Mathématiques générales 2008

Préambule

Ce problème a pour objectif de démontrer le théorème de finitude sur les classes d'équivalence de groupes libres quadratiques en utilisant l'inégalité de Hermite-Minkovski. On étudie dans la partie I les sous-groupes finis de $GL_n(\mathbf{Z})$. La partie II est consacrée à l'étude des réseaux et en particulier la démonstration de l'inégalité de Hermite. On étudie dans la partie III les cristalloïdes. On démontre enfin le théorème de finitude dans la partie IV. Les deux premières parties sont indépendantes. La troisième n'utilise que les questions II-1 et II-3. Les parties III et IV sont indépendantes.

Notations

- Dans tout le problème, E est un espace vectoriel réel de dimension finie $n \geq 1$.
- On note $\mathbf{R}$ le corps des nombres réels, $\mathbf{C}$ le corps des nombres complexes, $\mathbf{Q}$ le corps des nombres rationnels, $\mathbf{Z}$ l'anneau des entiers relatifs et $\mathbf{N}$ l'ensemble des entiers naturels. On note $\mathbf{Z}^*$ l'ensemble des entiers relatifs privé de 0 et $\mathbf{N}^*$ l'ensemble des entiers naturels privé de 0.
- Si A et B sont deux ensembles, on note $A \setminus B$ l'ensemble des éléments de A qui n'appartiennent pas à B.
- Si F est un espace vectoriel réel, on note $L(E, F)$ l'ensemble des applications linéaires de E dans F et $GL(E)$ le groupe linéaire de E. Si f est un endomorphisme de E et e une base de E, on note $\mathrm{Mat}(f, e)$ la matrice de f dans la base e.
- Si $(e_1, \ldots, e_p)$ est une famille de vecteurs de E, on note $\langle e_1, \ldots, e_p \rangle$ le sous-espace vectoriel de E engendré par la famille $(e_1, \ldots, e_p)$.
- On note $M_n(\mathbf{Z})$ l'anneau des matrices à coefficients entiers de taille n et $GL_n(\mathbf{Z})$ le groupe des éléments inversibles de cet anneau. Si $k \in N^*$ on note $kM_n(\mathbf{Z})$ l'ensemble des matrices de $M_n(\mathbf{Z})$ dont tous les coefficients sont des multiples de k.

Rappels

- On rappelle qu'une matrice de $M_n(\mathbf{Z})$ appartient à $GL_n(\mathbf{Z})$ si et seulement si son déterminant est égal à 1 ou -1. Si $\mathbf{K}$ est un corps, on note $M_n(\mathbf{K})$ l'ensemble des matrices de taille n à coefficients dans le corps $\mathbf{K}$ et I_n la matrice identité de taille n.
- Si p et q sont deux entiers naturels, on note $p \wedge q$ le plus grand commun diviseur de p et q, on note également $p \mid q$ si p divise q. Si m est un entier supérieur ou égal à 1, on note $\Phi_m(X)$ le polynôme cyclotomique d'ordre m. On rappelle que

$$\Phi_m(X) = \prod_{\{k \in \{1,\ldots,m\}/k \wedge m = 1\}} (X - e^{2ik\pi/m}) \, .$$

- On rappelle également que $\Phi_m(X)$ est un polynôme unitaire à coefficients entiers, irréductible dans $\mathbf{Q}[X]$. Le degré de $\Phi_m(X)$ est $\varphi(m)$ où φ est la fonction indicatrice d'Euler, définie de $\mathbf{N}^*$ dans $\mathbf{N}^*$

par : si p est un nombre premier et $r \in \mathbf{N}^*$ on a $\varphi(p^r) = p^r - p^{r-1}$ et si $p \in N^*$ et $q \in N^*$ sont premiers entre eux, alors $\varphi(pq) = \varphi(p)\,\varphi(q)$.

