Mathématiques générales 2011 - Indications

Michel Coste*

Révision du 14 décembre 2011

I. Préliminaires

A. Matrices à coefficients dans K

1.(a) M est diagonalisable sur K si et seulement si $a \neq c$ ou $b = 0$.

1.(b) Les matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ne sont pas semblables et ont toutes deux X^2 comme polynôme caractéristique.

1.(c) Puisque $\chi_{M'} = \chi_M$, les deux matrices M et M' ont les mêmes valeurs propres, avec les mêmes multiplicités, dans K. Puisqu'elles sont toutes les deux diagonalisables sur K, elles sont toutes les deux semblables sur K à une même matrice diagonale, et donc semblables entre elles sur K.

2.(a) On peut, sans changer le déterminant de $XI_n - C(P)$, ajouter à la première ligne X fois la deuxième et X^2 fois la troisième et ...et X^{n-1} fois la dernière. On développe ensuite suivant la première ligne, qui ne contient plus que P en bout. On trouve $(-1)^{n+1}P \times (-1)^{n-1} = P$.

2.(b) Les $n-1$ premières colonnes de $C(P) - \lambda I_n$ sont visiblement linéairement indépendantes (échelonnement).

2.(c) (i) entraîne (ii) : Toute matrice de $\mathcal{E}_K(P)$ a un polynôme annulateur P (Cayley-Hamilton) scindé sur K à racines simples, donc est diagonalisable sur K.
(ii) entraîne (iii) : $C(P) \in \mathcal{E}_K(P)$.
(iii) entraîne (i) : puisque $C(P)$ est diagonalisable sur K, $\chi_{C(P)} = P$ est scindé sur K ; si λ est une racine de P, c.-à-d. une valeur propre de $C(P)$, alors la multiplicité de λ comme racine de P (égale à la dimension du sous-espace propre associé puisque $C(P)$ est diagonalisable) vaut 1 d'après (b) et le théorème du rang.

3. Si $U^{-1}AU$ et $V^{-1}A'V$ sont diagonales alors, avec $Q = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix}$, $Q^{-1}MQ$ est aussi diagonale. Réciproquement, si M est diagonalisable sur K, elle admet un polynôme annulateur P scindé sur K à racines simples ; comme $0 = P(M) = \begin{pmatrix} P(A) & 0 \\ 0 & P(A') \end{pmatrix}$, P annule aussi A et A'.

4. Le résultat admis montre qu'il y a une surjection de l'ensemble des factorisations de P en produit de polynômes unitaires non constants sur l'ensemble des classes de similitude contenues dans $\mathcal{E}_K(P)$. Comme $K[X]$ est factoriel, il y a un nombre fini de telles factorisations.

B. Polynômes

1. Puisque a est racine de P, $P = (X-a)Q$, d'où $P' = (X-a)Q' + Q$ et $P'(a) = Q(a)$. Donc a est racine simple si et seulement si $Q(a) \neq 0$ si et seulement si $P'(a) \neq 0$.
2. Puisque P est irréductible dans $\mathbb{Q}[X]$ et ne divise pas P', il est premier avec lui et on a une identité de Bézout $UP + VP' = 1$. Si $a \in \mathbb{C}$ est racine de P, alors $V(a)P'(a) = 1$ et a est racine simple d'après 1.
3. Soit $P = QR$ dans $\mathbb{Q}[X]$. Soit k (resp. ℓ) le plus petit entier > 0 tel que kQ (resp. ℓR) soit à coefficients entiers. On a $c(kQ) = 1$; en effet $(k/c(kQ))Q$ est à coefficients entiers et $k/c(kQ)$ est entier car Q est unitaire. De même, puisque R est unitaire, $c(\ell R) = 1$. D'après le lemme de Gauss, $k\ell\, c(P) = c(k\ell P) = c(kQ)c(\ell R) = 1$ et donc $k = \ell = 1$.

*Remarques et questions bienvenues à `michel.coste@univ-rennes1.fr`. Merci aux intervenants de `les-mathematiques.net` pour leurs remarques.

4. Soit $P = P_1 \cdots P_r$ une décomposition de P en produit de facteurs irréductibles unitaires sur $\mathbb{Q}$. D'après 3, les P_i sont à coefficients entiers. Les P_i sont scindés sur $\mathbb{C}$ à racines simples d'après 2. D'après A.2.(c) les $C(P_i)$ sont diagonalisables et, d'après A.3, la matrice diagonale par blocs dont les blocs diagonaux sont $C(P_1), \ldots, C(P_r)$ est dans $\mathcal{D}_{\mathbb{Z}}(P)$.

