Mathématiques Générales 2008 - corrigé

Michel Coste*†
Université de Rennes 1

12 août 2008

Ce document provient de la préparation à l'agrégation de mathématiques de l'Université de Rennes 1 :

`http://agreg-maths.univ-rennes1.fr`

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 $(e_1,\dots,e_p)$ est une famille de vecteurs de E, on note $\langle e_1,\dots,e_p\rangle$ le sous-espace vectoriel de E engendré par la famille $(e_1,\dots,e_p)$.*
- *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.*

*Remarques et questions bienvenues à `michel.coste@univ-rennes1.fr`
†Merci à Olivier Ayasssou pour une correction de coquille

– *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*

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

– *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.*

   Numérotons les lignes L_i pour i allant de 1 à n. On ne change pas le déterminant de la matrice $XI_n - M$ en remplaçant L_1 par $L_1 + XL_2 + \cdots + X^{n-1}L_n$. La nouvelle première ligne est alors $0 \dots 0\ P$, et on obtient en développant suivant cette ligne $C_M = (-1)^{n+1}P \times (-1)^{n-1} = P$.

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 $X^m - 1$.*

   Le polynôme $X^m - 1$ annule M, donc toute valeur propre de z est racine de $X^m - 1$.

   (b) *Montrer, en résolvant avec soin l'équation $\varphi(k) = 1$, qu'il y a exactement deux polynômes cyclotomiques de degré un.*

   Si p est premier et $r \geq 1$, on a $\varphi(p^r) = 1$ si et seulement si $p^{r-1} = 1$ et $p - 1 = 1$, donc si et seulement si $p = 2$ et $r = 1$. Donc $\varphi(k) = 1$ si et seulement si $k = 1$ ou $k = 2$. Les seuls polynômes cyclotomiques de degré 1 sont $\Phi_1 = X - 1$ et $\Phi_2 = X + 1$.

   (c) *Montrer de même qu'il y a exactement trois polynômes cyclotomiques de degré deux dont on donnera les expressions développées.*

   Si p est premier et $r \geq 1$, on a $\varphi(p^r) = 2$ si et seulement si $p = 3$ et $r = 1$, ou $p = 2$ et $r = 2$. Donc $\varphi(k) = 2$ si et seulement si $k = 3$ ou $k = 4$ ou $k = 6$. Les seuls polynômes cyclotomiques de degré 2 sont $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$ et $\Phi_6 = X^2 - X + 1$.

(d) *En déduire que le polynôme $C_M(X)$ appartient à l'ensemble*

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

Le polynôme $C_M(X)$ est de degré 2, à coefficients entiers et toutes ses racines complexes sont des racines de l'unité. C'est donc un polynômes cyclotomique de degré 2, ou le produit de deux polynômes cyclotomiques de degré 1. Il appartient bien à l'ensemble ci-dessus.

(e) *En déduire que $m \in \{1,2,3,4,6\}$.*
La matrice M est diagonalisable sur $\mathbf{C}$ car elle est annulée par un polynôme à racines simples, et donc son ordre est le ppcm des ordres de ses valeurs propres. Suivant que $C_M(X)$ est l'un des éléments de l'ensemble de la question d), on trouve $m = 3,4,6,2,1,2$ respectivement.

(f) *Donner un élément de $GL_2(\mathbf{Z})$ d'ordre 6.*

D'après ce qui précède, il suffit de prendre $C_{\Phi_6} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

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 a

$$I_n = (I_n + p^r\,N)^m = I_n + m\,p^r\,N + p^{2r}\,N^2\,Q\ ,$$

où Q est un polynôme à coeffcients entiers en N. Donc $m\,p^r\,N \in p^{2r}M_n(\mathbf{Z})$. Si p ne divisait pas m on aurait d'après le lemme de Gauss $N \in p^r M_n(\mathbf{Z})$, ce qui n'est pas. Donc $p \mid m$.

On pose alors $m = pm'$ et $M' = M^p$.