– On rappelle enfin que

$$X^m - 1 = \prod_{d|m} \varphi_d(X)\ .$$

– Si $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ est un polynôme unitaire de degré n à coefficients complexes, on note M_P la matrice compagnon de $M_n(\mathbf{C})$ dont le (i,j)-ème terme vaut 1 si $i = j+1$, vaut $-a_{i-1}$ si $j = n$, vaut 0 dans les autres cas. Ainsi pour le polynôme $P = X^3 + a_2X^2 + a_1X + a_0$, la matrice M_P est de la forme

$$M_P = \begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix}\ .$$

Si $M \in M_n(\mathbf{C})$, on note $C_M(X) = \det(XI_n - M)$ le polynôme caractéristique de M.

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

1. Soit P un polynôme à coefficients complexes unitaire de degré n et M_P la matrice compagnon qui lui est associée. Démontrer que P est le polynôme caractéristique de la matrice M_P.
2. Soit $M \in GL_2(\mathbf{Z})$, d'ordre fini m.
   (a) Montrer que si z est une racine complexe du polynôme $C_M(X)$ alors z est racine du polynôme $X^m - 1$.
   (b) Montrer, en résolvant avec soin l'équation $\varphi(k) = 1$, qu'il y a exactement deux polynômes cyclotomiques de degré un.
   (c) Montrer de même qu'il y a exactement trois polynômes cyclotomiques de degré deux dont on donnera les expressions développées.
   (d) En déduire que le polynôme $C_M(X)$ appartient à l'ensemble

$$\{X^2 + X + 1,\ X^2 + 1,\ X^2 - X + 1,\ X^2 - 1,\ (X-1)^2,\ (X+1)^2\}\ .$$

   (e) En déduire que $m \in \{1, 2, 3, 4, 6\}$.
   (f) Donner un élément de $GL_2(\mathbf{Z})$ d'ordre 6.
3. Soit $M \in GL_n(\mathbf{Z})$ d'ordre $m \geq 2$ et p un nombre premier, $p \geq 3$. On suppose que $M = I_n + p^r N$ avec $r \in N^*$ et $N \in M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$.
   (a) Montrer que $m\,p^r\,N \in p^{2r} M_n(\mathbf{Z})$. En déduire que p divise m.

   On pose alors $m = pm'$ et $M' = M^p$.
   (b) Montrer que p divise m'.
   (c) Conclure à une contradiction.
4. Soit p un nombre premier, $p \geq 3$. Soit G un sous-groupe fini de $GL_n(\mathbf{Z})$. On note $\mathbf{F}_p$ un corps de cardinal p, unique à isomorphisme près. On rappelle que la surjection naturelle $\mathbf{Z} \to \mathbf{F}_p$ induit un morphisme de groupes

$$GL_n(\mathbf{Z}) \to GL_n(\mathbf{F}_p)\ .$$

   Montrer que G est isomorphe à un sous-groupe de $GL_n(\mathbf{F}_p)$.
5. Soit G un sous-groupe fini de $GL_2(\mathbf{Z})$.
   (a) Montrer que le cardinal de G est un diviseur de 48.
   (b) Montrer que le cardinal de G ne peut pas être égal à 48. (*On pourra, éventuellement, étudier* $\Phi_8(X)$ *considéré comme un polynôme à coefficients dans* $\mathbf{F}_3$.)

II Réseaux

On suppose dans la suite du problème que l'espace vectoriel E est muni d'un produit scalaire $(\cdot,\cdot)$ et de la norme $\|\ \|$ associée. Si F est un sous-espace vectoriel de E, on note $F^\perp$ son orthogonal. On rappelle qu'un réseau $\mathcal{R}$ de E est un ensemble de vecteurs de la forme

$$\left\{ \sum_{i=1}^{n} a_i e_i \ / \ \forall i \in \{1,\dots,n\},\ a_i \in \mathbf{Z} \right\} ,$$

où $e = (e_1,\dots,e_n)$ est une base de E. La famille e est dite $\mathbf{Z}$-base de $\mathcal{R}$. Un élément v de $\mathcal{R}$ est dit primitif s'il existe une $\mathbf{Z}$-base e de $\mathcal{R}$ telle que les coordonnées de v dans e sont premières entre elles dans leur ensemble. On admet le résultat suivant qui pourra être utilisé librement : si v est un vecteur primitif d'un réseau $\mathcal{R}$, il existe une $\mathbf{Z}$-base de $\mathcal{R}$ de la forme $(v, v_2,\dots,v_n)$.