C. Similitude sur K de matrices blocs

1. Puisque $UX - XV = (UXQ - XQU)Q^{-1}$, l'automorphisme $X \mapsto XQ$ envoie $\ker \Phi_{U,V}$ sur $\ker \Phi_{U,U}$.
2. On vérifie que $\begin{pmatrix} I_m & -Y \\ 0 & I_{n-m} \end{pmatrix}$ est l'inverse de P, et $P^{-1}NP = \begin{pmatrix} A & AY - YA' \\ 0 & A' \end{pmatrix}$. Si $B = AY - YA'$, ceci montre que M est semblable à N.

3.(a) Soit $X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ 0 & 0 \end{pmatrix} \in \ker \tau$. Alors $\Phi_{N,N}(X) = \begin{pmatrix} AX_{1,1} - X_{1,1}A & AX_{1,2} - X_{1,2}A' \\ 0 & 0 \end{pmatrix} = \Phi_{M,N}(X)$. Donc

$$\ker \tau \cap \ker \Phi_{N,N} = \ker \tau \cap \ker \Phi_{M,N} \ .$$

Si $X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix}$ est dans $\ker \Phi_{M,N}$, alors $A'X_{2,1} - X_{2,1}A = 0$ et $A'X_{2,2} - X_{2,2}A' = 0$. Ceci entraîne que $\begin{pmatrix} 0 & 0 \\ X_{2,1} & X_{2,2} \end{pmatrix}$ est dans $\ker \Phi_{N,N}$. Donc

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

3.(b) D'après la deuxième relation de (a) il suffit de montrer $\dim(\tau(\ker \Phi_{M,N})) = \dim(\tau(\ker \Phi_{N,N}))$. D'après 1 on sait que $\dim(\ker \Phi_{M,N}) = \dim(\ker \Phi_{N,N})$. La première relation de (a) et le théorème du rang appliqué aux restrictions de τ à $\ker \Phi_{M,N}$ et $\ker \Phi_{N,N}$ permettent de conclure.

3.(c) Il suffit d'appliquer (b) en prenant $I_n \in \ker \Phi_{N,N}$. On en déduit qu'il existe une matrice $\begin{pmatrix} X_{1,1} & -Y \\ 0 & I_{n-m} \end{pmatrix}$ dans $\ker \Phi_{M,N}$, ce qui entraîne $B = AY - YA'$.

4. (i) entraîne (ii) : Soit P un polynôme annulateur de M scindé sur K à racines simples. Alors $0 = P(M) = \begin{pmatrix} P(A) & * \\ 0 & P(A') \end{pmatrix}$, donc P annule A et A' et ces matrices sont diagonalisables. Alors N est diagonalisable (A.3) et est donc semblable à M car elle a même polynôme caractéristique (A.1.(c)). Donc il existe Y tel que $B = AY - YA'$ (3.(c)).
(ii) entraîne (i) : M est semblable à N (2) qui est diagonalisable puisque A et A' le sont (A.3).

II. Similitude entière

A. Généralités, premier exemple

1. Remarquons d'abord que si $M \in M_n(A)$, alors $\det(M) \in A$ et $\mathrm{Com}(M) \in M_n(A)$ (où $\mathrm{Com}(M)$ est la matrice des cofacteurs de M). Le fait que $\det(MN) = \det(M)\det(N)$ et que $\det(I_n) = 1$ montre qu'une matrice inversible sur A a un déterminant inversible dans A. La formule $M\,{}^t\mathrm{Com}(M) = \det(M)\, I_n$ montre qu'une matrice qui a un déterminant inversible dans A est inversible sur A. Sur $\mathbb{Z}$, les matrices inversibles sont celles de déterminant ± 1.
2. L'homomorphisme canonique $\mathbb{Z} \to \mathbb{F}_p$ induit un homomorphisme d'anneaux $M \mapsto \overline{M}$ de $\mathcal{M}_n(\mathbb{Z})$ sur $\mathcal{M}_n(\mathbb{F}_p)$. Donc, si P appartient à $\mathrm{GL}_n(\mathbb{Z})$, alors $\overline{P}$ est inversible et $\overline{P}^{-1} = \overline{P^{-1}}$. Si $M = P^{-1}NP$, alors $\overline{M} = \overline{P}^{-1}\overline{N}\,\overline{P}$.