(b) *Montrer que p divise m'.*
Montrons que $m' \geq 2$, c.-à-d. que $m \neq p$. Si on avait $m = p$, alors on aurait

$$I_n = M^p = I_n + p^{r+1}N + \frac{p(p-1)}{2}p^{2r}\,N^2 + p^{3r}\,N^3\,R\ ,$$

où R est un polynôme à coefficients entiers en N. Il en suivrait, puisque p est premier ≥ 3, $p^{r+1}N \in p^{2r+1}M_n(\mathbf{Z})$, d'où $N \in p^r M_n(\mathbf{Z})$ contrairement à l'hypothèse faite sur N. Cette contradiction montre $m' \geq 2$.[1]
La matrice M' est d'ordre $m' \geq 2$, et $M' - I_n \in pM_n(\mathbf{Z}) \setminus \{0\}$. On peut donc trouver $r' \in \mathbf{N}^*$ et $N' \in M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$ tels que $M' = I_n + p^{r'}N'$. D'après le a), p divise m'.

(c) *Conclure à une contradiction.*
Les résultats de a) et b) permettent de montrer par récurrence sur k que, si M vérifie les hypothèses de la question 3), alors m est divisible par p^k pour tout entier k. Ceci est impossible, donc il n'y a pas de matrice M vérifiant les hypothèses de la question 3).

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

Il suffit de montrer que l'intersection du noyau de $GL_n(\mathbf{Z}) \to GL_n(\mathbf{F}_p)$ avec G est réduite à $\{I_n\}$. Ce noyau est l'ensemble des matrices de la forme $I_n + pQ$ avec $Q \in M_n(\mathbf{Z})$. Si ce noyau contenait une matrice M de G différente de I_n, alors M serait d'ordre $m \geq 2$ et vérifierait les hypothèses de la question 3). Or on a vu qu'une telle matrice n'existe pas. En conclusion, le morphisme $G \to GL_n(\mathbf{F}_p)$ est injectif et G est isomorphe à son image qui est un sous-groupe de $GL_n(\mathbf{F}_p)$.

[1] Il est curieux que ce point un peu délicat (montrer $m \neq p$) soit un peu escamoté dans l'énoncé. C'est d'ailleurs le seul endroit où on utilise $p \geq 3$.

5. *Soit G un sous-groupe fini de $GL_2(\mathbf{Z})$.*
   (a) *Montrer que le cardinal de G est un diviseur de 48.*
   On a montré que G s'injecte dans $GL_2(\mathbf{F}_3)$, et le cardinal de ce dernier groupe, qui est égal au cardinal de l'ensemble des bases de $(\mathbf{F}_3)^2$, est 48. On choisit le premier vecteur de base parmi les $9-1=8$ vecteurs non nuls de $(\mathbf{F}_3)^2$, et le deuxième vecteur de base parmi les $9-3=6$ vecteurs non colinéaires au premier ; ceci fait bien $8\times 6=48$ choix possibles.
   (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 $\mathbf{F}_3$.)*[2]
   Le polynôme cyclotomique $\Phi_8(X)$ a pour racines les quatre racines quatrièmes de -1, c'est X^4+1. Ce polynôme se factorise sur $\mathbf{F}_3$ en $X^4+1=(X^2+X-1)(X^2-X-1)$, et les deux facteurs de degré 2 sont irréductibles sur $\mathbf{F}_3$ puisqu'ils n'y ont pas de racine[3]. La matrice compagnon M de X^2+X-1 sur $\mathbf{F}_3$ est un élément d'ordre 8 de $GL_2(\mathbf{F}_3)$ (elle vérifie $M^8=I_2$, et on remarque que X^8-1 n'a pas de racine multiple dans une extension de $\mathbf{F}_3$, donc X^4-1 est premier avec X^2+X-1 sur $\mathbf{F}_3$ et M^4-I_2 est inversible). Comme G ne contient pas d'élément d'ordre 8, la matrice M n'est pas dans l'image du morphisme injectif $G\to GL_2(\mathbf{F}_3)$. Le cardinal de G est donc strictement inférieur à 48.

