap \ker(\Phi_{N,N})$ ont même dimension. En définitive on a $\dim(\tau(\ker(\Phi_{M,N}))) = \dim(\tau(\ker(\Phi_{N,N}))$ et l'égalité $\tau(\ker(\Phi_{M,N})) = \tau(\ker(\Phi_{N,N}))$ d'après l'inclusion de **I.C.3.a.**

(e) On suppose que M et N sont semblables sur $\mathbb{K}$. Montrer qu'il existe Y dans $\mathcal{M}_{m,n-m}(\mathbb{K})$ tel que $B = AY - YA'$.

(f) Si M et N sont semblables sur $\mathbb{K}$, on a alors $\tau(\ker(\Phi_{M,N})) = \tau(\ker(\Phi_{N,N}))$.
La matrice $I_n = \begin{pmatrix} I_m & 0 \\ 0 & I_{n-m} \end{pmatrix}$ étant dans $\ker(\Phi_{N,N})$, il existe une matrice $X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ 0 & I_{n-m} \end{pmatrix}$ dans $\ker(\Phi_{M,N})$ ($\tau(I_n) = \tau(X) = (0, I_{n-m})$), ce qui se traduit par :

$$\begin{aligned} \Phi_{M,N}(X) &= \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix} \begin{pmatrix} X_{1,1} & X_{1,2} \\ 0 & I_{n-m} \end{pmatrix} - \begin{pmatrix} X_{1,1} & X_{1,2} \\ 0 & I_{n-m} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} \\ &= \begin{pmatrix} AX_{1,1} - X_{1,1}A & AX_{1,2} + B - X_{1,2}A' \\ 0 & 0 \end{pmatrix} = 0 \end{aligned}$$

et nous dit que $B = X_{1,2}A' - AX_{1,2}$. Posant $Y = -X_{1,2} \in \mathcal{M}_{m,n-m}(\mathbb{K})$, on a $B = AY - YA'$.

6. Montrer l'équivalence entre les deux assertions suivantes :

   (i) M est diagonalisable sur $\mathbb{K}$;

   (ii) A et A' sont diagonalisables sur $\mathbb{K}$ et B est de la forme $AY - YA'$ avec Y dans $\mathcal{M}_{m,n-m}(\mathbb{K})$.

7. Dire que $M = \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix}$ est diagonalisable sur $\mathbb{K}$ équivaut à dire que son polynôme minimal π_M est alors scindé sur $\mathbb{K}$ à racines simples. Avec :

$$0 = \pi_M(M) = \begin{pmatrix} \pi_M(A) & C \\ 0 & \pi_M(A') \end{pmatrix}$$

on déduit que les matrices A et A' sont annulées par un polynôme scindé sur $\mathbb{K}$ et à racines simples, elles sont donc diagonalisables sur $\mathbb{K}$.

De **I.A.3.** on déduit que $N = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}$ est diagonalisable sur $\mathbb{K}$. Comme M et N sont diagonalisable sur $\mathbb{K}$ avec le même polynôme caractéristique (à savoir $\chi_A \cdot \chi_{A'}$), elles sont semblables (d'après **I.A.1.c.**) et $B = AY - YA'$ avec $Y \in \mathcal{M}_{m,n-m}(\mathbb{K})$ d'après **I.C.3.c.** Si $B = AY - YA'$ avec $Y \in \mathcal{M}_{m,n-m}(\mathbb{K})$, la matrice $M = \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix}$ est alors semblable sur $\mathbb{K}$ à $N = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}$ d'après **I.C.2.** Si de plus, A et A' sont diagonalisables sur $\mathbb{K}$, il en est de même de N d'après **I.A.3.** et M est diagonalisable sur $\mathbb{K}$.

– II – Similitudes entières

– A – Généralités, premier exemple

1. Soit $\mathbb{A}$ un sous-anneau d'un corps. Montrer que $GL_n(\mathbb{A})$ est l'ensemble des matrices de $\mathcal{M}_n(\mathbb{A})$ dont le déterminant est un élément inversible de $\mathbb{A}$. Expliciter ce résultat pour $\mathbb{A} = \mathbb{Z}$.
2. Dire que $M \in \mathcal{M}_n(\mathbb{A})$ est inversible, signifie qu'il existe une matrice $M' \in \mathcal{M}_n(\mathbb{A})$ telle que $MM' = I_n$, ce qui entraîne $\det(M)\det(M') = 1$ dans l'anneau $\mathbb{A}$, donc $\det(M)$ est inversible dans $\mathbb{A}$.
   Réciproquement si $M \in \mathcal{M}_n(\mathbb{A})$ est telle que $\det(M)$ soit inversible dans $\mathbb{A}$, la relation $M \cdot {}^t\widetilde{M} = \det(M)\, I_n$, où $\widetilde{M} \in \mathcal{M}_n(\mathbb{A})$ est la comatrice de M, nous dit que M est inversible dans $\mathbb{A}$ avec $M^{-12} = (\det(M))^{-1}\ {}^t\widetilde{M}$.
   Pour $\mathbb{A} = \mathbb{Z}$, on obtient l'ensemble des matrices de $\mathcal{M}_n(\mathbb{Z})$ de déterminant égal à ± 1.
3. Soient p un nombre premier, $\mathbb{F}_p$ le corps fini $\mathbb{Z}/p\mathbb{Z}$. Si M est une matrice de $\mathcal{M}_n(\mathbb{Z})$, on note $\overline{M}$ la matrice de $\mathcal{M}_n(\mathbb{F}_p)$ obtenue en réduisant M modulo p.
   Montrer que si M et N sont deux matrices de $\mathcal{M}_n(\mathbb{Z})$ semblables sur $\mathbb{Z}$, les matrices $\overline{M}$ et $\overline{N}$ sont semblables sur $\mathbb{F}_p$.
4. On vérifie facilement que pour toutes matrices P, Q dans $\mathcal{M}_n(\mathbb{Z})$, on a $\overline{P+Q} = \overline{P} + \overline{Q}$ $\overline{PQ} = \overline{P} \cdot \overline{Q}$, c'est-à-dire que l'application $M \mapsto \overline{M}$ est un morphisme d'anneau de $\mathcal{M}_n(\mathbb{Z})$ sur $\mathcal{M}_n(\mathbb{F}_p)$ (il est surjectif). Si de plus P est inversibles, on a alors $PP^{-1} = I_n$ dans $\mathcal{M}_n(\mathbb{Z})$ et $\overline{PP^{-1}} = \overline{I_n}$ dans $\mathcal{M}_n(\mathbb{F}_p)$, c'est-à-dire que $\overline{P}$ est inversible dans $\mathcal{M}_n(\mathbb{F}_p)$ d'inverse $\overline{P}^{-1} = \overline{P^{-1}}$.
   Si M et N sont semblables dans $\mathcal{M}_n(\mathbb{Z})$, il existe alors $P \in GL_n(\mathbb{Z})$ telle que $N = P^{-1}MP$ et avec $\overline{N} = \overline{P}^{-1}\overline{MP}$, on déduit que $\overline{M}$ et $\overline{N}$ sont semblables dans $\mathcal{M}_n(\mathbb{F}_p)$.
5. Pour a dans $\mathbb{Z}$, soient :

$$S_a = \begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix},\ T_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

   (a) Montrer que S_0 et S_1 sont semblables sur $\mathbb{Q}$, mais ne sont pas semblables sur $\mathbb{Z}$.
   Soit M dans $\mathcal{M}_2(\mathbb{Z})$ telle que $\chi_M = X^2 - 1$.

   (b) Pour tout $a \in \mathbb{Z}$, la matrice $S_a \in \mathcal{M}_2(\mathbb{Q})$ a deux valeurs propres distinctes dans $\mathbb{Q}$, elle est donc diagonalisable semblable à $S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ sur $\mathbb{Q}$.
   Si S_a est semblable à S_0 sur $\mathbb{Z}$, pour tout nombre premier $p \geq 2$, la matrice $\overline{S_a}$

est semblable à $\overline{S_0}$ sur $\mathbb{Z}_p$. Prenant $p=2$ et a impair, on a $\overline{S_0}=\begin{pmatrix}\overline{1}&\overline{0}\\ \overline{0}&\overline{1}\end{pmatrix}=\overline{I_2}$ et $\overline{S_a}=\begin{pmatrix}\overline{1}&\overline{1}\\ \overline{0}&\overline{1}\end{pmatrix}\neq\overline{I_2}$ ne peut être semblable à $\overline{S_0}=\overline{I_2}$ dans $\mathcal{M}_2(\mathbb{F}_2)$, ce qui contredit **II.A.2.** Donc S_0 et S_a, pour a impair, ne sont pas semblables sur $\mathbb{Z}$.