3.(a) S_0 et S_1 sont toutes les deux semblables à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ sur $\mathbb{Q}$. Sur $\mathbb{F}_2$, $\overline{S_0} = I_2$ et $\overline{S_1} \neq I_2$ ne sont pas semblables. Donc S_0 et S_1 ne sont pas semblables sur $\mathbb{Z}$ (2).

3.(b) 1 est valeur propre de M, donc il existe un vecteur propre de valeur propre associée 1 dans $\mathbb{Q}^2$. Quitte à multiplier ce vecteur propre par un rationnel, on peut supposer ses coordonnées entières et premières entre elles.

3.(c) Par Bézout, il existe des entiers y_1, y_2 tels que $x_1y_2 - y_1x_2 = 1$. Alors $P = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z})$, et $P^{-1}MP = S_a$ pour un certain entier a.

3.(d) On a $T_x S_a T_x^{-1} = S_{a-2x}$. Donc, pour tout a pair (resp. impair), S_a est semblable à S_0 (resp. S_1). Ceci entraîne que M est semblable à S_0 ou S_1.

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

1.(a) Si $\chi_M = P$, alors la trace de M est nulle et son déterminant est $-\delta$. Donc M est de la forme $\begin{pmatrix} a & c \\ b & -a \end{pmatrix}$ avec $a^2 + bc = \delta$. Si b divise $\delta - a^2$, alors $b \neq 0$ car δ n'est pas un carré et il y a une unique matrice $M_{(a,b)}$ de cette forme dans $\mathcal{E}_{\mathbb{Z}}(X^2 - \delta)$: celle où $c = (\delta - a^2)/b$.

1.(b) Les changements de base $M \mapsto P^{-1}MP$ ($P \in \mathrm{GL}_n(\mathbb{Z})$) donnés par les matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ transforment $M_{(a,b)}$ en $M_{(a,-b)}$, $M_{(a+\lambda b,b)}$ et $M_{(-a,(\delta-a^2)/b)}$ respectivement.

2.(a) Soit $d \in \mathbb{Z}$ tel que $M_{(d,\beta(M))} \in \mathcal{E}_{\mathbb{Z}}(P)$. il existe un unique entier relatif λ tel que $-\beta(M)/2 \leq a = d + \lambda\beta(M) < \beta(M)/2$. D'après 1.(b), $M_{(a,\beta(M))} \in \mathcal{E}_{\mathbb{Z}}(P)$.

2.(b) Pour tout $b \in \mathcal{B}$, $|\delta - a^2|/b \in \mathcal{B}$ (1.(b)). Donc $\beta(M) \leq |\delta - a^2|/\beta(M)$, c.-à-d. $\beta(M)^2 \leq |\delta - a^2|$. Si $\delta < a^2$, alors

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

ce qui entraîne $\delta < 0$ et $\beta(M) \leq \sqrt{4|\delta|/3}$. Si $\delta > 0$, alors nécessairement $\delta > a^2$ d'après ce qu'on vient de voir, et donc $\beta(M) \leq \sqrt{\delta}$.

2.(c) Posons $m(\delta) = \sqrt{\delta}$ si $\delta > 0$ et $\sqrt{4|\delta|/3}$ si $\delta < 0$. On a vu que toute matrice de $\mathcal{E}_{\mathbb{Z}}(P)$ est semblable sur $\mathbb{Z}$ à une matrice $M_{(a,b)}$ avec $0 < b \leq m(\delta)$ et $|a| \leq m(\delta)/2$. Comme il y a un nombre fini de telles matrices, $\mathcal{E}_{\mathbb{Z}}(P)$ est réunion d'un nombre fini de classes de similitude entière.

C. Diagonalisabilité et réduction modulo p

1.(a) Les polynômes P et P' sont premiers entre eux dans $\mathbb{Q}[X]$, car une racine dans $\mathbb{C}$ d'un diviseur commun non constant de P et P' serait une racine multiple de P. D'après Bézout, il existe des polynômes S_1, T_1 dans $\mathbb{Q}[X]$ tels que $S_1P + T_1P' = 1$. En multipliant par $d \in \mathbb{N}^*$ tel que dS_1 et dT_1 soient à coefficients entiers, on obtient S et T dans $\mathbb{Z}[X]$ tels que $SP + TP' = d$.