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 $GL_n(\mathbf{Z})$.*
   Notons $P_e^{e'}$ la matrice e passage de e à e'. Si e' est une autre $\mathbf{Z}$-base de $\mathcal{R}$, alors $P_e^{e'}$ et son inverse sont à coefficients entiers, donc $P_e^{e'}\in GL_n(\mathbf{Z})$. Réciproquement, si e' est une base de E telle que $P_e^{e'}\in GL_n(\mathbf{Z})$, alors tous les vecteurs de e' sont dans $\mathcal{R}$, et tout vecteur de $\mathcal{R}$ a des coordonnées entières dans la base e' ; donc e' est une $\mathbf{Z}$-base de $\mathcal{R}$.
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 $\Delta(\mathcal{R})$.*
   Soit e' une autre $\mathbf{Z}$-base de $\mathcal{R}$. notons G (respectivement G') la matrice de coefficients (e_i,e_j) (resp. (e'_i,e'_j)). Alors $G'={}^tP_e^{e'}\,G\,P_e^{e'}$, d'où $\det(G')=\det(G)\,\det(P_e^{e'})^2=\det(G)$ puisque $P_e^{e'}\in GL_n(\mathbf{Z})$.

[2] On pourrait montrer que G est isomorphe à un sous-groupe de $O_2(\mathbf{R})$; comme on connaît les sous-groupes de $O_2(\mathbf{R})$ (ce sont les groupes cycliques et diédraux), et qu'on sait que l'ordre maximal d'un élément de G est 6, on voit que le cardinal de G ne peut en fait pas dépasser 12, qui est le cardinal du groupe diédral D_6.

[3] Le groupe multiplicatif de $\mathbf{F}_9$ est cyclique d'ordre 8 et est donc formé des 8 racines de X^8-1 ; une racine primitive huitième de 1 est donc algébrique de degré 2 sur $\mathbf{F}_3$, ce qui montre que Φ_8 doit se décomposer en deux facteurs irréductibles du second degré sur $\mathbf{F}_3$

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.
Soit e une $\mathbf{Z}$-base de $\mathcal{R}$. La fonction qui à $x \in E$ associe le maximum des valeurs absolues de ses coordonnées dans e est continue. Soit M le maximum de cette fonction sur le compact $B(a,r)$. Alors le cardinal de $B(a,r) \cap \mathcal{R}$ est majoré par $(2\lfloor M \rfloor + 1)^n$, où $\lfloor M \rfloor$ est la partie entière de M.

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 $\|v\| = m(\mathcal{R})$.*
D'après la question 3) appliquée à $B(0, m(\mathcal{R})+1)$, il y a un nombre fini de vecteurs u de $\mathcal{R}$ vérifiant $\|u\| \leq m(\mathcal{R})+1$. Donc la borne inférieure $m(\mathcal{R})$ est atteinte pour un $v \in \mathcal{R} \setminus \{0\}$, et par conséquent $m(\mathcal{R}) > 0$.

5. *On suppose $n \geq 2$ dans les questions 5-a, 5-b et 5-c. Soit $k \in \{1, \ldots, n-1\}$ et $(v_1, \ldots, v_k, e_{k+1}, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathcal{R}$. On pose $W_k = \langle v_1, \ldots, v_k \rangle$ 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.*
   Puisque $\langle e_{k+1}, \ldots, e_n \rangle$ est un supplémentaire de W_k et que π_k est la projection sur $W_k^\perp$ parallèlement à W_k, alors $(\pi_k(e_{k+1}), \ldots, \pi_k(e_n))$ est une base de $W_k^\perp$. Ces vecteurs sont dans $\pi_k(\mathcal{R})$ ainsi que leurs combinaisons linéaires à coefficients entiers, et tout vecteur de $\pi_k(\mathcal{R})$ est combinaison linéaire à coefficients entiers de $\pi_k(e_{k+1}), \ldots, \pi_k(e_n)$. Donc $\pi_k(\mathcal{R})$ est un réseau de $W_k^\perp$ et $(\pi_k(e_{k+1}), \ldots, \pi_k(e_n))$ en est une $\mathbf{Z}$-base.

