Corrigé du problème de Mathématiques générales 2011

- Partie IA -

1(a). Si $c \neq a$, la matrice a ses deux valeurs propres distinctes donc est diagonalisable. Si $c = a$, la matrice est diagonalisable si et seulement si elle est égale à aI_2, ce qui équivaut à $b = 0$. On a donc l'équivalence :

$$M \text{ est diagonalisable } \Leftrightarrow a \neq c \text{ ou } b = 0.$$

1(b). Les matrices 0 et $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ont le même polynôme caractéristique X^2 mais ne sont pas semblables.

1(c). Soit M une matrice diagonalisable. On note $\lambda_1, ..., \lambda_r$ ses valeurs propres, qui sont donc les racines du polynôme caractéristique de M, noté χ_M. Soient $m_1, ..., m_r$ les multiplicités respectives de $\lambda_1, ..., \lambda_r$ dans χ_M. Alors, pour tout i, $m_i = \dim \ker (M - \lambda_i I)$ et M est semblable à la matrice :

$$\begin{pmatrix} \lambda_1 I_{m_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_r I_{m_r} \end{pmatrix}.$$

En particulier, deux matrices diagonalisables ayent le même polynôme caractéristique sont semblables à une même matrice diagonale, donc sont semblables.

2(a). Posons $P(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n$. Par définition :

$$\chi_{C(P)}(X) = \begin{vmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & & 0 & a_2 \\ \vdots & \ddots & \ddots & & \vdots \\ 0 & 0 & \cdots & -1 & a_{n-1} + X \end{vmatrix}$$

On effectue des opérations élémentaires sur la première ligne de ce déterminant (la i-ème ligne de la matrice est notée L_i, pour i entre 1 et n), ce qui ne modifie pas sa valeur. on remplace cette première ligne par $L_1 + XL_2 + X^2 L_3 + \cdots + X^{n-1} L_{n-1}$

$$C(P)(X) = \begin{vmatrix} 0 & 0 & \cdots & 0 & a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & & 0 & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & a_{n-1} + X \end{vmatrix}$$

On développe par rapport à la première ligne :

$$C(P)(X) = (-1)^{n+1}(a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n)(-1)^{n-1} = P.$$

2(b). Soit $\lambda \in K$. La matrice $C(P) - \lambda I_n$ a un mineur de taille $n - 1$ non nul, par exemple celui obtenu en supprimant la première ligne et la dernière colonne (matrice triangulaire supérieure avec des 1 sur la diagonale). Donc la matrice $C(P) - \lambda I_n$ est au moins de rang $n - 1$.

On peut aussi invoquer le fait que le polynôme minimal de $C(P)$ est P et qu'une réduite de Jordan de $C(P)$ ne pourrait donc comprendre qu'un unique bloc de Jordan par valeur propre, ce qui fournit le même résultat. C'est du cours usuel pour un agrégatif, mais ce n'est pas tellement dans l'esprit du problème de l'utiliser, vues les questions posées.

2(c).

(i)⇒ (ii) Par le théorème d'Hamilton-Cayley, toutes les matrices de $\mathcal{E}(P)$ annulent un polynôme scindé à racines simples donc sont diagonalisables.

(ii)⇒ (iii) Par IA2(a), la matrice $C(P)$ est dans $\mathcal{E}(P)$.

(iii)⇒ (i) Si la matrice $C(P)$ est diagonalisable, son polynôme minimal est scindé à racines simples. Or son polynôme minimal est P (en effet, P annule $C(P)$, donc le polynôme minimal de $C(P)$ est un diviseur de P. De plus en notant $(e_1, ..., e_n)$ la base canonique, on a : $C(P)e_1 = e_2, C(P)^2e_1 = C(P)e_2 = e_3, \cdots, C(P)^{n-1}e_1 = e_n$, ce qui démontre que $(I_n, C(P), ..., C(P)^{n-1})$ est une famille libre, donc que le polynôme minimal de $C(P)$ est de degré au moins n, et donc égal à P.)

3. Supposons M diagonalisable. Alors M est annulée par un polynôme non nul scindé à racines simples. Ce polynôme annule aussi les matrices A et A' (calcul matriciel par blocs) donc les matrices A et A' sont diagonalisables. Réciproquement, si les matrices A et A' sont diagonalisables, une base de E réunion d'une base de diagonalisation de A et d'une base de diagonalisation de A' est une base de diagonalisation de M, qui est donc diagonalisable.