(c) Montrer qu'il existe x_1 et x_2 dans $\mathbb{Z}$ premiers entre eux tels que le vecteur colonne $x={}^t(x_1,x_2)$ vérifie $Mx=x$.

(d) Comme $\chi_M=(X-1)(X+1)$ est scindé à racines simples dans $\mathbb{Q}$, la matrice M est diagonalisable sur $\mathbb{Q}$, semblable à S_0. En particulier, il existe un vecteur $y=\begin{pmatrix}y_1\\ y_2\end{pmatrix}\in\mathbb{Q}^2$ tel que $My=y$. Multipliant y par un entier λ judicieusement choisi, le vecteur $x=\lambda y=\begin{pmatrix}x_1\\ x_2\end{pmatrix}$ est dans $\mathbb{Z}^2$, encore valeur propre de M associé à la valeur propre 1, avec x_1, x_2 premiers entre eux.

(e) Montrer que M est semblable sur $\mathbb{Z}$ à une matrice S_a avec a dans $\mathbb{Z}$.

(f) Comme $x_1\wedge x_2=1$, le théorème de Bézout nous dit qu'il existe $\begin{pmatrix}u\\ v\end{pmatrix}\in\mathbb{Z}^2$ tel que $ux_1+vx_2=1$. En notant $P=\begin{pmatrix}x_1&-v\\ x_2&u\end{pmatrix}$ dans $\mathcal{M}_2(\mathbb{Z})$, on a $\det(P)=1$, donc P est inversible dans $\mathcal{M}_2(\mathbb{Z})$ et $P^{-1}MP=\begin{pmatrix}1&a\\ 0&-1\end{pmatrix}$ avec $a\in\mathbb{Z}$, puisque P est la matrice de passage de la base canonique de $\mathbb{Q}^2$ à la base (x,y) où $y=\begin{pmatrix}-v\\ u\end{pmatrix}$ et $Mx=x$.

(g) Pour a et x dans $\mathbb{Z}$, déterminer $T_xS_aT_x^{-1}$; conclure que M est semblable sur $\mathbb{Z}$ à l'une des deux matrices S_0, S_1.

(h) Pour $(a,x)\in\mathbb{Z}^2$, on a :

$$\begin{aligned}T_xS_aT_x^{-1}&=\begin{pmatrix}1&x\\ 0&1\end{pmatrix}\begin{pmatrix}1&a\\ 0&-1\end{pmatrix}\begin{pmatrix}1&-x\\ 0&1\end{pmatrix}\\&=\begin{pmatrix}1&a-2x\\ 0&-1\end{pmatrix}=S_{a-2x}\end{aligned}$$

Comme M est semblable sur $\mathbb{Z}$ à une matrice S_a avec a dans $\mathbb{Z}$, on en déduit qu'elle est aussi semblable sur $\mathbb{Z}$ à S_{a-2x} pour tout $x\in\mathbb{Z}$. Si a est pair [resp. impair], on a $a=2x$ [resp. $a=2x+1$] avec $x\in\mathbb{Z}$, et M est semblable à S_0 [resp. à S_1].

– B – Les ensembles $\mathcal{E}_{\mathbb{Z}}(X^2-\delta)$

Dans cette partie, on fixe un élément δ de $\mathbb{Z}^*$ qui n'est pas le carré d'un entier et on considère $P=X^2-\delta$.

1.

(a) Vérifier que $\mathcal{E}_{\mathbb{Z}}(P)$ est l'ensemble des matrices de la forme :

$$\begin{pmatrix}a&c\\ b&-a\end{pmatrix}$$

où a, b, c sont dans $\mathbb{Z}$ et vérifient : $a^2+bc=\delta$. Si a et b sont deux entiers relatifs tels que b divise $\delta - a^2$, vérifier que l'ensemble $\mathcal{E}_{\mathbb{Z}}(P)$ contient une unique matrice de la forme :

$$\begin{pmatrix} a & c \\ b & -a \end{pmatrix}$$

Cette matrice sera notée $M_{(a,b)}$ dans la suite.

(b) Si $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{E}_{\mathbb{Z}}(P)$, on a $M \in \mathcal{M}_2(\mathbb{Z})$ et :

$$\chi_M(X) = X^2 - \operatorname{tr}(M)X + \det(M) = X^2 - \delta$$

donc $\operatorname{tr}(M) = a + d = 0$ et $\det(M) = ad - bc = -a^2 - bc = -\delta$. La matrice M est donc de la forme :

$$M = \begin{pmatrix} a & c \\ b & -a \end{pmatrix}$$

avec $(a, b, c) \in \mathbb{Z}^3$ tel que $a^2 + bc = \delta$.
Pour $(a, b) \in \mathbb{Z}^2$ tel que b divise $\delta - a^2$, on a $\delta - a^2 = bc$ avec $c \in \mathbb{Z}$ uniquement déterminé et $M_{(a,b)} = \begin{pmatrix} a & \frac{\delta-a^2}{b} \\ b & -a \end{pmatrix}$ est l'unique élément de $\mathcal{E}_{\mathbb{Z}}(P)$.

(c) Soient a, b dans $\mathbb{Z}$ tels que b divise $\delta - a^2$, λ dans $\mathbb{Z}$. Montrer que les matrices $M_{(a,b)}$, $M_{(a,-b)}$, $M_{(a+\lambda b,b)}$, $M_{\left(-a,\frac{\delta-a^2}{b}\right)}$ sont semblables sur $\mathbb{Z}$.

(d) Pour $P = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in GL_2(\mathbb{Z})$, on a $\det(P) = \varepsilon \in \{-1, 1\}$, $P^{-1} = \varepsilon \begin{pmatrix} t & -z \\ -y & x \end{pmatrix}$ et :

$$\begin{aligned} P^{-1}M_{(a,b)}P &= \varepsilon \begin{pmatrix} t & -z \\ -y & x \end{pmatrix} \begin{pmatrix} a & \frac{\delta-a^2}{b} \\ b & -a \end{pmatrix} \begin{pmatrix} x & z \\ y & t \end{pmatrix} \\ &= \varepsilon \begin{pmatrix} x(at-bz) + y\left(az + \frac{1}{b}t(\delta-a^2)\right) & z(at-bz) + t\left(az + \frac{1}{b}t(\delta-a^2\right. \\ x(-ay+bx) + y\left(-ax - \frac{1}{b}y(\delta-a^2)\right) & z(-ay+bx) + t\left(-ax - \frac{1}{b}y(\delta-a^2\right. \end{pmatrix} \end{aligned}$$

Pour $y = z = 0$, cela donne :

$$P^{-1}M_{(a,b)}P = \varepsilon \begin{pmatrix} axt & \frac{1}{b}(\delta-a^2)t^2 \\ bx^2 & -axt \end{pmatrix} = \begin{pmatrix} a & \frac{\varepsilon}{b}(\delta-a^2) \\ b\varepsilon & -a \end{pmatrix}$$

Prenant $\varepsilon = -1$ (i. e. $x = \pm 1$ et $t = -x$), on obtient :

$$P^{-1}M_{(a,b)}P = \begin{pmatrix} a & -\frac{1}{b}(\delta-a^2) \\ -b & -a \end{pmatrix} = M_{(a,-b)}$$

Pour $y=0$, $z=-\lambda$, $x=t=1$, cela donne :

$$P^{-1}M_{(a,b)}P=\begin{pmatrix} a+b\lambda & -\lambda(a+b\lambda)-a\lambda+\dfrac{1}{b}(\delta-a^2) \\ b & -\lambda b-a \end{pmatrix}$$
$$=\begin{pmatrix} a+b\lambda & -b\lambda^2-2\lambda a+\dfrac{1}{b}(\delta-a^2) \\ b & -\lambda b-a \end{pmatrix}$$
$$=\begin{pmatrix} a+\lambda b & \frac{\delta-(a+\lambda b)^2}{b} \\ b & -a-\lambda b \end{pmatrix}=M_{(a+\lambda b,b)}$$