   (b) *Montrer qu'il existe un vecteur v_{k+1} du réseau $\mathcal{R}$ vérifiant*

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

   Soit w de $\pi_k(\mathcal{R})$ tel que $\|w\| = m(\pi_k(\mathcal{R}))$. Un tel vecteur existe d'après 4). On peut prendre pour v_{k+1} un vecteur de $\mathcal{R}$ tel que $\pi_k(v_{k+1}) = w$.

   (c) *Montrer qu'il existe une famille $(f_{k+2}, \ldots, f_n)$ de E telle que la famille $(v_1, \ldots, v_{k+1}, f_{k+2}, \ldots, f_n)$ est une $\mathbf{Z}$-base de $\mathcal{R}$. (On pourra montrer que $\pi_k(v_{k+1})$ est un vecteur primitif du réseau $\pi_k(\mathcal{R})$.)*
   Si $\pi_k(v_{k+1})$ n'était un vecteur primitif du réseau $\pi_k(\mathcal{R})$, il existerait un vecteur x de $\pi_k(\mathcal{R})$ et un entier $d > 1$ tel que $\pi_k(v_{k+1}) = d\,x$. Alors on aurait $\|x\| = \dfrac{1}{d}\, m(\pi_k(\mathcal{R})) < m(\pi_k(\mathcal{R}))$, contrairement à la définition de $m(\pi_k(\mathcal{R}))$. Donc $\pi_k(v_{k+1})$ n'était un vecteur primitif du réseau $\pi_k(\mathcal{R})$, et on peut le compléter en une $\mathbf{Z}$-base $(\pi_k(v_{k+1}), w_{k+2}, \ldots, w_n)$ de ce réseau. Soient f_i des vecteurs de $\mathcal{R}$ tels que $\pi_k(f_i) = w_i$ pour $i = k+2, \ldots, n$. Alors $(v_1, \ldots, v_{k+1}, f_{k+2}, \ldots, f_n)$ est une $\mathbf{Z}$-base de $\mathcal{R}$. Il suffit de vérifier que tout vecteur x de $\mathcal{R}$ est bien combinaison linéaire à coefficients entiers de $v_1, \ldots, v_{k+1}, f_{k+2}, \ldots, f_n$. Or il y a des entiers $a_{k+1}, \ldots, a_n$ tels que $\pi_k(x) = a_{k+1}\pi_k(v_{k+1}) + \sum_{i=k+2}^n a_i \pi_k(f_i)$; donc $x - (a_{k+1}v_{k+1} + \sum_{i=k+2}^n a_i f_i$ appartient à $W_k \cap \mathcal{R}$, et il s'écrit $\sum_{i=1}^k a_i v_i$ avec $a_i \in \mathbf{Z}$.

   (d) *En déduire qu'il existe une $\mathbf{Z}$-base $(v_1, \ldots, v_n)$ de $\mathcal{R}$ vérifiant $\|v_1\| = m(\mathcal{R})$ et*

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

   où l'on note π_k la projection orthogonale sur $\langle v_1, \ldots, v_k \rangle^\perp$. Une telle base est appelée base réduite du réseau $\mathcal{R}$.
   On construit, par récurrence sur k pour $k = 1, \ldots, n$, une $\mathbf{Z}$-base $(v_1, \ldots, v_k, e_{k,k+1}, \ldots, e_{k,n})$ vérifiant $\|v_1\| = m(\mathcal{R})$ et $\forall \ell \in \{1, \ldots, k-1\}$ $\|\pi_\ell(v_{\ell+1})\| = m(\pi_\ell(\mathcal{R}))$. L'initialisation se fait en complétant un vecteur v_1 de $\mathcal{R}$ vérifiant $\|v_1\| = m(\mathcal{R})$ (forcément primitif par le raisonnement de c)) en une $\mathbf{Z}$-base de $\mathcal{R}$. Le pas de récurrence est fourni par b) et c).

