3.3 Corrigé

Présentation du sujet

Comme dans l'énoncé, n est un élément de $\mathbf{N}^*$, K un corps. Si P est un polynôme unitaire de degré n de $K[X]$ (resp. $\mathbf{Z}[X]$), $\mathscr{E}_K(P)$ (resp. $\mathscr{E}_{\mathbf{Z}}(P)$) désigne l'ensemble des matrices de $\mathscr{M}_n(K)$ (resp. $\mathscr{M}_n(\mathbf{Z})$) dont le polynôme caractéristique est P.

Il est immédiat de vérifier que $\mathscr{E}_K(P)$ (resp. $\mathscr{E}_{\mathbf{Z}}(P)$) est réunion de classes de similitude (resp. de classes de similitude entière). En utilisant la théorie des invariants de similitude (ou la réduction de Jordan et l'inertie de la similitude par extension de corps), on voit facilement que $\mathscr{E}_K(P)$ est une réunion finie de classes de similitude. Le but du problème est d'étudier la question correspondante en remplaçant le corps K par l'anneau $\mathbf{Z}$.

La première partie est consacrée à divers préliminaires relatifs à la similitude sur un corps et aux polynômes. On y établit notamment le résultat suivant.

Theorème 1. Soient m un entier tel que $0 < m < n$, A dans $\mathscr{M}_m(K)$, A' dans $\mathscr{M}_{n-m}(K)$, B dans $\mathscr{M}_{m,n-m}(K)$, M et N les matrices :

$$M = \left(\begin{array}{c|c} A & B \\ \hline 0 & A' \end{array}\right) \qquad \text{et} \qquad N = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & A' \end{array}\right).$$

(i) Les matrices M et N sont semblables sur K si et seulement s'il existe $X \in \mathscr{M}_{m,n-m}(K)$ telle que $B = AX - XA'$.

(ii) La matrice M est diagonalisable sur K si et seulement si A et A' sont diagonalisables sur K et s'il existe $X \in \mathscr{M}_{m,n-m}(K)$ telle que : $B = AX - XA'$.

L'assertion (ii), seule utilisée dans le problème, est vue ici comme conséquence immédiate de (i) ; on peut en donner une preuve directe très simple en traitant d'abord le cas où les matrices A et A' sont diagonales.

L'énoncé (i) est dû à W. Roth ([6]). La preuve originale est moins élémentaire mais plus instructive que celle proposée dans le sujet, laquelle est extraite de [4].

Dans toute la suite, on fixe P dans $\mathbf{Z}[X]$ unitaire de degré n.

L'étude de la similitude entière est plus subtile que celle de la similitude sur un corps. Posons en effet, pour d dans $\mathbf{N}$:

$$J_d = \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}.$$

Alors d est le p.g.c.d des coefficients de J_d, et le p.g.c.d des coefficients est invariant par $\mathbf{Z}$-équivalence, ce qui entraîne que si $d \neq d'$, J_d et $J_{d'}$ ne sont équivalentes sur $\mathbf{Z}$, donc a fortiori pas semblables sur $\mathbf{Z}$. Il s'ensuit que l'ensemble $\mathscr{E}_{\mathbf{Z}}(X^2)$ n'est pas réunion finie de classes de similitude entière.

La partie **II.D** du problème généralise cette observation de la façon suivante.

Théorème 2. Si les racine de P dans $\mathbf{C}$ ne sont pas toutes simples, alors $\mathscr{E}_{\mathbf{Z}}(P)$ n'est pas réunion finie de classes de similitude entière.

La preuve, très simple, repose sur le théorème 1 et la réduction modulo un nombre premier.

On dispose cependant de résultats positifs. Si $P = X^2 - 1$, on montre en **II.A** que toute matrice de $\mathscr{E}_{\mathbf{Z}}(P)$ est semblable à une et une seule des deux matrices :

$$\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}, \quad a \in \{0, 1\}.$$

Si δ est un élément de $\mathbf{Z}$ qui n'est pas un carré parfait et $P = X^2 - \delta$, on montre en **II.B** par des opérations élémentaires que $\mathscr{E}_{\mathbf{Z}}(P)$ est réunion finie de classes de similitude entière. Ce dernier résultat est en fait à peu de choses près une reformulation d'un théorème de finitude dû à Lagrange : l'ensemble des classes de formes quadratiques binaires entières de discriminant $d \in \mathbf{Z}^*$ fixé est fini.

Plus généralement, la restriction aux classes de similitude semi-simples permet de formuler un résultat de finitude. Notons comme dans l'énoncé $\mathscr{D}_{\mathbf{Z}}(P)$ l'ensemble des matrices de $\mathscr{E}_{\mathbf{Z}}(P)$ semi-simples, i.e diagonalisables sur $\mathbf{C}$ (ou sur $\overline{\mathbb{Q}}$). L'ensemble $\mathscr{D}_{\mathbf{Z}}(P)$ n'est pas vide et on a le :

Théorème 3. (i) L'ensemble $\mathscr{D}_{\mathbf{Z}}(P)$ est réunion finie de classes de similitude entières.

(ii) Si les racines de P dans $\mathbf{C}$ sont simples, $\mathscr{E}_{\mathbf{Z}}(P)$ est réunion finie de classes de similitude entières.

Ce théorème, établi dans la partie **III** du texte, est le résultat essentiel du sujet. Il est implicite dans l'article [5] de Latimer et Mac-Duffee. Le second point est conséquence immédiate du premier ; sous l'hypothèse de (ii), on a en effet :

$$\mathscr{E}_{\mathbf{Z}}(P) = \mathscr{D}_{\mathbf{Z}}(P).$$

La sous-partie **III.A** rassemble quelques généralités relatives aux groupes abéliens libres de type fini. La suite du sujet est consacrée à la preuve du premier énoncé du théorème 3. Elle se décompose en deux étapes.

On commence par supposer P irréductible. Dans ce cas, l'ensemble $\mathscr{E}_{\mathbf{Z}}(P)$ est, comme l'a observé Olga Taussky, en bijection avec l'ensemble des "classes d'idéaux" de l'anneau $\mathbf{Z}[X]/P$; la démonstration de ce fait, suivant [7], est proposée dans la partie **III.C**. Or, si R est un ordre d'un corps de nombres, l'ensemble des classes d'idéaux de R est fini, d'où le résultat puisque $\mathbf{Z}[X]/P$ est un ordre du corps de nombres $\mathbb{Q}[X]/P$. Ce résultat classique de théorie algébrique des nombres est établi, pour l'ordre $\mathbf{Z}[X]/P$, dans la partie **III.B**.