Pour $x=t=0$, cela donne :

$$P^{-1}M_{(a,b)}P=\varepsilon\begin{pmatrix} ayz & -bz^2 \\ -\dfrac{1}{b}(\delta-a^2)y^2 & -ayz \end{pmatrix}=\begin{pmatrix} -a & -b\varepsilon \\ -\dfrac{\varepsilon}{b}(\delta-a^2) & a \end{pmatrix}$$

Prenant $\varepsilon=-1$ (i. e. $y=\pm1$ et $z=-y$), on obtient :

$$P^{-1}M_{(a,b)}P=\begin{pmatrix} -a & b \\ \frac{\delta-a^2}{b} & a \end{pmatrix}=M_{\left(-a,\frac{\delta-a^2}{b}\right)}$$

2. Soit M dans $\mathcal{E}_{\mathbb{Z}}(P)$. Puisque $M_{(a,b)}$ et $M_{(a,-b)}$ sont semblables sur $\mathbb{Z}$, l'ensemble $\mathcal{B}$ des b de $\mathbb{N}^*$ tels qu'il existe une matrice $M_{(a,b)}$ semblable sur $\mathbb{Z}$ à M n'est pas vide ; on note $\beta(M)$ le plus petit élément de $\mathcal{B}$.

   (a) Montrer qu'il existe un entier a tel que $|a|\leq\dfrac{\beta(M)}{2}$ et tel que M soit semblable sur $\mathbb{Z}$ à $M_{(a,\beta(M))}$.

   (b) Soit a' un entier tel que $M_{(a',\beta(M))}$ soit semblable sur $\mathbb{Z}$ à M. En effectuant la division euclidienne de a' par $\beta(M)$, il existe un unique couple d'entiers (q,r) tel que $a'=q\beta(M)+r$ et $-\dfrac{\beta(M)}{2}\leq r<\dfrac{\beta(M)}{2}$. La matrice $M_{(a'-q\beta(M),\beta(M))}=M_{(r,\beta(M))}$ est alors semblable sur $\mathbb{Z}$ à $M_{(a',\beta(M))}$, donc à M, avec $|r|\leq\dfrac{\beta(M)}{2}$.

   (c) Comparer $|\delta-a^2|$ et $\beta(M)^2$. En déduire que $\beta(M)$ est majoré par $\sqrt{\delta}$ si $\delta>0$, par $\sqrt{\dfrac{4|\delta|}{3}}$ si $\delta<0$.

   (d) Pour tout $b\in\mathcal{B}$, la matrice $M_{(a,b)}$ est semblable sur $\mathbb{Z}$ à M, donc aussi la matrice $M_{\left(-a,\frac{\delta-a^2}{b}\right)}$ et la matrice $M_{\left(-a,\frac{|\delta-a^2|}{b}\right)}$ d'après **II.B1.b.** Il en résulte que $\beta(M)\leq\dfrac{|\delta-a^2|}{b}$. En particulier, on a $\beta(M)\leq\dfrac{|\delta-a^2|}{\beta(M)}$, donc $\beta(M)^2\leq|\delta-a^2|$.
   Si $\delta<a^2$, on a alors :

$$\beta(M)^2\leq a^2-\delta\leq\frac{\beta(M)^2}{4}-\delta$$

   donc $\delta<0$ et $\beta(M)\leq\sqrt{\dfrac{4|\delta|}{3}}$.
   Si $\delta>0$, on a alors nécessairement $\delta>a^2$ (sinon $\delta<0$ et δ n'est pas un carré) et :

$$\beta(M)^2\leq\delta-a^2\leq\delta$$

   soit $\beta(M)\leq\sqrt{\delta}$.

(e) Montrer que $\mathcal{E}_{\mathbb{Z}}(P)$ est réunion d'un nombre fini de classes de similitude entière.

(f) Ce qui précède nous dit que toute matrice $M \in \mathcal{E}_{\mathbb{Z}}(P)$ est semblable sur $\mathbb{Z}$ à une matrice $M(a,b)$ avec $b = \beta(M)$ compris entre 1 et $\max\left(\sqrt{\delta}, \sqrt{\frac{4|\delta|}{3}}\right)$ et $|a| \leq \frac{\beta(M)}{2} \leq \max\left(\sqrt{\delta}, \sqrt{\frac{4|\delta|}{3}}\right)$. L'ensemble de ces matrices étant fini, il n'y a qu'un nombre fini de classes de similitude entière.

– C – Diagonalisabilité et réduction modulo p

Soient p un nombre premier, $\overline{\mathbb{F}_p}$ une clôture algébrique su corps $\mathbb{F}_p$ défini en **II.A.2.** ℓ dans $\mathbb{N}^*$. Pour P dans $\mathbb{Z}[X]$, on note $\overline{P}$ l'élément de $\mathbb{F}_p[X]$ obtenu en réduisant P modulo P. Si M est dans $\mathcal{M}_\ell(\mathbb{Z})$, on note $\overline{M}$ la matrice de $\mathcal{M}_\ell(\mathbb{F}_p)$ obtenue en réduisant M modulo p.

1. Soit P dans $\mathbb{Z}[X]$ non constant dont les racines dans $\mathbb{C}$ sont simples.

   (a) Montrer qu'il existe d dans $\mathbb{N}^*$, S et T dans $\mathbb{Z}[X]$ tels que :

   $$SP + TP' = d$$

   (b) Comme toutes les racines complexes de P sont simples, les polynômes P et P' sont premiers entre eux dans $\mathbb{Q}[X]$ et le théorème de Bézout nous dit qu'il existe U, V dans $\mathbb{Q}[X]$ tels que $UP + VP' = 1$. Désignant par d un entier naturel non nul tel que $S = dU$ et $T = dV$ soient dans $\mathbb{Z}[X]$, on a $SP + TP' = d$.

   (c) Si p ne divise pas d, montrer que les racines de $\overline{P}$ dans $\overline{\mathbb{F}_p}$ sont simples.

   (d) Si $\alpha \in \overline{\mathbb{F}_p}$ est une racine de $\overline{P}$, on a $\overline{T}(\alpha)\overline{P}'(\alpha) = \overline{d} \neq \overline{0}$ si p ne divise pas d, donc $\overline{P}'(\alpha) \neq 0$ et α est racine simple de $\overline{P}$.

2. Soit M dans $\mathcal{M}_\ell(\mathbb{Z})$ diagonalisable sur $\mathbb{C}$.

   (a) Montrer qu'il existe un élément P de $\mathbb{Z}[X]$ unitaire, dont les racines complexes sont toutes simples et tel que $P(M) = 0$.

   (b) Soient $\chi_M \in \mathbb{Z}[X]$ le polynôme caractéristique de M et $\chi_M = \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$ sa décomposition en facteurs irréductibles dans $\mathbb{C}[X]$, les λ_k étant deux à deux distincts. Le pgcd de χ_M et χ'_M est :

   $$\Delta = \prod_{k=1}^{r} (X - \lambda_k)^{m_k - 1} \in \mathbb{Q}[X]$$

   (le pgcd est le même dans $\mathbb{Q}[X]$ et $\mathbb{C}[X]$) et, pour M diagonalisable, le polynôme minimal de M est :

   $$\pi_M = \prod_{k=1}^{r} (X - \lambda_k) = \frac{\chi_M}{\Delta} \in \mathbb{Q}[X]$$

   On a donc $\chi_M = \Delta \cdot \pi_M$ avec χ_M et Δ unitaires dans $\mathbb{Q}[X]$, $\chi_M \in \mathbb{Z}[X]$ et π_M divise χ_M dans $\mathbb{Q}[X]$, ce qui implique que $\pi_M \in \mathbb{Z}[X]$ d'après **I.B.3.** Ce polynôme $P = \pi_M$ convient.

(c) Montrer qu'il existe un entier d_M tel que si p ne divise pas d_M alors $\overline{M}$ est diagonalisable sur $\overline{\mathbb{F}_p}$.