4. Deux matrices semblables ont le même polynôme caractéristique. Donc $\mathcal{E}(P)$ est une réunion de classes de similitudes. Soit M une matrice dans $\mathcal{E}(P)$. Soit r un entier naturel non nul et soit $P_1, ..., P_r$ les r polynômes unitaires tels que M est semblable à la matrice diagonale par blocs dont les blocs diagonaux sont $C(P_1), ..., C(P(r)$. Alors $P = P_1...P_r$ (cf. IA2(a)). Donc r est majoré par n et les P_i étant des diviseurs unitaires non constants de P, il n'y a qu'un nombre fini de possibilités pour chaque P_i (au plus 2^n). On majore ainsi le nombre de familles possibles $P_1, ..., P_r$ par 2^{n^2}, soit le nombre de classes de similitudes contenues dans $\mathcal{E}(P)$.

- Partie IB -

1. Soit d le degré du polynôme $P>$ Le K-espace vectoriel formé par les polynômes de degré $\leqslant d$, est de dimension $d+1$ et la famille (libre car étagée et de cardinal $d+1$) $((X-a)^i, 0 \leq i \leq d$ en est une base. On décompose le polynôme P sur cette base : $P = \sum_{i=0}^{d} \alpha_i (X-a)^i$. On a : $\alpha_0 = P(a) = 0$ et $\alpha_1 = P'(a)$ (puisque $P = \sum_{i=1}^{d} \alpha_i i (X-a)^{i-1}$). Donc a est racine au moins double si et seulement si $(X-a)^2$ divise P si et seulement si $P'(a) = 0$.

2 Soit P un polynôme irréductible dans $\mathbb{Q}[X]$. En particulier P est de degré $\geqslant 1$ et son polynôme dérivé, P', est non nul. Ces deux polynômes sont donc premiers entre eux. Une relation de Bezout entre P et P', de la forme $AP + BP' = 1$, assure qu'une racine de P n'est pas une racine de P' et donc est une racine simple de P d'après IB1.

3 Soit R dans $\mathbb{Q}[X]$ tel que $P = QR$. Comme Q et R sont à coefficients dans $\mathbb{Q}$, il existe q et r des entiers naturels non nuls tels que $qQ \in \mathbb{Z}[X]$ et $rR \in Z[X]$. Si on choisit r et q minimaux pour cette propriété, alors $C(qQ) = C(rR) = 1$; en effet, les polynômes Q et R étant unitaires, le p.g.c.d. des coefficients de qQ (resp. rR) divise le coefficient du terme de plus haut degré de Q (resp. de R) soit q (resp. r). On a alors : $qrP = (qQ)(rR)$, et, en utilisant le lemme de Gauss rappelé dans l'énoncé (on prend le contenu de chaque côté de cette égalité), $qrC(P) = C(qrP) = C(qQ)c(rR) = 1$. Comme P est dans $\mathbb{Z}[X]$ et unitaire, $C(P) = 1$. On en déduit que q et r sont inversibles dans $\mathbb{Z}$, donc $q = r = 1$.

4 Soit P dans $\mathbb{Z}[X]$ unitaire. D'après IB3, on peut supposer qu'un polynôme irréductible dans $\mathbb{Q}[X]$ diviseur de P est à coefficients dans $\mathbb{Z}$. On peut donc décomposer P sous la forme $P = Q_1^{\alpha_1} \cdots Q_r^{\alpha_r}$ où les Q_i sont des polynômes de $\mathbb{Z}[X]$, irréductibles dans $\mathbb{Q}[X]$, deux à deux non associés, et les α_i sont des entiers naturels $\geqslant 1$.

Les matrices $C(Q_i)$ sont alors à coefficients dans $\mathbb{Z}$ et diagonalisables dans $\mathbb{C}$ (par IB2, Q_i est irréductible sur $\mathbb{Q}$ donc n'a que des racines simples dans $\mathbb{C}$; $C(Q_i)$ est alors diagonalisable dans $\mathbb{C}$ par IA2(c)). On en déduit, en utilisant IA3, que la matrice diagonale par blocs, donc les blocs diagonaux sont $C(Q_1)$ α_1 fois, ..., $C(Q_r)$ α_r fois, est diagonalisable sur C. Son polynôme caractéristique est le produit des polynômes caractéristiques de chacun des blocs, soit $Q_1^{\alpha_1}\cdots Q_r^{\alpha_r} = P$, donc cette matrice est dans $\mathcal{D}_{\mathbb{Z}}(P)$, ce qui démontre que $\mathcal{D}_{\mathbb{Z}}(P)$ est non vide.

- Partie IC -

1. Soit $X \in \mathcal{M}_n(K)$. Alors :
$X \in \ker \Phi_{U,V} \Leftrightarrow UX = XV \Leftrightarrow UX = X(QUQ^{-1}) \Leftrightarrow UXQ = XQU \Leftrightarrow XQ \in \ker \Phi_{U,U}$. Donc l'automorphisme de $\mathcal{M}_n(K)$, $X \to XQ$ (d'inverse $X \to XQ^{-1}$), envoie le noyau $\ker \Phi_{U,V}$ sur le noyau $\ker \Phi_{U,U}$.

