Corrigé de l'épreuve de mathématiques générales 2011

Préparation à l'agrégation externe
Nice–Sophia Antipolis

E. Aubry

I Préliminaires

A Matrices à coefficients dans K

1. (a) Les valeurs propres de A sont $\{a, c\}$. Si $a \neq c$ alors M est diagonalisable car elle admet 2 valeurs propres distinctes en dimension 2. Si $a = c$ et $b = 0$ alors M est diagonale (donc diagonalisable). Enfin, si $a = c$ et $b \neq 0$, alors M n'est pas diagonalisable car sinon elle serait semblable à aI_2 donc égale à aI_2. Donc M est diagonalisable sauf si $a = c$ et $b \neq 0$.

   (b) D'après ce qui précède I_2 et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ne sont pas semblables (car l'une est diagonalisable et pas l'autre), mais ont le même polynôme caractéristique $(X-1)^2$.

   (c) Si M est diagonalisable, alors elle est semblable à une matrice diagonale de diagonale $(\lambda_1, \cdots, \lambda_n)$ et son polynôme caractéristique est alors $\prod_{i=1}^{n}(X - \lambda_i)$. Donc si deux matrices diagonalisables ont le même polynôme caractéristique, alors elles sont semblables à la même matrice diagonale (à permutation prés des éléments diagonaux, mais comme deux matrices diagonales égales à permutation prés des éléments diagonaux sont conjugués par une matrice de permutation, on obtient le résultat).

2. (a) On peut le faire par opérations élémentaires sur les lignes et les colonnes. Voici une autre méthode : soit (e_i) la base canonique de K^n. L'idéal $I = \{Q \in K[X]/Q(C(P))(e_1) = 0\}$ est engendré par un polynôme unitaire m_1. Or, pour tout $Q = \sum_{i=0}^{n-1} a_i X^i \in K_{n-1}[X] \setminus \{0\}$, on a $Q(C(P))(e_1) = \sum_{i=1}^{n-1} a_i e_{i+1} \neq 0$ car la famille (e_i) est libre et un calcul direct donne $P(C(P))(e_1) = 0$. Donc m_1 est de degré n et divise P. Comme les deux sont unitaires, on a $m_1 = P$. Enfin, d'après Cayley-Hamilton, on a $\chi_{C(P)} \in I$ et donc $P = m_1$ divise $\chi_{C(P)}$. Comme les deux polynômes sont unitaires, on a $P = \chi_{C(P)}$.

   (b) La matrice carrée extraite de la matrice $C(P) - \lambda I_n$ constituée des $n-1$ premières colonnes et des $n-1$ dernières lignes est triangulaire supérieure avec que des 1 sur la diagonale et donc inversible. On en déduit que le rang de $C(P) - \lambda I_n$ est toujours supérieur ou égal à $n-1$.

   (c) (i)⇒(ii) car si $M \in \mathcal{E}_K(P)$, alors d'après Cayley-Hamilton, M est annulé par un polynôme simplement scindé. (ii)⇒(iii) car $C(P) \in \mathcal{E}_K(P)$. (iii)⇒(i) car d'après la question précédente et le théorème du rang, tout espace propre de $C(P)$ est de dimension 1. Donc si $C(P)$ est diagonalisable, $C(P)$ a nécessairement n valeurs propres distinctes et donc $P = \chi_{C(P)}$ est simplement scindé.

3. Pour tout polynôme P, $P(M)$ est une matrice diagonale par blocs $P(A)$ et $P(A')$. Donc si M est diagonalisable, elle admet un polynôme annulateur simplement scindé qui annule aussi A et A'. On en déduit qu'alors A et A' sont diagonalisables. Réciproquement, si A et A' sont diagonalisables, alors elle admettent des polynômes annulateurs simplement scindés dont le ppcm annule M. Comme le ppcm de deux polynômes simplement scindés est simplement scindé, on en déduit que M est diagonalisable.

4. Comme deux matrices semblables ont le même polynôme caractéristique, $\mathcal{E}_K(P)$ est bien réunion de classes de similitudes sur K. D'après l'existence d'une réduite de Jordan, tout élément de $\mathcal{E}_K(P)$ est semblable à une matrice diagonale par blocs $C(P_i)$. Enfin, on a $\chi_M = \prod_i \chi_{C(P_i)} = P_1 \cdots P_r$. Donc le nombre de classe de similitudes de $\mathcal{E}_K(P)$ est majoré par le nombre de façon de décomposer P en produit de facteurs unitaires. Quitte à se placer dans un corps de décomposition de P, on peut supposer que P est le produit de n facteurs de degré 1 et on voit que ce nombre est majoré par $\sum_{r=1}^{n} r! C_{n-1}^{r-1}$.

B Polynômes

1. Par division Euclidienne, il existe $Q \in K[X]$ telle que $P = (X-a)Q$. Donc $P'(a) = Q(a)$. Si $P'(a) = 0$ alors $Q = (X-a)R$ et donc a est racine au moins double de P. Réciproquement, si a est racine au moins double, alors on a $P = (X-a)^2 R$ et donc $P'(X) = 2(X-a)R + (X-a)^2 R'$ s'annule en a.

   Par contraposition on obtient le résultat demandé. Ne pas utiliser la formule de Taylor car le corps n'est pas supposé de caractéristique nulle.

2. Si P est irréductible dans $\mathbb{Q}[X]$, alors $P' \wedge P = 1$. En effet, sinon le pgcd vaut P (car P est irréductible) et donc P divise P', ce qui par raisonnement sur le degré n'est possible que si $P' = 0$. Comme $\mathbb{Q}$ est de caractéristique nulle, on a alors P constant et donc non irréductible.