Le cas général est traité dans **III.D**. On part des deux remarques suivantes.

(i) Si $P = QR$ avec Q et R dans $\mathbf{Z}[X]$ unitaires non constants et Q irréductible, toute matrice de $\mathscr{E}_{\mathbf{Z}}(P)$ est semblable sur $\mathbf{Z}$ à une matrice

$$\left(\begin{array}{c|c} A & B \\ \hline 0 & A' \end{array}\right)$$

avec A dans $\mathscr{E}_{\mathbf{Z}}(Q)$, A' dans $\mathscr{E}_{\mathbf{Z}}(R)$. Ce fait résulte d'une observation simple : si V est un sous-espace de $\mathbb{Q}^n$, il existe un sous-groupe Γ de $V \cap \mathbf{Z}^n$ engendrant le $\mathbb{Q}$-espace V et facteur direct dans $\mathbf{Z}^n$.

(ii) Si A est dans $\mathscr{M}_m(\mathbf{Z})$ et A' dans $\mathscr{M}_{n-m}(\mathbf{Z})$ l'ensemble :

$$\Gamma_{A,A'} = \{AX - XA' \ ; \ X \in \mathscr{M}_{m,n-m}(\mathbf{Z})\}$$

est un sous-groupe d'indice fini du groupe $\Gamma'_{A,A'}$ des matrices de $\mathscr{M}_{m,n-m}(\mathbf{Z})$ de la forme : $AX - XA'$ pour X dans $\mathscr{M}_{m,n-m}(\mathbb{Q})$. En effet, $\Gamma'_{A,A'}$ est un g.a.l.f et $\Gamma_{A,A'}$ en est un sous-groupe de rang maximal.

Raisonnons alors par récurrence et notons $A_1, \ldots, A_r$ (resp. $A'_1, \ldots, A'_s$) un système fini de représentants de $\mathscr{D}_{\mathbf{Z}}(Q)$ (resp. $\mathscr{D}_{\mathbf{Z}}(R)$) pour la similitude entière. Soit, pour $1 \leqslant i \leqslant r$ et $1 \leqslant j \leqslant s$, $B_1, \ldots, B_{t_{i,j}}$ un système fini de représentants de Γ'_{A_i,A'_j} modulo Γ_{A_i,A'_j}. En utilisant le théorème 1, on montre alors que toute matrice de $\mathscr{D}_{\mathbf{Z}}(P)$ est semblable sur $\mathbf{Z}$ à une des :

$$\left(\begin{array}{cc} A_i & B_k \\ 0 & A'_j \end{array}\right)$$

ce qui prouve que $\mathscr{D}_{\mathbf{Z}}(P)$ est réunion finie de classes de similitude entière.

La première assertion du théorème 3 est en fait un cas particulier d'un énoncé de Zassenhauss concernant les représentations entières d'algèbres semi-simples que l'on trouvera dans [1] ou [3]. On peut également déduire cette assertion d'un résultat de Borel et et Harish-Chandra : cf [2], paragraphes 6.4 et 9.11.

Terminons en suggérant au lecteur les deux exercices suivants.

1. Si $0 \leqslant k \leqslant n$ et $P = X^k(X-1)^{n-k}$, montrer que $\mathscr{D}_{\mathbf{Z}}(P)$ est une classe de similitude entière.

2. Si $0 \leqslant k \leqslant n$ et $P = (X-1)^k(X+1)^{n-k}$, dénombrer les classes de similitude entière contenues dans $\mathscr{D}_{\mathbf{Z}}(P)$.

Bibliographie

[1] J.M. ARNAUDIES, J. BERTIN, *Groupes, Algèbres et Géométrie, tome 2*, Ellipses, 1995

[2] A. BOREL, *Introduction aux groupes arithmétiques*, Hermann, 1969

[3] C.W. CURTIS, I.REINER, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, 1962

[4] R.A. HORN, C.R. JOHNSON, *Topics in Matrix Analysis*, Cambridge, 1991

[5] C.G. LATIMER, C.C. MACDUFFEE, *A correspondence between classes of ideals and classes of matrices*, Annals of Maths, vol 34, 1933

[6] W. ROTH, *The Equations $AX - YB = C$ and $AX - XB = C$ in Matrices*, Proc. Amer. Math. Soc. 3, 1952

[7] O. TAUSSKY, *On a theorem of Latimer and MacDuffee*, Canad. J. Math, vol 1, 1949

Corrigé du problème

Partie I

I.A.1. a) Si $a \neq c$, M admet deux valeurs propres distinctes a et b et est donc diagonalisable (un endomorphisme d'un espace de dimension m possédant m valeurs propres distinctes est diagonalisable).

Si $a = c$, la seule valeur propre de M est a. Donc M est diagonalisable si et seulement si elle est semblable à aI_2, i.e égale à aI_2 i.e si et seulement si $b = 0$.

b) Il suffit de considérer J_0 et J_1 où :

$$J_x = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}.$$

Les matrices J_a ont bien X^2 pour polynôme caractéristique et la classe de similitude de J_0 est réduite à J_0 donc ne contient pas J_1. On peut également utiliser a) en remarquant que J_1 n'est pas diagonalisable.

c) Puisque A et B sont diagonalisables, donc en particulier trigonalisables, sur K, le polynôme caractéristique commun de A et B est scindé sur K. Notons le :

$$\prod_{i=1}^{r} (X - \lambda_i)^{n_i}$$

où les λ_i sont des éléments de K deux à deux distincts et les n_i des éléments de $\mathbf{N}^*$. Puisque A (resp. B) est diagonalisable, l'espace propre de A (resp. B) associé à λ_i est, pour tout i, de dimension égale à n_i. Les matrices A et B sont donc semblables à une même matrice diagonale dont les termes diagonaux sont $\lambda_1, \ldots \lambda_r$, chaque λ_i étant répété n_i fois ; le résultat suit.