2. En utilisant la structure triangulaire par blocs de la matrice P, on calcule le déterminant de P : $\det P = \det I_m \det I_{n-m} = 1$, donc P est inversible. Le calcul matriciel, en utilisant la structure triangulaire par blocs des matrices P et N montre que :

$$P^{-1} = \begin{pmatrix} I_m & -Y \\ 0 & I_{n-m} \end{pmatrix} \text{ et } P^{-1}NP = \begin{pmatrix} A & AY - YA' \\ 0 & A' \end{pmatrix}.$$

Donc s'il existe une matrice Y telle que $B = AY - YA'$, en considérant la matrice P définie ci-dessus pour cette matrice Y, on a : $P^{-1}NPM$, donc M et N sont semblables.

3(a). On remarque que :

$$MX = \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix}\begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} = \begin{pmatrix} AX_{1,1} + BX_{2,1} & AX_{1,2} + BX_{2,2} \\ A'X_{2,1} & A'X_{2,2} \end{pmatrix}.$$

$$\text{Donc } NX = \begin{pmatrix} AX_{1,1} & AX_{1,2} \\ A'X_{2,1} & A'X_{2,2} \end{pmatrix} \text{ et de même, } XN = \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} = \begin{pmatrix} X_{1,1}A & X_{1,2}A' \\ X_{2,1}A & X_{2,2}A' \end{pmatrix}.$$

La matrice $X \in \ker \tau$ si et seulement si $X_{2,1} = 0$ et $X_{2,2} = 0$. Une telle matrice est dans $\ker \Phi_{N,N}$ si et seulement si $NX = XN$, soit utilisant les calculs ci-dessus,si et seulement si $AX_{1,1} = X_{1,1}A$, $AX_{1,2} = X_{1,2}A'$. Une telle matrice est dans $\ker \Phi_{M,N}$ si et seulement si $MX = XN$, soit utilisant les calculs ci-dessus,si et seulement si $AX_{1,1} = AX_{1,1} + BX_{2,1} = X_{1,1}A$, $AX_{1,2} = AX_{1,2} + BX_{2,2} = X_{1,2}A'$. Donc, pour une matrice X dans $\ker \tau$, $X \in \ker \Phi_{N,N}$ si et seulement si $X \in \ker \Phi_{M,N}$. Ce qui démontre $\ker \tau \cap \ker \Phi_{N,N} = \ker \tau \cap \ker \Phi_{M,N}$.

Soit $X \in \ker \Phi_{M,N}$. Donc en notant $X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix}$, on a : $AX_{1,1} + BX_{2,1} = X_{1,1}A, AX_{1,2} + BX_{2,2} = X_{1,2}A', A'X_{2,1} = X_{2,1}A, A'X_{2,2} = X_{2,2}A'$. Ces deux dernières égalités assurent que la matrice Y, définie par $Y = \begin{pmatrix} 0 & 0 \\ X_{2,1} & X_{2,2} \end{pmatrix}$ vérifie $Y \in \ker \Phi_{N,N}$. Et $\tau(X) = \begin{pmatrix} X_{2,1} & X_{2,2} \end{pmatrix} = \tau(Y)$. On a donc l'inclusion : $\tau(\ker \Phi_{M,N}) \subset \tau(\ker \Phi_{N,N})$.

3(b). On applique le théorème du rang à τ sur $\ker \Phi_{M,N}$: $\dim \ker \Phi_{M,N} = \dim \ker \tau \cap \ker \Phi_{M,N} + \dim \tau(\ker \Phi_{M,N})$. De même, le théorème du rang appliqué à τ sur $\ker \Phi_{N,N}$ fournit l'égalité $\dim \ker \Phi_{N,N} = \dim \ker \tau \cap \ker \Phi_{N,N} + \dim \tau(\ker \Phi_{N,N})$. Or, par IC3(a), $\dim \ker \tau \cap \ker \Phi_{M,N} = \dim \ker \tau \cap \ker \Phi_{N,N}$, et si M et N sont semblables, par IC1, $\dim \ker \Phi_{M,N} = \dim \ker \Phi_{N,N}$. Donc $\dim \tau(\ker \Phi_{M,N}) = \dim \tau(\ker \Phi_{N,N})$ et l'inclusion IC3(a) $\tau(\ker \Phi_{M,N}) \subset \tau(\ker \Phi_{N,N})$ est en fait une égalité.

3(c). La matrice $Z = \begin{pmatrix} 0 & 0 \\ 0 & I_{n-m} \end{pmatrix}$ est dans $\ker \Phi_{N,N}$, donc, par IC3(b), il existe X dans $\ker \Phi_{M,N}$ telle que $\tau(X) = \tau(Z) = (O, I_{n-m})$. Posons $X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ 0 & I_{n-m} \end{pmatrix}$. Alors $B = A(-X_{1,2}) - (-X_{1,2})A'$.