   On a alors aussi $P' \wedge P = 1$ dans $\mathbb{C}[X]$ (par Bézout) et donc les racines de P dans $\mathbb{C}$ sont forcément simples (d'après la question précédente). On dit que $\mathbb{Q}$ est un corps parfait (remarquez qu'on a juste utilisé que $\mathbb{Q}$ est de caractéristique nulle).

3. Soit $P = QR$ avec $P \in \mathbb{Z}[X]$ unitaire, $Q, R \in \mathbb{Q}[X]$ et Q unitaire. Alors R est unitaire (il suffit de calculer le coefficient dominant du produit). On écrit $Q = \frac{1}{q}\tilde{Q} = \frac{C(\tilde{Q})}{q}\bar{Q}$ et $R = \frac{1}{r}\tilde{R} = \frac{C(\tilde{R})}{r}\bar{R}$ avec $\tilde{Q}, \tilde{R}, \bar{R}, \bar{Q} \in \mathbb{Z}[X]$, $C(\bar{Q}) = 1$ et $C(\bar{R}) = 1$. Comme Q est unitaire, on a que le coefficient dominant c de $\bar{Q}$ vérifie $cC(\tilde{Q}) = q$ et celui r de $\bar{R}$ vérifie $dC(\tilde{R}) = r$. On a donc $Q = \frac{1}{c}\bar{Q}$ et $R = \frac{1}{d}\bar{R}$. Enfin, on a $C(P) = 1$ car P est unitaire et $cdP = \bar{Q}\bar{R}$ et donc $cd = cdC(P) = C(cdP) = C(\bar{Q}\bar{R}) = 1$ donc $c = d = 1$ et on obtient $Q = \bar{Q} \in \mathbb{Z}[X]$.

4. Soit $P \in U_n(\mathbb{Z})$ et $P = \prod P_i^{\alpha_i}$ sa décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$. Comme P est unitaire, on peut supposer tous les P_i unitaires. En itérant la question précédente, on a alors tous les P_i dans $\mathbb{Z}[X]$. On considère alors la matrice de $\mathscr{M}_n(\mathbb{Z})$ diagonale par blocs $C(P_i)$, chaque bloc apparaissant α_i fois. C'est bien une matrice de $\mathcal{E}_{\mathbb{Z}}(P)$ et chaque bloc diagonal est diagonalisable sur $\mathbb{C}$, d'après I.A.2.(c), puisque P_i étant irréductible dans $\mathbb{Q}[X]$, il est à racines simples dans $\mathbb{C}$ d'après I.B.2. On en déduit que $M \in \mathcal{D}_{\mathbb{Z}}(P)$ d'après I.A.3.

C Similitude sur K de matrices blocs

1. L'endomorphisme de $\mathscr{M}_n(K)$ défini par $R_Q(X) = XQ$ est un automorphisme (d'inverse $R_{Q^{-1}}$) et $X \in \ker \Phi_{U,V}$ ssi $UX = XV$ ssi $UXQ = XQU$ ssi $UR_Q(X) = R_Q(X)U$ ssi $R_Q(X) \in \ker \Phi_{U,U}$.

2. Un produit par blocs donne directement $P^{-1} = \begin{pmatrix} I_m & -Y \\ 0 & I_{n-m} \end{pmatrix}$ et $P^{-1}NP = \begin{pmatrix} A & AY - YA' \\ 0 & A' \end{pmatrix}$, d'où la dernière assertion.

3. (a) Si X est dans $\ker \tau \cap \ker \Phi_{N,N}$ ssi $X_{2,1} = X_{2,2} = 0$, $AX_{1,1} = X_{1,1}A$ et $AX_{1,2} = X_{1,2}A'$ ssi X est dans $\ker \tau \cap \ker \Phi_{M,N}$.

   De plus, si $X \in \ker \Phi_{M,N}$, alors on a $A'X_{21} = X_{21}A$, $A'X_{2,2} = X_{2,2}A$ et donc $X' = \begin{pmatrix} 0 & 0 \\ X_{21} & X_{22} \end{pmatrix}$ est dans $\ker \Phi_{N,N}$ et vérifie $\tau(X) = \tau(X') \in \tau(\ker \Phi_{N,N})$.

   (b) Si M et N sont semblables, alors $\ker \Phi_{M,N}$ et $\ker \Phi_{N,N}$ sont isomorphes d'après I.C.1 et les restrictions de τ à ces deux sous-espaces ont les mêmes noyaux, d'après la question précédente. Le théorème du rang implique alors que ces restrictions ont le même rang. Donc $\tau(\ker \Phi_{N,M})$ et $\tau(\ker \Phi_{N,N})$ ont même dimension et donc sont égaux d'après l'inclusion de la question précédente.

(c) On a $\begin{pmatrix} 0 & 0 \\ 0 & I_{n-m} \end{pmatrix} \in \ker \Phi_{N,N}$. Donc d'après la question précédente, si N et M sont semblables, alors il existe $X = \begin{pmatrix} X_{11} & X_{12} \\ 0 & I_{n-m} \end{pmatrix} \in \ker \Phi_{M,N}$, et alors $B = AY - YA'$ avec $Y = -X_{12}$.

4. (ii)⇒(i) car alors M est semblable à N d'après I.C.2 et N est diagonalisable d'après I.A.3.
(i)⇒(ii) car $P(M) = \begin{pmatrix} P(A) & ? \\ 0 & P(A') \end{pmatrix}$ et donc si M est diagonalisable alors M admet un polynôme annulateur simplement scindé qui annule A et A', qui sont donc diagonalisables. Donc M et N sont diagonalisables (d'après I.A.3. pour N) et ont même polynôme caractéristique. On en déduit qu'elles sont semblables d'après I.A.1.(c), et donc il existe Y tel que $B = AY - YA'$ d'après la question précédente.