Dans toute la suite du problème, $\mathcal{R}$ est un réseau de E

1. Soit e une $\mathbf{Z}$-base de $\mathcal{R}$ et e' une famille de n vecteurs de E. Montrer que e' est une $\mathbf{Z}$-base de $\mathcal{R}$ si et seulement si e' est une base de E et la matrice de passage de e à e' appartient à $GL_n(\mathbf{Z})$.
2. Soit $e = (e_1,\dots,e_n)$ une $\mathbf{Z}$-base de $\mathcal{R}$. Montrer que le déterminant de la matrice de $M_n(\mathbf{R})$ dont le (i,j)-ème coefficient est égal à (e_i, e_j) est indépendant du choix de la $\mathbf{Z}$-base e de $\mathcal{R}$. C'est le discriminant du réseau $\mathcal{R}$, on le note $\Delta(\mathcal{R})$.
3. Soit r un réel strictement positif et a un élément de E. On note

   $$B(a,r) = \{x \in E \ / \ \|x - a\| \leq r\} .$$

   Montrer que $B(a,r) \cap \mathcal{R}$ est de cardinal fini.

   Si A est un sous-ensemble non vide minoré de $\mathbf{R}$, on note $\inf A$ la borne inférieure de A. On note $m(\mathcal{R}) = \inf\{\|x\| \ / \ x \in \mathcal{R} \setminus \{0\}\}$.
4. Montrer que le réel $m(\mathcal{R})$ est strictement positif et qu'il existe $v \in \mathcal{R} \setminus \{0\}$ vérifiant $\|v\| = m(\mathcal{R})$.
5. On suppose $n \geq 2$ dans les questions 5-a, 5-b et 5-c. Soit $k \in \{1,\dots,n-1\}$ et $(v_1,\dots,v_k,e_{k+1},\dots,e_n)$ une $\mathbf{Z}$-base de $\mathcal{R}$. On pose $W_k = \langle v_1,\dots,v_k\rangle$ et π_k la projection orthogonale sur $W_k^\perp$.
   (a) Montrer que $\pi_k(\mathcal{R})$ est un réseau de $W_k^\perp$ dont on précisera une $\mathbf{Z}$-base.
   (b) Montrer qu'il existe un vecteur v_{k+1} du réseau $\mathcal{R}$ vérifiant

   $$\|\pi_k(v_{k+1})\| = m(\pi_k(\mathcal{R})) .$$

   (c) Montrer qu'il existe une famille $(f_{k+2},\dots,f_n)$ de E telle que la famille $(v_1,\dots,v_{k+1},f_{k+2},\dots,f_n)$ est une $\mathbf{Z}$-base de $\mathcal{R}$. (*On pourra montrer que $\pi_k(v_{k+1})$ est un vecteur primitif du réseau $\pi_k(\mathcal{R})$.*)
   (d) En déduire qu'il existe une $\mathbf{Z}$-base $(v_1,\dots,v_n)$ de $\mathcal{R}$ vérifiant $\|v_1\| = m(\mathcal{R})$ et