(d) Le polynôme π_M étant non constant dans $\mathbb{Z}[X]$ à racines complexes simples, on déduit de **II.C.1.** que pour tout $d \in \mathbb{N}^*$ non multiple de p, les racines de $\overline{\pi_M}$ dans $\overline{\mathbb{F}_p}$ sont simples. Ce polynôme $\overline{\pi_M} \in \overline{\mathbb{F}_p}[X]$ étant annulateur de $\overline{M}$, on en déduit que $\overline{M}$ est diagonalisable sur $\overline{\mathbb{F}_p}$.

– D – Un résultat de non finitude

Soit P un élément de $U_n(\mathbb{Z})$ dont les racines dans $\mathbb{C}$ ne sont pas toutes simples.

1. Montrer qu'il existe ℓ dans $\mathbb{N}^*$, m dans $\mathbb{N}$, Q dans $U_\ell(\mathbb{Z})$, R dans $U_m(\mathbb{Z})$ tels que $P = Q^2R$.
   Grâce à **I.B.4.** on dispose de A dans $\mathcal{D}_{\mathbb{Z}}(Q)$ et, si $m > 0$, de B dans $\mathcal{D}_{\mathbb{Z}}(R)$.
   Si p est un nombre premier, soit E_p la matrice :
   $$\begin{pmatrix} A & pI_\ell & 0 \\ 0 & A & 0 \\ 0 & 0 & B \end{pmatrix} \text{ si } m > 0, \quad \begin{pmatrix} A & pI_\ell \\ 0 & A \end{pmatrix} \text{ si } m = 0$$
2. Dans l'anneau factoriel $\mathbb{Q}[X]$, on a la décomposition de $P \in U_n(\mathbb{Z})$ en facteurs irréductibles unitaires, $P = \prod_{k=1}^{r} P_k^{m_k}$. De **I.B.3.** on déduit que les P_k sont dans $\mathbb{Z}[X]$ et de **I.B.2.** qu'ils sont à racines complexes simples. Les m_k ne peuvent être tous égaux à 1, sinon toutes les racines de P sont simples (pour $j \neq k$, on a $P_k \wedge P_j = 1$ dans $\mathbb{Q}[X]$ et $\mathbb{C}[X]$, donc les racines complexes de P_k sont distinctes de celles de P_j). Il existe donc un indice j tel que $m_j \geq 2$ et posant $Q = P_j \in U_\ell(\mathbb{Z})$, avec $1 \leq \ell \leq r$, $R = P_j^{m_j-2} \prod_{\substack{k=1 \\ k\neq j}}^{r} P_k^{m_k} \in U_m(\mathbb{Z})$ avec $m + 2\ell = r$, on a $P = Q^2R$.
3. Les entiers d_A et d_B (si $m > 0$) sont ceux définis en **II.C.** Soient p et q deux nombres premiers distincts tels que p ne divise ni d_A, ni ℓ, ni d_B si $m > 0$. Montrer que E_p et E_q ne sont pas semblables sur $\mathbb{Z}$.
4. Comme p ne divise ni d_A, ni d_B, les matrices $\overline{A}$ et $\overline{B}$ sont diagonalisable sur $\overline{\mathbb{F}_p}$ d'après **II.C.2.** Comme :
   $$\overline{E_p} = \begin{pmatrix} \overline{A} & \overline{0} & \overline{0} \\ \overline{0} & \overline{A} & \overline{0} \\ \overline{0} & \overline{0} & \overline{B} \end{pmatrix} \text{ si } m > 0, \quad \begin{pmatrix} \overline{A} & \overline{0} \\ \overline{0} & \overline{A} \end{pmatrix} \text{ si } m = 0$$
   on déduit de **I.A.3.** que $\overline{E_p}$ est aussi diagonalisable sur $\overline{\mathbb{F}_p}$.
   Soit q un nombre premier distinct de p. Si $\overline{E_q}$ est diagonalisable sur $\overline{\mathbb{F}_p}$ il en est de même de $\begin{pmatrix} \overline{A} & \overline{q}\overline{I_\ell} \\ 0 & \overline{A} \end{pmatrix}$ et **I.C.4.** nous dit que $\overline{q}\overline{I_\ell}$ doit être de la forme $\overline{AY} - \overline{YA}$, ce qui entraîne $\mathrm{Tr}\left(\overline{q}\overline{I_\ell}\right) = \overline{\ell q} = \mathrm{Tr}\left(\overline{AY} - \overline{YA}\right) = \overline{0}$ dans $\mathbb{F}_p$ et est en contradiction avec l'hypothèse, p ne divise pas ℓ.
   On en déduit que les matrices $\overline{E_p}$ et $\overline{E_q}$ ne peuvent être semblables sur $\overline{\mathbb{F}_p}$, donc elles ne peuvent être semblables sur $\mathbb{F}_p$ et les matrices E_p et E_q ne peuvent être semblables sur $\mathbb{Z}$.

5. Conclure que $\mathcal{E}_{\mathbb{Z}}(P)$ n'est pas réunion d'un nombre fini de classes de similitude entière.
6. On a une infinité de nombres premiers p ne ne divisant ni d_A, ni ℓ, ni d_B et pour de tels entiers $p \neq q$, on a E_p, E_q dans $\mathcal{E}_{\mathbb{Z}}(P)$ non semblables sur $\mathbb{Z}$. Donc $\mathcal{E}_{\mathbb{Z}}(P)$ n'est pas réunion d'un nombre fini de classes de similitude entière.

– III – Un théorème de finitude

Si $(\Gamma, +)$ est un groupe abélien et r un élément de $\mathbb{N}^*$, on dit que la famille $(e_i)_{1\leq i\leq r}$ d'éléments de Γ est une $\mathbb{Z}$-base de Γ si, et seulement si, tout élément de Γ s'écrit de façon unique $\lambda_1 e_1 + \cdots + \lambda_r e_r$ avec $(\lambda_1, \cdots, \lambda_r)$ dans $\mathbb{Z}^r$.

Si Γ admet une $\mathbb{Z}$-base finie, on dit que Γ est un groupe abélien libre de type fini ou, en abrégé, un g.a.l.t.f. On sait alors qu'alors toutes les $\mathbb{Z}$-bases de Γ ont même cardinal ; ce cardinal commun est appelé rang de Γ. par exemple, $(\mathbb{Z}^r, +)$ est un g.a.l.t.f. de rang r (et tout g.a.l.t.f. de rang r est isomorphe à $\mathbb{Z}^r$).

On pourra admettre et utiliser le résultat suivant.

Soient $(\Gamma, +)$ un g.a.l.t.f. de rang r, Γ' un sous-groupe non nul de Γ. Alors il existe une $\mathbb{Z}$-base $(e_i)_{1\leq i\leq r}$ de Γ, un entier naturel non nul $s \leq r$ et des éléments $d_1, \cdots, d_s$ de $\mathbb{N}^*$ tels que $(d_i e_i)_{1\leq i\leq s}$ soit une une $\mathbb{Z}$-base de Γ'. En particulier, Γ' est un g.a.l.t.f. de rang $\leq r$.

– A – Groupes abéliens libres de type fini

1. Soient Γ un g.a.l.t.f. de rang n, $(e_i)_{1\leq i\leq n}$ une $\mathbb{Z}$-base de Γ, $(f_j)_{1\leq j\leq n}$ une famille d'éléments de Γ. Si $1 \leq j \leq n$, on écrit :
$$f_j = \sum_{i=1}^{n} p_{i,j} e_i$$
où la matrice $P = (p_{i,j})_{1\leq i,j}$ est dans $\mathcal{M}_n(\mathbb{Z})$. Montrer que $(f_j)_{1\leq j\leq n}$ est une $\mathbb{Z}$-base de Γ si, et seulement si, P appartient à $GL_n(\mathbb{Z})$.
2. Dire que $(f_j)_{1\leq j\leq n}$ est une $\mathbb{Z}$-base de Γ équivaut à dire que pour tout $g = \sum_{i=1}^{n} \mu_i e_i \in \Gamma$, il existe un unique $\lambda = (\lambda_j)_{1\leq j\leq n} \in \mathbb{Z}^n$ tel que :
$$g = \sum_{j=1}^{n} \lambda_j f_j = \sum_{j=1}^{n} \lambda_j \left(\sum_{i=1}^{n} p_{i,j} e_i \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} p_{i,j} \lambda_j \right) e_i$$
ce qui équivaut à dire que pour tout $\mu = (\mu_i)_{1\leq i\leq n} \in \mathbb{Z}^n$, il existe un unique $\lambda = (\lambda_j)_{1\leq j\leq n} \in \mathbb{Z}^n$ tel que :
$$\mu_i = \sum_{j=1}^{n} p_{i,j} \lambda_j \ \ (1 \leq i \leq n)$$
ce qui est encore équivalent à dire que le morphisme de groupes $\lambda \mapsto \mu$ défini par les relations précédentes est bijectif et se traduit par la condition $P \in GL_n(\mathbb{Z})$.
3. Soient $(\Gamma, +)$ un g.a.l.t.f. et Γ' un sous-groupe de Γ. Montrer que le groupe quotient Γ/Γ' est fini si, et seulement si, Γ et Γ' ont même rang.