4. Supposons M diagonalisable. Alors A et A' annulent le polynôme minimal de M, donc sont diagonalisables ; Donc N est diagonalisable par IA3. Comme $\chi_M = \chi_A\chi_{A'} = \chi_N$, M et N ont le même ensemble de valeurs propres

et, pour chaque valeur propre, les deux sous-espaces propres respectivement de M et de N, relatifs à cette valeur propre, ont la même dimension (multiplicité de cette valeur propre comme racine du polynôme $\chi_M = \chi_N$, donc M et N sont semblables. On applique alors IC3(c), il existe Y telle que $B = AY - YA'$. Réciproquement, supposons qu'il existe Y telle que $B = AY - YA'$, donc par IC2, M est semblable à la matrice $N = \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}$. Si de plus, A et A' sont supposées diagonalisables, alors la matrice N est diagonalisable par IA3, et M, qui lui est semblable, aussi.

- Partie IIA -

1. Soit $M \in GL_n(A)$ et soit N son inverse. Alors $1 = \det M \det N$; comme $\det M$ et $\det N$ sont dans A en tant que déterminants de matrices à coefficients dans A, $\det M$ est un élément inversible de A. Réciproquement, soit M une matrice dans $\mathcal{M}_n(A)$. On note $\tilde{M}$ la transposée de sa comatrice. Les coefficients de $\tilde{M}$ sont au signe près des mineurs extraits de M donc sont à coefficients dans A. Et $M\tilde{M} = \det M I_n$. Donc lorsque $\det M$ est un élément inversible de A, M est inversible dans $\mathcal{M}_n(A)$ d'inverse $\det M^{-1}\tilde{M}$. Les inversibles de $\mathbb{Z}$ sont 1 et -1. Donc une matrice de $\mathcal{M}_n(\mathbb{Z})$ appartient à $GL_n(\mathbb{Z})$ si et seulement si son déterminant est égal à ± 1.

2. La réduction modulo p est un morphisme d'anneaux de $\mathcal{M}_n(\mathbb{Z})$ sur $\mathcal{M}_n(\mathbb{F}_p)$ qui envoie la matrice identité sur la matrice identité.

3(a). $\forall a \in \mathbb{Q}$, la matrice S_a est diagonalisable avec les deux valeurs propres distinctes 1 et -1 donc est semblable sur $\mathbb{Q}$ à S_0. En particulier, S_0 et S_1 sont semblables sur $\mathbb{Q}$. Soit $N = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$ telle que $NS_0 = S_1N$.

$$\begin{pmatrix} x & -y \\ z & -t \end{pmatrix} = NS_0 = S_1N = \begin{pmatrix} x+z & y+t \\ -z & -t \end{pmatrix}.$$

Donc $z = 0$ et $t = -2y$; en particulier $\det N = xt = -2xy \in 2\mathbb{Z}$, donc N n'est pas inversible dans $\mathcal{M}_2(\mathbb{Z})$ par II1.

3(b). Soit $M \in \mathcal{M}_2(\mathbb{Z})$ de polynôme caractéristique $X^2 - 1$. Alors M annule un polynome scindé à racines simples (théorème d'Hamilton-Cayley) donc est diagonalisable sur $\mathbb{Q}$ de valeurs propres 1 et -1. Soit un vecteur propre (non nul) de M relatif à la valeur propre 1. Alors en multipliant les coordonnées de y par le produit de leurs dénominateurs, on obtient un vecteur propre (non nul) z dont les coordonnées sont entières. En divisant les coordonnées de z par leur p.g.c.d., on obtient un un vecteur propre (non nul) dont les coordonnées sont entières et premières entre elles.

3(c) Par II3(b), il existe un vecteur x de coordonnées x_1, x_2 entières et premières entre elles tel que $Mx = x$. On écrit une relation de Bezout entre x_1 et x_2 : $y_1x_1 - y_2x_2 = 1$. Alors la matrice $P = \begin{pmatrix} x_1 & y_2 \\ x_2 & y_1 \end{pmatrix}$ est une matrice à coefficients dans $\mathbb{Z}$ de déterminant égal à 1 donc inversible dans $\mathcal{M}_2(\mathbb{Z})$. Donc la matrice $P^{-1}MP$ est dela forme $\begin{pmatrix} 1 & u \\ 0 & v \end{pmatrix}$; comme de plus, elle est de déterminant -1 comme M, $v = -1$ donc $P^{-1}MP = S_u$.

3(d) On a :

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

Donc la matrice S_a est semblable sur $\mathbb{Z}$ à S_0 si a est pair et à S_1 si a est impair. Il y a donc au plus deux classes de similitudes sur Z de matrices S_a, $a \in \mathbb{Z}$. Il y en a au moins deux par II3(a), donc il y en a exactement deux : celle de S_0 qui contient les matrices S_a, $a \in 2\mathbb{Z}$, et celle de S_1 qui contient les matrices S_a, $a \in 2\mathbb{Z} + 1$.