(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* $\mathcal{R}_1$.
Par l'identification de $\mathbf{R}^2$ à $\mathbf{C}$, on a $e = (1, j)$ où $j = e^{2i\pi/3}$. Le carré de la norme d'un élément $a + bj$ de $\mathcal{R}_1$ (où $(a,b) \in \mathbf{Z}^2$) est $(a+bj)(a+bj^2) = a^2 + b^2 - ab \in \mathbf{N}$. Donc 1 est bien un vecteur non nul de plus petite norme dans $\mathcal{R}_1$; l'orthogonal de $\langle 1 \rangle$ est l'axe imaginaire, et j est bien un vecteur de $\mathcal{R}_1$ de plus petite partie imaginaire non nulle.

6. *On suppose* $n \geq 2$ *dans les questions 6-a, 6-b et 6-c. Soit* $e = (e_1, \ldots, e_n)$ *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* $\{2, \ldots, n\}^2$ *on a*

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

Pour $j = 2, \ldots, n$ on a la formule de la projection orthogonale :

$$e_j = \pi_1(e_j) + \frac{1}{\|e_1\|^2} (e_1, e_j)\, e_1 .$$

De là on peut calculer (e_j, e_k) :

$$(e_j, e_k) = (\pi_1(e_j), \pi_1(e_k)) + \frac{1}{\|e_1\|^2} (e_1, e_j)(e_1, e_k) ,$$

ce qui donne bien la formule voulue puisque $\|e_1\| = m(\mathcal{R})$.
(b) *Montrer que* $\Delta(\mathcal{R}) = m(\mathcal{R})^2\, \Delta(\pi_1(\mathcal{R}))$.
Soit G' la matrice du produit scalaire dans la base $e' = (e_1, \pi_1(e_2), \ldots, \pi_1(e_n))$. Puisque e_1 est orthogonal aux autres vecteurs de cette base et que ces derniers forment une $\mathbf{Z}$-base de $\pi_1(\mathcal{R})$, on a $\det(G') = \|e_1\|^2\, \Delta(\pi_1(\mathcal{R}))$. Puisque la matrice $P_e^{e'}$ de changement de base de e à e' est triangulaire supérieure avec des 1 sur la diagonale et que $G' = {}^t P_e^{e'}\, G\, P_e^{e'}$, on a $\Delta(\mathcal{R}) = \det(G) = \det(G')$. Donc $\Delta(\mathcal{R}) = m(\mathcal{R})^2\, \Delta(\pi_1(\mathcal{R}))$.
(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*

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

C'est une conséquence immédiate de $\|v\|^2 = t^2\, \|e_1\|^2 + \|v'\|^2$ et du fait que $\|v\|^2 \geq m(\mathcal{R})^2 = \|e_1\|^2$.
(d) *En déduire l'inégalité de Hermite :*

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

Montrons d'abord que $m(\pi_1(\mathcal{R}))^2 \geq \dfrac{3}{4}\, m(\mathcal{R})^2$. Si v' est un vecteur de $\pi_1(\mathcal{R})$, alors on peut trouver $v \in \mathcal{R}$ tel que $v = te_1 + v'$ et on peut supposer $|t| \leq 1/2$, quitte à ajouter un multiple entier convenable de e_1. Si $v' \neq 0$, alors $v \neq 0$ et d'après le (c) on a $\|v'\|^2 \geq (1 - t^2)\, m(\mathcal{R})^2 \geq \dfrac{3}{4}\, m(\mathcal{R})^2$. On en déduit $m(\pi_1(\mathcal{R}))^2 \geq \dfrac{3}{4}\, m(\mathcal{R})^2$.
On peut maintenant démontrer l'inégalité de Hermite par récurrence sur n. Pour $n = 1$, on a bien sûr $m(\mathcal{R})^2 = \Delta(\mathcal{R})$. Supposons $n > 1$ et l'inégalité de Hermite démontrée jusqu'à la dimension $n - 1$. Par l'hypothèse de récurrence on a $(3/4)^{(n-1)(n-2)/2}\, m(\pi_1(\mathcal{R}))^{2(n-1)} \leq \Delta(\pi_1(\mathcal{R}))$. Donc

$$\begin{aligned} \Delta(\mathcal{R}) &= m(\mathcal{R})^2\, \Delta(\pi_1(\mathcal{R})) \geq (3/4)^{\frac{(n-1)(n-2)}{2}}\, m(\mathcal{R})^2\, m(\pi_1(\mathcal{R}))^{2(n-1)} \\ &\geq (3/4)^{\frac{(n-1)(n-2)}{2}+n-1}\, m(\mathcal{R})^{2n} = (3/4)^{\frac{n(n-1)}{2}}\, m(\mathcal{R})^{2n} , \end{aligned}$$

ce qui établit bien l'inégalité de Hermite.