II Similitude entière

A Généralités, premier exemple

1. Si M admet un inverse $M' \in \mathscr{M}_n(A)$, alors $1 = \det I_n = \det MM' = \det M \det M'$ et on a bien $\det M \in A^\times$. Inversement, si $\det A \in A^\times$, alors $M' = (\det A)^{-1}\ {}^t(ComA) \in \mathscr{M}_n(A)$ et vérifie $MM' = I_n$.
Comme les seuls inversibles de $\mathbb{Z}$ sont 1 et -1, on obtient $Gl_n(\mathbb{Z}) = \{M \in \mathscr{M}_n(\mathbb{Z}) / \det M = \pm 1\}$.
2. Comme la réduction modulo p est un morphisme d'anneau de $\mathbb{Z}$ dans $\mathbb{F}_p$, on a facilement $\overline{M \times N} = \overline{M} \times \overline{N}$ et $\overline{M}^{-1} = \overline{M^{-1}}$. On en déduit que si M et N sont semblables dans $\mathscr{M}_n(\mathbb{Z})$, alors $\overline{M}$ et $\overline{N}$ sont semblables dans $\mathscr{M}_n(\mathbb{F}_p)$.
3. (a) S_1 a deux valeurs propres $\{-1, 1\}$ distinctes donc elles diagonalisable, i.e. semblable à S_0 dans $\mathscr{M}_2(\mathbb{Q})$. Elles ne sont pas semblables sur $\mathbb{Z}$ car leur réduction modulo 2 donne T_1 et I_2 qui ne peuvent être semblables dans $\mathscr{M}_2(\mathbb{F}_2)$ d'après notre réponse à la question I.1(b).
   (b) 1 est racine de χ_M donc il existe $y = {}^t(a_1/b_1, a_2/b_2) \in \mathbb{Q}^2 \setminus \{(0,0)\}$ tel que $My = y$. Alors $x = \frac{b_1 b_2}{a_1 b_2 \wedge a_2 b_1} y$ vérifie les propriétés demandées.
   (c) d'après le critère de Bezout, il existe $(a, b) \in \mathbb{Z}^2$ tel que $ax_1 + bx_2 = 1$. La matrice $P = \begin{pmatrix} x_1 & -b \\ x_2 & a \end{pmatrix}$ est donc dans $Gl_2(\mathbb{Z})$ et on a $MP\ {}^t(1,0) = M\ {}^t(x_1, x_2) = {}^t(x_1, x_2) = P\ {}^t(1,0)$. On en déduit que $P^{-1}MP$ est triangulaire supérieure avec un 1 en haut à gauche. Comme le polynôme caractéristique de $P^{-1}MP$ est $X^2 - 1$, on en déduit qu'il existe $a \in \mathbb{Z}$ tel que $P^{-1}MP = S_a$.
   (d) En reprenant le calcul de la partie II.C, on a $T_x S_a T_x^{-1} = S_{-a-2x}$ et donc S_a est semblable à $S_{\overline{a}}$ où $\overline{a}$ est la réduction de a modulo 2, et donc M est bien semblable à S_0 ou S_1 sur $\mathbb{Z}$.

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

1. (a) Pour une matrice 2×2, on a $\chi_M = X^2 - \operatorname{tr} MX + \det M$. Les matrices recherchées sont donc a coefficients dans $\mathbb{Z}$, de trace nulle et de déterminant $-\delta$. Elle sont donc de la forme $\begin{pmatrix} a & c \\ b & -a \end{pmatrix}$ avec $a^2 + bc = \delta$ et $a, b, c \in \mathbb{Z}$. Réciproquement, ces matrices sont toutes dans $\mathcal{E}_\mathbb{Z}(X^2 - \delta)$.
   Si $a, b \in \mathbb{Z}$ vérifient $b / \delta - a^2$, alors $M_{(a,b)} = \begin{pmatrix} a & \frac{\delta - a^2}{b} \\ b & -a \end{pmatrix}$ est l'unique matrice de $\mathcal{E}_\mathbb{Z}(X^2 - \delta)$ de la forme $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ (notez qu'on a une conclusion plus forte que celle demandée, et on l'utilisera dans la suite).

(b) Soit L l'endomorphisme de $\mathbb{Q}^2$ obtenu par multiplication par $M_{(a,b)}$. Sa matrice dans la base canonique (e_1, e_2) de $\mathbb{Q}^2$ est $M_{(a,b)}$. Sa matrice dans la base $(e_1, -e_2)$ est semblable à $M_{(a,b)}$ sur $\mathbb{Z}$ car la matrice de passage entre les deux bases est à coefficients entiers et déterminant ± 1, donc inversible sur $\mathbb{Z}$. Enfin, cette matrice est dans $\mathcal{E}_{\mathbb{Z}}(X^2 - \delta)$ et sa première colonne est $(a, -b)$ (car $L(e_1) = ae_1 - b(-e_2)$). Donc d'après notre version renforcée de la question précédente, cette matrice est $M_{(a,-b)}$.

De même, en considérant la base $(e_1, e_2 - \lambda e_1)$ de $\mathbb{Q}^2$, on obtient que $M_{(a,b)}$ est semblable à $M_{(a+\lambda b,b)}$, et en considérant la base (e_2, e_1), qu'elle est semblable à $M_{(-a,(\delta-a^2)/b)}$.

