3.2 Corrigé

I. - Sous-groupes finis de $GL_n(\mathbf{Z})$

1. Il s'agit d'un résultat classique : montrons le par récurrence sur le degré $n \in \mathbf{N}^*$ du polynôme P.
Pour $n = 1$, P est de la forme $X + a_0$, $M_P = (-a_0)$ et $C_{M_P}(X) = |X + a_0| = X + a_0 = P$. Pour $n \geqslant 2$, supposons avoir établi le résultat au rang $n-1$. Un polynôme P à coefficients complexes unitaire de degré n est de la forme $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = XQ + a_0$, où
$Q = X^{n-1} + a_{n-1}X^{n-2} + \ldots + a_2X + a_1$.
Or, $C_{M_P}(X) = \det(XI_n - M_P) = \begin{vmatrix} X & 0 & \ldots & \ldots & \ldots & 0 & a_0 \\ -1 & X & 0 & \ldots & \ldots & 0 & a_1 \\ 0 & -1 & X & 0 & \ldots & 0 & a_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & -1 & X & 0 & a_{n-3} \\ 0 & \ldots & \ldots & 0 & -1 & X & a_{n-2} \\ 0 & \ldots & \ldots & \ldots & 0 & -1 & X + a_{n-1} \end{vmatrix}$.
En développant ce déterminant par rapport à la première ligne, il vient :
$C_{M_P}(X) = X\det(XI_{n-1} - M_Q) + a_0(-1)^{n+1}(-1)^{n-1} = XC_{M_Q}(X) + a_0$.
Or, par hypothèse de récurrence, $C_{M_Q}(X) = Q$; d'où $C_{M_P}(X) = XQ + a_0 = P$.
Par conséquent, pour tout polynôme P à coefficients complexes unitaire de degré n, le polynôme caractéristique de la matrice compagnon qui lui est associée est le polynôme P lui-même.

2. (a) Soit $M \in GL_2(\mathbf{Z})$ d'ordre fini $m \in \mathbf{N}^*$. Le complexe z étant racine de $C_M(X)$ est valeur propre de la matrice M, donc racine de tout polynôme annulateur de M. La matrice M étant d'ordre m, le polynôme $X^m - 1$ est annulateur pour M, donc z est racine de ce polynôme.

   (b) Le nombre de polynômes cyclotomiques de degré 1 est égal au nombre de solutions de l'équation $\varphi(k) = 1$ d'inconnue $k \in \mathbf{N}^*$. Soit p un nombre premier et r un entier strictement positif tel que $\varphi(p^r) \leqslant 1$. On obtient donc
   $$p^{r-1}(p-1) \leqslant 1.$$
   On en déduit que $p - 1 \leqslant 1$ donc p est égal à 2. Si $p = 2$ on a alors $r \leqslant 1$ (la fonction $r \to 2^{r-1}$ est strictement croissante sur $\mathbf{N}^*$). Donc une solution k n'admet comme facteur premier que le nombre 2 avec exposant inférieur ou égal à 1. L'équation n'admet donc que deux solutions, $k = 1$ ou $k = 2$. Il y a donc exactement deux polynômes cyclotomiques de degré 1, les polynômes $\Phi_1(X) = X - 1$ et $\Phi_2(X) = X + 1$.

   (c) Le nombre de polynômes cyclotomiques de degré 2 est égal au nombre de solutions de l'équation $\varphi(k) = 2$ d'inconnue $k \in \mathbf{N}^*$. Soit p un nombre premier et r un entier strictement positif tel que $\varphi(p^r) \leqslant 2$. On obtient donc
   $$p^{r-1}(p-1) \leqslant 2.$$
   Par conséquent, $p - 1 \leqslant 2$. Si $p = 2$ on a $r = 1$ ou $r = 2$, et si $p = 3$ alors $r = 1$. Donc le nombre k n'admet dans sa décomposition en facteurs irréductibles que les nombres premiers 2 avec exposant possible inférieur à 2 et 3 avec exposant possible inférieur à 1. On obtient alors aisément $\varphi(k) = 2$ si et seulement si $k = 3, 4$ ou 6. Par conséquent les polynômes cyclotomiques de degré 2 sont $\Phi_3(X) = (X - j)(X - j^2) = X^2 + X + 1$, $\Phi_4(X) = (X - i)(X + i) = X^2 + 1$ et
   $\Phi_6(X) = (X + j)(X + j^2) = X^2 - X + 1$.

   (d) Soit P un facteur irréductible dans $\mathbf{Q}[X]$ de $C_M(X)$. D'après la question (a), toute racine complexe z de P est racine de $C_M(X)$, donc de $X^m - 1$: c'est donc une racine m-ième de l'unité. Comme P est scindé sur $\mathbf{C}$, il divise donc $X^m - 1$ dans $\mathbf{C}[X]$, mais aussi dans $\mathbf{Q}[X]$. Par unicité de la décomposition du polynôme $X^m - 1$ en produit de polynômes irréductibles dans $\mathbf{Q}[X]$, et connaissant la décomposition $X^m - 1 = \prod_{d|m} \Phi_d(X)$, P est nécessairement un polynôme cyclotomique.

$C_M(X)$ étant unitaire, c'est donc un produit de polynômes cyclotomiques. Comme il est de degré 2, on déduit, d'après les questions (b) et (c), que :

- ou bien c'est un polynôme cyclotomique de degré 2, c'est-à -dire : Φ_3, Φ_4 ou Φ_6 ;
- ou bien c'est le produit de deux polynômes cyclotomiques de degré 1, c'est-à-dire : $\Phi_1^2, \Phi_1\Phi_2$ ou Φ_2^2.

Ainsi, $C_M(X)$ est l'un des six polynômes unitaires suivant : X^2+X+1, X^2+1, X^2-X+1, $(X-1)^2$, $(X-1)(X+1)$ ou $(X+1)^2$.

(e) La matrice M est d'ordre m, donc admet le polynôme X^m-1 comme polynôme annulateur. Ce polynôme étant scindé à racines simples dans $\mathbf{C}$, la matrice M est diagonalisable dans $\mathbf{C}$. Son ordre est donc le PPCM des ordres de ses valeurs propres (vues comme éléments du goupe $(\mathbf{C}^*, *)$). Si $C_M(X) = \Phi_4(X)$, les valeurs propres de M sont i et $-i$ donc $m = 4$. Dans tous les autres cas, les valeurs propres sont des racines sixièmes de l'unité, donc m est un diviseur de 6, d'où le résultat.

(f) $M = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ appartient à $GL_2(\mathbf{Z})$ car $\det(M) = 1$.

De plus, $C_M(X) = X^2 - X + 1$ (c'est une matrice compagnon), donc M est diagonalisable dans $\mathbf{C}$ avec deux valeurs propres qui sont des racines primitives sixième de l'unité, donc M est d'ordre 6.

3. (a)
- $M^m = I_n$ donc, par application de la formule du binôme de Newton (valide ici puisque N permute avec I_n), il vient :

$$I_n = \sum_{k=0}^{m} \begin{pmatrix} m \\ k \end{pmatrix} p^{rk} N^k = I_n + mp^r N + p^{2r} \sum_{k=2}^{m} \begin{pmatrix} m \\ k \end{pmatrix} p^{(k-2)r} N^k.$$

Ainsi : $mp^r N = p^{2r} A$, avec $A = -\sum_{k=2}^{m} \begin{pmatrix} m \\ k \end{pmatrix} p^{(k-2)r} N^k \in M_n(\mathbf{Z})$; d'où $mp^r N \in p^{2r} M_n(\mathbf{Z})$.

- Par conséquent mN appartient à $p^r M_n(\mathbf{Z})$ et, comme $r \in \mathbf{N}^*$, p divise chaque coefficient de la matrice mN. Or, comme N appartient à $M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$, il existe un coefficient $n_{i,j}$ de N que p ne divise pas. Comme p est premier et qu'il divise $mn_{i,j}$, il divise m ou $n_{i,j}$: donc nécessairement p divise m.

(b) Par une nouvelle application de la formule du binôme,

$$\begin{aligned} M' = M^p = (I_n + p^r N)^p &= I_n + p^r \sum_{k=1}^{p} \begin{pmatrix} p \\ k \end{pmatrix} p^{r(k-1)} N^k \\ &= I_n + p^r (pN + p^r \sum_{k=2}^{p} \begin{pmatrix} p \\ k \end{pmatrix} p^{r(k-2)} N^k) \\ &= I_n + p^{r+1} N', \end{aligned}$$

en posant $N' = N + p^{r-1} \sum_{k=2}^{p} \begin{pmatrix} p \\ k \end{pmatrix} p^{r(k-2)} N^k$.

On a $N \in M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$. Montrons que $p^{r-1} \sum_{k=2}^{p} \begin{pmatrix} p \\ k \end{pmatrix} p^{r(k-2)} N^k \in pM_n(\mathbf{Z})$. En effet,

- Si $k = p$, l'entier $\begin{pmatrix} p \\ k \end{pmatrix} p^{r(k-2)}$ devient $p^{r(p-2)}$ divisible par p car $p \geqslant 3$ (**c'est ici que l'on utilise l'hypothèse** $p \neq 2$).
- Si $k \in \{2, \ldots, p-1\}$ le coefficient binômial $\begin{pmatrix} p \\ k \end{pmatrix}$ est divisible par le nombre premier p.

Dans tous les cas les entiers $\begin{pmatrix} p \\ k \end{pmatrix} p^{r(k-2)}$ qui apparaissent dans la définition de N' sont divisibles par p, donc $p^{r-1} \sum_{k=2}^{p} \begin{pmatrix} p \\ k \end{pmatrix} p^{r(k-2)} N^k \in pM_n(\mathbf{Z})$ et l'on déduit $N' \in M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$.

Ainsi $M' = I_n + p^{r+1} N'$, avec $r+1 \in \mathbf{N}^*$ et $N' \in M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$, M' est d'ordre m' (puisque $M' = M^p$ et que M est d'ordre pm') et $m' \geqslant 2$ car $N' \neq 0$; donc, par le même raisonnement qu'à la question (a), on obtient que p divise m'.