   $$\forall k \in \{1,\dots,n-1\}\ \|\pi_k(v_{k+1})\| = m(\pi_k(\mathcal{R})) ,$$

   où l'on note π_k la projection orthogonale sur $\langle v_1,\dots,v_k\rangle^\perp$. Une telle base est appelée base réduite du réseau $\mathcal{R}$.
   (e) On considère $\mathbf{R}^2$ muni de sa structure euclidienne usuelle. Soit $\mathcal{R}_1$ le réseau de $\mathbf{R}^2$ déterminé par la $\mathbf{Z}$-base $e = ((1,0),(-1/2,\sqrt{3}/2))$. Vérifier que e est une base réduite de $\mathcal{R}_1$.
6. On suppose $n \geq 2$ dans les questions 6-a, 6-b et 6-c. Soit $e = (e_1,\dots,e_n)$ une base réduite de $\mathcal{R}$. Soit π_1 la projection orthogonale sur l'hyperplan $\langle e_1\rangle^\perp$

(a) Montrer que pour tout couple (j,k) appartenant à $\{2,\dots,n\}^2$ on a

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

(b) Montrer que $\Delta(\mathcal{R}) = m(\mathcal{R})^2\,\Delta(\pi_1(\mathcal{R}))$

(c) Soit $v \in \mathcal{R}\setminus\{0\}$. On suppose que $v = te_1 + v'$ avec $t \in \mathbf{R}$ et $v' \in \langle e_1\rangle^\perp$. Vérifier que

$$m(\mathcal{R})^2 \le t^2\,m(\mathcal{R})^2 + \|v'\|^2\ .$$

(d) En déduire l'inégalité de Hermite :

$$m(\mathcal{R})^2 \le (4/3)^{(n-1)/2}\,\Delta(\mathcal{R})^{1/n}\ .$$

7. On note H_n l'ensemble des réels $\rho \ge 0$ tels que pour tout réseau $\mathcal{R}$ de E on a $m(\mathcal{R})^2 \le \rho\,\Delta(\mathcal{R})^{1/n}$. On note alors $\eta_n = \inf H_n$

(a) Montrer que $\eta_n \ge 1$

(b) Montrer que $\eta_2 = 2/\sqrt{3}$

III Cristalloïdes

On suppose dans cette partie $n \ge 2$. On note $O(E)$ le groupe orthogonal de E et $O(\mathcal{R})$ l'ensemble des isométries de E qui stabilisent $\mathcal{R}$. c'est à dire qui induisent une bijection de $\mathcal{R}$ sur $\mathcal{R}$. $O(\mathcal{R})$ est un sous-groupe de $O(E)$. Si e est une $\mathbf{Z}$-base de $\mathcal{R}$, l'application $\psi_e : g \mapsto \mathrm{Mat}(g,e)$ est un morphisme injectif de groupes de$O(\mathcal{R})$ dans $GL_n(\mathbf{Z})$ qui permet d'identifier $O(\mathcal{R})$ à un sous-groupe de $GL_n(\mathbf{Z})$. Un cristalloïde de E est un couple $(\mathcal{R},\Gamma)$ où $\mathcal{R}$ est un réseau de E et Γ un sous-groupe de $O(\mathcal{R})$.

1. Montrer que $O(\mathcal{R})$ est de cardinal fini.

   On dit que deux cristalloïdes de E notés $(\mathcal{R},\Gamma)$ et $(\mathcal{R}',\Gamma')$ sont équivalents s'il existe $u \in GL(E)$ vérifiant $u(\mathcal{R}) = \mathcal{R}'$ et $u\Gamma u^{-1} = \Gamma'$. On définit ainsi une relation d'équivalence sur les cristalloïdes de E. Deux sous-groupes G et G' de $GL_n(\mathbf{Z})$ sont dits $\mathbf{Z}$-conjugués s'il existe $M \in GL_n(\mathbf{Z})$ vérifiant $MGM^{-1} = G'$. On définit ainsi une relation d'équivalence sur les sous-groupes de $GL_n(\mathbf{Z})$.