2. (a) Soit $M_{(a',\beta(M))} \in \mathcal{E}_{\mathbb{Z}}(X^2 - \delta)$ semblable à M sur $\mathbb{Z}$ (existe puisque le minimum de la partie $\mathcal{B}$ de $\mathbb{N}^*$ est atteint et donc réalisé par une matrice). D'après la question précédente, pour tout $\lambda \in \mathbb{Z}$, $M_{(a'+\lambda\beta(M),\beta(M))}$ est aussi semblable à M sur $\mathbb{Z}$. On choisit λ de manière à ce que $a = a' + \lambda\beta(M)$ soit de valeur absolue minimale. On a alors $|a| \leqslant \frac{\beta(M)}{2}$.

(b) Comme $M_{(a,\beta(M))} \in \mathcal{E}_{\mathbb{Z}}(X^2 - \delta)$, on a $\beta(M)/(\delta - a^2)$ et donc $\beta(M)/|\delta - a^2|$. De plus, si $c = |\delta - a^2|/\beta(M) < \beta(M)$, alors M est semblable à $M_{(-a,c)}$ et $M_{(-a,-c)}$ d'après la question II.B.1.(b), ce qui contredit la minimalité de $\beta(M)$. On en déduit que $\beta(M)^2 \leqslant |\delta - a^2|$.

Si $\delta \geqslant a^2/2$, alors on a $\delta \geqslant \delta - a^2 \geqslant -\delta$ et donc $\beta(M)^2 \leqslant |\delta - a^2| \leqslant \delta$, soit $\beta(M) \leqslant \sqrt{\delta}$.

Si $0 \leqslant \delta < a^2/2$, alors on a $a^2 \geqslant a^2 - \delta \geqslant \frac{a^2}{2}$ et donc $\beta(M)^2 \leqslant |a^2 - \delta| \leqslant a^2 \leqslant \beta(M)^2/4$, ce qui est impossible.

Enfin, si $\delta < 0$ alors on a $\beta(M)^2 \leqslant |a^2 - \delta| \leqslant a^2 + |\delta| \leqslant \beta(M)^2/4 + |\delta|$ et donc $\beta(M) \leqslant \sqrt{\frac{4|\delta|}{3}}$.

(c) Si $M \in \mathcal{E}_{\mathbb{Z}}(X^2 - \delta)$, alors M est semblable à $M_{(a,b)}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ vérifiant $b \leqslant \sqrt{\frac{4|\delta|}{3}}$, $|a| \leqslant b/2$. Comme on a un nombre fini de couples vérifiant ces conditions, $\mathcal{E}_{\mathbb{Z}}(X^2 - \delta)$ contient un nombre fini de classes de similitude entière.

C Diagonalisation et réduction modulo p

1. (a) P et P' sont premiers entre-eux dans $\mathbb{Q}[X]$ car sinon il ont facteur commun de degré au moins 1 qui a une racine dans $\mathbb{C}$ qui est nécessairement une racine double de P sur $\mathbb{C}$. Il existe donc $\tilde{S}, \tilde{T} \in \mathbb{Q}[X]$ tels que $\tilde{S}P + \tilde{T}P' = 1$. En multipliant ces polynômes par le produit des ppcm des dénominateurs de leur coefficients, on obtient $S, T \in \mathbb{Z}[X]$ tels que $SP + TP' = d$, avec $d \in \mathbb{N}^*$.

(b) si p ne divise pas d, alors $\overline{d}$ est inversible dans $\mathbb{F}_p$, et la réduction modulo p de la relation précédente nous donne $(\frac{1}{\overline{d}}\overline{S})\overline{P} + (\frac{1}{\overline{d}}\overline{T})\overline{P'} = 1$, et donc $\overline{P}$ et $\overline{P'} = \overline{P}'$ sont premiers dans $\overline{F}_p[X]$. On en déduit que les racines de $\overline{P}$ dans $\overline{F}_p[X]$ sont simples.

1. (a) Si M est diagonalisable sur $\mathbb{C}$, alors son polynôme minimal m_M sur $\mathbb{C}$ est simplement scindé. Or $M \in \mathscr{M}_l(\mathbb{Q})$ donc son polynôme minimal (qui ne dépend pas du corps) est dans $\mathbb{Q}[X]$. Comme ce polynôme minimal est unitaire et divise $\chi_M \in \mathbb{Z}[X]$ dans $\mathbb{Q}[X]$ qui est lui même unitaire, on obtient $m_M \in \mathbb{Z}[X]$ d'après la question I.B.3.

(b) En appliquant le résultat de la question II.C.1. à m_M, on en déduit qu'il existe $d_M \in \mathbb{N}^*$ tel que si p ne divise pas d_M, alors $\overline{m_M}$ est scindé à racines simples sur le corps algébriquement clos $\overline{\mathbb{F}}_p$. Comme $\overline{m_M}$ annule $\overline{M}$, on en déduit qu'alors $\overline{M}$ est diagonalisable sur $\overline{F}_p$.

D Un résultat de non finitude

1. Soit $P = \beta \prod_{i=1}^{r} P_i^{\alpha_i}$ la décomposition de P en facteurs irréductibles dans $\mathbb{Q}[X]$. Comme P est unitaire et que chaque P_i peut-être prit unitaire, on obtient $\beta = 1$ et d'après la question I.B.3., chaque P_i est dans $\mathbb{Z}[X]$. Il suffit donc de montrer qu'au moins un des α_i est supérieur ou égal à 2. Or les P_i sont premiers entre-eux dans $\mathbb{Q}[X]$ donc dans $\mathbb{C}[X]$ (en passant par l'identité de Bezout). On en déduit qu'ils n'ont pas de racines communes dans $\mathbb{C}$. Si tous les α_i valent 1 alors P n'a que des racines simples dans $\mathbb{C}$. On conclut par contraposée.