- Partie IIB -

1(a). Le polynôme caractéristique d'une matrice $(2,2)$, M, est $X^2 - \mathrm{tr}(M)X + \det M$. Donc $\mathcal{E}_{\mathbb{Z}}(X^2-\delta)$ est l'ensemble des matrices $(2,2)$ de trace nulle et de déterminant $-\delta$, c'est-à-dire de la forme $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ avec $a^2+bc=\delta$.

Si a et b sont deux entiers tels que b divise $\delta - a^2$, il existe une unique matrice M de la forme $\begin{pmatrix} a & c \\ b & -a \end{pmatrix}$ et dans $\mathcal{E}_{\mathbb{Z}}(X^2-\delta)$, puisqu'il existe un unique entier c tel que $a^2+bc=\delta$.

1(b). Posons $c = (\delta - a^2)/b$. On a, avec les notations de la question IIA3 : $S_0 M_(a,b) S_0^{-1} = M_(a,-b)$, $(-S_0)M_(a,b)(-S_0)^{-1} = M_(-a,c)$, et

$$T_\lambda M_{(a,b)} T_\lambda^{-1} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & c \\ b & -a \end{pmatrix}\begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a +_\lambda b & c - 2a\lambda - b\lambda^2 \\ b & -(a+\lambda b) \end{pmatrix} = M_{(a+\lambda b,b)}.$$

Les matrices $S_0, -S_0, T_\lambda$ sont à coefficients dans $\mathbb{Z}$ et de déterminants respectifs $-1,-1,1$ donc dans $GL_n(\mathbb{Z})$.

2(a). On effectue la division euclidienne de a par b avec plus petit reste : il existe $q \in \mathbb{Z}$ et $r \in \mathbb{Z}$ tels que $a = bq + r$ abec $|r| \leqslant b/2$. On choisit $M_{(a,b)}$ semblable à M telel que $b = \beta(M)$. Alors, en utilisant IIB2(a), $M_{(r,b)} = T_{-q} M_{(a,b)} T_{-q}^{-1}$ convient.

2(b). On a : $(\delta - a^2) = bc = \beta(M)c$. Or par IIB1(b), il existe une matrice $M_(\pm a, |c|)$ semblable à $M_{(a,b)}$ sur $\mathbb{Z}$; donc, par minimalité de $\beta(M)$, $\beta(M) \leqslant |c|$), soit $\beta(M)^2 \leqslant |\delta - a^2|$.

Donc, si $\delta > 0$, $\beta(M)^2 \leqslant |\delta - a^2| \leqslant \delta$ donc $\beta(M) \leqslant \sqrt(\delta)$; si $\delta < 0$, $\beta(M)^2 \leqslant |\delta - a^2| \leqslant \delta + a^2 \leqslant \delta + \beta(M)^2/4$, donc $3\beta(M)^2/4 \leqslant \delta$, donc $\beta(M) \leqslant 2\sqrt(\delta/3)$.

2(c). Les valeurs possiblement prises par β sont des entiers dans un intervalle borné, d'après IIB2(b), donc sont dans un ensemble fini, noté E. Il y a donc un nombre fini de matrices $M_{a,b}$ possibles, avec les conditions $|a| \leqslant b/2$ et $b \in E$. Comme chaque classe de similitude dans $\mathcal{E}(P)$ contient une telle matrice, il n'y a qu'un nombre fini de classes de similitudes dans $\mathcal{E}(P)$.

- Partie IIC -

1(a). Les polynômes P et P' n'ont pas de racines complexes communes (P n'a que des racines simples) donc sont premiers entre eux sur $\mathbb{Q}$. ILs vérifient dans $\mathbb{Q}[X]$ une relation de Bezout : Il existe A, B dans $\mathbb{Q}[X]$ tels que $AP + BP' = 1$. Soit d le p.p.c.m. (positif) des dénominateurs des coefficients de A et B. Alors les polynômes $S = dA$ et $T = dB$ sont dans $\mathbb{Z}[X]$ et vérifient $SP + TP' = d$.