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

   (a) *Montrer que $\eta_n \geq 1$.*

   On a surement pour un réseau $\mathcal{R}$ engendré par une base orthonormée $\Delta(\mathcal{R}) = m(\mathcal{R})^{2n}$. Ceci entraîne $\eta_n \geq 1$.

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

   On a $\eta_2 \leq \frac{2}{\sqrt{3}}$ par l'inégalité de Hermite. L'exemple du réseau $\mathcal{R}_1$ de la question 5-(e), pour lequel $m(\mathcal{R}_1) = 1$ et $\Delta(\mathcal{R}_1) = \frac{3}{4}$, montre que $\eta_2 \geq \frac{2}{\sqrt{3}}$. On a donc égalité.

III Cristalloïdes

On suppose dans cette partie $n \geq 2$. On note $O(E)$ le groupe orthogonal de E et $0(\mathcal{R})$ l'ensemble des isométries de E qui stabilisent $\mathcal{R}$. c'est à dire qui induisent une bijection de $\mathcal{R}$ sur $\mathcal{R}$. $0(\mathcal{R})$ 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 $(\mathcal{R}, F)$ 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.*

   Soit e une $\mathbf{Z}$-base de $\mathcal{R}$ et r le maximum des normes des vecteurs de e. On a montré qu'il n'y a qu'un nombre fini de vecteurs de $\mathcal{R}$ dans $B(0, r)$. Un élément g de $O(\mathcal{R})$ est entièrement déterminé par l'image par g des vecteurs de e, et ces images sont toutes dans $\mathcal{R} \cap B(0, r)$. Donc $O(\mathcal{R})$ est 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 $G = \psi_{e'}(\Gamma)$.*

   Soit $G = P^{-1}\,\psi_e(\Gamma)\,P$ un sous-groupe de $GL_n(\mathbf{Z})$ $\mathbf{Z}$-conjugué à $\psi_e(\Gamma)$, avec $P \in GL_n(\mathbf{Z})$. Soit e' la $\mathbf{Z}$-base de $\mathcal{R}$ telle que la matrice de passage de e à e' soit P. Alors $G = \psi_{e'}(\Gamma)$. Réciproquement, si e et e' sont deux $\mathbf{Z}$-bases de $\mathcal{R}$, alors la matrice de passage P de e à e' appartient à $GL_n(\mathbf{Z})$ et $\psi_{e'}(\Gamma) = P^{-1}\,\psi_e(\Gamma)\,P$, donc $\psi_{e'}(\Gamma)$ et $\psi_e(\Gamma)$ sont $\mathbf{Z}$-conjugués.

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.*

   Supposons que $u(\mathcal{R}) = \mathcal{R}'$ et $u\Gamma u^{-1} = \Gamma'$ avec $u \in GL(E)$. Alors $u(e)$ est une $\mathbf{Z}$-base de $\mathcal{R}'$ et $\psi_e(\Gamma) = \psi_{u(e)}(\Gamma')$ est donc $\mathbf{Z}$-conjugué à $\psi_{e'}(\Gamma')$ d'après 3). Réciproquement, si $\psi_e(\Gamma) = P^{-1}\,\psi_{e'}(\Gamma')\,P$ avec $P \in GL(n, \mathbf{Z})$, soit f la $\mathbf{Z}$-base de $\mathcal{R}'$ telle que la matrice de passage de e' à f soit P ; on a $\psi_f(\Gamma') = \psi_e(\Gamma)$. Alors l'élément $u \in GL(E)$ qui envoie e sur f vérifie $u(\mathcal{R}) = \mathcal{R}'$ et $\Gamma' = u\Gamma u^{-1}$.