1.(b) Soit $a \in \overline{\mathbb{F}_p}$ une racine de P. Alors $\overline{T}(a)\overline{P'}(a) = \overline{d} \neq 0$ montre que a est racine simple (I.B.1).

2.(a) Soit D le pgcd unitaire de χ_M et χ'_M (sur $\mathbb{Q}$ ou sur $\mathbb{C}$, c'est pareil) et soit $P = \chi_M/D$ qui est non constant, unitaire et à coefficients entiers (I.B.3). Si $\chi_M = \prod_{i=1}^r (X - \lambda_i)^{\alpha_i}$ sur $\mathbb{C}$, où les λ_i sont les valeurs propres distinctes de M sur $\mathbb{C}$, alors $P = \prod_{i=1}^r (X - \lambda_i)$. Puisque M est diagonalisable, $P(M) = 0$ et les racines λ_i de P dans $\mathbb{C}$ sont simples.[1]

2.(b) D'après 1, on a un entier d_M tel que, pour tout nombre premier p ne divisant pas d_M, la réduction modulo p de P est un polynôme annulateur de $\overline{M}$ scindé sur $\overline{F_p}$ à racines simples ; ceci entraîne que $\overline{M}$ est diagonalisable sur $\overline{F_p}$.

D. Un résultat de non finitude

1. Soit $P = \prod_{i=1}^r P_i^{\alpha_i}$ la décomposition de P en produit de polynômes irréductibles unitaires dans $\mathbb{Q}(X)$ (les P_i sont distincts). Les P_i sont à coefficients entiers (I.B.3). Pour chaque i, les racines de P_i dans $\mathbb{C}$ sont simples (I.B.2). Pour $i \neq j$, P_i et P_j n'ont pas de racine commune dans $\mathbb{C}$ car ils sont premiers entre eux sur $\mathbb{Q}$ et donc aussi sur $\mathbb{C}$ (Bézout). Puisque les racines de P dans $\mathbb{C}$ ne sont pas toutes simples, au moins un des exposants α_i est ≥ 2 ; on peut supposer $\alpha_1 \geq 2$. Alors en posant $P_1 = Q$ (unitaire non constant à coefficients entiers) et $R = P/P_1^2$ (unitaire à coefficients entiers), on a bien $P = Q^2R$.

2. D'après les hypothèses sur p et C.1.(b), $\overline{A}$ et $\overline{B}$ (si $m > 0$) sont diagonalisables sur $\overline{\mathbb{F}_p}$. Donc $\overline{E_p}$ l'est aussi, puisqu'elle est diagonale par blocs diagonalisables (I.A.3).

[1] Il ne suffit pas ici de parler du polynôme minimal de M : en effet, il faudrait alors montrer que le polynôme minimal de M sur $\mathbb{C}$ est à coeffcients dans $\mathbb{Q}$.

Par contre, $\overline{E_q}$ n'est pas diagonalisable. En effet, si elle l'était, la matrice $\begin{pmatrix} \overline{A} & \overline{q}I_\ell \\ 0 & \overline{A} \end{pmatrix}$ devrait l'être (I.A.3 pour $m > 0$). Or $\overline{q}I_\ell$ n'est pas de la forme $\overline{A}Y - Y\overline{A}$ car la trace de la première matrice est $\overline{q\ell} \neq 0$ tandis que la trace de la deuxième est nulle ; ceci contredit I.C.4.
Ainsi $\overline{E_p}$ et $\overline{E_q}$ ne sont pas semblables sur $\overline{\mathbb{F}_p}$, donc non plus sur $\mathbb{F}_p$, ce qui entraîne que E_p et E_q ne sont pas semblables sur $\mathbb{Z}$ (A.2).

3. Il y a une infinité de nombres premiers p ne divisant ni d_A, ni ℓ, ni d_B. Pour chacun de ces p, $E_p \in \mathcal{E}_{\mathbb{Z}}(P)$ et ces E_p sont deux à deux non semblables sur $\mathbb{Z}$ d'après 2. Donc $\mathcal{E}_{\mathbb{Z}}(P)$ n'est pas réunion finie de classes de similitude entière.