1(b). L'application $M \to \bar{M}$ est un morphisme d'anneaux donc $\bar{S}\overline{P} + \bar{T}\overline{P'} = \bar{d}$. Comme p ne divise pas d, $\bar{d}$ est inversible dans $\mathbb{F}_p$. De plus, $\overline{P'}$ est le polynôme dérivé de $\overline{P}$ dans $\mathbb{F}_p[X]$, donc le polynôme $\overline{P}$ et son polynôme dérivé dans $\mathbb{F}_p[X]$ n'ont pas de racine commune dans $\overline{\mathbb{F}_p}$, ce qui démontre que les racines de $\overline{P}$ dans $\overline{\mathbb{F}_p}$ sont simples. *Attention, un morphisme d'anneaux en général, n'envoie pas toujours un élément inversible sur un élément inversible. Ce n'est vrai que s'il envoie l'élément neutre multiplicatif de l'anneau de départ sur l'élément neutre multiplicatif de l'anneau d'arrivée.*

2(a). Par le théorème d'Hamilton Cayley, la matrice M annule son polynôme caractéristique $\chi_M = \det(XI_l - M)$, polynôme unitaire dans $\mathbb{Z}[X]$. Le polynôme minimal π_M de M est un diviseur unitaire de χ_M dans $\mathbb{Q}[X]$. Donc, par IB3, on sait que π_M est dans $\mathbb{Z}[X]$. Comme M est diagonalisable sur $\mathbb{C}$, son polynôme minimal n'a que des racines simples dans $\mathbb{C}$. Donc π_M convient.

2(b). Posons $P = \pi_M$. Par IIC2(a), il existe des polynômes S et T dans $\mathbb{Z}[X]$ et un entier naturel non nul d tels question $SP + TP' = d$. Soit p un nombre premier ne divisant pas d ; d'après IIC1(b), les racines de $\overline{P}$ dans $\overline{\mathbb{F}_p}$ sont simples. Alors, en utilisant le fait que $M \to \overline{M}$ est un morphisme d'anneaux, $0 = \overline{P(M)} = \overline{P}(\overline{M})$, donc $\overline{M}$ est annulée par un polynôme scindé à racines simples dans $\overline{\mathbb{F}_p}$, donc est diagonalisable sur $\overline{\mathbb{F}_p}$.

- Partie IID -

1. Soit α une racine complexe au moins double de P et soit Q son polynome minimal sur $\mathbb{Q}$, qu'on choisit unitaire. Alors α est racine simple de Q (Q est irréductible sur $\mathbb{Q}$, cf. IB2.) donc Q^2 divise P. On décompose P sous la forme $P = Q^2R$, avec $R \in \mathbb{Q}[X]$. Par IB3 (appliqué deux fois, une fois à la décomposition $P = Q(QR)$ puis à la décomposition $P = Q^2.R$), les polynômes Q et R sont en fait dans $\mathbb{Z}$.

2. Par contraposée, supposons E_p et E_q semblables sur $\mathbb{Z}$, et donc, par IIA2, les matrices $\overline{E_p}$ et $\overline{E_q}$ sont semblables sur $\mathbb{F}_p$. Par IIC2(b), puisqu' on suppose que p ne divise ni d_A, ni d_B, les matrices $\overline{A}$ et $\overline{B}$ sont diagonalisables sur $\overline{\mathbb{F}_p}$. On a :

$$\overline{E_p} = \begin{pmatrix} \overline{A} & 0 & 0 \\ 0 & \overline{A} & 0 \\ 0 & 0 & \overline{B} \end{pmatrix} \text{ si } m > 0, \ \overline{E_p} = \begin{pmatrix} \overline{A} & 0 \\ 0 & \overline{A} \end{pmatrix} \text{ si } m = 0.$$

Donc la matrice $\overline{E_p}$ est diagonalisable sur $\mathbb{F}_p$, par IA3. Donc la matrice $\overline{E_q}$ est diagonalisable sur $\mathbb{F}_p$
Soit $\overline{q}$ la classe de q modulo p. Par hypothèse $\overline{q} \neq 0$. On a :

$$\overline{E_q} = \begin{pmatrix} \overline{A} & \overline{q}I_l & 0 \\ 0 & \overline{A} & 0 \\ 0 & 0 & \overline{B} \end{pmatrix} \text{ si } m > 0, \ \overline{E_q} = \begin{pmatrix} \overline{A} & \overline{q}I_l \\ 0 & \overline{A} \end{pmatrix} \text{ si } m = 0.$$

Comme $\overline{E_q}$ est diagonalisable sur $\mathbb{F}_p$, il en est de même de la matrice $\begin{pmatrix} \overline{A} & \overline{q}I_l \\ 0 & \overline{A} \end{pmatrix}$ par IA3. Par IC4, on en déduit qu'il existe une matrice Y dans $\mathcal{M}_l(\mathbb{F}_p)$ telle que $\overline{q}I_l = AY - YA$; en prenant la trace de cette matrice, on obtient $\overline{q}\overline{l} = 0$ donc, puisque $\overline{q} \neq 0$, $\overline{l} = 0$ donc $p|l$.

3. Avec les notations précédentes, il n'y a qu'un nombre fini de nombres premiers diviseurs de l'entier ld_Ad_B. Donc l'ensemble infini des nombres premiers ne divisant pas ld_Ad_B s'injecte dans l'ensemble des classes de similitude contenues dans $\mathcal{E}_{\mathbb{Z}}(P)$ par l'application $p \to \{UE_pU^{-1} \ ; \ U \in GL_n(\mathbb{Z})\}$ dont on a montré l'injectivité en IID2. Donc $\mathcal{E}_{\mathbb{Z}}(P)$ n'est pas réunion finie de classes de similitude.