(c) Si les hypothèses faites au début de la question 3 étaient valides, en réitérant le processus précédent k fois, on obtiendrait que m s'écrive sous la forme $m = p^k m_k$, avec $m_k \in \mathbf{N}^*$ ($m_k \neq 0$ car $m \neq 0$), d'où $m \geqslant p^k \geqslant 3^k$ pour tout $k \in \mathbf{N}$. Ceci est bien sûr impossible puisque la suite (3^k) diverge vers $+\infty$.
Par conséquent, aucune matrice $M \in GL_n(\mathbf{Z})$ d'ordre $m \geqslant 2$ ne peut s'écrire sous la forme énoncée au début de la question 3 pour aucun nombre premier $p \geqslant 3$. Autrement dit, toute matrice $M \in GL_n(\mathbf{Z})$ d'ordre $m \geqslant 2$ est de la forme $M = I_n + N$, où le PGCD des coefficients de $N \in M_n(\mathbf{Z})$ est une puissance de 2.

4. Notons ω le morphisme de groupes de $GL_n(\mathbf{Z})$ dans $GL_n(\mathbf{F}_p)$ introduit par l'énoncé. Etant induit par la surjection naturelle de $\mathbf{Z}$ sur $\mathbf{F}_p$, ω est surjectif.
Soit G un sous-groupe fini de $GL_n(\mathbf{Z})$ d'ordre $m \geqslant 2$ (on écarte le cas trivial où $G = \{I_n\}$).
$\omega(G)$ est un sous-groupe fini de $GL_n(\mathbf{F}_p)$ et la restriction $\omega_{|G}$ de ω à G induit un morphisme surjectif de G sur $\omega(G)$.
Montrons que $\omega_{|G}$ est injective, c'est-à-dire que $\mathrm{Ker}(\omega_{|G}) = \{I_n\}$.
Soit $M \in G \cap \mathrm{Ker}(\omega)$. Alors $\omega(M) = I_n$, d'où $M = I_n + pN_1$ avec $N_1 \in M_n(\mathbf{Z})$. En factorisant au maximum par p l'ensemble des coefficients de la matrice N_1, M s'écrit alors sous la forme $M = I_n + p^r N$ avec $r \in \mathbf{N}^*$ et $N \in M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$. D'après la question 3, M ne peut donc pas être d'ordre $m \geqslant 2$. Or M est bien d'ordre fini, puisqu'elle appartient à un groupe G fini : donc M est d'ordre 1, c'est-à-dire que $M = I_n$. Ainsi $\mathrm{Ker}(\omega_{|G}) = G \cap \mathrm{Ker}(\omega) = \{I_n\}$: $\omega_{|G}$ est injective.
$\omega_{|G}$ est donc un isomorphisme de G sur $\omega(G)$: G est donc bien isomorphe à un sous-groupe de $GL_n(\mathbf{F}_p)$.

5. (a) Soit G un sous-groupe fini de $GL_2(\mathbf{Z})$. D'après la question 4, G est isomorphe à un sous-groupe de $GL_2(\mathbf{F}_3)$. Or le cardinal de $GL_2(\mathbf{F}_3)$ est $(3^2-1) \times (3^2-3) = 8 \times 6 = 48$ (ce résultat s'obtient en comptant les bases de $\mathbf{F}_3^2$).
Donc, d'après le théorème de Lagrange, le cardinal de G divise 48.

(b) Si le cardinal de G est égal à 48, alors G est isomorphe à $GL_2(\mathbf{F}_3)$. Or on sait que G ne contient pas d'élément d'ordre 8 ; en exhibant un élément d'ordre 8 dans $GL_2(\mathbf{F}_3)$, on montre ainsi qu'il n'est pas possible que G soit de cardinal 48.
Deux méthodes sont possibles pour exhiber un tel élément :
- soit directement, par tâtonnement sur les éléments de $GL_2(\mathbf{F}_3)$: on vérifie facilement que la matrice $\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$, par exemple, est un élément de $GL_2(\mathbf{F}_3)$ d'ordre 8 ;
- soit en considérant le polynôme cyclotomique

$$\Phi_8(X) = (X - e^{i\pi/4})(X - e^{-i\pi/4})(X - e^{3i\pi/4})(X - e^{-3i\pi/4}) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) = X^4 + 1$$

qui apparaît dans la décomposition de $X^8 - 1$: dans $\mathbf{F}_3[X]$, $X^4 + 1 = (X^2 + X + 2)(X^2 + 2X + 2)$ et la matrice compagnon associée au polynôme $X^2 + X + 2$ est la matrice $M = \begin{pmatrix} 0 & -2 \\ 1 & -1 \end{pmatrix}$, elle appartient à $GL_2(\mathbf{F}_3)$ car son déterminant est non nul. Elle est annulée par le polynôme $X^2 + X + 2$, donc par le polynôme $X^4 + 1$. Donc $M^4 = -I_2$ et $M^8 = I_2$, ce qui montre que la matrice M est d'ordre 8.

II. - Réseaux

1. • Supposons que $e' = (e'_1, \ldots, e'_n)$ soit une $\mathbf{Z}$-base de $\mathscr{R}$.
Alors $\mathscr{R} = \{\sum_{i=1}^{n} a'_i e'_i \ / \ \forall\, i \in \{1, \ldots, n\}, a'_i \in \mathbf{Z}\}$.
Or, pour tout $j \in [[1, n]]$, $e_j \in \mathscr{R}$, donc il existe $(p'_{1,j}, \ldots, p'_{n,j}) \in \mathbf{Z}^n$ tel que $e_j = \sum_{i=1}^{n} p'_{i,j} e'_i$. Par conséquent, e étant une famille génératrice de E, e' l'est aussi.

Comme e' est de cardinal égal à $n = \dim(E)$, e' est donc une base de E.
De plus, la matrice de passage de e' à e est la matrice des $p'_{i,j}$: elle appartient à $M_n(\mathbf{Z})$ et est inversible. Par un raisonnement symétrique son inverse appartient à $M_n(\mathbf{Z})$. Cette matrice de passage est donc dans $GL_n(\mathbf{Z})$.
Une implication est ainsi établie.

- Réciproquement, supposons que e' soit une base de E et que la matrice de passage de e à e' appartienne à $GL_n(\mathbf{Z})$. Notons $P = (p_{i,j})$ cette matrice et $P^{-1} = (p'_{i,j})$ sa matrice inverse.

  Pour tout $j \in [[1,n]]$, $e'_j = \sum_{i=1}^{n} p_{i,j} e_i$, donc $e'_j \in \mathscr{R}$.

  De plus :

  – $\forall\, (a'_1,\dots,a'_n) \in \mathbf{Z}^n$, $\sum_{j=1}^{n} a'_j e'_j = \sum_{j=1}^{n} a'_j \left(\sum_{i=1}^{n} p_{i,j} e_i\right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a'_{i,j} p_{i,j}\right) e_i$.

  Or $\forall\, i \in [[1,n]]$, $\sum_{j=1}^{n} a'_{i,j} p_{i,j} \in \mathbf{Z}$, donc $\sum_{j=1}^{n} a'_j e'_j \in \mathscr{R}$.

  Ainsi : $\{\sum_{j=1}^{n} a'_j e'_j \;/\; \forall\, j \in \{1,\dots,n\}, a'_j \in \mathbf{Z}\} \subset \mathscr{R}$.

  – Réciproquement, soit $x \in \mathscr{R}$. Il existe alors $(a_1,\dots,a_n) \in \mathbf{Z}^n$ tel que
  $x = \sum_{j=1}^{n} a_j e_j = \sum_{j=1}^{n} a_j \left(\sum_{i=1}^{n} p'_{i,j} e'_i\right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_j p'_{i,j}\right) e'_i$, avec $\sum_{j=1}^{n} a_j p'_{i,j} \in \mathbf{Z}$ pour tout $i \in [[1,n]]$, donc
  $\mathscr{R} \subset \{\sum_{i=1}^{n} a'_i e'_i \;/\; \forall\, i \in \{1,\dots,n\}, a'_i \in \mathbf{Z}\}$.

  Donc $\mathscr{R} = \{\sum_{i=1}^{n} a'_i e'_i \;/\; \forall\, i \in \{1,\dots,n\}, a'_i \in \mathbf{Z}\}$, où e' est une base de E, si bien que e' est une $\mathbf{Z}$-base de $\mathscr{R}$.

2. Considérons deux $\mathbf{Z}$-bases $e = (e_1,\dots,e_n)$ et $e' = (e'_1,\dots,e'_n)$ de $\mathscr{R}$.
Notons M (resp. M') la matrice de $M_n(\mathbf{R})$ dont le coefficient d'indice (i,j) est égal au produit scalaire (e_i, e_j) (resp. (e'_i, e'_j)), et P la matrice de passage de e à e'.
Les matrices M et M' sont alors congruentes, et plus précisément : $M' = {}^tPMP$. En effet, il s'agit de la formule de changement de base pour une forme bilinéaire symétrique appliquée au produit scalaire avec les deux bases e et e'.
Par conséquent, $\det(M') = \det({}^tP)\det(M)\det(P) = \det(M)(\det(P))^2$.
Or $\det(P) = \pm 1$ donc $\det(M') = \det(M)$.
Ceci prouve le résultat demandé et justifie la définition du discriminant du réseau $\mathscr{R}$: $\Delta(\mathscr{R}) = \det(M)$, où M est la matrice dont le coefficient d'indice (i,j) est (e_i, e_j), pour n'importe quelle $\mathbf{Z}$-base $e = (e_1,\dots,e_n)$ de $\mathscr{R}$.