2. La réduction $\overline{E_p}$ de E_p modulo p est un matrice diagonale par blocs $\overline{A}$ et $\overline{B}$. Par hypothèse A et B sont diagonalisables sur $\mathbb{C}$ et comme p ne divise pas d_A et d_B, on déduit de II.C.2.(b) que $\overline{A}$ et $\overline{B}$ sont diagonalisable sur $\overline{F}_p$. On en déduit que $\overline{E_p}$ est diagonalisable sur $\overline{\mathbb{F}}_p$. La matrice $\overline{E_q}$ obtenue par réduction modulo p est diagonale par blocs avec au moins un bloc égal à $\begin{pmatrix} \overline{A} & \overline{q}I_l \\ 0 & \overline{A} \end{pmatrix}$. D'après la question I.C.4. ce bloc n'est pas diagonalisable sur $\overline{\mathbb{F}}_p$ car sinon on aurait $\overline{q}I_l = \overline{A}Y - Y\overline{A}$, or $\mathrm{tr}(\overline{A}Y - Y\overline{A}) = 0$ et $\mathrm{tr}(\overline{q}I_l) = l\overline{q} \neq 0$ puisque p est premier et ne divise ni q ni l. On en déduit que $\overline{E_q}$ n'est pas diagonalisable sur $\overline{\mathbb{F}}_p$ (toujours par I.C.4). Donc $\overline{E_p}$ et $\overline{E_q}$ ne sont pas semblables sur $\overline{\mathbb{F}}_p$. On en déduit que E_p et E_q ne sont pas semblables sur $\mathbb{Z}$.
3. Comme $\mathbb{N}$ contient une infinité de nombre premiers distincts et donc une infinité de nombre premiers plus grands que d_A, l et d_B (si $m = 0$), il existe une infinité de matrices (E_p) qui ne sont pas semblables sur $\mathbb{Z}$. Comme toutes ces matrices sont dans $\mathcal{D}_{\mathbb{Z}}(P)$, on en déduit que $\mathcal{D}_{\mathbb{Z}}(P)$ contient une infinité de classes de similitude entière.

III Un théorème de finitude

A Groupes abéliens libres de type fini

1. Si (f_j) est une famille génératrice, alors pour tout $i \in [\![1, n]\!]$ il existe $M = (m_{i,j}) \in \mathscr{M}_n(\mathbb{Z})$ tel que $e_i = \sum_{j=1}^n m_{i,j} f_j = \sum_{k,j=1}^n m_{i,j} p_{j,k} e_k$ et par unicité de la décomposition sur (e_i), on a $MP = I_n$. On en déduit que $P \in Gl_n(\mathbb{Z})$. Réciproquement, si $P \in Gl_n(\mathbb{Z})$, alors $\sum_j (P^{-1})_{i,j} f_j = \sum_j \sum_k (P^{-1})_{i,j} p_{j,k} e_k = e_i$, donc la famille (f_j) est génératrice et si $\sum_j \lambda_j f_j = 0$ alors $(\lambda_1, \cdots, \lambda_n)P = 0$ et donc $\lambda_i = 0$ pour tout i. Donc la famille (f_j) est une base.

   On a donc montrer que si Γ est de rang n, alors $(f_1, \cdots, f_n)$ est une famille génératrice de Γ ssi c'est une base de Γ ssi $P \in Gl_n(\mathbb{Z})$.
2. On reprend les notations du théorème de structure rappelé en introduction. L'application $(z_i) \in \mathbb{Z}^r \mapsto \pi(\sum_i z_i e_i) \in \Gamma/\Gamma'$, où $\pi : \Gamma \to \Gamma/\Gamma'$ est la projection canonique, est surjective de noyau $\prod_{i=1}^s d_i\mathbb{Z} \times \{0\}^{r-s}$ par unicité de la décomposition sur la famille (e_i). On en déduit que Γ/Γ' est isomorphe à $\mathbb{Z}^r / \prod_{i=1}^s d_i\mathbb{Z} \times \{0\}^{r-s} \simeq \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z} \times \mathbb{Z}^{r-s}$, et donc est fini ssi $r = s$.
3. (a) I est un sous-groupe non nul de R donc d'après le théorème de structure, il existe une base $(e_i)_{1 \leqslant i \leqslant r}$ de R, $s \leqslant r$, $d_1, \cdots, d_s \in \mathbb{N}^*$ tels que $(d_1 e_1, \cdots, d_s e_s)$ forme une base de I. Soit $L : x \in R \mapsto e_1.x \in I$. C'est un morphisme de groupe injectif (car R est intègre). On note $M = (m_{ij}) \in \mathscr{M}_{r,s}(\mathbb{Z})$ telle que $L(e_j) = \sum_{i=1}^s m_{ij} d_i e_i$. Si $s < r$ alors les colonnes de M sont liées sur $\mathbb{Q}$, et donc il existe $(q_1, \cdots, q_r) \in \mathbb{Q}^r$ non nul tels que $\sum_{j=1}^r q_j m_{i,j} = 0$ pour tout i. Quitte à multiplier les q_i par le ppcm de leur dénominateur, on peut même supposer $(q_1, \cdots, q_r) \in \mathbb{Z}^r$. Alors on a $0 = \sum_{i=1}^s \sum_{j=1}^r q_j m_{i,j} d_i e_i = \sum_{j=1}^r q_j e_1.e_j = e_1. \sum_{j=1}^r q_j e_j$. Comme R est intègre, on en déduit que $\sum_{j=1}^r q_j e_j = 0$ et donc tous les q_j sont nuls, ce qui est absurde.