2. Soit $(\mathcal{R},\Gamma)$ un cristalloïde de E, e une $\mathbf{Z}$-base de $\mathcal{R}$ et G un sous-groupe de $GL_n(\mathbf{Z})$. Montrer que G est $\mathbf{Z}$-conjugué à $\psi_e(\Gamma)$ si et seulement s'il existe une $\mathbf{Z}$-base e' de $\mathcal{R}$ telle que $G = \psi_{e'}(\Gamma)$.

3. Soit $(\mathcal{R},\Gamma)$ et $(\mathcal{R}',\Gamma')$ deux cristalloïdes de E, e une $\mathbf{Z}$-base de $\mathcal{R}$ et e' une $\mathbf{Z}$-base de $\mathcal{R}'$. Montrer que $(\mathcal{R},\Gamma)$ est équivalent à $(\mathcal{R}',\Gamma')$ si et seulement si les groupes $\psi_e(\Gamma)$ et $\psi_{e'}(\Gamma')$ sont $\mathbf{Z}$-conjugués.

   On peut ainsi définir une application ψ qui à toute classe d'équivalence de cristalloïdes de E de représentant $(\mathcal{R},\Gamma)$ associe une classe de $\mathbf{Z}$-conjugaison de sous-groupes finis de $GL_n(\mathbf{Z})$ de représentant $\psi_e(\Gamma)$ où e est une $\mathbf{Z}$-base quelconque de $\mathcal{R}$.

4. Montrer que l'application ψ est 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. En déduire que $GL_2(\mathbf{Z})$ possède un sous-groupe isomorphe au groupe diédral D_6.

IV Groupes libres quadratiques

On suppose dans les questions 1,2 et 3 que E est muni d'une forme bilinéaire symétrique non dégénérée b de signature (p,q) avec $p \ge 1$. On suppose que la forme b vérifie

$$\forall (x,y) \in \mathcal{R}^2,\ b(x,y) \in \mathbf{Q}\ .$$

Si F est un sous-espace vectoriel de E, on note $F^{\perp b}$ l'orthogonal de F pour la forme b. On note également

$$m_b(\mathcal{R}) = \inf\{b(x,x)^{1/2} \ / \ x \in \mathcal{R},\ b(x,x) > 0\} \ .$$

De même que dans le cas euclidien, un élément v de $\mathcal{R}$ est dit primitif s'il existe une $\mathbf{Z}$-base e de $\mathcal{R}$ telle que les coordonnées de v dans e sont premières entre elles dans leur ensemble. On admet encore le résultat suivant : si v est un vecteur primitif d'un réseau $\mathcal{R}$, il existe une $\mathbf{Z}$-base de $\mathcal{R}$ de la forme $v, v_2, \ldots, v_n$).

1. Montrer qu'il existe $v \in \mathcal{R} \setminus \{0\}$ tel que $m_b(\mathcal{R}) = b(v,v)^{1/2}$.

   On note $W = \langle v \rangle^{\perp b}$ et b' la forme bilinéaire définie sur W par restriction de la forme b.

2. Déterminer la signature de b'. Soit $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathcal{R}$. Le déterminant de la matrice de $M_n(\mathbf{Q})$ de (i,j)-ème terme $b(e_i, e_j)$ est indépendant du choix de la $\mathbf{Z}$-base e. On le note $\Delta_b(\mathcal{R})$.

3. Démontrer l'inégalité de Hermite-Minkovski

   $$m_b(\mathcal{R})^2 \leq 3^{(n-p)/n}\,(4/3)^{(n-1)/2}\,|\Delta_b(\mathcal{R})|^{1/n} \ .$$

   (*On pourra s'inspirer du raisonnement effectué dans la partie II pour démontrer l'inégalité de Hermite.*)