3. L'idée consiste à prouver qu'un réseau $\mathscr{R}$ de E n'est pas dense dans E, la raison intuitive étant que $\mathbf{Z}$ n'est pas dense dans $\mathbf{R}$.
Considérons un réel r strictement positif, un vecteur a de E et une $\mathbf{Z}$-base $e = (e_1,\dots,e_n)$ de $\mathscr{R}$. Raisonnons par l'absurde : supposons que l'ensemble $B(a,r) \cap \mathscr{R}$ soit de cardinal infini. Il contient donc un sous-ensemble infini dénombrable et on peut alors construire une suite (x_p) de vecteurs deux à deux distincts de $B(a,r) \cap \mathscr{R}$. Cette suite étant bornée dans un espace vectoriel isomorphe à $\mathbf{R}^n$, elle admet, d'après le théorème de Bolzano-Weierstrass, une suite extraite (y_p) convergente. Or, pour tout $n \in \mathbf{N}$, $y_p \neq y_{p+1}$ donc, comme les systèmes de coordonnées de y_p et y_{p+1} dans la base e sont deux n-uplets distincts d'entiers, on a nécessairement $||y_p - y_{p+1}||_\infty \geqslant 1$ (où $||\ ||_\infty$ désigne la norme infinie). Comme la norme euclidienne majore la norme infinie (ou comme toutes les normes sont équivalentes en dimension finie), l'inégalité ci-dessus obtenue pour tout $p \in \mathbf{N}$ contredit la convergence de la suite (y_p).
Par conséquent, la supposition est fausse : $B(a,r) \cap \mathscr{R}$ est bien de cardinal fini.

4. L'ensemble $\{||x|| \;/\; x \in \mathscr{R}\backslash\{0\}\}$ est bien une partie de $\mathbf{R}$ non vide et minorée par 0, donc la quantité

$m(\mathscr{R})$ est bien définie, du fait que $\mathbf{R}$ vérifie l'axiome de la borne inférieure.
De plus, soit e un vecteur quelconque non nul de $\mathscr{R}$. D'après la question précédente, l'ensemble $A = B(0,||e||) \cap \mathscr{R}$ est non vide et de cardinal fini, on peut donc considérer un vecteur v de plus petite norme de cet ensemble : v est donc un vecteur non nul de $\mathscr{R}$ et

$$||v|| = \text{Inf}\{||x|| \ / \ x \in A\} = \text{Inf}\{||x|| \ / \ x \in \mathscr{R}\backslash\{0\}\} = m(\mathscr{R})$$

Ainsi $m(\mathscr{R}) = ||v||$ pour un vecteur $v \in \mathscr{R}\backslash\{0\}$; cette borne inférieure est atteinte : c'est un plus petit élément.

5. (a) L'image par π_k de la base $(v_1,\dots,v_k,e_{k+1},\dots,e_n)$ de E est une famille génératrice de $\pi_k(E)$. Or, comme π_k est surjective de E sur $W_k^\perp$, $\pi_k(E) = W_k^\perp$; et, comme $\pi_k(v_1) = \dots \pi_k(v_k) = 0$, $(\pi_k(e_{k+1}),\dots,\pi_k(e_n))$ est une famille génératrice de $W_k^\perp$. Étant de cardinal $n-k = \dim(W_k^\perp)$, c'est donc une base de $W_k^\perp$. De plus,

$$\begin{aligned}
\pi_k(\mathscr{R}) &= \left\{ \pi_k\left(\sum_{i=1}^{k} a_i v_i + \sum_{i=k+1}^{n} a_i e_i\right) \ / \ \forall\, i \in \{1,\dots,n\}, a_i \in \mathbf{Z} \right\} \\
&= \left\{ \sum_{i=1}^{k} a_i \pi_k(v_i) + \sum_{i=k+1}^{n} a_i \pi_k(e_i) \ / \ \forall\, i \in \{1,\dots,n\}, a_i \in \mathbf{Z} \right\} \\
&= \left\{ \sum_{i=k+1}^{n} a_i \pi_k(e_i) \ / \ \forall\, i \in \{k+1,\dots,n\}, a_i \in \mathbf{Z} \right\}.
\end{aligned}$$

On a ainsi prouvé que $\pi_k(\mathscr{R})$ est un réseau de $W_k^\perp$ de $\mathbf{Z}$-base $(\pi_k(e_{k+1}),\dots,\pi_k(e_n))$.

(b) Comme $e_{k+1} \notin W_k$, $||\pi_k(e_{k+1})|| > 0$.
Comme à la question 4, l'ensemble $A = B(0,||\pi_k(e_{k+1})||) \cap \pi_k(\mathscr{R})\backslash\{0\}$ est un ensemble non vide (car il contient $\pi_k(e_{k+1})$) de cardinal fini ; on peut donc considérer un vecteur u de plus petite norme de A. Alors $||u|| > 0$ et comme $u \in \pi_k(\mathscr{R})$, il existe $v_{k+1} \in \mathscr{R}$ tel que $u = \pi_k(v_{k+1})$.
Alors $||\pi_k(v_{k+1})|| = \inf\{||u|| \ / \ u \in A\} = \inf\{||u|| \ / \ u \in \pi_k(\mathscr{R})\backslash\{0\}\} = m(\pi_k(\mathscr{R}))$.

(c) • D'après ce qui précède, il existe $(n-k)$ entiers $a_{k+1},\dots,a_n$ tels que $\pi_k(v_{k+1}) = a_{k+1}\pi_k(e_{k+1}) + \dots + a_n\pi_k(e_n)$. Notons d le PGCD de $a_{k+1},\dots,a_n$. Il existe alors $(a'_{k+1},\dots,a'_n) \in \mathbf{Z}^{n-k}$ tel que $a_i = d a'_i$ pour tout $i \in [[k+1,n]]$ et $a'_{k+1},\dots,a'_n$ sont premiers entre eux dans leur ensemble. Posons $v'_{k+1} = \dfrac{1}{d} v_{k+1}$. Alors $\pi_k(v'_{k+1}) \in \pi_k(\mathscr{R})\backslash\{0\}$. Si $d > 1$, alors $||\pi_k(v'_{k+1})|| = \dfrac{1}{d}||\pi_k(v_{k+1})|| < ||\pi_k(v_{k+1})||$, ce qui contredit le fait que $||\pi_k(v_{k+1})|| = m(\pi_k(\mathscr{R}))$. Donc $d = 1$, ce qui prouve que $\pi_k(v_{k+1})$ est un vecteur primitif du réseau $\pi_k(\mathscr{R})$.

• D'après le résultat admis par l'énoncé, il existe une famille $(f'_{k+2},\dots,f'_n)$ de vecteurs de E telle que $(\pi_k(v_{k+1}), f'_{k+2},\dots,f'_n)$ soit une $\mathbf{Z}$-base de $\pi_k(\mathscr{R})$. Il existe alors une famille $(f_{k+2},\dots,f_n)$ de vecteurs de $\mathscr{R}$ vérifiant pour tout $i \in \{k+2,\dots,n\}$, $\pi_k(f_i) = f'_i$. Nous allons montrer que $(v_1,\dots,v_k,v_{k+1},f_{k+2},\dots,f_n)$ est une base de E. La famille étant de cardinal n, il suffit de montrer qu'elle est libre. Supposons que l'on ait une relation de la forme

$$\sum_{i=1}^{k+1} a_i v_i + \sum_{i=k+2}^{n} a_i f_i = 0.$$

En appliquant π_k nous obtenons

$$a_{k+1}\pi_k(v_{k+1}) + \sum_{i=k+2}^{n} a_i f'_i = 0.$$

La famille $(\pi_k(v_{k+1}), f'_{k+2},\dots,f'_n)$ étant une $\mathbf{Z}$-base de $\mathscr{R}$ est une famille libre, donc les a_i sont nuls pour $i \in \{k+1,\dots,n\}$. On conclut alors à la nullité des autres a_i en remarquant que la famille $(v_1,\dots,v_k)$ est libre. Donc la famille $(v_1,\dots,v_k,v_{k+1},f_{k+2},\dots,f_n)$ est une base de E.

- Nous allons montrer que cette famille est une $\mathbf{Z}$-base de $\mathscr{R}$. Tous les éléments de cette famille étant des éléments de $\mathscr{R}$, nous avons l'inclusion

$$\{\sum_{i=1}^{k+1} a_i v_i + \sum_{i=k+2}^{n} a_i f_i \ / \ \forall i \in \{1,\dots,n\} \ \ a_i \in \mathbf{Z}\} \subset \mathscr{R}.$$

Soit alors $x \in \mathscr{R}$. Par construction il existe une famille $(a_{k+1},\dots,a_n)$ d'entiers tels que $\pi_k(x) = a_{k+1}\pi_k(v_{k+1}) + \sum_{i=k+2}^{n} a_i f_i'$. Donc le vecteur $y = x - a_{k+1}v_{k+1} - \sum_{i=k+2}^{n} a_i f_i$ appartient au noyau de π_k et à $\mathscr{R}$. Il existe donc une famille d'entiers $(b_1,\dots,b_n)$ telle que $y = \sum_{i=1}^{k} b_i v_i + \sum_{i=k+1}^{n} b_i e_i$. La famille $(v_1,\dots,v_k)$ forme une base du noyau de π_k et la famille $(e_{k+1},\dots,e_n)$ forme une base d'un supplémentaire de ce noyau. Le vecteur y appartenant au noyau de π_k, nous obtenons $y = \sum_{i=1}^{k} b_i v_i$. D'où

$$x = \sum_{i=1}^{k} b_i v_i + a_{k+1} v_{k+1} + \sum_{i=k+2}^{n} a_i f_i.$$

Nous avons donc montré l'inclusion

$$\mathscr{R} \subset \{\sum_{i=1}^{k+1} a_i v_i + \sum_{i=k+2}^{n} a_i f_i \ / \ \forall i \in \{1,\dots,n\} \ \ a_i \in \mathbf{Z}\}.$$

Il résulte de tout cela que $(v_1,\dots,v_{k+1},f_{k+2},\dots,f_n)$ est une $\mathbf{Z}$-base de $\mathscr{R}$.