      On a donc R et I de même rang et donc R/I est (un groupe) fini d'après la question précédente.

   (b) Comme R/I est fini il admet un nombre fini de sous-partie, donc un nombre fini d'idéaux. Comme l'ensemble des idéaux de R/I est en bijection avec l'ensemble des idéaux de R contenant I, on obtient le résultat demandé.
4. Soit $(f_j)_{j \leqslant m}$ une base de V comme $\mathbb{Q}$-espace vectoriel. Il existe $M = (m_{ij}) \in \mathscr{M}_{n,m}(\mathbb{Q})$ tels que $f_j = \sum_i m_{ij} e_i$. Quitte à multiplier f_j par le ppcm des dénominateurs des $(m_{i,j})_i$, on peut supposer que $\mathscr{M}_{n,m}(\mathbb{Z})$ ((f_j) est toujours une $\mathbb{Q}$-base de V). Alors les f_j sont des éléments de $\mathbb{Z}^n$ qui engendre un sous-groupe Γ' de $\Gamma = \mathbb{Z}^n$. Comme (f_j) est $\mathbb{Q}$-libre, donc $\mathbb{Z}$-libre, Γ' est un g.a.l.t.f. de rang m. Le théorème de structure donne alors une base (e_i) de $\mathbb{Z}^n$ et $d_1, \cdots, d_m \in \mathbb{N}^*$ tels que $(d_1 e_1, \cdots, d_m e_m)$ forme une $\mathbb{Z}$-base de Γ'. En particulier, $(e_1, \cdots, e_m)$ est un famille libre et comme $d_i e_i \in \Gamma' \subset V$ pour tout $i \leqslant m$, on a $e_i \in V$ pour tout $i \leqslant m$. Comme V est de dimension m, $(e_1, \cdots, e_m)$ est une base de V.

B Classes d'idéaux

1. Soit $x = \sum_i x_i \alpha^i$ et $y = \sum_i y_i \alpha^i$ deux éléments de $\mathbb{Q}[\alpha]$. On a alors

$$\mathcal{N}(xy) = \max_k |\sum_{i+j=k} x_i y_j| \leqslant \max_{k \leqslant n-1} (k+1) \max_i |x_i| \max_j |x_j| \leqslant n\mathcal{N}(x)\mathcal{N}(y)$$

2. Suivant l'indication, la famille $(jy_0 - [jy_0], \cdots, jy_{n-1} - [jy_{n-1}])_j$ est constituée de $M^n + 1$ points de $[0,1]^n$. Comme ce cube peut se partitionner en M^n sous-cubes d'arête de longueur $1/M$, on en déduit qu'au moins deux points de la famille sont dans le même sous-cube. Il existe donc $0 \leqslant j' < j \leqslant M^n$ tels que $\mathcal{N}((j-j')y - a) = \max_i |jy_i - [jy_i] - (j'y_i - [j'y_i])| \leqslant 1/M$, où on a posé $a = \sum_{i=0}^{n-1} ([jy_i] - [j'y_i])\alpha^i \in \mathbb{Z}[\alpha]$.

3. (a) D'après la question 2., il existe $a \in \mathbb{Z}[\alpha]$ et $m \leqslant M^n$ tel que $\mathcal{N}(m\frac{y}{z} - a) \leqslant \frac{1}{M}$. Alors on a $\mathcal{N}(mx - za) \leqslant C\mathcal{N}(z)\mathcal{N}(m\frac{y}{z} - a) \leqslant \frac{C}{M}\mathcal{N}(z) < \mathcal{N}(z)$. Comme x, z appartiennent à l'idéal I, on a $mx - az \in I$ et donc par minimalité de z, on obtient $mx = az \in z\mathbb{Z}[\alpha]$. On en déduit que $lx \in z\mathbb{Z}[\alpha]$ pour tout $x \in I$.

   (b) Comme I est un idéal de $\mathbb{Z}[\alpha]$, $\frac{l}{z}I$ est un groupe stable par multiplication par tout élément de $\mathbb{Z}[\alpha]$. De plus il contenu dans $\mathbb{Z}[\alpha]$, d'après ce qui précède, donc c'est bien un idéal de $\mathbb{Z}[\alpha]$. Enfin, comme z appartient à l'idéal I, on a $zx \in I$ pour tout $x \in \mathbb{Z}[\alpha]$, et donc $lx = \frac{l}{z}zx \in J$. On en déduit que $l\mathbb{Z}[\alpha] \subset J$.

   Comme $\mathbb{Z}[\alpha]$ est un anneau intègre et un g.l.a.t.f. et que $l\mathbb{Z}[\alpha]$ est un idéal de $\mathbb{Z}[\alpha]$, l'ensemble des idéaux de $\mathbb{Z}[\alpha]$ contenant $l\mathbb{Z}[\alpha]$ est fini (d'après III.A.3.(b)). Or on vient de voir que tout idéal de $\mathbb{Z}[\alpha]$ est équivalent à un idéal contenant $l\mathbb{Z}[\alpha]$, donc il y a un nombre fini de classes d'idéaux de $\mathbb{Z}[\alpha]$ pour la relation $\sim$.

C Classes de similitude et classes d'idéaux

1. (a) M agit par multiplication sur le $\mathbb{Q}[\alpha]$-espace vectoriel $(\mathbb{Q}[\alpha])^n$. Comme le polynôme caractéristique de cet endomorphisme est P, le même que celui de M, et que α est une racine de P, on en déduit qu'il existe un vecteur propre ${}^t x = {}^t(x_1, \cdots, x_n)$ dans $(\mathbb{Q}[\alpha])^n$ associé à la valeur propre α. Quitte à multiplier x par le produit des dénominateurs des x_i, on peut supposer que $x \in (\mathbb{Z}[\alpha])^n$. Donc X_M n'est pas vide.