I.A.2. a) C'est le calcul classique du polynôme caractéristique d'une matrice compagnon. Il peut se mener en raisonnant par récurrence en développant par rapport à la première colonne. On peut aussi procéder de la façon suivante. Notant f l'endomorphisme de K^n canoniquement associé à $C(P)$, $(e_1, \ldots, e_n)$ la base canonique de K^n, on a :

$$\forall i \in \{0, \ldots, n-1\}, \qquad e_{i+1} = f^{(i)}(e_1),$$

de sorte que $(f^{(i)}(e_1))_{0 \leqslant i \leqslant n-1}$ est libre et que le polynôme minimal ponctuel de f relatif à e_1 est de degré supérieur ou égal à n. La lecture de la dernière colonne de $C(P)$ nous dit d'autre part que $P(f)(e_1) = 0$. Le polynôme minimal ponctuel de f relativement à e_1 est donc P. Or, ce polynôme divise le polynôme minimal de f, donc (théorème de Cayley-Hamilton) le polynôme caractéristique de f, c'est-à-dire $\chi_{C(P)}$. Par égalité des degrés on obtient l'égalité désirée.

b) La matrice extraite de $M - \lambda I_n$ en ôtant à cette dernière la première ligne et la dernière colonne est trivialement inversible (triangulaire supérieure à termes diagonaux égaux à 1), d'où le résultat.

c) Si P est simplement scindé sur K, toutes les matrices de $\mathscr{E}_K(P)$ ont leur polynôme caractéristique simplement scindé sur K et sont donc diagonalisables sur K, les espaces propres étant de dimension 1, d'où $(i) \Rightarrow (ii)$.

L'implication $(ii) \Rightarrow (iii)$ est immédiate car $C(P)$ appartient à $\mathscr{E}_K(P)$.

Enfin, la question b) montre que les éventuels espaces propres de $C(P)$ sont de dimension 1. La diagonalisabilité de $C(P)$ sur K implique donc que cette matrice a n valeurs propres distinctes dans K, c'est-à-dire que $P = \chi_{C(P)}$ est simplement scindé sur K. C'est dire que $(iii) \Rightarrow (i)$.

I.A.3. Pour P dans $K[X]$, on a :

$$P(M) = \left(\begin{array}{c|c} P(A) & 0 \\ \hline 0 & P(A') \end{array}\right).$$

Le polynôme minimal de M est donc égal au ppcm des polynômes minimaux de A et A'. Il est donc simplement scindé sur K si et seulement si ces derniers le sont également. Comme une matrice de $\mathscr{M}_n(K)$ est diagonalisable sur K si et seulement si son polynôme minimal est simplement scindé sur K, on en déduit le résultat.

Variante. Raisonnant géométriquement, un sens est immédiat : si les restrictions d'un endomorphisme f de E à deux sous-espaces stables et supplémentaires sont diagonalisables, f l'est aussi (on obtient une base propre de f en concaténant des bases propres des restrictions). L'autre sens se déduit de la diagonalisabilité de la restriction d'un endomorphisme diagonalisable à un sous-espace stable.

I.A.4. Si M est semblable à une matrice diagonale par blocs, les blocs diagonaux étant $C(P_1),\dots,C(P_r)$, le polynôme caractéristique de M est, grâce au calcul du déterminant d'une matrice diagonale par blocs et à la question 1.a), égal à : $\prod_{i=1}^r P_i$. On a en particulier $r \leqslant n$. Il résulte alors du résultat rappelé ("invariants de similitude") que l'on dipose d'une surjection de l'ensemble des listes $(P_1,\dots,P_r)$ de longueur $\leqslant n$ de polynômes unitaires non constants tels que $\prod_{i=1}^r P_i = P$ dans celui des classes de similitude de $\mathscr{E}_K(P)$. La factorialité de $K[X]$ montre que P n'admet qu'un nombre fini de diviseurs unitaires dans $K[X]$; le premier ensemble est donc fini.

I.B.1. Ecrivons $P = (X-a)Q$ avec Q dans $K[X]$. Alors :

$$P' = (X-a)Q' + Q, \quad P'(a) = Q(a).$$

Or a est racine simple de P si et seulement si $X-a$ ne divise pas Q, i.e si $Q(a) \neq 0$, i.e si $P'(a) \neq 0$.

En caractéristique nulle, on dispose d'un résultat plus précis : la multiplicité de la racine a de P est le plus petit j tel que $P^{(j)}(a) \neq 0$. Ce résultat ne subsiste évidemment pas en caractéristique p (les éléments de $K[X^p]$ ont alors une dérivée nulle).

I.B.2. Comme P n'est pas constant et $\mathbb{Q}$ est de caractéristique nulle, P' n'est pas nul. Puisque P est irréductible et P' est non nul et de degré strictement inférieur au degré de P, P et P' sont premiers entre eux dans $\mathbb{Q}[X]$. Or le p.g.c.d de deux polynômes ne dépend pas du corps de base (conséquence, par exemple, de l'algorithme d'Euclide) ; on en déduit que les racines complexes de P sont simples.

On peut aussi, après les deux premières phrases, écrire une relation de Bezout dans $\mathbb{Q}[X]$ et conclure.

I.B.3. Posons : $P = QR$ où Q et R sont dans $\mathbb{Q}[X]$ et unitaires. Choisissons a et b dans $\mathbf{N}^*$ tels que aQ et bR appartiennent à $\mathbf{Z}[X]$. On a ainsi, compte-tenu du lemme de Gauss rappelé dans l'énoncé :

$$abP = (aQ)(bR)\ ; \quad ab = c(aQ)c(bR).$$

Par suite :

$$P = \frac{aQ}{c(aQ)}\frac{bR}{c(bR)}.$$

Les deux polynômes du membre de droite sont dans $\mathbf{Z}[X]$, de coefficients dominants > 0. Leur produit P est unitaire et chacun d'eux est donc unitaire. En particulier, $\dfrac{aQ}{c(aQ)}$ est un élément unitaire de $\mathbf{Z}[X]$. Mais ce polynôme est produit du polynôme unitaire Q par le rationnel $\dfrac{a}{c(aQ)}$, ce qui impose $a = c(aQ)$, d'où l'appartenance de $Q = \dfrac{aQ}{c(aQ)}$ à $\mathbf{Z}[X]$.

I.B.4. Si P est irréductible sur $\mathbb{Q}$, la matrice $C(P)$ appartient à $\mathscr{D}_{\mathbf{Z}}(P)$ grâce à **I.A.2.**c) et **I.B.2**.