(d) Ce résultat s'obtient par récurrence limitée sur $l \in [[1,n]]$ dans laquelle il suffit d'utiliser correctement les résultats des questions (a), (b) et (c). Considérons l'hypothèse de récurrence suivante $\mathscr{H}_l$: « il existe une $\mathbf{Z}$-base $(v_1,\dots,v_l,e_{l+1},\dots,e_n)$ de $\mathscr{R}$ vérifiant $||v_1|| = m(\mathscr{R})$ et $\forall\, k \in [[1,l-1]]$, $||\pi_k(v_{k+1})|| = m(\pi_k(\mathscr{R}))$, où π_k est la projection orthogonale sur $< v_1,\dots,v_k >^{\perp}$. »

- Pour $l = 1$, d'après la question 4, il existe un vecteur $v_1 \in \mathscr{R}\backslash\{0\}$ tel que $||v_1|| = m(\mathscr{R})$. v_1 est nécessairement un vecteur primitif de $\mathscr{R}$ (par une argumentation analogue à celle faite à la question (c)), donc il existe une $\mathbf{Z}$-base de $\mathscr{R}$ de la forme $(v_1,e_2,\dots,e_n)$ et $\mathscr{H}_1$ est vérifiée.
- Supposons avoir établi $\mathscr{H}_l$ pour une valeur $l \leqslant n-1$: il existe alors une $\mathbf{Z}$-base $(v_1,\dots,v_l,e_{l+1},\dots,e_n)$ de $\mathscr{R}$ vérifiant $||v_1|| = m(\mathscr{R})$ et $\forall\, k \in [[1,l-1]]$, $||\pi_k(v_{k+1})|| = m(\pi_k(\mathscr{R}))$. Cette base vérifie donc les hypothèses du début de la question 4 : on en déduit donc successivement que :
  - $\pi_l(\mathscr{R})$ est un réseau de $< v_1,\dots,v_l >^{\perp}$ (question (a)) ;
  - il existe un vecteur v_{l+1} de $\mathscr{R}$ vérifiant $||\pi_l(v_{l+1})|| = m(\pi_l(\mathscr{R}))$ (question (b)) ;
  - il existe une $\mathbf{Z}$-base de $\mathscr{R}$ de la forme $(v_1,\dots,v_l,v_{l+1},f_{l+2},\dots,f_n)$ (question (c)).

  Ceci prouve bien que $\mathscr{H}_{l+1}$ est aussi vérifiée.

D'après le principe de récurrence, $\mathscr{H}_l$ est donc vraie pour tout entier $l \in [[1,n]]$; donc $\mathscr{H}_n$ est vérifiée, ce qui répond à la question.

(e) Le réseau $\mathscr{R}_1$ considéré ici est le réseau plan constitué par un maillage de triangles équilatéraux de côté égal à 1. Posons $e_1 = (1,0)$ et $e_2 = (-1/2,\sqrt{3}/2)$. Il est manifeste que $m(\mathscr{R}_1) = 1 = ||e_1||$. Avec les notations de l'énoncé, π_1 est donc la projection orthogonale sur $< e_1' >$, avec $e_1' = (0,1)$. D'après la question (a), $\pi_1(\mathscr{R}_1)$ est un réseau de $< e_1' >$ de $\mathbf{Z}$-base $(\pi_1(e_2))$. Il est alors manifeste également que $||\pi_1(e_2)|| = m(\pi_1(\mathscr{R}_1))$ (un calcul très simple aboutit d'ailleurs à $||\pi_1(e_2)|| = ||(e_2,e_1')e_1'|| = \sqrt{3}/2||e_1'|| = \sqrt{3}/2$). Ainsi, e est une base réduite de $\mathscr{R}_1$.

6. (a) Soit $(j,k) \in [[2,n]]^2$.
$\pi_1(e_j) = e_j - \lambda e_1$ où λ est un réel tel que $(e_1,\pi_1(e_j)) = 0$. Or $(e_1,\pi_1(e_j)) = (e_1,e_j) - \lambda||e_1||^2$, avec $||e_1|| = m(\mathscr{R})$; donc $\lambda = \dfrac{(e_1,e_j)}{m(\mathscr{R})^2}$ et $\pi_1(e_j) = e_j - \dfrac{(e_1,e_j)}{m(\mathscr{R})^2}e_1$.
De même, $\pi_1(e_k) = e_k - \dfrac{(e_1,e_k)}{m(\mathscr{R})^2}e_1$. Ainsi :

$$\begin{aligned}(\pi_1(e_j),\pi_1(e_k)) &= (e_j - \frac{(e_1,e_j)}{m(\mathscr{R})^2}e_1, e_k - \frac{(e_1,e_k)}{m(\mathscr{R})^2}e_1)\\ &= (e_j,e_k) - 2\frac{(e_1,e_j)(e_1,e_k)}{m(\mathscr{R})^2} + \frac{(e_1,e_j)(e_1,e_k)}{m(\mathscr{R})^4}||e_1||^2\\ &= (e_j,e_k) - \frac{1}{m(\mathscr{R})^2}(e_1,e_j)(e_1,e_k).\end{aligned}$$

(b) Notons $A = (a_{i,j})$ la matrice de $M_n(\mathbf{R})$ dont le coefficient d'indice (i,j) (pour $1 \leqslant i,j \leqslant n$) est égal à $a_{i,j} = (e_i, e_j)$ et A_1 la matrice de $M_{n-1}(\mathbf{R})$ dont le coefficient d'indice (i,j) (pour $2 \leqslant i,j \leqslant n$) est égal à $(\pi_1(e_i), \pi_1(e_j))$.

Pour $j \in [[2,n]]$, effectuons successivement les transvections $L_j \leftarrow L_j - \dfrac{a_{j,1}}{a_{1,1}} L_1$ à partir des lignes de la matrice A. La matrice A' ainsi obtenue se déduit donc de A par multiplications à gauche par $(n-1)$ matrices de tranvection. Or, comme une matrice de tranvection est de déterminant égal à 1, il vient : $\det(A) = \det(A')$.

De plus, les lignes L'_j de A' pour $j \in [[2,n]]$ ont pour coefficients 0 en première colonne et, en colonne $k \in [[2,n]]$:

$$a_{j,k} - \frac{a_{j,1}}{a_{1,1}} a_{1,k} = (e_j, e_k) - \frac{(e_j,e_1)}{(e_1,e_1)}(e_1,e_k) = (e_j,e_k) - \frac{1}{m(\mathscr{R})^2}(e_1,e_j)(e_1,e_k) = (\pi_1(e_j), \pi_1(e_k)).$$

A' a donc pour première ligne la première ligne L_1 de A et le reste de A' est constitué d'une colonne de zéros juxtaposée à la matrice A_1. Par un calcul de déterminant par blocs on a $\det(A') = (e_1,e_1)\det(A_1)$ (car (e_1,e_1) est le coefficient en première ligne et première colonne de A'). Or, d'après la question 4, $(e_1,e_1) = m(\mathscr{R})^2$ et, d'après la question 2, $\det(A) = \Delta(\mathscr{R})$ et $\det(A_1) = \Delta(\pi_1(\mathscr{R}))$.

Ainsi : $\Delta(\mathscr{R}) = m(\mathscr{R})^2 \Delta(\pi_1(\mathscr{R}))$.

(c) D'après le théorème de Pythagore, puisque e_1 et v' sont orthogonaux, on a :
$||v||^2 = ||te_1 + v'||^2 = t^2||e_1||^2 + ||v'||^2 = t^2 m(\mathscr{R})^2 + ||v'||^2$.
Or $v \neq 0$ donc $m(\mathscr{R}) \leqslant ||v||$.
Ainsi : $m(\mathscr{R})^2 \leqslant t^2 m(\mathscr{R})^2 + ||v'||^2$.

(d) Nous allons montrer l'égalité de Hermite en raisonnant par récurrence sur n. Pour $n = 1$, l'inégalité est clairement vérifiée : si (e_1) est une $\mathbf{Z}$-base de $\mathscr{R}$, nous avons $m(\mathscr{R})^2 = (e_1,e_1) = \Delta(\mathscr{R})$. Cela donne le résultat.

Supposons donc $n \geqslant 2$ et l'inégalité vérifiée à l'ordre $n-1$. Choisissons $(e_1,\dots,e_n)$ une base réduite de $\mathscr{R}$. Il existe, par hypothèse de récurrence, un vecteur v' du réseau $\pi_1(\mathscr{R})$ vérifiant la relation (*)

$$||v'||^2 \leqslant (4/3)^{(n-2)/2} \Delta(\pi_1(\mathscr{R}))^{1/(n-1)}.$$

Soit alors $v \in \mathscr{R}$ tel que $\pi_1(v) = v'$. Il existe un réel t tel que $v = te_1 + v'$ et l'on peut choisir v de manière à ce que $|t| \leqslant 1/2$ (quitte à remplacer v par $v - ke_1$ où l'entier k est tel que $|t-k| \leqslant 1/2$). En appliquant la question 6-c nous obtenons

$$m(\mathscr{R})^2 \leqslant ||v'||^2/(1-t^2) \leqslant (4/3)||v'||^2.$$

Nous avons donc par (*)

$$m(\mathscr{R})^2 \leqslant (4/3)^{n/2} \Delta(\pi_1(\mathscr{R}))^{1/(n-1)}.$$

D'après la question 6-b $\Delta(\pi_1(\mathscr{R})) = \Delta(\mathscr{R})/m(\mathscr{R})^2$, ce qui permet de conclure à la véracité de l'inégalité à l'ordre n.

7. H_n est une partie de $\mathbf{R}^+$ non vide (car d'après l'inégalité de Hermite, $(4/3)^{(n-1)/2} \in H_n$), donc elle admet une borne inférieure η_n qui vérifie alors $m(\mathscr{R})^2 \leqslant \eta_n \Delta(\mathscr{R})^{1/n}$.

(a) Considérons le réseau $\mathbf{Z}^n$ de $\mathbf{R}^n$ euclidien usuel. La base canonique $e = (e_1,\dots,e_n)$ de $\mathbf{R}^n$ est orthonormale et c'est de manière immédiate une base réduite de $\mathbf{Z}^n$, avec $m(\mathscr{R})^2 = ||e_1||^2 = 1$ et $\Delta(\mathscr{R}) = \det(I_n) = 1$.

Ainsi $m(\mathscr{R})^2 = \Delta(\mathscr{R})^{1/n}$, et comme $m(\mathscr{R})^2 \leqslant \eta_n \Delta(\mathscr{R})^{1/n}$, on en déduit que $\eta_n \geqslant 1$.