   Comme P est irréductible sur $\mathbb{Q}$ α est racine simple de $P = \chi_M$ d'après I.B.2. On en déduit que l'espace propre de M dans $(\mathbb{Q}[\alpha])^n$ associé à la valeur propre α est de dimension 1. Donc si $x, y \in X_M$ alors il existe $\lambda \in \mathbb{Q}[\alpha]$ tel que $y = \lambda x$. Comme $\mathbb{Q}[\alpha]$ est le corps des fractions de $\mathbb{Z}[\alpha]$, il existe $a, b \in \mathbb{Z}[\alpha]$ tels que $\lambda = \frac{a}{b}$. On a alors $ax = by$.

   (b) Si $z \in \mathbb{Z}[\alpha]$, alors il existe $Q \in \mathbb{Z}[\alpha]$ tel que $Q(M)(x) = zx$. Comme $Q(M) = (q_{ij}) \in \mathcal{M}_n(\mathbb{Z})$, on en déduit que $zx_i = \sum_j q_{ij}x_j \in (x)$ et ce pour tout x_i. Donc $z(x) \subset (x)$ pour tout $z \in \mathbb{Z}[\alpha]$, et (x) est bien un idéal de $\mathbb{Z}[\alpha]$.

   Comme $\mathbb{Z}[\alpha]$ est un anneau intègre dont le groupe additif est un g.a.l.t.f. de rang n, on en déduit que (x) est un g.a.l.t.f. de rang n, d'après III.A.3.(a) et III.A.2. Or la famille $(x_1, \cdots, x_n)$ est $\mathbb{Z}$-génératrice dans (x) et on a vu en III.A.1 que cela suffit pour que ce soit une $\mathbb{Z}$-base de (x).

   Enfin, si $x, y \in X_M$ alors d'après la question précédente, on a $(x) \sim (y)$.

2. (a) Soit I un idéal de $\mathbb{Z}[\alpha]$. C'est un g.a.l.t.f. de rang n (en raisonnant comme pour (x) dans la question précédente). Soit $(x_1, \cdots, x_n)$ une $\mathbb{Z}$-base de I et $M \in \mathscr{M}_n(\mathbb{Z})$ telle que $\alpha x_i = \sum_j m_{ij}x_j$ pour tout i (M existe puisque I est un idéal de $\mathbb{Z}[X]$). On a donc $M\ {}^t x = \alpha\ {}^t x$ et $P(M)\ {}^t x = P(\alpha)\ {}^t x = 0$. Comme $P(M) \in \mathscr{M}_n(\mathbb{Z})$ et $(x_1, \cdots, x_n)$ est $\mathbb{Z}$-libre, on en déduit que $P(M) = 0$. Or P est unitaire et irréductible sur $\mathbb{Q}$, donc P est le polynôme minimal de M. Comme P est de degré n, on a $\chi_M = P$ par le théorème de Cayley-Hamilton, et donc $M \in \mathcal{E}_{\mathbb{Z}}(P)$. Enfin, par construction, on a bien $j(M) = I$, donc j est surjective.

   (b) S'il existe $P \in Gl_n(\mathbb{Z})$ telle que $MP = PM'$ et si x est un vecteur propre de M' pour la valeur propre α, alors $y = Px$ est un vecteur propre de M' pour la valeur propre α. Comme $y_j = \sum_i p_{ji}x_i$ est aussi une $\mathbb{Z}$-base de (x) d'après III.A.1., on a $(x) = (y)$ et donc $j(M') = j(M)$.

Réciproquement, si $j(M) = j(M')$, alors $(y) \sim (x)$ pour $x \in X_M$ et $y \in X_{M'}$. Il existe donc $a, b \in \mathbb{Z}[\alpha]$ non nuls tels que $a(x) = b(y)$. On note I cet idéal. $(ax_1, \cdots, ax_n)$ et $(by_1, \cdots, by_n)$ sont deux familles génératrices de I et donc deux bases de I (qui est de rang n comme idéal de $\mathbb{Z}[\alpha]$). Il existe donc $P \in Gl_n(\mathbb{Z})$ telle que $ax_i = \sum_j p_{ij} by_j$ pour tout i. Comme par construction, on a $\sum_k \sum_j m_{ij} p_{jk} by_k = a \sum_i m_{ij} x_j = a\alpha x_i = \sum_j p_{ij} b\alpha y_j = \sum_{j,k} p_{ij} b \sum m'_{jk} y_k$ et que la famille (y_k) est $\mathbb{Z}$-libre, on a $b(\sum_{jk} m_{ij} p_{jk} - p_{ij} m'_{jk}) = 0$, et donc $MP = PM'$, donc M et M' sont $\mathbb{Z}$-semblables.