Dans le cas général, décomposons P en facteurs irréductibles unitaires dans $\mathbb{Q}[X]$:

$$P = \prod_{i=1}^{r} P_i.$$

Grâce à **I.B.3**, les P_i sont dans $\mathbf{Z}[X]$. La matrice diagonale par blocs dont les blocs diagonaux sont $C(P_1),\dots,C(P_r)$ est diagonalisable sur $\mathbf{C}$ (grâce à **I.A.3**) et appartient donc à $\mathscr{D}_{\mathbf{Z}}(P)$.

I.C.1. La matrice X est dans $\operatorname{Ker}\Phi_{U,V}$ si et seulement si : $UX = XQUQ^{-1}$, i.e si et seulement si XQ est dans $\operatorname{Ker}\Phi_{U,U}$. Or, Q étant inversible,

$$X \mapsto XQ$$

est un automorphisme du K-espace $\mathscr{M}_n(K)$, d'où le résultat.

I.C.2. D'abord, P est inversible d'inverse :

$$\left(\begin{array}{c|c} I_m & -Y \\ \hline O & I_{n-m} \end{array}\right).$$

Un calcul par blocs montre que $P^{-1}NP$ n'est autre que la matrice :

$$\left(\begin{array}{c|c} A & AY - YA' \\ \hline O & A' \end{array}\right).$$

La seconde partie de la question est alors évidente.

I.C.3.a) Adoptons les notations de l'énoncé. La matrice $\Phi_{M,N}(X)$ n'est autre que :

$$\left(\begin{array}{c|c} AX_{1,1} - X_{1,1}A + BX_{2,1} & AX_{1,2} - X_{1,2}A' + BX_{2,2} \\ \hline A'X_{2,1} - X_{2,1}A & A'X_{2,2} - X_{2,2}A' \end{array}\right).$$

La matrice $\Phi_{N,N}(X)$ s'en déduit en substituant 0 à B.

On voit ainsi que si $X_{2,1}$ et $X_{2,2}$ sont nulles, on a :

$$X \in \operatorname{Ker}\Phi_{M,N} \Leftrightarrow X \in \operatorname{Ker}\Phi_{N,N},$$

ce qui donne la première des deux relations.

D'autre part, l'élément $(X_{2,1}, X_{2,2})$ de $\mathscr{M}_{n-m,m}(K) \times \mathscr{M}_{n-m}(K)$ est dans $\tau(\operatorname{Ker}\Phi_{M,N})$ si et seulement si :

$$A'X_{2,1} = X_{2,1}A, \quad A'X_{2,2} = X_{2,2}A'$$

et s'il existe $X_{1,1}$ dans $\mathscr{M}_m(K)$ et $X_{1,2}$ dans $\mathscr{M}_{m,n-m}(K)$ telles que :

$$AX_{1,1} - X_{1,1}A = -BX_{2,1}, \quad AX_{1,2} - X_{1,2}A' = -BX_{2,2}.$$

Dans le cas $M = N$, i.e $B = 0$, le second groupe de conditions est vide comme on le voit en prenant $X_{1,1}$ et $X_{1,2}$ nulles. Ceci prouve la seconde des relations demandées.

I.C.3.b) L'application du théorème du rang aux restrictions de τ aux noyaux de $\Phi_{M,N}$ et $\Phi_{N,N}$ entraîne :

$$\dim(\operatorname{Ker}\Phi_{M,N}) = \dim(\tau(\operatorname{Ker}\Phi_{M,N})) + \dim(\operatorname{Ker}\tau \cap \operatorname{Ker}\Phi_{M,N})$$

ainsi que la relation analogue pour $\Phi_{N,N}$. En utilisant **I.C.1**, il s'ensuit que les images des noyaux de $\Phi_{M,N}$ et $\Phi_{N,N}$ par τ ont même dimension, donc sont égales au vu de l'inclusion obtenue dans la question précédente.

I.C.3.c) La matrice :

$$\left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & -I_{n-m} \end{array}\right)$$

appartient à Ker $\Phi_{N,N}$, ce qui entraîne que

$$(0, -I_{n-m})$$

appartient à $\tau(\text{Ker } \Phi_{N,N})$ c'est-à-dire à $\tau(\text{Ker } \Phi_{M,N})$; ceci donne l'existence de Y.

I.C.4. Supposons A et A' diagonalisables sur K, R de la forme $AY - YA'$. La question **I.C.2** dit que M est semblable sur K à N, tandis que la question **I.A.3** assure que N est diagonalisable sur K. Il s'ensuit que M est diagonalisable sur K.

Réciproquement, supposons M diagonalisable sur K. L'argument de polynôme annulateur utilisé en **I.A.3** montre que A et A' sont diagonalisables sur K. Les matrices M et N sont alors toutes deux diagonalisables sur K et ont même polynôme caractéristique, donc sont semblables par **I.A.1.**c). La question **I.C.3**c) garantit alors que B est de la forme $AY - YA'$.

Partie II

II.A.1. Si M est dans $GL_n(A)$ d'inverse M^{-1}, les déterminants de M et M^{-1} sont éléments de A et leur produit vaut 1. Ces deux déterminants sont donc des inversibles de A. La réciproque se déduit du calcul de l'inverse à l'aide de la comatrice :

$$M^{-1} = \frac{1}{\det(M)} \, {}^t(\text{com}(M))$$

et du fait que les cofacteurs de M appartiennent à l'anneau A comme déterminants de matrices à coefficients dans A.

Si $A = \mathbf{Z}$, les inversibles de A sont 1 et -1 d'où la description de $\text{GL}_n(\mathbf{Z})$ comme ensemble des matrices de $\mathscr{M}_n(\mathbf{Z})$ de déterminant ± 1.

II.A.2. Il suffit d'observer que l'application $M \mapsto \overline{M}$ est un morphisme d'anneaux de $\mathscr{M}_n(\mathbf{Z})$ sur $\mathscr{M}_n(\mathbb{F}_p)$, ce qui implique que la réduction modulo p d'un élément de $\text{GL}_n(\mathbf{Z})$ appartient à $\text{GL}_n(\mathbb{F}_p)$, et de réduire modulo p la relation :

$$B = PAP^{-1}.$$

II.A.3.a) La matrice S_1 a deux valeurs propres rationnelles 1 et -1. Puisqu'elle appartient à $\mathscr{M}_2(\mathbb{Q})$, elle est diagonalisable sur $\mathbb{Q}$, les espaces propres étant des droites. Autrement dit, elle est semblable sur $\mathbb{Q}$ à S_0.