- Partie IIIA -

1. Supposons $P \in GL_n(\mathbb{Z})$. Soient $\alpha_1, ..., \alpha_n$ dans $\mathbb{Z}$ tels que $\sum_i \alpha_i f_i = 0$. Alors le vecteur $(\alpha_i)_i$ est dans le noyau de P, donc est nul. La famille $(f_i)_i$ est donc libre. Soit Γ' le sous-groupe engendré par la famille (f_i). Alors $\Gamma' = P\Gamma$ donc $\Gamma = P^{-1}\Gamma'$, ce qui justifie que la famille $(f_i)_i$ est génératrice. C'est donc une $\mathbb{Z}$-base de Γ.

Réciproquement, si la famille $(f_i)_i$ est une $\mathbb{Z}$-base de Γ, on peut décomposer chaque e_j comme une combinaison linéaire à coefficients entiers des f_i, ce qui définit une matrice Q dans $\mathcal{M}_n(\mathbb{Z})$. Comme $(e_i)_i = Q(f_i)_i = QP(e_i)_i$, la liberté de la famille $(e_i)_i$ assure que $QP = I_n$, donc P est inversible dans $\mathcal{M}_n(\mathbb{Z})$, d'inverse Q.

2. On utilise la version légère du théorème de la base adaptée rappelée dans l'enoncé : Soit Γ un g.a.l.t.f. de rang n. Soit Γ' un sous-groupe non nul de Γ. Il existe un entier naturel non nul $s \leqslant n$, des entiers naturels non nuls $d_1, ..., d_s$ et une $\mathbb{Z}$-base $(e_1, ..., e_n)$ de Γ tels que $(d_1e_1, ..., d_se_s)$ est une $\mathbb{Z}$-base de Γ'. Soit π la surjection canonique de Γ sur son quotient Γ/Γ'. Alors l'application surjective qui envoie $(\lambda_1, ..., \lambda_n)$ dans $\mathbb{Z}^n$ sur $\pi(\sum_i \lambda_i e_i$ se factorise coefficient par coefficient en un isomorphisme de $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}^{n-s}$. Donc Γ/Γ' est fini si et seulement si $n = s$, i.e. Γ et Γ' ont même rang.

3(a). Soit Γ un g.a.l.t.f.. Soit Γ' un sous-groupe de Γ qui contient un sous-groupe Γ" de même rang que Γ. Alors Γ/Γ'' est fini par IIIA2. L'inclusion de Γ' dans Γ induit un morphisme injectif de Γ'/Γ'' dans Γ/Γ'' qui permet d'identifier Γ'/Γ'' à un sous-groupe de Γ/Γ''. La composée de la surjection canonique de Γ sur Γ/Γ'' composée avec la surjection canonique de Γ/Γ'' sur $(\Gamma/\Gamma'')/(\Gamma'/\Gamma'')$ définit un morphisme surjectif de noyau Γ'. Donc le quotient Γ/Γ' est fini et, par IIIA2, Γ' est un sous-groupe de même rang que Γ.

Soit alors $(e_1, ..., e_n)$ une $\mathbb{Z}$-base de R. Soit $a \neq 0$ un élément de I. Alors, R étant supposé intègre, $(ae_1, ..., ae_n)$ est aussi une $\mathbb{Z}$-partie libre de R et chacun des vecteurs $ae_i \in I$. On applique alors la remarque ci dessus à $\Gamma'' = \oplus_i \mathbb{Z}ae_i \subset \Gamma' = I \subset \Gamma = R$.

3(b). Soit π la surjection canonique de R sur R/I. Alors l'application $J \to \pi(J)$ induit une bijection de l'ensemble des idéaux de R contenant I sur l'ensemble des idéaux de R/I (d' inverse $\overline{J} \to \pi^{-1}(\overline{J})$). Comme R/I est fini (IIIA3(a)), il n'a qu' un nombre fini de parties, donc un nombre fini d'idéaux. Donc l'ensemble des idéaux de R contenant I est fini.

4. Considérons $V \cap \mathbb{Z}^n$, sous-groupe de $\mathbb{Z}^n$. On lui applique la version légère du théorème de la base adaptée rappelée dans l'enoncé : Il existe un entier naturel non nul $m \leqslant n$, des entiers naturels non nuls $d_1, ..., d_s$ et une $\mathbb{Z}$-base $(e_1, ..., e_n)$ de $\mathbb{Z}^n$ tels que $(d_1e_1, ..., d_me_m)$ est une $\mathbb{Z}$-base de $V \cap \mathbb{Z}^n$. Soit i un entier compris entre 1 et m ; $e_i \in \mathbb{Z}^n$ et, comme V est un $\mathbb{Q}$-espace vectoriel, $e_i = \frac{1}{d_i} d_i e_i \in V$. Donc $e_i \in V \cap \mathbb{Z}^n$. On en déduit que $d_1 = \cdots = d_m = 1$.