4. Soient $(e_i)_{1\leq i\leq r}$ une $\mathbb{Z}$-base de Γ et $(d_i)_{1\leq i\leq s}$ dans $(\mathbb{N}^*)^s$ avec $1\leq s\leq r$ tels que $(d_ie_i)_{1\leq i\leq s}$ soit une une $\mathbb{Z}$-base de Γ'. Le morphisme de groupes :

$$\begin{array}{rccc}\varphi: & \Gamma & \to & \displaystyle\prod_{k=1}^{s}\frac{\mathbb{Z}}{d_k\mathbb{Z}}\times\mathbb{Z}^{r-s}\\ & \displaystyle g=\sum_{i=1}^{r}\lambda_ie_i & \mapsto & (\lambda_1+d_1\mathbb{Z},\cdots,\lambda_s+d_s\mathbb{Z},\lambda_{s+1},\cdots,\lambda_r)\end{array}$$

est surjectif de noyau Γ', il induit donc un isomorphisme :

$$\begin{array}{rccc}\overline{\varphi}: & \Gamma/\Gamma' & \to & \displaystyle\prod_{k=1}^{s}\frac{\mathbb{Z}}{d_k\mathbb{Z}}\times\mathbb{Z}^{r-s}\\ & \displaystyle \overline{g}=\sum_{i=1}^{r}\lambda_ie_i+\Gamma' & \mapsto & (\lambda_1+d_1\mathbb{Z},\cdots,\lambda_s+d_s\mathbb{Z},\lambda_{s+1},\cdots,\lambda_r)\end{array}$$

Il en résulte que Γ/Γ' est fini si, et seulement si, $r=s$, ce qui revient à dire que Γ et Γ' ont même rang.

5. Soient R un anneau commutatif intègre dont le groupe additif est un g.a.l.t.f. et I un idéal non nul de R.

   (a) Montrer que l'anneau quotient R/I est fini.

   (b) L'idéal I étant en particulier un sous-groupe additif de R, c'est un g.a.l.t.f. de rang $s\leq r=\mathrm{rg}\,(R)$.
   Si $(e_i)_{1\leq i\leq r}$ est une $\mathbb{Z}$-base de R, comme I est un idéal, pour tout $d\in R^*$, la famille $(de_i)_{1\leq i\leq r}$ engendre un sous-groupe R' de R contenu dans I.
   Pour $\lambda=(\lambda_i)_{1\leq i\leq r}\in\mathbb{Z}^r$ l'égalité $\displaystyle\sum_{i=1}^{r}\lambda_ide_i=0$ équivaut à $\displaystyle d\left(\sum_{i=1}^{r}\lambda_ie_i\right)=0$, soit à $\displaystyle\sum_{i=1}^{r}\lambda_ie_i$ puisque $d\neq 0$ et R est intègre et cette dernière égalité équivaut à la nullité de tous les λ_i puisque $(e_i)_{1\leq i\leq r}$ est une $\mathbb{Z}$-base de R. En définitive, $(de_i)_{1\leq i\leq r}$ est une $\mathbb{Z}$-base de R' qui est donc de rang r. Comme $R'\subset I\subset R$, on en déduit que le rang de I est aussi égal à r. La question précédente nous dit alors que l'anneau quotient R/I est fini.

   (c) Montrer que l'ensemble des idéaux de R contenant I est fini.

   (d) La surjection canonique $\pi: R\to R/I$ induit une bijection entre les idéaux de R qui contiennent I et les idéaux de R/I, donc cet ensemble est fini.

6. Soient m et n dans $\mathbb{N}^*$ avec $m\leq n$, V un sous-espace de dimension m de $\mathbb{Q}^n$. Montrer qu'il existe une $\mathbb{Z}$-base $(e_i)_{1\leq i\leq n}$ de $\mathbb{Z}^n$ telle que $(e_i)_{1\leq i\leq m}$ soit une $\mathbb{Q}$-base de V.

7. Comme $V\cap\mathbb{Z}^n$ est un sous groupe de $\mathbb{Z}^n$, il existe une $\mathbb{Z}$-base $(e_i)_{1\leq i\leq n}$ de $\mathbb{Z}^n$, un entier naturel non nul $m\leq n$ et des éléments $d_1,\cdots,d_m$ de $\mathbb{N}^*$ tels que $(d_ie_i)_{1\leq i\leq m}$ soit une une $\mathbb{Z}$-base de $V\cap\mathbb{Z}^n$. Comme V est un $\mathbb{Q}$-sous-espace vectoriel de $\mathbb{Q}^n$, pour tout $x\in V$, on peut trouver un entier naturel non nul d tel que $dx\in V\cap\mathbb{Z}^n$ et en conséquence, il existe des entiers $\lambda_1,\cdots,\lambda_m$ tels que $\displaystyle dx=\sum_{i=1}^{m}\lambda_id_ie_i$ et $\displaystyle x=\sum_{i=1}^{m}\frac{\lambda_id_i}{d}e_i$, les $\displaystyle\frac{\lambda_id_i}{d}$ étant dans $\mathbb{Q}$.

La famille $(e_i)_{1\leq i\leq m}$ est donc génératrice pour V et comme cette famille est $\mathbb{Q}$-libre, c'est une base de V.
La dimension de V est donc égale au rang du groupe $V\cap\mathbb{Z}^n$.

Dans les parties **III.B.** et **III.C.** P est un élément de $U_n(\mathbb{Z})$ irréductible sur $\mathbb{Q}$, α une racine de P dans $\mathbb{C}$, $\mathbb{Q}[\alpha]$ la $\mathbb{Q}$-sous-algèbre de $\mathbb{C}$ engendrée par α, c'est-à-dire le sous-espace du $\mathbb{Q}$-espace vectoriel $\mathbb{C}$ dont $(\alpha^i)_{0\leq i\leq n-1}$ est une base. On rappelle que $\mathbb{Q}[\alpha]$ est un-sous-corps de $\mathbb{C}$. Si l'élément z de $\mathbb{Q}[\alpha]$ s'écrit $x_0+x_1\alpha+\cdots+x_{n-1}\alpha^{n-1}$ où $(x_0,\cdots,x_{n-1})$ est dans $\mathbb{Q}^n$, on pose :

$$\mathcal{N}(x)=\max_{0\leq i\leq n-1}|x_i|$$

On note $\mathbb{Z}[\alpha]$ le sous-anneau de $\mathbb{Q}[\alpha]$:

$$\mathbb{Z}[\alpha]=\left\{\sum_{i=0}^{n-1}x_i\alpha^i,\ (x_0,\cdots,x_{n-1})\in\mathbb{Z}^n\right\}$$

On vérifie que $\mathbb{Q}[\alpha]$ est le corps des fractions de $\mathbb{Z}[\alpha]$; la justification n'est pas demandée. Si P est une partie non vide de $\mathbb{Q}[\alpha]$ et a un élément de $\mathbb{Q}[\alpha]$, on note aP l'ensemble :

$$\{ax,\ x\in P\}$$

On note $\mathcal{I}$ l'ensemble des idéaux non nuls de $\mathbb{Z}[\alpha]$.