III. Un théorème de finitude

A. Groupes abéliens libres de type fini

1. Un élément $g \in \Gamma$ s'écrit $g = \sum_{i=1}^n \mu_i f_i$ (avec $(\mu_1, ..., \mu_r) \in \mathbb{Z}^r$) si et seulement s'il s'écrit $g = \sum_{i=1}^n \lambda_i e_i$ avec $\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = P \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$. Ceci montre que tout élément $g \in \Gamma$ s'écrit de manière unique $g = \sum_{i=1}^n \mu_i f_i$ avec $(\mu_1, ..., \mu_r) \in \mathbb{Z}^r$ si et seulement si l'application $\mathbb{Z}$-linéaire $\mathbb{Z}^n \to \mathbb{Z}^n$ de matrice P est bijective, c.-à-d. si et seulement si $P \in \mathrm{GL}_n(\mathbb{Z})$.

2. D'après le théorème rappelé dans l'introduction de la section III, il existe une $\mathbb{Z}$-base $(e_i)_{i=1,...,r}$ de Γ (r rang de Γ) et des éléments $d_1, \ldots, d_s$ de $\mathbb{N}^*$ (s rang de Γ', $s \leq r$) tels que $(d_i e_i)_{1 \leq i \leq s}$ soit une $\mathbb{Z}$-base de Γ'. L'isomorphisme

$$\begin{array}{ccc} \Gamma & \longrightarrow & \mathbb{Z}^r \\ \displaystyle\sum_{i=1}^r a_i e_i & \longmapsto & (a_1, \ldots, a_r) \end{array}$$

envoie Γ' sur le sous-groupe $d_1\mathbb{Z} \times \cdots \times d_s\mathbb{Z} \times \{0\}^{r-s}$ de $\mathbb{Z}^s$. Donc le quotient Γ/Γ' est isomorphe au groupe abélien $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}^{r-s}$. Ce groupe est fini si et seulement si $r = s$ (et il est alors de cardinal $d_1 \times \cdots \times d_r$).

3.(a) On sait que I est un sous-groupe du groupe additif de R, donc c'est un g.a.l.t.f. Soit $(e_1, \ldots, e_r)$ une $\mathbb{Z}$-base de R et soit a un élément non nul de I. Alors $(e_1 a, \ldots, e_r a)$ engendre un sous-groupe Γ de I. Soient $\lambda_1, \ldots, \lambda_r$ des entiers tels que $0 = \sum_{i=1}^r \lambda_i e_i a = (\sum_{i=1}^r \lambda_i e_i)a$; puisque R est intègre, $\sum_{i=1}^r \lambda_i e_i = 0$ et donc les λ_i sont tous nuls. Ceci montre que $(e_1 a, \ldots, e_r a)$ est une $\mathbb{Z}$-base de Γ et donc le rang de ce dernier est égal au rang r de R. Il suit que le rang de I, qui est compris entre Γ et R, est également r. D'après 2, R/I est fini.

3.(b) Soit $p : R \to R/I$ la surjection canonique. L'application $J \mapsto p^{-1}(J)$ réalise une bijection entre l'ensemble des idéaux de R/I et celui des idéaux de R contenant I. Puisque R/I est fini, on en déduit qu'il n'y a qu'un nombre fini d'idéaux de R contenant I.

4. On sait qu'il existe une $\mathbb{Z}$-base $(e_i)_{1 \leq i \leq n}$ de $\mathbb{Z}^n$, un entier $r \leq n$ et des éléments $d_1, \ldots, d_r$ de $\mathbb{N}^*$ tels que $(d_i e_i)_{1 \leq i \leq r}$ soit une $\mathbb{Z}$-base de $V \cap \mathbb{Z}^n$. Si $x \in V$, il existe $d \in \mathbb{N}^*$ tel que $dx \in V \cap \mathbb{Z}^n$. Alors dx est combinaison linéaire à coefficients entiers des $d_1 e_1, \ldots, d_r e_r$ et donc x est combinaison linéaire à coefficients rationnels de $e_1, \ldots, e_r$. Par ailleurs, le fait que $(e_i)_{1 \leq i \leq n}$ soit une $\mathbb{Z}$-base entraîne que cette famille est libre sur $\mathbb{Q}$. Par conséquent $(e_i)_{1 \leq i \leq r}$ est une base de V sur $\mathbb{Q}$, ce qui montre aussi que $r = m$.