Pour le second point, on applique **II.A.2** avec $p = 2$: $\overline{S_0}$ est la matrice identité de $\mathscr{M}_2(\mathbb{F}_2)$, donc sa classe de similitude sur $\mathbb{F}_2$ est réduite à elle -même, en particulier ne contient pas $\overline{S_1}$.

II.A.3.b) Par hypothèse, 1 est valeur propre de M ; on dispose donc d'un vecteur propre de M dans $\mathbb{Q}^2$. Multipliant ce vecteur par un entier convenable, on obtient un vecteur propre de M à coordonnées entières et premières entre elles.

II.A.3.c) Puisque x_1 et x_2 sont premiers entre eux, il existe (Bezout) y_1 et y_2 dans $\mathbf{Z}$ tels que $x_1 y_2 - x_2 y_1 = 1$. La matrice

$$P = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$$

appartient à $\text{GL}_2(\mathbf{Z})$ et $P^{-1}MP$ a pour première colonne ${}^t(1,0)$; puisque cette matrice a pour polynôme caractéristique $X^2 - 1$, elle est de la forme S_a avec a dans $\mathbf{Z}$.

II.A.3.d) Un calcul simple montre :

$$T_x S_a T_x^{-1} = T_x S_a T_{-x} = S_{a-2x}.$$

Il s'ensuit que toute matrice S_a avec a dans $\mathbf{Z}$ est semblable sur $\mathbf{Z}$ à S_0 ou S_1. Le résultat s'en déduit à l'aide de la question précédente.

II.B.1.a) Si M est dans $\mathscr{M}_2(\mathbf{Z})$, $\chi_M = X^2 - \mathrm{Tr}\,(M)\,X + \det(M)$. La première assertion s'en déduit aussitôt.

Pour la seconde il suffit d'observer que puisque δ n'est pas un carré, $\delta - a^2$ n'est pas nul et donc b détermine c.

II.B.1.b) On établit que $M_{(a,-b)}$, $M_{(a+\lambda b,b)}$ et $M_{(-a,(\delta-a^2)/b)}$ sont semblables sur $\mathbf{Z}$ à $M_{(a,b)}$ en choisissant les matrices de passage :

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

et en notant que $c = (\delta - a^2)/b$.

II.B.2.a) Posons $b = \beta(M)$ et choisissons λ dans $\mathbf{Z}$ tel que :

$$|a + \lambda b| \leqslant \beta(M)/2.$$

La matrice $M_{(a+\lambda b,b)}$ est semblable sur $\mathbf{Z}$ à M et vérifie la condition demandée.

II.B.2.b) Les résultats de **II.B.1.**b) montrent que $M_{(a,b)}$ et $M_{(a,\pm\frac{\delta-a^2}{b})}$ sont semblables sur $\mathbf{Z}$. Le choix de $\beta(M)$ entraîne alors :

$$\beta(M) \leqslant \frac{|a^2-\delta|}{\beta(M)} \quad \text{i.e :} \quad \beta(M)^2 \leqslant |a^2-\delta|.$$

Si $\delta < 0$, $|a^2-\delta| = a^2 - \delta$ et l'inégalité demandée découle de : $a^2 \leqslant \beta(M)^2/4$.

Si $\delta > 0$, on a : $\delta \geqslant a^2$, sans quoi il viendrait :

$$a^2 - \delta \geqslant \beta(M)^2, \quad \text{et :} \quad \delta \leqslant a^2 - \beta(M)^2 \leqslant -\frac{3\beta(M)^2}{4} < 0.$$

L'inégalité voulue suit aussitôt.

II.B.2.c) Toute classe de similitude entière contenue dans $\mathscr{E}_{\mathbf{Z}}(P)$ contient donc une matrice $M_{(a,b)}$ telle que :

$$|a| \leqslant b/2 \leqslant \sqrt{\delta}/2 \quad \text{si} \quad \delta > 0,$$

$$|a| \leqslant b/2 \leqslant \sqrt{|\delta|/3} \quad \text{si} \quad \delta < 0.$$

Dans chaque cas, l'ensemble des couples (a,b) possibles est fini, d'où le résultat.

II.C.1.a) Puisque P et P' sont premiers entre eux dans $\mathbf{C}[X]$, donc dans $\mathbb{Q}[X]$ (argument de **I.B.2**), on peut écrire une relation de Bezout entre P et P' dans $\mathbb{Q}[X]$. Multipliant cette relation par un entier relatif non nul convenable de façon à "chasser les dénominateurs" et obtenir un résultat > 0, on obtient une égalité de la forme demandée par l'énoncé.

II.C.1.b) Il suffit de réduire modulo p la relation obtenue dans la question précédente et d'utiliser **I.B.1**.

II.C.2.a) Notons Π_M le polynôme minimal de M (qui est le même vu sur $\mathbf{C}$ ou sur $\mathbb{Q}$ puisque le rang du système de matrices $(M^i)_{i\in\mathbf{N}}$ est indépendant du corps de base). Comme diviseur unitaire de χ_M (**I.B.3**), Π_M appartient à $\mathbf{Z}[X]$. Les racines de Π_M dans $\mathbf{C}$ sont simples (diagonalisabilité), d'où le résultat avec $P = \Pi_M$.

II.C.2.b) La question précédente permet d'appliquer **II.C.1** : il existe d_M dans $\mathbf{N}^*$ tel que, pour tout nombre premier p ne divisant pas d_M, la réduction de Π_M modulo p est à racines simples dans $\overline{\mathbb{F}_p}$. Mais la réduction modulo p de l'égalité $\Pi_M(M) = 0$ montre que $\overline{\Pi_M}$ annule $\overline{M}$, d'où la diagonalisabilité de $\overline{M}$ sur $\overline{\mathbb{F}_p}$.