– B – Classes d'idéaux

1. Montrer qu'il existe $C>0$ tel que :

$$\forall(x,y)\in\mathbb{Q}[\alpha]^2,\ \mathcal{N}(xy)\leq C\mathcal{N}(x)\mathcal{N}(y)$$

2. Pour $x=\sum_{i=0}^{n-1}x_i\alpha^i$ et $y=\sum_{j=0}^{n-1}y_j\alpha^j$ dans $\mathbb{Q}[\alpha]$, on a :

$$\begin{aligned}\mathcal{N}(xy)&=\mathcal{N}\left(\sum_{0\leq i,j\leq n-1}x_iy_j\alpha^{i+j}\right)\leq\sum_{0\leq i,j\leq n-1}\mathcal{N}\left(x_iy_j\alpha^{i+j}\right)\\&\leq\sum_{0\leq i,j\leq n-1}|x_iy_j|\mathcal{N}\left(\alpha^{i+j}\right)\end{aligned}$$

puisque $\mathcal{N}(\lambda x+y)\leq|\lambda|\mathcal{N}(x)+\mathcal{N}(y)$ pour tous x,y dans $\mathbb{Q}[\alpha]$ et tout λ dans $\mathbb{Q}$ et $\alpha^k\in\mathbb{Q}[\alpha]$ pour tout entier naturel k.
Et avec $|x_iy_j|\leq\mathcal{N}(x)\mathcal{N}(y)$ pour tous i,j, on en déduit que :

$$\mathcal{N}(xy)\leq\left(\sum_{0\leq i,j\leq n-1}\mathcal{N}\left(\alpha^{i+j}\right)\right)\mathcal{N}(x)\mathcal{N}(y)=C\mathcal{N}(x)\mathcal{N}(y)$$

3. Si y est dans $\mathbb{Q}[\alpha]$ et M dans $\mathbb{N}^*$, montrer qu'il existe m dans $\{1, \cdots, M^m\}$ et α dans $\mathbb{Z}[\alpha]$ tels que :
$$\mathcal{N}(my - a) \leq \frac{1}{M}$$
Indication : Posant $y = y_0 + y_1\alpha + \cdots + y_{n-1}\alpha^{n-1}$ avec $(y_0, \cdots, y_{n-1})$ dans $\mathbb{Q}^n$, on pourra considérer, pour $0 \leq j \leq M^n$:
$$u_j = \sum_{i=0}^{n-1} (jy_i - [jy_i])\,\alpha^i$$
où $[x]$ désigne, pour x dans $\mathbb{R}$, la partie entière de x.
4. Pour $0 \leq j \leq M^n$ et $1 \leq m \leq M^n$, on a :
$$\begin{aligned} u_{m+j} - u_j &= \sum_{i=0}^{n-1} (my_i - ([jy_i] - [(m+j)\,y_i]))\,\alpha^i \\ &= m\sum_{i=0}^{n-1} y_i\alpha^i - \sum_{i=0}^{n-1} ([jy_i] - [(m+j)\,y_i])\,\alpha^i \\ &= my - a \end{aligned}$$
avec $a = \displaystyle\sum_{i=0}^{n-1} ([jy_i] - [(m+j)\,y_i])\,\alpha^i \in \mathbb{Z}[\alpha]$.
Pour tout i compris entre 0 et $n-1$, on a $0 \leq jy_i - [jy_i] < 1$ et en utilisant la partition $[0,1[= \left[0, \frac{1}{M}\right[\cup \left[\frac{1}{M}, \frac{2}{M}\right[\cup \cdots \cup \left[\frac{M-1}{M}, 1\right[$, on a un entier k_i compris entre 0 et $M-1$ tel que $jy_i - [jy_i] \in \left[\frac{k_i}{M}, \frac{k_i+1}{M}\right[$. Les $M^n + 1$ éléments u_j sont donc dans l'un des M^n pavés $\displaystyle\prod_{i=1}^{n} \left[\frac{k_i}{M}, \frac{k_i+1}{M}\right[$, il existe donc deux entiers $0 \leq j < k = m + j \leq M^n$ tels que u_j et u_{m+j} soient dans le même pavé, ce qui nous donne :
$$\mathcal{N}(my - a) = \mathcal{N}(my - a) = \mathcal{N}(u_{m+j} - u_j) \leq \frac{1}{M}$$
5. On définit la relation $\sim$ sur $\mathcal{I}$ en convenant que $I_1 \sim I_2$ si, et seulement si, il existe a et b dans $\mathbb{Z}[\alpha] \setminus \{0\}$ tels que $aI_1 = bI_2$, c'est-à-dire s'il existe x dans $\mathbb{Q}[\alpha] \setminus \{0\}$ tel que $I_2 = xI_1$. Il est clair que $\sim$ est une relation d'équivalence sur $\mathcal{I}$. On se propose de montrer que le nombre de classes de cette relation est fini.
On fixe I dans $\mathcal{I}$, z dans $I \setminus \{0\}$ tel que $\mathcal{N}(z)$ soit minimal (ce qui est possible car l'image d'un élément non nul de $\mathbb{Z}[\alpha]$ par $\mathcal{N}$ appartient à $\mathbb{N}^*$).
Soient également M un entier strictement supérieur à C et ℓ le ppcm des éléments de $\mathbb{N}^*$ inférieurs ou égaux à M^n.
   (a) Soit x dans I. En appliquant la question **2.** à $y = \dfrac{x}{z}$ montrer que :
$$\ell I \subset z\mathbb{Z}[\alpha]$$

(b) Pour tous $x \in I \subset \mathbb{Z}[\alpha]$ et $z \in I \setminus \{0\}$, on a $y = \dfrac{x}{z} \in \mathbb{Q}[\alpha]$. Pour tout $M \in \mathbb{N}^*$, il existe $m \in \{1, \cdots, M^m\}$ et $\alpha \in \mathbb{Z}[\alpha]$ tels que :

$$\mathcal{N}(my - a) \leq \frac{1}{M}$$

ce qui nous donne :

$$\begin{aligned}\mathcal{N}(mx - az) = \mathcal{N}((my - a)z) &\leq C\mathcal{N}(my - a)\mathcal{N}(z) \\ &\leq \frac{C}{M}\mathcal{N}(z)\end{aligned}$$

et choisissant $M > C$, cela donne $\mathcal{N}(mx - az) < \mathcal{N}(z)$.
Comme x, z sont dans l'idéal I et a dans $\mathbb{Z}[\alpha]$, on a $mx - az \in I$ et choisissant z tel que $\mathcal{N}(z) = \inf_{t \in I \setminus \{0\}} \mathcal{N}(t)$, on a nécessairement $mx - az = 0$, ce qui nous donne, pour $\ell = \text{ppcm}\{1, \cdots, M^m\}$, $\ell x = \dfrac{\ell}{m} az \in z\mathbb{Z}[\alpha]$ ($m \in \{1, \cdots, M^m\}$ divise ℓ).
On a donc ainsi montré que $\ell I \subset z\mathbb{Z}[\alpha]$.

(c) Vérifier que $J = \dfrac{\ell}{z} I$ est un idéal de $\mathbb{Z}[\alpha]$ contenant $\ell \cdot \mathbb{Z}[\alpha]$ et conclure.

(d) La question précédente nous dit que, pour tout idéal non nul I de $\mathbb{Z}[\alpha]$, l'ensemble $J = \dfrac{z}{\ell} I$ est contenu dans $\mathbb{Z}[\alpha]$. De plus, il est clair que J est un idéal non nul de $\mathbb{Z}[\alpha]$ et il est équivalent à I ($\dfrac{z}{\ell} \in \mathbb{Q}[\alpha] \setminus \{0\}$).
On a $\ell = \dfrac{z}{\ell} \ell \in J$, donc $\ell \cdot \mathbb{Z}[\alpha] \subset J$.
En définitive, on a montré que tout idéal de $\mathbb{Z}[\alpha]$ est équivalent à un idéal de de $\mathbb{Z}[\alpha]$ qui contient un idéal donné non nul, à savoir $\ell \cdot \mathbb{Z}[\alpha]$. En **III.A.3.b.** on a vu qu'il n'y a qu'un nombre fini de tels idéaux, ce qui nous dit que le nombre de classes d'équivalences, pour la relation $\sim$ sur $\mathcal{I}$, est fini.