   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$GL_n(\mathbf{Z})$.*

   Les questions précédentes ont permis de montrer que ψ est bien définie et injective. Il reste à voir que tout sous-groupe fini G de $GL_n(\mathbf{Z})$ est de la forme $\psi_e(\Gamma)$ pour e une $\mathbf{Z}$ base d'un réseau $\mathcal{R}$ de E et Γ un sous-groupe de $O(\mathcal{R})$. Soit $(x, y) \mapsto x \cdot y$ le produit scalaire usuel sur $\mathbf{R}^n$ et définissons une

nouvelle forme bilinéaire symétrique b par $b(x,y) = \sum_{g\in G}(gx \cdot gy)$. Alors b est définie positive, et préservée par tout élément $g \in G$. Ainsi G est un sous-groupe du groupe orthogonal de b. Soit u une isométrie de $(\mathbf{R}^n, b)$ sur l'espace euclidien E, e l'image par u de la base canonique de $\mathbf{R}^n$, $\mathcal{R}$ l'image par u de $\mathbf{Z}^n$ et $\Gamma = uGu^{-1}$. Alors $(\mathcal{R}, \Gamma)$ est un cristalloïde, e une $\mathbf{Z}$-base de $\mathcal{R}$, et $G = \psi_e(\Gamma)$.

5. *En déduire que $GL_2(\mathbf{Z})$ possède un sous-groupe isomorphe au groupe diédral D_6.*
   Reprenons le réseau $\mathcal{R}_1$ engendré par 1 et j dans $\mathbf{C}$ avec sa structure euclidienne (question II-5-(e)). Le groupe $O(\mathcal{R}_1)$ a un sous-groupe isomorphe à D_6, engendré par la rotation d'angle $\pi/3$ (qui envoie 1 sur $1+j$ et j sur -1) et par la symétrie par rapport à l'axe réel (qui envoie j sur $-j-1$). En écrivant les matrices des isométries de ce sous-groupe dans la $\mathbf{Z}$-base $(1, j)$ de $\mathcal{R}_1$, on obtient un sous-groupe fini de $GL_2(\mathbf{Z})$ isomorphe à D_6, engendré par $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ d'ordre 6 et $\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ d'ordre 2.[4]

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 $p \geq 1$. 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 $m_b(\mathcal{R}) = b(v,v)^{1/2}$.*
   Soit $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathcal{R}$ et $d \in \mathbf{N}^*$ un dénominateur commun des $b(e_i, e_j) \in \mathbf{Q}$. Alors, pour tout $x \in \mathcal{R}$, on a $b(x,x) \in \frac{1}{d}\,\mathbf{Z}$, et donc la borne inférieure $m_b(\mathcal{R})$ est atteinte pour un $v \in \mathcal{R}$ tels que $b(v,v) > 0$ (et donc forcément$v \neq 0$).

   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'.*
   On voit la signature de b' en comptant les $+$ et les $-$ sur la diagonale de la matrice de b' dans une base orthogonale de W. En ajoutant v à cette base, on obtient une base orthogonale de E et on sait que la signature de b est (p,q) et que $b(v,v) > 0$. Donc la signature de b' est $(p-1, q)$.

   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*

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

[4] Le « En déduire » de la question 5 ne paraît pas justifié ; en effet, on obtient cette copie de D_6 dans $GL_2(\mathbf{Z})$ en utilisant juste ce qui est dit dans le préambule de cette section, et en aucune façon les résultats des questions précédentes. En particulier, la surjectivité de ψ qui est le point clé de la question 4, et qui repose sur le fait classique que tout sous-groupe fini de $GL_n(\mathbf{R})$ est conjugué à un sous-groupe de $O_n(\mathbf{R})$, ne joue aucun rôle.