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

1. On considère M comme agissant sur $\mathbb{Q}^n$ par multiplication. Si $\ker Q(M) = \{0\}$, alors d'après Cayley-Hamilton on a $0 = P(M) = Q^\alpha(M) \circ R(M)$ et donc $R(M) = 0$. On en déduit que le polynôme minimal de M n'admet par Q comme facteur irréductible. Comme les facteurs irréductibles des polynômes minimaux et caractéristiques sont les mêmes, P n'admet pas Q comme facteur irréductible ce qui est absurde.
   Soit donc $x \in V \setminus \{0\}$. L'idéal $I_x = \{R \in \mathbb{Q}[X] / R(M)(x) = 0\}$ contient Q mais pas 1 donc il est engendré par Q (car Q est irréductible). On en déduit que la famille $\{x, \cdots, M^{m-1}x\}$ est une base de $V = \{R(M)(x), M \in \mathbb{Q}[X]\} \simeq \mathbb{Q}[X]/(Q)$. Comme la matrice de $M_{|V}$ est la matrice compagnon de Q, le polynôme caractéristique de $M_{|V}$ est Q.
   D'après la question II.A.4, il existe une $\mathbb{Z}$-base $(e_1, \cdots, e_n)$ de $\mathbb{Z}^n$ telle que $(e_1, \cdots, e_m)$ soit une $\mathbb{Q}$-base de V. Comme V est stable par M, on en déduit que la matrice de M dans la base $(e_1, \cdots, e_n)$ est $\mathbb{Z}$-semblable à M et de la forme $M' = \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix}$, où A est la matrice de $M_{|V}$ dans la base $(e_1, \cdots, e_m)$. Comme M est à coefficients entiers, M', A et A' sont à coefficients entiers. Enfin, $\chi_A = \chi_{M_{|V}} = Q$ et $P = \chi_{M'} = \chi_A \chi_{A'} = Q\chi_{A'}$ donc $\chi_{A'} = P/Q$. On en déduit que $A \in \mathcal{E}_{\mathbb{Z}}(P)$ et $A' \in \mathcal{E}_{\mathcal{Z}}(P/Q)$. Enfin, M' est diagonalisable sur $\mathbb{C}$ et donc d'après la question I.C.4., A et A' sont diagonalisables sur $\mathbb{C}$ et donc dans $\mathcal{D}_{\mathbb{Z}}(Q)$ et $\mathcal{D}_{\mathbb{Z}}(P/Q)$. Par hypothèse de récurrence, il existe $G \in Gl_m(\mathbb{Z})$, $G' \in Gl_{n-m}(\mathbb{Z})$, i et j telles que $A = G^{-1} A_i G$ et $A' = (G')^{-1} A'_j G'$. On a alors $G'' = \begin{pmatrix} G & 0 \\ 0 & G' \end{pmatrix} \in Gl_n(\mathbb{Z})$ et $(G'')^{-1} M' G''$ est de la forme demandée.
2. $\mathcal{M}_{m,n-m}(\mathbb{Z})$ est un g.a.l.t.f. (de rang $m(n-m)$) dont Γ est un sous-groupe, donc lui-même un g.a.l.t.f. De même, Γ' est un sous-groupe de Γ donc un g.a.l.t.f de rang inférieur à celui de Γ.
   Réciproquement, si (M_k) est une $\mathbb{Z}$-base de Γ, alors il existe $X_k \in \mathcal{M}_{m,n-m}(\mathbb{Q})$ telle que $M_k = A_i X_k - X_k A'_j$. Soit d_k le ppcm des dénominateurs des coefficients de X_k, alors $d_k X_k \in \mathcal{M}_{m,n-m}(\mathbb{Z})$ et $d_k M_k \in \Gamma'$. Le groupe engendré par $(d_k M_k)$ est donc un sous-groupe libre de Γ' de même rang que Γ. On en déduit que le rang de Γ' est supérieur à celui de Γ.
3. Tout élément M de $\mathcal{D}_{\mathbb{Z}}(P)$ sont semblables sur $\mathbb{Z}$ à une matrice $M' = \begin{pmatrix} A_i & B \\ 0 & A'_j \end{pmatrix}$. De plus, toute ces matrices M' sont diagonalisables sur $\mathbb{C}$ et de même polynôme caractéristique P, donc elles sont semblables sur $\mathbb{C}$ (d'après I.A.1.(c)). Comme elles sont dans $\mathcal{M}_n(\mathbb{Q})$, elles sont aussi semblables sur $\mathbb{Q}$ (résultat classique qu'on peut démontrer via les invariants de similitudes ou l'unicité de la décomposition de Frobenius) et donc M' est semblable sur $\mathbb{Q}$ à $N = \begin{pmatrix} A_i & 0 \\ 0 & A'_j \end{pmatrix}$ (on peut aussi utiliser la question I.A.4. et dire que les classes de similitude rationnelle de ces matrices forment un ensemble fini et donc qu'on peut supposer qu'elle sont $\mathbb{Q}$-semblables dans la suite). D'après I.C.3.(c), on en déduit que $B \in \Gamma$. Or, en reprenant le calcul de la question I.C.2., on voit que si $Y \in \mathcal{M}_{m,n-m}(\mathbb{Z})$, alors $P = \begin{pmatrix} I_m & Y \\ 0 & I_{n-m} \end{pmatrix} \in Gl_n(\mathbb{Z})$ et $P^{-1} \begin{pmatrix} A_i & B \\ 0 & A'_j \end{pmatrix} P = \begin{pmatrix} A_i & B + AY - YA' \\ 0 & A'_j \end{pmatrix}$ et donc deux éléments de Γ égaux modulo Γ' correspondent à des matrices de $\mathcal{D}_{\mathbb{Z}}(P)$ qui sont $\mathbb{Z}$-semblables.Comme Γ et Γ' on le même rang, Γ/Γ' est fini. Donc le nombre de classes de similitude entière de $\mathcal{D}_{\mathbb{Z}}(P)$ est majoré par $r \times s \times \max_{i,j} \#\Gamma(A_i, A'_j)/\Gamma'(A_i, A'_j)$ (éventuellement fois le nombre de classes de similitudes rationnelle de $\mathcal{E}_{\mathbb{Q}}(P)$ qui est fini par la question I.A.4.).