B. Classes d'idéaux

1. On remarque d'abord que, pour tous $\lambda \in \mathbb{Q}$, $x, y \in \mathbb{Q}[\alpha]$, on a $\mathcal{N}(\lambda x) = |\lambda|\mathcal{N}(x)$ et $\mathcal{N}(x + y) \leq \mathcal{N}(x) + \mathcal{N}(y)$.
Soient $x = \sum_{i=0}^{n-1} x_i \alpha^i$, $y = \sum_{i=0}^{n-1} y_i \alpha^i$ dans $\mathbb{Q}[\alpha]$. Alors

$$\mathcal{N}(xy) = \mathcal{N}\left(\sum_{0 \leq i,j \leq n-1} x_i y_j \alpha^{i+j} \right) \leq (n^2 \max_{0 \leq k \leq 2n-2} \mathcal{N}(\alpha^k)) \mathcal{N}(x)\mathcal{N}(y) .$$

On peut prendre $C = n^2 \max_{0 \leq k \leq 2n-2} \mathcal{N}(\alpha^k)$.

2. Suivant les indications, associons à chaque u_j l'élément $U_j = (jy_i - [jy_i])_{1\le i\le n} \in \mathbb{Q}^n$. On obtient ainsi $M^n + 1$ éléments de $[0,1[^n$. Partitionnons ce "cube" en M^n petits cubes de la forme $\prod_{i=1}^n [k_i/M, (k_i+1)/M[$, où $0 \le k_i \le M-1$ pour $i = 1, \dots, n$. Le principe des tiroirs nous dit qu'il existe deux entiers distinct j_1, j_2 avec $0 \le j_1 < j_2 \le M^n$ tels que U_{j_1} et U_{j_2} sont dans le même petit cube. Alors $\mathcal{N}(u_{j_2} - u_{j_1}) \le 1/M$. En posant $m = j_2 - j_1$ et $a = \sum_{i=0}^{n-1}([j_2 y_i] - [j_1 y_i])\alpha^i$, on a bien $1 \le m \le M^n$, $a \in \mathbb{Z}[\alpha]$ et $\mathcal{N}(my - a) \le 1/M$.

3.(a) D'après la question 2, il existe m parmi $1, \dots, M^n$ et $a \in \mathbb{Z}[\alpha]$ tels que $\mathcal{N}(m\dfrac{x}{z} - a) \le \dfrac{1}{M}$. Alors

$$\mathcal{N}(mx - az) \le C\,\mathcal{N}(m\frac{x}{z} - a)\,\mathcal{N}(z) \le \frac{C}{M}\,\mathcal{N}(z) < \mathcal{N}(z)\ .$$

Remarquons que $mx - az$ appartient à I ; vu le choix de z dans I, l'inégalité stricte ci-dessus impose que $\mathcal{N}(mx - az) = 0$, d'où $mx = az$. Puisque m divise ℓ, on en déduit $\ell x = \dfrac{\ell}{m}\,az \in z\,\mathbb{Z}[\alpha]$. Puisque ceci vaut pour tout $x \in I$, on a montré $\ell I \subset z\,\mathbb{Z}[\alpha]$.

3.(b) Le résultat obtenu en (a) montre que $J = \dfrac{\ell}{z}\,I$ est contenu dans $\mathbb{Z}[\alpha]$; puisque I est un idéal de $\mathbb{Z}[\alpha]$, J est un sous-groupe additif de $\mathbb{Z}[\alpha]$, stable par multiplication par un élément de $\mathbb{Z}[\alpha]$, bref un idéal de $\mathbb{Z}[\alpha]$. Il contient $\ell = \dfrac{\ell}{z}\,z$, donc il contient l'idéal $\ell\,\mathbb{Z}[\alpha]$.

On a montré que tout idéal I de $\mathbb{Z}[\alpha]$ est équivalent à un idéal de $\mathbb{Z}[\alpha]$ contenant $\ell\,\mathbb{Z}[\alpha]$, qui est un idéal non nul de $\mathbb{Z}[\alpha]$ défini indépendamment de I. D'après A.3.(b), il y a donc un nombre fini de classes d'idéaux non nuls de $\mathbb{Z}[\alpha]$.