– C – Classes de similitudes et classes d'idéaux

1. Soient M dans $\mathcal{E}_{\mathbb{Z}}(P)$, X_M l'ensemble des éléments $x = (x_1, \cdots, x_n)$ non nuls de $\mathbb{Z}[\alpha]^n$ tels que le vecteur colonne ${}^t x$ soit vecteur propre de M associé à α.

(a) Montrer que X_M n'est pas vide, que si x et y sont dans X_M, il existe a et b dans $\mathbb{Z}[\alpha] \setminus \{0\}$ tels que $ax = by$.

(b) Si $M \in \mathcal{E}_{\mathbb{Z}}(P)$, on a alors $M \in \mathcal{M}_n(\mathbb{Z})$ et $\chi_M = P$, donc α qui est racine complexe de P, est valeur propre de M dans le corps $\mathbb{Q}[\alpha]$, il existe donc $y = (y_1, \cdots, y_n)$ dans $\mathbb{Q}[\alpha]^n \setminus \{0\}$ tel que ${}^t y\, M$ soit vecteur propre de M associé à α et pour un entier non nul r bien choisi, l'élément $x = ry \in \mathbb{Z}[\alpha]^n \setminus \{0\}$ est tel que ${}^t x$ soit vecteur propre de M associé à α. Donc X_M n'est pas vide.
Comme le polynôme $\chi_M = P$ est irréductible dans $\mathbb{Q}[X]$, cette racine $\alpha \in \mathbb{Q}[\alpha]$ est simple (conséquence du théorème de Bézout comme en **I.B.2.**) et le sous espace propre associé dans $\mathbb{Q}[\alpha]^n$ est de dimension 1. Il en résulte que deux éléments x, y de $X_M \setminus \{0\}$ sont nécessairement $\mathbb{Q}[\alpha]$-colinéaires, ce qui revient à dire qu'il existe a et b dans $\mathbb{Z}[\alpha] \setminus \{0\}$ tels que $ax = by$.

(c) Si $x=(x_1,\cdots,x_n)$ est dans X_M, soit (x) le sous-groupe de $(\mathbb{Z}[\alpha],+)$ engendré par $x_1,\cdots,x_n$. Montrer que (x) est un idéal de $\mathbb{Z}[\alpha]$, que $(x_1,\cdots,x_n)$ en est une $\mathbb{Z}$-base, que si y est dans X_M, alors $(x)\sim(y)$.
On notera j l'application de $\mathcal{E}_{\mathbb{Z}}(P)$ dans l'ensemble quotient $\mathcal{I}/\sim$ qui à M associe la classe de (x) pour $\sim$.

(d) On sait déjà que (x) est un sous-groupe de $(\mathbb{Z}[\alpha],+)$. Comme $M\ {}^t x=\alpha\ {}^t x$, on a $\alpha x_i=\sum_{j=1}^{n} m_{ij}x_j\in(x)$ pour tout j compris entre 1 et n, puisque $M\in\mathcal{M}_n(\mathbb{Z})$. Il en résulte que $\alpha^k x_i\in(x)$ pour tout entier naturel k et tout i, donc $ax_i\in(x)$ pour tout $a\in\mathbb{Z}[\alpha]$ et tout i compris entre 1 et n. Donc (x) est un idéal de $\mathbb{Z}[\alpha]$.
De manière analogue, on voit que le $\mathbb{Q}$-sous-espace vectoriel $\mathrm{Vect}(x)$ de $\mathbb{Q}[\alpha]$ engendré par $x_1,\cdots,x_n$ est un idéal non réduit à $\{0\}$ de $\mathbb{Q}[\alpha]$ et comme $\mathbb{Q}[\alpha]$ est un corps, on a nécessairement $\mathrm{Vect}(x)=\mathbb{Q}[\alpha]$. Il en résulte que $\dim_{\mathbb{Q}}(\mathrm{Vect}(x))=\dim_{\mathbb{Q}}(\mathbb{Q}[\alpha])=n$ et la famille $(x_1,\cdots,x_n)$ est $\mathbb{Q}$-libre, donc $\mathbb{Z}$-libre et c'est une $\mathbb{Z}$-base de (x).
On a vu en **a.** que tout $y\in X_M$ s'écrit $y=\lambda x$ avec $\lambda\in\mathbb{Q}[\alpha]\setminus\{0\}$, donc $(y)=\lambda(x)$ et $(x)\sim(y)$.

2.

(a) Montrer que l'application j est surjective.

(b) Soit $I\in\mathcal{I}$, comme $\mathbb{Z}[\alpha]$ est de rang n, on déduit de **III.A.3.b.** que l'anneau quotient $\mathbb{Z}[\alpha]/I$ est fini et I est de rang n d'après **III.A.2.** En désignant par $x=(x_i)_{1\leq i\leq n}$ une $\mathbb{Z}$-base de I, il existe des entiers m_{ij} tels que, pour tout i compris entre 1 et n, on ait $\alpha x_i=\sum_{j=1}^{n} m_{ij}x_j$ (on a $\alpha x_i\in I$ puisque I est un idéal de $\mathbb{Z}[\alpha]$), ce qui se traduit par $M\ {}^t x=\alpha\ {}^t x$ avec $M=((m_{ij}))_{1s<i,jS<n}\in\mathcal{M}_n(\mathbb{Z})$. En conséquence, α est racine dans $\mathbb{Q}[\alpha]$ du polynôme caractéristique χ_M. Comme $P\in\mathbb{Q}[X]$ est le polynôme minimal de α, il va diviser χ_M et nécessairement $P=\chi_M$ puisque ces polynômes sont de même degré et unitaires. En définitive, $M\in\mathcal{E}_{\mathbb{Z}}(P)$ et $j(M)$ est la classe de (x).

(c) Soient M et M' dans $\mathcal{E}_{\mathbb{Z}}(P)$. Montrer que M et M' sont semblables sur $\mathbb{Z}$ si, et seulement si, $j(M)=j(M')$.

(d) Si M et M' sont semblables sur $\mathbb{Z}$, il existe alors $Q\in GL_n(\mathbb{Z})$ telle que $M'=Q^{-1}MQ$. Pour tout $x'\in X_{M'}$, en notant ${}^t x=Q\ {}^t x'$, on a :

$$M\ {}^t x=QM'Q^{-1}\ {}^t x=QM'\ {}^t x'=\alpha Q\ {}^t x'=\alpha\ {}^t x$$

et $x\in X_M$, donc $(x)\sim(x')$ et $j(M)=j(M')$.
Si $j(M)=j(M')$, il existe alors $x\in X_M$ et $x'\in X_{M'}$ tels que $(x)\sim(x')$, ce qui signifie qu'il existe a,b dans $\mathbb{Z}[\alpha]\setminus\{0\}$ tels que $a(x)=b(x')$. Les familles $y=ax\in X_M$ et $y'=bx'\in X_{M'}$ sont deux $\mathbb{Z}$-bases du même g.a.l.t.f. $a(x)=b(x')$, donc il existe $Q\in GL_n(\mathbb{Z})$ telle que ${}^t y=Q\ {}^t y'$ (question **III.A.1.**). En notant $M''=Q^{-1}MQ$, on a :

$$M''\ {}^t y'=Q^{-1}MQQ^{-1}\ {}^t y=Q^{-1}M\ {}^t y=Q^{-1}\alpha\ {}^t y=\alpha\ {}^t y'=M'\ {}^t y'$$

Il en résulte que $M' = M''$ puisque la matrice $M' \in \mathcal{M}_n(\mathbb{Z})$ telle que $\alpha\, {}^t y' = M'\, {}^t y'$ est uniquement déterminée par le fait que y' est une $\mathbb{Z}$-base de (y') et les $\alpha y'_i$ sont dans (y') pour tout i compris entre 1 et n. Les matrices M et M' sont donc semblables sur $\mathbb{Z}$.

– D – Finitude de l'ensemble $\mathcal{D}_{\mathbb{Z}}(P)$

On se propose d'établir que, pour tout polynôme unitaire non constant P de $\mathbb{Z}[X]$, l'ensemble $\mathcal{D}_{\mathbb{Z}}(P)$ est réunion finie de classes de similitude entière. On raisonne par récurrence sur le degré de P. Le cas où ce degré est 1 est évident, on suppose $n \geq 2$ et le résultat prouvé pour tout P de degré majoré par $n-1$.