- Partie IIIB -

1. On remarque que $\mathcal{N}$ est une norme (la norme sup associée à une base) et en particulier vérifie l'inégalité triangulaire. Avec les notations de l'énoncé, pour un entier k compris entre 0 et n^2, $|\sum_{i+j=k} x_i y_j| \leqslant \sum_{i+j=k} |x_i y_j| \leqslant (k+1)\mathcal{N}(x)\mathcal{N}(y)$. Donc :

$$\begin{aligned} \mathcal{N}(xy) &= \mathcal{N}(\textstyle\sum_{k=0}^{n^2}(\sum_{i+j=k} x_i y_j)\alpha^k) \\ &\leqslant \textstyle\sum_{k=0}^{n^2} \mathcal{N}(\sum_{i+j=k} x_i y_j)\alpha^k) \\ &\leqslant \textstyle\sum_{k=0}^{n^2} |\sum_{i+j=k} x_i y_j| \mathcal{N}(\alpha^k) \\ &\leqslant (\textstyle\sum_{k=0}^{n^2}(k+1)\mathcal{N}(\alpha^k))\mathcal{N}(x)\mathcal{N}(y) \end{aligned}$$

On peut donc poser $C = \sum_{k=0}^{n^2}(k+1)\mathcal{N}(\alpha^k$.

2. Soit $K = \{x = \sum_{i=0}^{n-1} x_i \alpha^i \in \mathbb{Q}[\alpha]\ ;\ 0 \leqslant x_i < 1\}$. Selon les indications de l'énoncé, on construit ainsi pour tout j entre 0 et M^n un élément a_j dans $\mathbb{Z}[\alpha]$ tel que $jy - a_j \in K$. On découpe l'ensemble en M^n parties disjointes de la forme $k_i/M \leqslant x_i < (k_i+1)/M$, pour $k_0, ..., k_{n-1}$ entiers entre 0 et $M-1$. Par le principe des tiroirs (il y a $M^n + 1$ éléments pour M^n parties), il existe $j < k$ entre 0 et M^n tels que $jy - a_j$ et $ky - a_k$ sont dans une même partie. Ainsi $(k-j)y - (a_k - a_j)$ est de la forme $\sum_{i=0}^{n-1} y_i \alpha^i \in \mathbb{Q}[\alpha]$ avec, pour tout i, $-1/M \leqslant y_i \leqslant 1/M$ et donc $\mathcal{N}((k-j)y - (a_k - a_j)) \leqslant 1/M$. On pose $m = k - j \in \{1, ..., M^n\}$ puisque $0 \leqslant j < k \leqslant M^n$ et $a = a_k - a_j \in \mathbb{Z}[\alpha]$.

3(a). Soit x dans $\mathcal{I}$. On applique la question IIIB2 à x/z : il existe m dans $\{1, ..., M^n\}$ et a dans $\mathbb{Z}[\alpha]$ tels que $\mathcal{N}(m(x/z) - a) \leqslant 1/M$, donc $\mathcal{N}(mx - az) = \mathcal{N}((m(x/z) - a)z) \leqslant C\mathcal{N}(m(x/z) - a)\mathcal{N}(z) \leqslant C/M\mathcal{N}(z) < \mathcal{N}(z)$. Or, $\mathcal{I}$ étant un ideal, $mx - az \in \mathcal{I}$. Par minimalité de $\mathcal{N}(z)$, on a alors, $\mathcal{N}(mx - az) = 0$ soit $mx = az$ ($\mathcal{N}$ est une norme). Donc $mx \in z\mathbb{Z}[\alpha]$. Comme m divise l dans $\mathbb{Z}$, $lx \in z\mathbb{Z}[\alpha]$. On a ainsi l'inclusion $l\mathcal{I} \subset z\mathbb{Z}[\alpha]$.

3(b). La question IIIB3(a) assure que $l\frac{l}{z}mathcalI \subset \mathbb{Z}[\alpha]$. On vérifie alors que $l\frac{l}{z}mathcalI$ est un idéal. Il contient $l\mathbb{Z}[\alpha]$ car $z \in \mathbb{Z}[\alpha]$. Donc $I \sim J$ o'u J est un idéal de $\mathbb{Z}[\alpha]$ contenant $l\mathbb{Z}[\alpha]$. Il y a un nombre fini de tels idéaux par IIA3(b) appliqué à $R = \mathbb{Z}[\alpha]$, $I = l\mathbb{Z}[\alpha]$, en utilisant IIIA2 pour justifier que R/I est fini.