C. Classes de similitude et classes d'idéaux

1.(a) Puisque α est valeur propre de M dans $\mathbb{Q}[\alpha]$, il y a un vecteur propre pour M dans $\mathbb{Q}[\alpha]^n$ de valeur propre associée α. Quitte à le multiplier par un entier non nul convenable, on peut supposer que ce vecteur propre est à coefficients dans $\mathbb{Z}[\alpha]$: c'est un élément de X_M.

Par ailleurs, puisque $P = \chi_M$ est irréductible sur $\mathbb{Q}$, sa racine α dans $\mathbb{Q}[\alpha]$ est simple (même argument que I.B.2). Donc le sous-espace propre associé à la valeur propre α est de dimension 1, et deux éléments quelconques x et y de X_M sont colinéaires sur $\mathbb{Q}[\alpha]$. Ceci veut dire qu'il existe a et b dans $\mathbb{Z}[\alpha] \setminus \{0\}$ tels que $ax = by$.

1.(b) Par définition, (x) est un sous-groupe de $\mathbb{Z}[\alpha]$. Il est stable par multiplication par α car $\alpha\,{}^t x = M\,{}^t x$ et toutes les coordonnées de $M\,{}^t x$ sont dans (x). Par conséquent (x) est aussi stable par multiplication par tout élément de $\mathbb{Z}[\alpha]$. Ainsi (x) est un idéal de $\mathbb{Z}[\alpha]$.

Pour la même raison, le sous-$\mathbb{Q}$-espace vectoriel V de $\mathbb{Q}[\alpha]$ engendré par $x_1, \dots, x_n$ est un idéal non nul de $\mathbb{Q}[\alpha]$. Mais comme $\mathbb{Q}[\alpha]$ est un corps, $V = Q[\alpha]$. Ainsi V est de dimension n sur $\mathbb{Q}$, ce qui montre que la famille $(x_1, \dots, x_n)$ est libre sur $\mathbb{Q}$. En conséquence, c'est une $\mathbb{Z}$-base de (x). Si y est dans X_M, il existe $z \in \mathbb{Q}[\alpha] \setminus \{0\}$ tel que $y = zx$ (a), d'où $(y) = z(x)$ et $(y) \sim (x)$.

2.(a) Soit I un idéal de $\mathbb{Z}[\alpha]$. Il est de rang n (A.3.(a)) et admet une $\mathbb{Z}$-base $x = (x_1, \dots, x_n)$. Pour $i = 1, \dots, n$, αx_i appartient à I et donc il existe des entiers $m_{i,j}$ avec $1 \le j \le n$ tels que $\alpha x_i = \sum_{i=1}^n m_{i,j} x_j$. La matrice $M = (m_{i,j})_{1\le i,j\le n}$ admet donc ${}^t x$ comme vecteur propre de valeur propre associée α sur $\mathbb{Q}[\alpha]$. Ceci entraîne que α est racine de χ_M dans $\mathbb{Q}[\alpha]$. Comme P est le polynôme minimal de α sur $\mathbb{Q}$, P divise χ_M dans $\mathbb{Q}[X]$ et comme les deux sont unitaires de même degré on a $\chi_M = P$. Donc $M \in \mathcal{E}_{\mathbb{Z}}(P)$, et $j(M) = I$.

2.(b) Supposons d'abord qu'il existe $Q \in \mathrm{GL}_n(\mathbb{Z})$ tel que $M' = Q^{-1}MQ$. Soit $x' \in X_{M'}$. Alors, si ${}^t x = Q\,{}^t x'$, on a $x \in X_M$ et $(x) = (x')$, donc $j(M) = j(M')$.

Réciproquement, supposons $j(M) = j(M')$. On a alors $x \in X_M$, $x' \in X_{M'}$ et $a, b \in \mathbb{Z}[\alpha] \setminus \{0\}$ tels que $a\,(x) = b\,(x')$, et donc $(bx') = (ax)$. Posons $y' = bx' \in X_{M'}$ et $y = ax \in X_M$. Puisqu'on a deux $\mathbb{Z}$-bases y et y' du même g.a.l.t.f, il existe $Q \in \mathrm{GL}_n(\mathbb{Z})$ tel que ${}^t y = Q\,{}^t y'$ (A.1). On a donc que y' appartient à $X_{Q^{-1}MQ}$. Puisque y' est une $\mathbb{Z}$-base de (y') et que $\alpha y' \in (y')$, M' est la seule matrice de $\mathcal{M}_n(\mathbb{Z})$ telle que $\alpha\,{}^t y' = M'\,{}^t y'$. Ainsi $M' = Q^{-1}MQ$, et les matrices M et M' sont semblabkles sur $\mathbb{Z}$.