   Un groupe libre quadratique est un couple $(\mathcal{R}, b)$ où $\mathcal{R}$ est un réseau d'un espace vectoriel réel E de dimension n et b une forme bilinéaire symétrique sur E, non dégénérée, vérifiant

   $$\forall (x,y) \in \mathcal{R}^2,\ b(x,y) \in \mathbf{Z} \ .$$

   Le discriminant du groupe libre quadratique $(\mathcal{R}, b)$ est l'entier $\Delta_b(\mathcal{R})$, son rang est l'entier n. Deux groupes libres quadratiques $(\mathcal{R}, b)$ et $(\mathcal{R}', b')$, associés à des espaces vectoriels E et E', sont dits équivalents s'il existe $u \in GL(E, E')$ qui induit une bijection de $\mathcal{R}$ sur $\mathcal{R}'$ vérifiant

   $$\forall (x,y) \in \mathcal{R}^2,\ b'(u(x), u(y)) = b(x,y) \ .$$

   On définit ainsi une relation d'équivalence sur l'ensemble des groupes libres quadratiques. Le but de cette partie est de démontrer le théorème suivant : pour tout couple $(\Delta, n) \in \mathbf{Z}^* \times \mathbf{N}^*$ il n'y a qu'un nombre fini de classes d'équivalence de groupes libres quadratiques de discriminant Δ et de rang n.

4. Soit $(\mathcal{R}, b)$ un groupe libre quadratique. On suppose b de signature (p,q) avec $p \geq 1$. On reprend les notations v, W et b' introduites à la question IV-1. On note π la projection sur W parallèlement à $\langle v \rangle$ et $\mathcal{R}' = \pi(\mathcal{R})$. On sait que $\mathcal{R}'$ est un réseau de W. On pose enfin

   $$\mathcal{R}'' = m_b(\mathcal{R})^2\,\mathcal{R}' = \{m_b(\mathcal{R})^2 x \ / \ x \in \mathcal{R}'\} \ .$$

   (a) Montrer que $\mathcal{R}'' \subset \mathcal{R}$ et que
   $$\forall (x,y) \in \mathcal{R}''^2,\ b'(x,y) \in \mathbf{Z} \ .$$

   (b) Montrer que $\Delta_{b'}(\mathcal{R}'')$ ne peut prendre qu'un nombre fini de valeurs, le discriminant $\Delta_b(\mathcal{R})$ étant fixé.

5. Soit $(\mathcal{R}_1, b_1)$ un groupe libre quadratique. On appelle extension de (R_1, b_1) tout groupe libre quadratique de la forme $(\mathcal{R}_2, b_1)$ avec $\mathcal{R}_1 \subset \mathcal{R}_2$. On appelle réseau complémentaire de $\mathbf{R}_1$ l'ensemble

   $$C(\mathcal{R}_1) = \{y \in E \ / \ \forall x \in \mathcal{R}_1,\ b_1(x,y) \in \mathbf{Z}\} \ .$$

   (a) Montrer que $C(\mathcal{R}_1)$ est un réseau de E et que pour toute extension $(\mathcal{R}_2, b_1)$ de $(\mathbf{R}_1, b_1)$ on a $\mathcal{R}_2 \subset C(\mathcal{R}_1)$.

(b) Montrer que le cardinal du groupe quotient $C(\mathcal{R}_1)/\mathcal{R}_1$ est fini.

6. Démontrer le théorème de finitude : pour tout couple $(\Delta, n) \in \mathbf{Z}^* \times \mathbf{N}^*$ il n'y a qu'un nombre fini de classes d'équivalence de groupes libres quadratiques de discriminant Δ et de rang n.

7. Exemples.

   (a) Montrer qu'il y a exactement une classe d'équivalence de groupes libres quadratiques de rang 2 et de discriminant -2. (*On pourra montrer, si* $(\mathcal{R}, b)$ *est un groupe libre quadratique de rang* 2 *et de discriminant* -2*, qu'il existe* $v \in \mathcal{R}$*, primitif, vérifiant* $b(v, v) \in \{1, 2\}$.)

   (b) Montrer qu'il y a exactement deux classes d'équivalence de groupes libres quadratiques de rang 2 et de discriminant -1.