II.D.1. Soient α dans **C** une racine de P de multiplicité $\geqslant 2$, Q le polynôme minimal unitaire de α sur $\mathbb{Q}$. Puisque α est racine simple de Q d'après **I.B.2**, Q divise P et P/Q dans $\mathbb{Q}[X]$, i.e Q^2 divise P dans $\mathbb{Q}[X]$. Mais grâce à **I.B.3**, Q et $P/Q^2 = R$ sont dans $\mathbf{Z}[X]$, d'où le résultat.

II.D.2. Par choix de p, la matrice E_p se réduit modulo p en une matrice diagonalisable sur $\overline{\mathbb{F}_p}$. Supposons par l'absurde E_p et E_q semblables sur **Z**. Les réductions modulo p de E_p et E_q sont alors semblables sur $\mathbb{F}_p$ et la réduction de E_q modulo p est diagonalisable sur $\overline{\mathbb{F}_p}$. Grâce à **I.A.3**, il en va de même de la réduction modulo p de la matrice :

$$E'_q = \left(\begin{array}{c|c} A & qI_l \\ \hline O & A \end{array}\right).$$

Grâce à **I.C.4**, ceci implique que $\overline{qI_l}$ est de la forme $\overline{A}X - X\overline{A}$ avec X dans $\mathscr{M}_l(\overline{\mathbb{F}_p})$ et est donc de trace nulle. Ainsi p divise ql, contradiction.

Variante. Supposons la réduction modulo q de E_q sur $\mathbb{F}_p$ diagonalisable sur $\overline{\mathbb{F}_p}$. Soit Q dans $\overline{F_p}[X]$ annulant cette matrice. Un calcul explicite montre que Q et Q' annulent $\overline{A}$. Cette dernière matrice est diagonalisable sur $\overline{\mathbb{F}_p}$. Si λ est une valeur propre de $\overline{A}$ dans $\overline{\mathbb{F}_p}$, λ est racine de Q et Q'. Un annulateur de Q ne peut donc être simplement scindé sur $\overline{\mathbb{F}_p}$, ce qui permet de conclure.

II.D.3. De la question précédente il découle en particulier que si les nombres premiers distincts p et q sont strictement supérieurs à d_A, d_B et l, les matrices E_p et E_q, qui appartiennent trivialement toutes deux à $\mathscr{E}_{\mathbf{Z}}(P)$, ne sont pas semblables sur **Z**. Puisque l'ensemble des nombres premiers est infini, on obtient ainsi une infinité de matrices de $\mathscr{E}_{\mathbf{Z}}(P)$ deux à deux non semblables sur **Z**.

Partie III

III.A.1. Si $(f_1, \ldots, f_n)$ est une **Z**-base de Γ, on peut écrire les e_i comme combinaisons **Z**-linéaires des f_j. On écrit, pour $1 \leqslant i \leqslant n$:

$$e_i = \sum_{j=1}^{n} q_{i,j} f_j.$$

On en déduit que $QP = I_n$, donc que P appartient à $\mathrm{GL}_n(\mathbf{Z})$.

Réciproquement, si P appartient à $\mathrm{GL}_n(\mathbf{Z})$, l'inversion du système montre que l'on peut écrire les e_i comme combinaisons **Z**-linéaires des f_j. La famille $(f_1, \ldots, f_n)$ engendre donc le g.a.l.t.f Γ. Cette famille est de plus trivialement **Z**-libre (l'inversibilité de P dans $\mathbb{Q}$ suffit pour ce second point), d'où le résultat demandé.

III.A.2. Adoptons les notations du début de **III**. Alors le quotient Γ/Γ' est isomorphe à :

$$\mathbf{Z}/d_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_s\mathbf{Z} \oplus \mathbf{Z}^{r-s}.$$

Il est fini si et seulement si $r = s$, ce qui est l'assertion demandée.

III.A.3. a) Soit a un élément non nul de I. Alors : $aR \subset I$ et R/I est un quotient de R/aR, de sorte qu'il suffit de prouver que R/aR est fini. Mais puisque l'anneau R est intègre, $x \mapsto ax$ est un isomorphisme de groupes abéliens de R sur aR, ce qui implique que aR est un g.a.l.t.f de même rang que R, d'où le résultat via la question précédente.

b) L'ensemble des idéaux de R contenant I est naturellement en bijection avec celui des idéaux du quotient R/I. Ce dernier ensemble, contenu dans $\mathscr{P}(R/I)$, est fini par a).

III.A.4. Le sous-groupe $V \cap \mathbf{Z}^n$ est un sous-groupe de $\mathbf{Z}^n$, donc un g.a.l.t.f. Montrons que son rang est m. Puisque V est de dimension m, toute famille de cardinal $> m$ de $V \cap \mathbf{Z}^n$ est $\mathbb{Q}$-liée, donc $\mathbf{Z}$-liée. Le rang de $V \cap \mathbf{Z}^n$ est ainsi majoré par m. Si maintenant $(f_1, \dots, f_m)$ est une $\mathbb{Q}$-base de V, il existe d dans $\mathbf{N}^*$ tel que :

$$\forall i \in \{1, \dots, m\}, \qquad d f_i \in \mathbf{Z}^n.$$

On a alors :

$$\bigoplus_{i=1}^{m} \mathbf{Z} d f_i \subset V \cap \mathbf{Z}^n,$$

d'où l'on déduit le résultat.

En appliquant le théorème de la base adaptée de l'énoncé, on obtient alors une $\mathbf{Z}$-base $(e_1, \dots, e_n)$ de $\mathbf{Z}^n$ et des éléments $d_1, \dots, d_m$ de $\mathbf{N}^*$ tels que la famille $(d_1 e_1, \dots, d_m e_m)$ soit une $\mathbf{Z}$-base de $V \cap \mathbf{Z}^n$. En particulier $(e_1, \dots, e_m)$ est une $\mathbb{Q}$-base de V.