On fixe désormais P dans $U_n(\mathbb{Z})$. Si P est irréductible sur $\mathbb{Q}$, on a vu à la fin de **III.C.** que $\mathcal{E}_{\mathbb{Z}}(P)$ est réunion finie de classes de similitude entière. On suppose donc P réductible sur $\mathbb{Q}$, et on se donne un diviseur irréductible Q de P dans $\mathbb{Q}[X]$ unitaire non constant, dont on note m le degré. D'après la question **I.B.3.** Q P/Q sont respectivement dans $U_m(\mathbb{Z})$ et $U_{n-m}(\mathbb{Z})$. On dispose donc (récurrence) de r et s dans $\mathbb{N}^*$, de r éléments $A_1, \cdots, A_r$ de $\mathcal{D}_{\mathbb{Z}}(Q)$ [resp. de de s éléments $A'_1, \cdots, A'_s$ de $\mathcal{D}_{\mathbb{Z}}(P/Q)$] tels que tout élément de $\mathcal{D}_{\mathbb{Z}}(Q)$ [resp. de $\mathcal{D}_{\mathbb{Z}}(P/Q)$] soit semblable sur $\mathbb{Z}$ à un et un seul A_i [resp. A'_j].

Soit M dans $\mathcal{D}_{\mathbb{Z}}(P)$.

1. Montrer que M est semblable sur $\mathbb{Z}$ à une matrice de la forme :
$$\begin{pmatrix} A_i & B \\ 0 & A'_j \end{pmatrix}$$
avec $1 \leq i \leq r$, $1 \leq j \leq s$, $B \in \mathcal{M}_{m,n-m}(\mathbb{Z})$.

2. On identifie M à l'endomorphisme de $\mathbb{Q}^n$ qu'il définit dans la base canonique.
On a $\chi_M = P = QR$ avec $Q \in U_m(\mathbb{Z})$ irréductible et $R \in U_{n-m}(\mathbb{Z})$, donc le polynôme minimal de M est de la forme $\pi_M = QS$ avec $R \in U_p(\mathbb{Z})$ (χ_M et π_M ont les mêmes facteurs irréductibles dans $\mathbb{Q}[X]$). On a donc $S(M) \neq 0$ et pour tout vecteur non nul x dans $\mathrm{Im}(S(M))$, on a $Q(M)(x) = 0$.
Le sous espace vectoriel de $\mathbb{Q}^n$, $V = \mathrm{Vect}\left\{M^k(x) \mid k \in \mathbb{N}\right\}$, est stable par M et il est de dimension m avec pour base $\left(M^k(x)\right)_{0 \leq k \leq m-1}$ puisque Q est le polynôme minimal de x relativement à M (i.e. le générateur unitaire dans $\mathbb{Q}[X]$ de l'idéal $\{\varphi \in \mathbb{Q}[X] \mid \varphi(M)(x) = 0\}$).
Le polynôme Q est donc le polynôme minimal et le polynôme caractéristique de la restriction de M à V. En utilisant le résultat de **III.A.4.** on déduit qu'il existe une $\mathbb{Z}$-base $(e_i)_{1 \leq i \leq n}$ de $\mathbb{Z}^n$ telle que $\mathcal{B} = (e_i)_{1 \leq i \leq m}$ soit une $\mathbb{Q}$-base de V.
En notant $A \in GL_n(\mathbb{Z})$ la matrice de passage de la base canonique de $\mathbb{Q}^n$ à la $\mathbb{Z}$-base $\mathcal{B}$, la matrice M est semblable à :
$$M' = A^{-1}MA = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$
avec B, C, D dans $\mathcal{M}(\mathbb{Z})$, la matrice $B \in \mathcal{M}_m(\mathbb{Z})$ ayant Q comme polynôme caractéristique. Le polynôme caractéristique D est alors $\dfrac{P}{Q}$. De **I.C.4.** on déduit que $B \in \mathcal{D}_{\mathbb{Z}}(Q)$, $D \in \mathcal{D}_{\mathbb{Z}}(P/Q)$ et l'hypothèse de récurrence nous dit qu'il existe une matrice A_i de $\mathcal{D}_{\mathbb{Z}}(Q)$ semblable sur $\mathbb{Z}$ à B et une matrice A'_j de $\mathcal{D}_{\mathbb{Z}}(P/Q)$ semblable sur $\mathbb{Z}$ à B. Il en résulte qu'il existe une matrice $B' \in \mathcal{M}(\mathbb{Z})$ telle que M soit semblable sur $\mathbb{Z}$ à $\begin{pmatrix} A_i & B' \\ 0 & A'_j \end{pmatrix}$.

3. Montrer que :

$$\Gamma = \mathcal{M}_{m,n-m}(\mathbb{Z}) \cap \left\{ A_i X - X A'_j \mid X \in \mathcal{M}_{m,n-m}(\mathbb{Q}) \right\}$$

$$\text{et } \Gamma' = \left\{ A_i X - X A'_j \mid X \in \mathcal{M}_{m,n-m}(\mathbb{Z}) \right\}$$

sont deux g.a.l.t.f. de même rang.

4. Soit φ_{ij} l'application $\mathbb{Q}$-linéaire :

$$\begin{array}{rccc} \varphi_{ij} : & \mathcal{M}_{m,n-m}(\mathbb{Q}) & \to & \mathcal{M}_{m,n-m}(\mathbb{Q}) \\ & X & \mapsto & A_i X - X A'_j \end{array}$$

On a $\Gamma = \mathcal{M}_{m,n-m}(\mathbb{Z}) \cap \mathrm{Im}(\varphi_{ij})$ et $\Gamma' = \varphi\left(\mathcal{M}_{m,n-m}(\mathbb{Z})\right)$, donc Γ et Γ' sont des g.a.l.t.f. comme sous-groupes du g.a.l.t.f. $\mathcal{M}_{m,n-m}(\mathbb{Z})$. Ces deux ensembles étant $\mathbb{Q}$-générateurs du $\mathbb{Q}$-sous-espace vectoriel $\mathrm{Im}(\varphi_{ij})$ de $\mathcal{M}_{m,n-m}(\mathbb{Q})$, ils sont de même rang.

5. Conclure que $\mathcal{D}_{\mathbb{Z}}(P)$ est réunion finie de classes de similitude entière.

6. Toute matrice $M \in \mathcal{D}_{\mathbb{Z}}(P)$ est semblable sur $\mathbb{Z}$ à une matrice de la forme :

$$\begin{pmatrix} A_i & B \\ 0 & A'_j \end{pmatrix}$$

avec $1 \leq i \leq r$, $1 \leq j \leq s$, $B \in \mathcal{M}_{m,n-m}(\mathbb{Z})$ et **I.C.4.** nous dit que $B \in \Gamma = \mathcal{M}_{m,n-m}(\mathbb{Z}) \cap \mathrm{Im}(\varphi_{ij})$.
Comme Γ est un sous-groupe de Γ' et ce sont des g.a.l.t.f. de même rang, l'ensemble quotient Γ/Γ' est fini d'après **III.A.2.** soit $\Gamma/\Gamma' = \left\{ \overline{B_1^{(i,j)}}, \cdots, \overline{B_{r_{ij}}^{(i,j)}} \right\}$. Avec :

$$\begin{pmatrix} I_m & B \\ 0 & I_{n-m} \end{pmatrix}^{-1} \begin{pmatrix} A_i & B \\ 0 & A'_j \end{pmatrix} \begin{pmatrix} I_m & B \\ 0 & I_{n-m} \end{pmatrix} = \begin{pmatrix} A_i & B + \varphi_{ij}(X) \\ 0 & A'_j \end{pmatrix}$$

on déduit que toute matrice $M \in \mathcal{D}_{\mathbb{Z}}(P)$ est semblable sur $\mathbb{Z}$ à une matrice de la forme :

$$\begin{pmatrix} A_i & B_k^{(i,j)} \\ 0 & A'_j \end{pmatrix}$$

Comme ces matrices sont en nombre fini, il en résulte que $\mathcal{D}_{\mathbb{Z}}(P)$ est réunion finie de classes de similitude entière.