(b)
- D'une part, l'inégalité de Hermite s'écrit, pour $n = 2$: $m(\mathscr{R})^2 \leqslant (2/\sqrt{3})\Delta(\mathscr{R})^{1/2}$; donc $2/\sqrt{3} \in H_2$, d'où $\eta_2 \leqslant 2/\sqrt{3}$.
- D'autre part, le réseau $\mathscr{R}_1$ étudié à la question 5.(e) vérifie : $m(\mathscr{R}_1)^2 = ||e_1||^2 = 1$ et $\Delta(\mathscr{R}_1) = \begin{vmatrix} 1 & -1/2 \\ -1/2 & 1 \end{vmatrix} = 3/4$; donc $m(\mathscr{R}_1)^2 = (2/\sqrt{3})\Delta(\mathscr{R}_1)^{1/2}$; or $m(\mathscr{R}_1)^2 \leqslant \eta_2 \Delta(\mathscr{R}_1)^{1/2}$; d'où $\eta_2 \geqslant 2/\sqrt{3}$.

Finalement : $\eta_2 = 2/\sqrt{3}$.
Ceci prouve que l'inégalité d'Hermite ne peut pas être améliorée pour tout $n \geqslant 2$ puisque la valeur $(4/3)^{(n-1)/2}$ est atteinte pour $n = 2$.

III. - Cristalloïdes

1. Soit g un élément de $O(\mathscr{R})$, où $\mathscr{R}$ est un réseau de E de $\mathbf{Z}$-base $e = (e_1, \ldots, e_n)$. L'application g est entièrement déterminée par la donnée des vecteurs $g(e_1), \ldots, g(e_n)$.
Soit $k \in [[1, n]]$. D'après la question II.3, $B(0, ||e_k||) \cap \mathscr{R}$ est de cardinal fini. Or $g(e_k)$ appartient à $B(0, ||e_k||) \cap \mathscr{R}$ (puisque $g(e_k) \in \mathscr{R}$ et $||g(e_k)|| = ||e_k||$). Il n'y a donc qu'un nombre fini α_k de vecteurs $g(e_k)$ possibles. D'où au total un nombre fini d'éléments $g \in O(\mathscr{R})$ possibles, inférieur à $\prod_{k=1}^{n} \alpha_k$. Par conséquent, $O(\mathscr{R})$ est de cardinal fini.

2. • Supposons que G est $\mathbf{Z}$-conjugué à $\psi_e(\Gamma)$. Alors il existe une matrice $M \in GL_n(\mathbf{Z})$ telle que $MGM^{-1} = \psi_e(\Gamma)$. Notons e' la base de E telle que M soit la matrice de passage de e à e'. D'après la question II.1, e' est une $\mathbf{Z}$-base de $\mathscr{R}$.
De plus, pour toute matrice $P \in M_n(\mathbf{R})$, on a :
$$\begin{aligned} P \in G \Leftrightarrow MPM^{-1} \in \psi_e(\Gamma) &\Leftrightarrow \exists\, g \in \Gamma,\ MPM^{-1} = \mathrm{Mat}(g, e) \\ &\Leftrightarrow \exists\, g \in \Gamma,\ P = M^{-1} \times \mathrm{Mat}(g, e) \times M = \mathrm{Mat}(g, e') \\ &\Leftrightarrow P \in \psi_{e'}(\Gamma) \end{aligned}$$
Donc $G = \psi_{e'}(\Gamma)$.
• Réciproquement, supposons qu'il existe une $\mathbf{Z}$-base e' de $\mathscr{R}$ telle que $G = \psi_{e'}(\Gamma)$. Notons M la matrice de passage de e à e'.
Pour toute matrice $P \in M_n(\mathbf{R})$, on a :
$$\begin{aligned} P \in MGM^{-1} \Leftrightarrow P \in M\psi_{e'}(\Gamma)M^{-1} &\Leftrightarrow \exists\, g \in \Gamma,\ P = M \times \mathrm{Mat}(g, e') \times M^{-1} = \mathrm{Mat}(g, e') \\ &\Leftrightarrow P \in \psi_e(\Gamma) \end{aligned}$$
Donc $MGM^{-1} = \psi_e(\Gamma)$: G et $\psi_e(\Gamma)$ sont $\mathbf{Z}$-conjugués.
L'équivalence à prouver est ainsi établie.

3. • Supposons que les deux cristalloïdes $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ sont équivalents. Alors il existe $u \in GL(E)$ tel que $u(\mathscr{R}) = \mathscr{R}'$ et $u\Gamma u^{-1} = \Gamma'$.
Comme e est une base de E et que u est un isomorphisme, $e'' = u(e)$ est une base de E. De plus :
$$\begin{aligned} \mathscr{R}' = u(\mathscr{R}) &= \left\{ u\left(\sum_{i=1}^{n} a_i e_i\right) \,/\, \forall\, i \in \{1, \ldots, n\}, a_i \in \mathbf{Z} \right\} \\ &= \left\{ \sum_{i=1}^{n} a_i e_i'' \,/\, \forall\, i \in \{1, \ldots, n\}, a_i \in \mathbf{Z} \right\} \end{aligned}$$
donc e'' est une $\mathbf{Z}$-base de $\mathscr{R}'$.
Posons $G = \psi_e(\Gamma)$, $G' = \psi_{e'}(\Gamma')$ et $G'' = \psi_{e''}(\Gamma')$. D'après la question 2, G' et G'' sont $\mathbf{Z}$-conjugués.
Notons $U = \mathrm{Mat}(u, e)$: U est aussi la matrice de passage de e à e''.
Pour tout $g' \in \Gamma'$, il existe $g \in \Gamma$ tel que $g' = ugu^{-1}$, si bien que :
$\mathrm{Mat}(g', e'') = \mathrm{Mat}(g', u(e)) = U^{-1} \times \mathrm{Mat}(g', e) \times U = U^{-1} \times \mathrm{Mat}(ugu^{-1}, e) \times U = U^{-1}U \times \mathrm{Mat}(g, e) \times U^{-1}U = \mathrm{Mat}(g, e)$.
Ainsi, pour toute matrice $P \in M_n(\mathbf{R})$, on a :
$P \in G'' \Leftrightarrow \exists\, g' \in \Gamma',\ P = \mathrm{Mat}(g', e'') \Leftrightarrow \exists\, g \in \Gamma,\ P = \mathrm{Mat}(g, e) \Leftrightarrow P \in G$.
Donc $G'' = G$. Par conséquent, $G = \psi_e(\Gamma)$ et $G' = \psi_{e'}(\Gamma')$ sont $\mathbf{Z}$-conjugués.
• Réciproquement, supposons que $G = \psi_e(\Gamma)$ et $G' = \psi_{e'}(\Gamma')$ sont $\mathbf{Z}$-conjugués. Alors il existe $M \in GL_n(\mathbf{Z})$ vérifiant $MGM^{-1} = G'$.
Notons $v \in GL(E)$ tel que $\mathrm{Mat}(v, e) = M^{-1}$ et $e'' = v(e)$. e'' est une base de E et $M \in GL_n(\mathbf{Z})$ est la matrice de passage de e à e'' donc e'' est une $\mathbf{Z}$-base de $\mathscr{R}$, d'après la question II.1.
Notons aussi $M' \in GL_n(\mathbf{R})$ la matrice de passage de e à e'' et $u \in GL(E)$ l'automorphisme tel que $\mathrm{Mat}(u, e'') = M'$, si bien que $e' = u(e'')$.

– D'une part : comme $e'' = v(e)$ est une base de E et que la matrice M^{-1} de passage de e à e'' appartient à $GL_n(\mathbf{Z})$, e'' est une $\mathbf{Z}$-base de $\mathscr{R}$ (toujours d'après la question II.1). Ainsi, comme $e' = u(e'')$ et que e'' et e' sont des $\mathbf{Z}$-bases respectives des réseaux $\mathscr{R}$ et $\mathscr{R}'$, on a $u(\mathscr{R}) = \mathscr{R}'$ (1).

– D'autre part, pour tout $g \in \Gamma$, on a :
$\mathrm{Mat}(ugu^{-1}, e') = \mathrm{Mat}(ugu^{-1}, u(e'')) = M'^{-1} \times \mathrm{Mat}(ugu^{-1}, e'') \times M' = M'^{-1}M' \times \mathrm{Mat}(g, e'') \times M'^{-1}M' = \mathrm{Mat}(g, e'') = \mathrm{Mat}(g, v(e)) = M \times \mathrm{Mat}(g, e) \times M^{-1}$.
Or $\mathrm{Mat}(g, e) \in G$, donc $\mathrm{Mat}(ugu^{-1}, e') \in MGM^{-1} = G'$. Ainsi $ugu^{-1} \in \Gamma'$, ce qui prouve que $u\Gamma u^{-1} \subset \Gamma'$.
On montre de la même manière que $u^{-1}\Gamma' u \subset \Gamma$, d'où $\Gamma' \subset u\Gamma u^{-1}$.
Finalement : $u\Gamma u^{-1} = \Gamma'$ (2).

Les relations (1) et (2) obtenues ci-dessus établissent que les cristalloïdes $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ sont équivalents.

L'équivalence à prouver dans cette question est donc établie.