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

1. Soit f l'endomorphisme de $\mathbb{Q}^n$ de matrice M dans la base canonique. Soit $u \in \mathbb{Q}^n \setminus \{0\}$ tel que $Q(f)(u) = 0$ (le polynôme minimal de f est de la forme QR, on choisit pour u un vecteur non nul

dans l'image de $R(f)$). Soit V le sous-espace vectoriel de $\mathbb{Q}^n$ engendré par les $f^k(u)$ pour $k \in \mathbb{N}$; c'est un sous-espace stable par f et il a pour base $(u, f(u), \ldots, f^{m-1}(u))$ car l'idéal des polynômes $F \in \mathbb{Q}[X]$ tels que $F(f)(u) = 0$ est engendré par Q. Donc V est de dimension m, le polynôme minimal de $f|_V$ est Q, et c'est également son polynôme caractéristique d'après Cayley-Hamilton.
D'après A.4, il existe une $\mathbb{Z}$-base $(e_i)_{1\leq i\leq n}$ de $\mathbb{Z}^n$ telle que $(e_i)_{1\leq i\leq m}$ est une base de V sur $\mathbb{Q}$. Soit $U \in \mathrm{GL}_n(\mathbb{Z})$ la matrice de changement de base de la base canonique à la $\mathbb{Z}$-base $(e_i)_{1\leq i\leq n}$. On a la matrice de f dans la base $(e_i)_{1\leq i\leq n}$ qui est $U^{-1}MU = \begin{pmatrix} C & D \\ 0 & E \end{pmatrix}$, où C, D, E sont à coefficients entiers, C de taille m avec Q comme polynôme caractéristique, et donc E de polynôme caractéristique P/Q. D'après I.C.4, on a $C \in \mathcal{D}_{\mathbb{Z}}(Q)$ et $E \in \mathcal{D}_{\mathbb{Z}}(P/Q)$. Il existe donc A_i semblable sur $\mathbb{Z}$ à C et A'_j semblable sur $\mathbb{Z}$ à E. On en déduit que M est semblable sur $\mathbb{Z}$ à $\begin{pmatrix} A_i & B \\ 0 & A'_j \end{pmatrix}$ pour une certaine matrice B à coefficients entiers.

2. Soit

$$\begin{array}{rcl} \Phi : \mathcal{M}_{m,n-m}(\mathbb{Q}) & \longrightarrow & \mathcal{M}_{m,n-m}(\mathbb{Q}) \\ X & \longmapsto & A_i X - X A'_j \, . \end{array}$$

On a $\Gamma = \mathrm{im}(\Phi) \cap \mathcal{M}_{m,n-m}(\mathbb{Z})$ et $\Gamma' = \Phi(\mathcal{M}_{m,n-m}(\mathbb{Z}))$ qui sont des sous-groupes additifs du g.a.l.t.f $\mathcal{M}_{m,n-m}(\mathbb{Z})$. Ce sont donc des g.a.l.t.f. Ils engendrent tous les deux le sous-espace vectoriel $\mathrm{im}(\Phi)$ de $\mathcal{M}_{m,n-m}(\mathbb{Q})$. Ils ont donc même rang, à savoir le rang de Φ.

3. D'après 1 et I.C.4, 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 $B \in \Gamma$ (noter que Γ et Γ' dépendent de i, j). On a Γ' sous-groupe de Γ, et ce sont deux g.a.l.t.f de même rang (2). Donc Γ/Γ' est fini (A.2). Soient $B_{i,j,1}, \ldots, B_{i,j,t(i,j)} \in \Gamma$ des représentants des classes de Γ/Γ'. Comme

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

on voit que toute matrice de $\mathcal{D}_{\mathbb{Z}}(P)$ est semblable sur $\mathbb{Z}$ à une matrice de la forme $\begin{pmatrix} A_i & B_{i,j,k} \\ 0 & A'_j \end{pmatrix}$ où $1 \leq i \leq r$, $1 \leq j \leq s$, $1 \leq k \leq t(i,j)$. En conclusion, $\mathcal{D}_{\mathbb{Z}}(P)$ est réunion finie de classes de similitude entière.