III.B.1. Décomposons les éléments x et y de $\mathbb{Q}[\alpha]$ sur la base $(\alpha^i)_{0 \leqslant i \leqslant n-1}$:

$$x = \sum_{i=0}^{n-1} x_i \alpha^i, \qquad y = \sum_{i=0}^{n-1} y_i \alpha^i,$$

avec $(x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1})$ dans $\mathbb{Q}^{2n}$. Alors :

$$xy = \sum_{0 \leqslant i,j \leqslant n-1} x_i y_j \alpha^{i+j}.$$

D'autre part, par définition de $\mathcal{N}$:

$$\forall (u, v) \in \mathbb{Q}[\alpha]^2, \qquad \mathcal{N}(u+v) \leqslant \mathcal{N}(u) + \mathcal{N}(v),$$

$$\forall (x, u) \in \mathbb{Q} \times \mathbb{Q}[\alpha], \qquad \mathcal{N}(xu) = |x| \mathcal{N}(u).$$

Donc : $\mathcal{N}(xy) \leqslant C \mathcal{N}(x)\, \mathcal{N}(y)$ où :

$$C = \sum_{0 \leqslant i,j \leqslant n-1} \mathcal{N}(\alpha^{i+j}).$$

III.B.2. On découpe le cube $[0,1[^n$ en les M^n sous-cubes

$$C_{a_1, \dots, a_n} = \prod_{k=0}^{n-1} \left[\frac{a_k}{M}, \frac{a_k + 1}{M} \right[, \qquad (a_0, \dots a_{n-1}) \in \{0, \dots M\}^n.$$

Si $a_1, \dots a_{M^n+1}$ sont $M^n + 1$ points distincts de $[0,1]^n$, le principe des tiroirs assure l'existence de i et j distincts dans $\{1, \dots M^n + 1\}$ tels que a_i et a_j appartiennent au même $C_{a_1, \dots, a_n}$.

Identifiant $\mathbb{Q}[\alpha]$ et $\mathbb{Q}^n$ par le choix de la base $(\alpha^i)_{0 \leqslant i \leqslant n-1}$, on obtient i et j tels que $0 \leqslant i < j \leqslant M^n$ tels que $\mathcal{N}(u_i - u_j) \leqslant \frac{1}{M}$. Mais $u_i - u_j$ s'écrit :

$$(j - i) y - a$$

pour un certain a dans $\mathbf{Z}[\alpha]$. Le résultat demandé suit en posant $m = j - i$.

III.B.3. a) On a donc :

$$\mathcal{N}\left(m \frac{x}{z} - a \right) \leqslant \frac{1}{M}$$

pour un certain m de $\{1, \dots, M^n\}$ et un certain a de $\mathbf{Z}[\alpha]$, d'où, grâce à **III.B.1.** :

$$\mathcal{N}(mx - az) \leqslant C \mathcal{N}(z) / M,$$

et, enfin :

$$\mathcal{N}(mx - az) < \mathcal{N}(z).$$

Mais $mx - az$ est dans I car x et z y sont. Le choix de z force alors :

$$mx - az = 0, \quad \text{donc :} \quad mx \in z\mathbf{Z}[\alpha].$$

Puisque m est dans $\{1, \dots M^n\}$, il divise ℓ, et on a donc :

$$\ell x \in z\mathbf{Z}[\alpha].$$

Ceci est vrai pour tout x de I, c'est le résultat voulu.

b) Le résultat de a) assure que J est contenu dans $\mathbf{Z}[\alpha]$. Il est immédiat que J est un idéal de $\mathbf{Z}[\alpha]$. D'autre part, puisque z appartient à I, J contient $\ell\mathbf{Z}[\alpha]$.

Finalement, tout idéal non nul de $\mathbf{Z}[\alpha]$ est équivalent (pour $\sim$) à un idéal contenant $\ell\mathbf{Z}[\alpha]$. Comme $(\mathbf{Z}[\alpha], +)$ est trivialement un g.a.l.t.f (dont $(\alpha^i)_{0\leqslant i\leqslant n-1}$ est une $\mathbf{Z}$-base), la question **III.A.3.**b) montre que l'ensemble des idéaux de $\mathbf{Z}[\alpha]$ contenant $\ell\mathbf{Z}[\alpha]$ est fini, d'où la conclusion attendue.

La démonstration donne bien sûr la finitude du "class-number" pour tout ordre d'un corps de nombres.

III.C.1. a) Puisque α est racine de $P = \chi_M$, donc valeur propre de M, on obtient, en voyant M comme un élément de $\mathcal{M}_n(\mathbb{Q}[\alpha])$, l'existence de $(x_1, \dots, x_n)$ dans $\mathbb{Q}[\alpha]^n \setminus \{0\}$ tel que ${}^t x$ soit vecteur propre de M associé à α. Puisque tout élément de $\mathbb{Q}[\alpha]$ s'écrit r/m avec r dans $\mathbf{Z}[\alpha]$ et m dans $\mathbf{N}^*$, on en déduit que l'ensemble X_M n'est pas vide. L'irréductibilité de P et la question **I.B.2** montrent que α est racine simple de χ_M, donc que l'espace propre associé est une droite. On peut donc, si x et y sont dans X_M, écrire : $x = \lambda y$ avec λ dans $\mathbb{Q}[\alpha]^*$. Il suffit pour terminer d'écrire $\lambda = b/a$ avec a dans $\mathbf{N}^*$ (donc dans $\mathbf{Z}[\alpha] \setminus \{0\}$) et b dans $\mathbf{Z}[\alpha] \setminus \{0\}$.

b) Il suffit de montrer que (x) est stable par multiplication par α pour établir que (x) est un idéal de $\mathbf{Z}[\alpha]$. Mais puisque ${}^t x$ est vecteur propre de M associé à α, tout αx_j est combinaison $\mathbf{Z}$-linéaire des x_i, d'où le résultat.

Par définition, $(x_1, \dots, x_n)$ engendre le g.a.l.t.f (x), lequel a, par **III.A.3**.a), le même rang que $\mathbf{Z}[\alpha]$, c'est-à-dire n. On en déduit aisément que $(x_1, \dots, x_n)$ est une $\mathbf{Z}$-base de (x).

Enfin, la deuxième partie de la question a) assure aussitôt que pour tout y de X_M, $(x) \sim (y)$.