4. Montrons que ψ est injective et surjective.
   - Considérons deux cristalloïdes $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ de E, de $\mathbf{Z}$-bases respectives e et e'. Supposons que les classes d'équivalence de cristalloïdes de $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ aient la même image par ψ. Alors $\psi_e(\Gamma)$ et $\psi_{e'}(\Gamma')$ sont $\mathbf{Z}$-conjugués ; donc, d'après la question 3, $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ sont équivalents, c'est-à-dire que leurs classes d'équivalence sont égales : ceci prouve l'injectivité de ψ.
   - Considérons une classe d'équivalence de sous-groupe de $GL_n(\mathbf{Z})$ de représentant G'. Considérons $\mathbf{R}^n$ muni de sa base canonique $e = (e_1, \ldots, e_n)$ et le réseau $\mathscr{R}$ de $\mathbf{Z}$-base e. Le groupe G' s'identifie par choix de la base e à un sous-groupe fini G de $GL(\mathbf{R}^n)$. Les matrices des éléments de G dans la base e étant des éléments de $GL_n(\mathbf{Z})$, les éléments de G stabilisent $\mathscr{R}$. Nous allons construire un produit scalaire sur $\mathbf{R}^n$ qui fait de G un sous-groupe du groupe orthogonal. Notons $(.,.)$ le produit scalaire usuel de $\mathbf{R}^n$ et $|G|$ le cardinal de G. La forme bilinéaire $(.,.)_G$ définie pour tout couple $(u, v) \in (\mathbf{R}^n)^2$ par
   $$(u, v)_G = \frac{1}{|G|} \sum_{g \in G} (g(u), g(v))$$
   est clairement un produit scalaire sur $\mathbf{R}^n$. De plus, si $g' \in G$, on a
   $$\begin{aligned}(g'(u), g'(v))_G &= \frac{1}{|G|} \sum_{g \in G} (g(g'(u)), g(g'(v))) \\ &= \frac{1}{|G|} \sum_{g'' \in G} (g''(u), g''(v)) \\ &= (u, v)_G\end{aligned}$$
   Donc, si l'on munit $\mathbf{R}^n$ du produit scalaire $(.,.)_G$, le groupe G est un sous-groupe du groupe orthogonal qui stabilise $\mathscr{R}$. Le couple $(\mathscr{R}, G)$ est donc un cristalloïde de l'espace euclidien $(\mathbf{R}^n, (.,.)_G)$. Les deux espaces euclidiens $(\mathbf{R}^n, (.,.)_G)$ et E étant de même dimension, il existe une isométrie $u : \mathbf{R}^n \longrightarrow E$. Le couple $(u(\mathscr{R}), uGu^{-1})$ est alors clairement un cristalloïde de E vérifiant $\psi_{u(e)}(uGu^{-1}) = G'$. Ceci montre la surjectivité de l'application ψ.

   L'application ψ est donc une bijection de l'ensemble des classes d'équivalence de cristalloïdes de E sur l'ensemble des classes de $\mathbf{Z}$-conjugaison de sous-groupes finis de $GL_n(\mathbf{Z})$.

5. Le groupe diédral D_6 est le groupe des isométries du plan euclidien conservant un hexagone régulier ; c'est un sous-groupe de $O(\mathscr{R}_1)$, où $\mathscr{R}_1$ est le réseau de $\mathbf{R}^2$ étudié à la question II.5.e qui contient l'hexagone régulier centré en l'origine 0 et de sommet le point de coordonnées $(0, 1)$. En effet, le groupe D_6 est engendré par deux éléments, la rotation d'angle $\pi/3$ et la symétrie de droite d'angle $\pi/6$. On vérifie que ces deux isométries sont dans $\mathscr{O}(\mathscr{R}_1)$ par exemple en vérifiant que les matrices de ces isométries dans la $\mathbf{Z}$-base e de la question II-5-e sont dans $GL_2(\mathbf{Z})$: on a respectivement $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$. On peut alors identifier D_6 à un sous-groupe de $\mathscr{O}(\mathscr{R}_1)$ (en fait on a égalité : une isométrie qui conserve

$\mathscr{R}_1$ permute les six vecteurs de norme 1 de $\mathscr{R}_1$, donc conserve l'hexagone). $(\mathscr{R}_1, D_6)$ est donc un cristalloïde de $\mathbf{R}^2$ et $\psi_e(D_6)$ est un sous-groupe de $GL_2(\mathbf{Z})$. Le groupe diédral D_6 est donc isomorphe à un sous-groupe de $GL_2(\mathbf{Z})$.

IV. - Groupes libres quadratiques

1. Considérons une $\mathbf{Z}$-base $e = (e_1, \ldots, e_n)$ de $\mathscr{R}$. Notons $b(e_i, e_j) = p_{i,j}/q_{i,j}$ avec $p_{i,j} \wedge q_{i,j} = 1$. Notons alors q le ppcm des $q_{i,j}$ (pour i et j variant dans l'ensemble $\{1, \ldots, n\}$). Pour tout couple $(x, y) \in \mathscr{R}^2$, on a $b(x, y) \in \frac{1}{q}\mathbf{Z}$. L'ensemble $\{b(x,x)^{1/2} \ / \ x \in \mathscr{R} \ , \ b(x,x) > 0\}$ est donc un sous-ensemble de $\frac{1}{\sqrt{q}}\mathbf{N}^*$. D'autre part c'est un ensemble non vide. En effet, puisque $p \geqslant 1$, il existe un vecteur a de E tel que $b(a,a) > 0$. Par continuité de la forme b, celle-ci est strictement positive sur une boule ouverte centrée en a de rayon $r > 0$. Par équivalence des normes en dimension fini, on peut choisir la norme infinie associée à la base e, et par homothétie, la forme b est strictement positive sur les boules centrée en λa et de rayon λr. Si l'on choisi le réel λ de manière à avoir $\lambda r > 1$, la boule considérée contient un élément du réseau $\mathscr{R}$. L'ensemble $\{b(x,x)^{1/2} \ / \ x \in \mathscr{R} \ , \ b(x,x) > 0\}$ est donc un sous-ensemble non vide de $\frac{1}{\sqrt{q}}\mathbf{N}^*$, il admet par conséquent un plus petit élément atteint en un vecteur v qui est non nul puisque $b(v,v) > 0$. D'où l'existence de v.
2. Puisque $b(v,v) > 0$ la restriction de b à la droite $< v >$ est non dégénérée. Nous avons donc une somme directe, orthogonale au sens de b, $E = W \oplus < v >$. Par additivité de la signature, la signature de b' est $(p-1, q)$.
3. Si $p = n$, l'inégalité de Hermite-Minkovski devient l'inégalité de Hermite, démontrée dans la partie II. Soit donc $n \geqslant 2$ et $1 \leqslant p < n$. Nous allons montrer l'inégalité par récurrence sur p. Pour simplifier les notations, nous notons $m = m_b(\mathscr{R})$, π la projection sur W parallèlement à $< v >$ et $\mathscr{R}' = \pi(\mathscr{R})$.
   - Supposons $p = 1$. La forme b' est définie négative, donc $-b'$ est définie positive. Notons $m' = m_{-b'}(\mathscr{R}')$. D'après IV-1 il existe $w' \in \mathscr{R}'$ tel que $-b'(w', w') = m'^2$ et $w \in \mathscr{R}$ tel que $\pi(w) = w'$. Par conséquent, $w = tv + w'$ et l'on peut choisir le réel t pour avoir $1/2 \leqslant |t| \leqslant 1$ (même technique qu'en II-6). On a alors $b(w,w) = t^2 m^2 + b(w', w') < m^2$ car $b(w', w') < 0$. Par minimalité de m^2 on en déduit $b(w,w) \leqslant 0$, donc
   $$t^2 m^2 \leqslant -b(w', w') = m'^2$$
   puis
   $$m^2/4 \leqslant m'^2.$$
   D'autre part, en appliquant l'inégalité de Hermite au réseau $\mathscr{R}'$ avec le produit scalaire $-b'$ nous obtenons l'inégalité
   $$m'^2 \leqslant (4/3)^{(n-2)/2} \Delta_{-b'}(\mathscr{R}')^{1/(n-1)}.$$
   Les deux inégalités précédentes combinées montrent alors que
   $$m^2 \leqslant 4(4/3)^{(n-2)/2} \Delta_{-b'}(\mathscr{R}')^{1/(n-1)}.$$
   Un raisonnement similaire à celui de la question II-6-b montre que
   $$|\Delta_b(\mathscr{R})| = m^2 |\Delta_{-b'}(\mathscr{R}')|.$$
   On en déduit
   $$m^2 \leqslant 4(4/3)^{(n-2)/2} m^{-2/(n-1)} |\Delta_b(\mathscr{R})|^{1/n-1}$$
   soit encore après simplification
   $$m^2 \leqslant 3^{(n-1)/n} (4/3)^{(n-1)/2} |\Delta_b(\mathscr{R})|^{1/n-1},$$
   ce qui est l'inégalité de Hermite-Minkovski dans le cas $p = 1$.

- Supposons maintenant $1 < p < n$ et l'inégalité vérifiée à l'ordre $p-1$. La forme b' est de signature $(p-1,q)$ avec $p-1 \geqslant 1$. Notons $m' = m_{b'}(\mathscr{R}')$. D'après IV-1 il existe $w' \in \mathscr{R}'$ tel que $b'(w',w') = m'^2$ et $w \in \mathscr{R}$ tel que $\pi(w) = w'$. Par conséquent, $w = tv + w'$ et l'on peut choisir le réel t pour avoir $|t| \leqslant 1/2$. On a
$$b(w,w) = t^2 m^2 + b(w',w') = t^2 m^2 + m'^2 > 0.$$
On en déduit par minimalité de m, $b(w,w) \geqslant m^2$, soit encore
$$m^2 \leqslant t^2 m^2 + m'^2 \leqslant m^2/4 + m'^2,$$
d'où l'on déduit $\frac{3}{4} m^2 \leqslant m'^2$. Par hypothèse de récurrence on a
$$m'^2 \leqslant 3^{\frac{n-p}{n-1}} (4/3)^{\frac{n-2}{2}} |\Delta_{b'}(\mathscr{R}')|^{1/(n-1)}.$$
On en déduit
$$m^2 \leqslant (4/3) 3^{\frac{n-p}{n-1}} (4/3)^{\frac{n-2}{2}} |\Delta_{b'}(\mathscr{R}')|^{1/(n-1)}.$$
Un raisonnement similaire à celui de la question II-6-b montre encore que
$$|\Delta_b(\mathscr{R})| = m^2 |\Delta_{-b'}(\mathscr{R}')|.$$
On en déduit
$$m^2 \leqslant (4/3) 3^{\frac{n-p}{n-1}} (4/3)^{\frac{n-2}{2}} m^{\frac{-2}{n-1}} |\Delta_b(\mathscr{R})|^{1/(n-1)}.$$
Après simplification on trouve exactement l'inégalité de Hermite-Minkovski à l'ordre p, ce qui conclut la démonstration.

4. (a) Soit $x \in \mathscr{R}''$. Il existe $y \in \mathscr{R}$ tel que $m_b(\mathscr{R})^2 \pi(y) = x$, et l'on a $m_b(\mathscr{R})^2 y = tv + x$ où $t \in \mathbf{R}$. En appliquant $b(.,v)$ à cette égalité, on trouve $m_b(\mathscr{R})^2 b(y,v) = t b(v,v)$ (car $b(v,x) = 0$) soit encore $t = b(y,v) \in \mathbf{Z}$. On déduit alors de $x = m_b(\mathscr{R})^2 y - tv$ que x appartient au réseau $\mathscr{R}$ ce qui montre l'inclusion $\mathscr{R}'' \subset \mathscr{R}$. La forme b' est restriction de la forme b qui est à valeurs entières sur $\mathscr{R}$ et $\mathscr{R}'' \subset \mathscr{R}$, on en déduit que b' est à valeurs entières sur $\mathscr{R}''$.

   (b) On suppose le discriminant $\Delta_b(\mathscr{R})$ fixé. D'après la question IV-3 l'entier $m_b(\mathscr{R})$ est borné donc ne peut prendre qu'un nombre fini de valeurs. On sait d'autre part que
$$|\Delta_b(\mathscr{R})| = m_b(\mathscr{R})^2 |\Delta_{b'}(\mathscr{R}')|,$$
et
$$|\Delta_{b'}(\mathscr{R}'')| = m_b(\mathscr{R})^{2(n-1)} |\Delta_{b'}(\mathscr{R}')| = m_b(\mathscr{R})^{2(n-2)} |\Delta_b(\mathscr{R})|.$$
On en déduit que le discriminant $|\Delta_{b'}(\mathscr{R}'')|$ ne peut prendre qu'un nombre fini de valeurs.

5. (a) Soit $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathscr{R}_1$. Dire qu'un vecteur $y \in E$ appartient à $\mathscr{C}(\mathscr{R}_1)$ équivaut à dire
$$\forall i \in \{1, \ldots, n\} \;\; b_1(y, e_i) \in \mathbf{Z}.$$
La forme b_1 étant non dégénérée, l'application $\psi' : x \longrightarrow b_1(.,x)$ est un isomorphisme de E sur son dual E^*. Notons $e_i^* = b_1(.,e_i)$. La famille $(e_1^*, \ldots, e_n^*)$ est une base de E^*. L'application $\psi : x \longrightarrow (e_1^*(x), \ldots, e_n^*(x))$ est un isomorphisme entre les espaces vectoriels E et $\mathbf{R}^n$. Notons $\mathscr{R}^*$ le réseau de $\mathbf{R}^n$ de $\mathbf{Z}$-base la base canonique $(c_1, \ldots, c_n)$ de $\mathbf{R}^n$. L'ensemble $\mathscr{C}(\mathscr{R}_1)$ est l'image réciproque de $\mathscr{R}^*$ par ψ, c'est donc un réseau de E de $\mathbf{Z}$-base $(\psi^{-1}(c_1), \ldots, \psi^{-1}(c_n))$ (c'est la base antéduale de la base $(e_1^*, \ldots, e_n^*)$). On remarque que $\mathscr{R}_1 \subset \mathscr{C}(\mathscr{R}_1))$.
Si $\mathscr{R}_2$ est une extension de $\mathscr{R}_1$, la forme b_1 étant à valeurs entières sur $\mathscr{R}_2$, on a pour tout $x \in \mathscr{R}_2$ et tout $i \in \{1, \ldots, n\}$, $b_1(x, e_i) \in \mathbf{Z}$. Cela montre que $\psi(\mathscr{R}_2) \subset \mathscr{R}^*$, soit $\mathscr{R}_2 \subset \mathscr{C}(\mathscr{R}_1)$.

   (b) Soit $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathscr{R}_1$. Tout élément de $\mathscr{C}(\mathscr{R}_1)/\mathscr{R}_1$ admet un unique représentant dans $\mathscr{C}(\mathscr{R}_1)$ de la forme $\sum_{i=1}^n x_i e_i$ où les réels x_i appartiennent à l'intervalle $[0,1[$. Le pavé construit sur la famille e est un ensemble borné de E, donc d'après la question II-3 ne contient qu'un nombre fini d'éléments de $\mathscr{C}(\mathscr{R}_1)$. Donc le cardinal du groupe quotient $\mathscr{C}(\mathscr{R}_1)/\mathscr{R}_1$ est fini.

6. On démontre le théorème par récurrence sur n. Quitte à prendre la forme $-b$, on se ramène au cas $p \geqslant 1$.
   - Si $n = 1$, la forme b est donnée par une matrice à un coefficient dans une base quelconque, donc est fixée par le choix du discriminant : il n'y a qu'une classe d'équivalence de groupe libre quadratique de rang 1 et de discriminant fixé.
   - Supposons le théorème vérifié à l'ordre $n-1$ et démontrons-le à l'ordre n. Fixons le discriminant Δ et considérons un groupe $(\mathscr{R}, b)$ de rang n et de discriminant Δ. D'après la question IV-3, il n'y a qu'un nombre fini de possibilités pour $m_b(\mathscr{R})$. Donc le groupe libre quadratique G_1 de rang 1, de $\mathbf{Z}$-base (v), et de forme la restriction de b à $< v >$ appartient à un nombre fini de classes d'équivalence. Le groupe libre quadratique $G_2 = (\mathscr{R}'', b')$ est de rang $n-1$ et son discriminant ne peut prendre qu'un nombre fini de valeurs d'après la question IV-4-b. Par hypothèse de récurrence, ce groupe n'appartient qu'à un nombre fini de classes d'équivalence. Le groupe libre quadratique G_3 obtenu par somme directe de G_1 et G_2 n'appartient donc qu'à un nombre fini de classes d'équivalence. D'après la question IV-4-a, le groupe $(\mathscr{R}, b)$ est une extension de G_3 et d'après la question IV-5, il n'y a qu'un nombre fini d'extensions d'un groupe libre quadratique. Cela conclut la démonstration du théorème.

7. (a) Soit e la base canonique de $\mathbf{R}^2$ et le groupe libre quadratique $G = (\mathscr{R}, b)$ tel que e est une $\mathbf{Z}$-base de $\mathscr{R}$ et la matrice de b dans e est $\begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix}$. Ce groupe est bien un groupe libre quadratique de rang 2 et de dicriminant -2 et nous allons montrer que tout groupe libre quadratique de rang 2 et de discriminant -2 est équivalent à celui-ci.. Soit $(\mathscr{R}, b)$ un groupe libre quadratique de rang 2 et de discriminant -2. Le discriminant étant strictement négatif, la signature de la forme b est $(1,1)$. D'après la question IV-3, on a $m_b(\mathscr{R})^2 \leqslant 3^{1/2}(4/3)^{1/2}2^{1/2} = 2\sqrt{2} < 3$. D'après la question IV-1, il existe un vecteur $v \in \mathscr{R}$ vérifiant $b(v,v) = m_b(\mathscr{R})^2$, donc étant obligatoirement primitif par minimalité de $m_b(\mathscr{R})$ et vérifiant $b(v,v) \in \{1,2\}$.
      - Supposons $b(v,v) = 1$. Le vecteur v étant primitif, on peut le compléter en une $\mathbf{Z}$-base (v, e_2) de $\mathscr{R}$. La matrice de b dans cette base est de la forme $\begin{pmatrix} 1 & \alpha \\ \alpha & \beta \end{pmatrix}$. Considérons la famille $e' = (v, -\alpha v + e_2)$. C'est une $\mathbf{Z}$-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix}$. Le groupe est équivalent à G
      - Supposons $b(v,v) = 2$. Le vecteur v étant primitif, on peut le compléter en une $\mathbf{Z}$-base (v, e_2) de $\mathscr{R}$. La matrice de b dans cette base est de la forme $\begin{pmatrix} 2 & \alpha \\ \alpha & \beta \end{pmatrix}$ avec $2\beta - \alpha^2 = -2$. Considérons la famille $e' = (v, e_2 - tv)$ où l'entier t est choisi de manière à ce que $\alpha - 2t \in \{0,1\}$. La famille e' est une $\mathbf{Z}$-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix} 2 & \alpha' \\ \alpha' & \beta' \end{pmatrix}$ avec $\alpha' \in \{0,1\}$ et $2\beta' - \alpha'^2 = -2$. Cela impose $\alpha' = 0$ et $\beta' = -1$. Le vecteur $v' = e'_1 - e'_2$ vérifie alors $b(v', v') = 1$ ce qui contredit l'hypothèse faite sur $m_b(\mathscr{R})$. Ce cas est impossible.

   (b) Soit e la base canonique de $\mathbf{R}^2$ et les groupes libres quadratiques $G_i = (\mathscr{R}, b_i)$ tel que e est une $\mathbf{Z}$-base de $\mathscr{R}$, la matrice de b_1 dans e est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et la matrice de b_2 dans e est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Ces groupes sont bien des groupes libres quadratiques de rang 2 et de discriminant -1. Ils ne sont pas équivalents car la forme b_2 ne prend que des valeurs paires alors que la forme b_1 prend des valeurs impaires. Nous allons montrer que tout groupe libre quadratique de rang 2 et de discriminant -1 est équivalent à l'un de ces deux groupes.
   Soit $(\mathscr{R}, b)$ un groupe libre quadratique de rang 2 et de discriminant -1. Le discriminant étant strictement négatif, la signature de la forme b est $(1,1)$. D'après la question IV-3, on a $m_b(\mathscr{R})^2 \leqslant 3^{1/2}(4/3)^{1/2}1^{1/2} = 2$. D'après la question IV-1, il existe un vecteur $v \in \mathscr{R}$ vérifiant $b(v,v) = m_b(\mathscr{R})^2$, donc étant obligatoirement primitif par minimalité de $m_b(\mathscr{R})$ et vérifiant

$b(v,v) \in \{1,2\}$.