III.C.2. a) On remonte l'argument de **III.C.1.**b). Si I est un idéal non nul de $\mathbf{Z}[\alpha]$, I est un g.a.l.t.f de rang n (**III.A.3.**a)). Soit $(x_1, \dots, x_n)$ une $\mathbf{Z}$-base de I. Chaque αx_j est dans I, donc est combinaison $\mathbf{Z}$-linéaire des x_i. Mais alors ${}^t x$ est vecteur propre associé à α d'une matrice M de $\mathcal{M}_n(\mathbf{Z})$. Le polynôme caractéristique de cette matrice annule α, donc est divisible par P, donc lui est égal pour raison de degré. C'est dire que M est dans $\mathcal{E}_{\mathbf{Z}}(P)$ et clairement $j(M)$ est la classe de I pour $\sim$.

b) Supposons : $M' = PMP^{-1}$ avec P dans $\mathrm{GL}_n(\mathbf{Z})$. Si $x = (x_1, \dots, x_n)$ est dans X_M, et si $y = (y_1, \dots, y_n)$ est défini par :

$${}^t y = P\,{}^t x$$

alors y est dans $X_{M'}$. Chaque y_j est combinaison $\mathbf{Z}$-linéaire des x_i ; en utilisant P^{-1} on voit réciproquement que chaque x_j est combinaison $\mathbf{Z}$-linéaire des y_i. Par suite : $(x) = (y)$ et : $j(M) = j(M')$.

Supposons réciproquement $j(M) = j(M')$. Soient $x = (x_1, \dots, x_n)$ dans X_M et $x' = (x'_1, \dots, x'_n)$ dans $X_{M'}$. Les idéaux (x) et (x') sont équivalents et on peut donc, quitte à multiplier x et x' par des éléments non nuls de $\mathbf{Z}[\alpha]$, supposer : $(x) = (x')$. Cela étant, $(x_1, \dots x_n)$ et $(x'_1, \dots, x'_n)$ sont deux $\mathbf{Z}$-bases d'un même idéal, donc se déduisent l'une de l'autre par un élément de $\mathrm{GL}_n(\mathbf{Z})$:

$$P\,{}^t x = {}^t x', \text{avec} \quad P \in \mathrm{GL}_n(\mathbf{Z}).$$

On voit alors que les deux matrices M' et $M'' = PMP^{-1}$ admettent toutes deux ${}^t x'$ pour vecteur propre associé à α. Ces deux matrices appartenant à $\mathscr{M}_n(\mathbf{Z})$, ceci implique qu'elles sont égales. Il suffit en effet d'expliciter coordonnée par coordonnée la relation :

$$M'({}^t x') = M''({}^t x'),$$

pour conclure en utilisant l'appartenance à $\mathscr{M}_n(\mathbf{Z})$ et la $\mathbf{Z}$-liberté de $(x'_1, \ldots, x'_n)$.

III.D.1. Observons d'abord que $Q(M)$ n'est pas inversible dans $\mathscr{M}_n(\mathbf{C})$: en effet, les racines de Q dans $\mathbf{C}$ sont racines de P donc valeurs propres de M. Une trigonalisation dans $\mathbf{C}$ permet alors de conclure.

Il s'ensuit que le sous-espace U de $\mathbb{Q}^n$ noyau de $Q(M)$ n'est pas nul. Soit donc v dans $U\setminus\{0\}$. Alors $(M^i(v))_{0\leqslant i\leqslant m-1}$ est $\mathbb{Q}$-libre (grâce à l'irréductibilité de Q). Si V est le sous-espace de U, engendré par cette famille, V est de dimension m et stable par M. Le calcul du polynôme caractéristique d'une matrice-compagnon effectué dans la question **I.A.2.**a) montre que $\chi_{M|V} = Q$.

En choisissant une $\mathbf{Z}$-base de $\mathbf{Z}^n$ adaptée à V au sens de la question **III.A.4**, on voit alors que M est semblable sur $\mathbf{Z}$ à une matrice :

$$M' = \left(\begin{array}{c|c} A & B \\ \hline O & A' \end{array}\right)$$

où $\chi_A = Q$, et donc nécessairement $\chi_{A'} = P/Q$. D'autre part, les matrices A et A' sont diagonalisables sur $\mathbf{C}$ (**I.C.4**), d'où l'existence de P dans $\mathrm{GL}_m(\mathbf{Z})$ et de i dans $\{1,\ldots,r\}$ tels que $PAP^{-1} = A_i$, de Q dans $\mathrm{GL}_{n-m}(\mathbf{Z})$ et de j dans $\{1,\ldots,s\}$ tels que $QA'Q^{-1} = A'_j$. Soit :

$$R = \left(\begin{array}{c|c} P & O \\ \hline O & Q \end{array}\right),$$

alors R est dans $\mathrm{GL}_n(\mathbf{Z})$ et $RM'R^{-1}$ est de la forme demandée par l'énoncé.

III.D.2. Il est clair que :

$$\Gamma = \{A_i X - X A'_j \ ; \ X \in \mathscr{M}_{m,n-m}(\mathbb{Q})\} \cap \mathscr{M}_{m,n-m}(\mathbf{Z})$$

et :

$$\Gamma' = \{A_i X - X A'_j \ ; \ X \in \mathscr{M}_{m,n-m}(\mathbf{Z})\}$$

sont deux sous-groupes du g.a.l.t.f $\mathscr{M}_{m,n-m}(\mathbf{Z})$ et que Γ contient Γ'. Si Y est un élément du premier de ces groupes, il existe d dans $\mathbf{N}^*$ tel que dY appartienne au second (il suffit de "chasser les dénominateurs"). On en déduit aisément l'assertion désirée.

III.D.3. Grâce à **III.A.2**, Γ/Γ' est fini. Soient $t_{i,j}$ le cardinal du groupe quotient, $B_1, \ldots, B_{t_{i,j}}$ un système fondamental de représentants du quotient Γ/Γ'.

Grâce à **I.C.4** et à la diagonalisabilité de M sur $\mathbf{C}$, la matrice B appartient à :

$$\{A_i X - X A'_j \ ; \ X \in \mathscr{M}_n(\mathbf{C})\}.$$

Elle appartient en fait à :

$$\{A_i X - X A'_j \ ; \ X \in \mathscr{M}_{m,n-m}(\mathbb{Q})\}$$

en vertu du résultat général suivant : si un système linéaire non homogène à coefficients dans un corps K à une solution dont les coordonnées appartiennent à une extension L de K, il a une solution dont les coordonnées appartiennent à K. Ce résultat est lui-même conséquence (entre autres) de la détermination du rang d'une matrice par les déterminants extraits.

Cela étant, le calcul de **I.C.2** montre que la matrice M est semblable sur $\mathbf{Z}$ à une matrice :

$$\left(\begin{array}{c|c} A_i & B_k \\ \hline O & A'_j \end{array}\right).$$

Ceci achève la preuve du théorème.