- Supposons $b(v,v)=1$. Le vecteur v étant primitif, on peut le compléter en une **Z**-base (v,e_2) de $\mathscr{R}$. La matrice de b dans cette base est de la forme $\begin{pmatrix}1 & \alpha\\ \alpha & \beta\end{pmatrix}$. Considérons la famille $e'=(v,-\alpha v+e_2)$. C'est une **Z**-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$. Le groupe est équivalent à G_1
- Supposons $b(v,v)=2$. Le vecteur v étant primitif, on peut le compléter en une **Z**-base (v,e_2) de $\mathscr{R}$. La matrice de b dans cette base est de la forme $\begin{pmatrix}2 & \alpha\\ \alpha & \beta\end{pmatrix}$ avec $2\beta-\alpha^2=-1$. Considérons la famille $e'=(v,e_2-tv)$ où l'entier t est choisi de manière à ce que $\alpha-2t\in\{0,1\}$. La famille e' est une **Z**-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix}2 & \alpha'\\ \alpha' & \beta'\end{pmatrix}$ avec $\alpha'\in\{0,1\}$ et $2\beta'-\alpha'^2=-1$. Cela impose $\alpha'=1$ et $\beta'=0$. Soit alors la famille $e''=(e'_1-e'_2,e'_2)$. C'est une **Z**-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Le groupe est donc équivalent à G_2.

3.3 Rapport sur l'épreuve écrite de mathématiques générales

Rapport des correcteurs

Remarques sur le problème

L'idée directrice du problème de mathématiques générales est un beau théorème de finitude sur les classes d'équivalence de groupes libres quadratiques. La démonstration s'appuie sur l'inégalité de Hermite-Minkovski, généralisation au cas quadratique de l'inégalité de Hermite. La première partie est centrée sur l'étude des sous-groupe finis de $GL_n(\mathbf{Z})$ et avait pour but principal de tester les capacités des candidats sur différents points du programme : algèbre linéaire, arithmétique de $\mathbf{Z}$ et $K[X]$, groupes,... La deuxième partie introduit les réseaux en démontrant quelques résultats classiques (en particulier l'existence de bases réduites) et en préparant la partie IV par la démonstration de l'inégalité de Hermite. La partie III met en oeuvre des techniques différentes du reste du problème en ouvrant une parenthèse sur la cristallographie, toujours dans le souci de permettre aux candidats de mettre en valeur leurs capacités. La partie IV démontre enfin l'inégalité de Hermite-Minkovski puis le théorème de finitude. On y combine dans une même structure les notions, souvent peu familières aux candidats, de réseaux et de formes quadratiques. Les candidats souhaitant approfondir les notions développées dans le problème pourront, par exemple, consulter l'ouvrage de J.M. Arnaudiès et J. Bertin, Groupes, algèbres et géométrie T2, où ils trouveront de nombreux exemples et développements ainsi qu'une bibliographie détaillée.

Remarques générales sur les copies

La plupart des remarques des années précédentes restent valables et peuvent être lues avec profit par les candidats. Nous développerons cependant les points qui nous semblent plus particulièrement utiles pour les futurs candidats.

La clarté, la rigueur, la précision et la concision de la rédaction sont des éléments importants d'appréciation des copies. De nombreux candidats perdent des points précieux dans les questions les plus accessibles du problème par des défauts de rédaction. Une première catégorie de défauts consiste en des démonstrations qui, bien que mathématiquement justes, sont maladroites, confuses, excessivement longues par multiplication inutiles des disjonctions de cas, utilisent des notations ou des notions qui ne font pas parties de l'énoncé et que le candidat n'a pas cru bon de définir (ou de définir avec précision),... Une deuxième catégorie de défauts, nettement plus graves et donc fortement sanctionnés, consiste en des démonstrations où manquent un ou plusieurs éléments essentiels dans l'enchaînement logique des arguments de la preuve : non initialisation d'une récurrence, utilisation du binôme de Newton dans un anneau non commutatif sans préciser que les éléments considérés commutent, oubli d'un argument crucial d'irréductibilité ou de non dégénérescence,... Il faut que les futurs candidats soient persuadés qu'ils ne perdront pas de temps ni de points, bien au contraire, en proposant une rédaction complète et rigoureuse des questions qu'ils auront résolues (tout en sachant rester concis...).

Il est par ailleurs indispensable que les candidats vérifient lors de leur préparation du concours qu'ils maîtrisent les bases de chaque chapitre du programme de l'agrégation et qu'ils savent mettre en oeuvre les théorèmes étudiés dans des situations concrètes de difficulté raisonnable : ce qui fait le plus souvent défaut aux candidats est moins la connaissance de résultats théoriques que leur assimilation par la pratique. C'est un entraînement extrêmement profitable pour la préparation des épreuves écrites et orales.

D'autre part, les problèmes d'agrégation sont volontairement de difficulté progressive et découpés en parties largement indépendantes pour permettre aux candidats de mettre en valeur leurs capacités. Si le grapillage est déconseillé, il est tout à fait possible qu'un candidat se sente peu à l'aise sur les notions développées dans une partie ou soit bloqué après une recherche sérieuse, lorsque la difficulté devient trop élevée. Le candidat a alors tout intérêt soit à regarder si les dernières questions de la partie, qui consistent souvent en une mise en application des résultats théoriques de la partie sur un exemple et sont abordables

en admettant les résultats en question, lui semblent accessibles, soit à regarder si il se sent plus habile sur les parties suivantes : malgré la progressivité du problème, les premières questions des parties sont à priori toujours de difficulté mesurée et peuvent être l'occasion pour un candidat de montrer ses capacités.

Signalons enfin qu'une copie a traité tout le problème parfaitement mais que la grande majorité des candidats n'a abordé de manière sérieuse que les parties I et II qui ont donc été les parties discriminantes.

Remarques sur les questions

I.1. La plupart des candidats ont traité cette question, avec pour nombre d'entre eux une rédaction qui manque de rigueur. Dans le cas d'un raisonnement par récurrence, la récurrence n'est pas toujours initialisée ou le passage de n à $n+1$ n'est pas clairement explicité. De même la méthode consistant à développer le déterminant donnant le polynôme caractéristique par rapport à la dernière colonne a souvent été sanctionnée par manque, parfois total, de détails sur les calculs menés.

I.2.a. La question a été particulièrement discriminante. Il suffisait de remarquer qu'une valeur propre d'un endomorphisme est racine d'un polynôme annulateur de cet endomorphisme. De nombreuses erreurs portant sur les liens entre polynôme caractéristique, polynôme annulateur et polynôme minimal annulateur d'un endomomorphisme ont été relevées, la plus fréquente consistant à affirmer que le polynôme $C_M(X)$ était un diviseur de X^m-1.

I.2.b-c. Les deux questions ont été traitées par la plupart des copies, avec un réel effort de rédaction. Les solutions proposées manquaient souvent de concision.

I.2.d. La question n'a été traité correctement que très rarement, les candidats n'utilisant pas (ou mal) l'irréductibilité des polynômes cyclotomiques et ayant des difficultés avec la notion de racine multiple.

I.2.e. Les solutions proposées par les candidats sont souvent longues ou incomplètes faute d'avoir remarqué que la matrice M était diagonalisable.

I.2.f. De nombreuses copies donnent une matrice d'ordre 6. Il était attendu une justification du fait que la matrice proposée était bien d'ordre 6. Rappelons que la vérification $M^6 = I_2$ prouve uniquement que l'ordre de M est un diviseur de 6.

I.3.b. Question plutôt bien traitée mis à part la difficulté technique qui imposait $p > 2$ qui n'a été traitée que de manière rarissime.

I.3.c. Dans cette question qui consistait essentiellement à réutiliser les deux questions précédentes, la rédaction manquait généralement de rigueur, ce qui a été sanctionné.

I.5.a. Il était attendu une justification pour le cardinal de $GL_2(\mathbf{F}_3)$.

I.5.b. La question n'a été traitée correctement que très rarement.

II.1. La question a été abordée dans la plupart des copies, la totalité des vérifications nécessaires n'étant que rarement faites.

II.2. L'erreur la plus fréquente a été de donner comme formule de changement de base $P^{-1}MP$.

II.3. La question a souvent été mal traitée. De nombreux candidats n'ont tenté de résoudre la question que dans un cas de norme particulière. D'autre ont voulu utiliser le fait que le réseau $\mathscr{R}$ était discret, sans démontrer cette propriété et en ne l'utilisant pas toujours à bon escient (rappelons en particulier que l'intersection d'un compact et d'un ensemble discret de $\mathbf{R}^n$ n'est pas obligatoirement un ensemble fini).

II.5.b. Il était suffisant de se ramener à la question 4.

II.5.d. La rédaction a été particulièrement discriminante dans cette question : il était nécessaire d'expliciter clairement le raisonnement par récurrence.

II.5.e. Seules les rares copies où étaient effectuées avec rigueur toutes les vérifications ont obtenues la totalité des points.

II.6.d. La question, délicate, n'a été que très rarement traitée.

II.7. Les deux questions ont souvent été abordées. Un nombre non négligeable de candidats perdent des points par manque de rigueur dans la rédaction ou mauvaise gestion des inégalités.

III.1. La question a été traitée par un nombre trop restreint de candidats au vu de sa difficulté, l'argument essentiel consistant à utiliser II.3.

III.2-3-4. Les questions 2-3-4 ont souvent donné lieu à une rédaction confuse. La principale difficulté consistait à comprendre la nature des objets manipulés.

III.5. La question 5 n'a été que très rarement abordée alors qu'elle proposait une application des résultats précédents, indépendante de leur démonstration. Elle devait permettre aux candidats de mettre en valeur leur connaissance du groupe diédral.

IV. La partie IV n'a été abordée que par une poignée d'excellents candidats. Les questions traitées sont alors le plus souvent très bien rédigées. Il est à remarquer que plusieurs questions de cette partie étaient de difficulté raisonnable et auraient pu être abordées par un nombre non négligeable de candidats.