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

L'inégalité est en fait une égalité si $n = p = 1$. Supposons pour le reste de cette question $n \geq 2$. Notons π la projection orthogonale sur W parallèlement à $\langle v \rangle$. Le calcul fait en II-6-(a) et (b) se copie exactement en remplaçant le produit scalaire par la forme b, et on obtient

$$(*) \qquad \Delta_b(\mathcal{R}) = m_b(\mathcal{R})^2 \, \Delta_{b'}(\pi(\mathcal{R})) \; .$$

(Note : l'hypothèse $p \geq 1$ ne joue pas de rôle dans la définition de Δ_b et on peut bien considérer $\Delta_{b'}$).

On procède maintenant par récurrence sur p. Considérons d'abord le cas $p = 1$. Alors b' est définie négative, et on peut appliquer l'inégalité de Hermite dans l'espace euclidien $(W, -b')$ (de dimension $q = n - 1$) pour le réseau $\pi(\mathcal{R})$. On obtient

$$|\Delta_{b'}(\pi(\mathcal{R}))| = \Delta_{-b'}(\pi(\mathcal{R})) \geq \left(\frac{3}{4}\right)^{\frac{q(q-1)}{2}} \, m_{-b'}(\pi(\mathcal{R}))^{2q} \; ,$$

et, en utilisant $(*)$,

$$|\Delta_b(\mathcal{R})| \geq \left(\frac{3}{4}\right)^{\frac{q(q-1)}{2}} \, m_{-b'}(\pi(\mathcal{R}))^{2q} \, m_b(\mathcal{R})^2 = \left(\frac{3}{4}\right)^{\frac{n(n-1)}{2}} \, \frac{4^q \, m_{-b'}(\pi(\mathcal{R}))^{2q}}{3^q} \, m_b(\mathcal{R})^2 \; .$$

comme l'inégalité à établir s'écrit

$$|\Delta_b(\mathcal{R})| \geq \left(\frac{3}{4}\right)^{\frac{n(n-1)}{2}} \, \frac{m_b(\mathcal{R})^{2n}}{3^q}$$

on voit qu'il suffit de montrer $4\, m_{-b'}(\pi(\mathcal{R}))^2 \geq m_b(\mathcal{R})^2$. Soit $w' \in \pi(\mathcal{R}) \setminus \{0\}$. Il existe $w \in \mathcal{R}$ tel que $w = w' + tv$, et quitte à ajouter un multiple entier de v on peut supposer $1/2 \leq t \leq 1$. On obtient $b(w, w) = b'(w', w') + t^2 \, b(v, v)$. On sait que $b'(w', w') < 0$ et donc $b(w, w) < b(v, v)$ ne peut pas être strictement positif par définition de v. Ainsi $-b'(w', w') \geq t^2 \, b(v, v) \geq \frac{1}{4} \, m_b(\mathcal{R})^2$. Ceci entraîne

$$4\, m_{-b'}(\pi(\mathcal{R}))^2 \geq m_b(\mathcal{R})^2$$

et donc l'inégalité de Hermite-Minkowski est établie pour $p = 1$.

Supposons maintenant $p > 1$ et l'inégalité de Hermite-Minkowski établie pour $p - 1$. On montre comme en II-6-(d) que

$$m_{b'}(\pi(\mathcal{R}))^2 \geq \frac{3}{4} \, m_b(\mathcal{R})^2 \; ,$$

et l'égalité $(*)$ avec l'hypothèse de récurrence permettent d'établir l'inégalité de Hermite-Minkowski pour p.

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*

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

   Soit $w' \in \mathcal{R}'$. On a $w' = \pi(w)$ pour un $w \in \mathcal{R}$, et donc

$$w' = w - \frac{b(w, v)}{b(v, v)}\, v \ .$$

   Par conséquent $m_b(\mathcal{R})^2 w' = m_b(\mathcal{R})^2 w - b(w, v)v$ appartient à $\mathcal{R}$ puisque $m_b(\mathcal{R})^2$ et $b(w, v)$ sont entiers. Ceci montre $\mathcal{R}'' \subset \mathcal{R}$. Puisque b' est la restriction de b et qu'on a $b(x, y) \in \mathbf{Z}$ pour tout $(x, y) \in \mathcal{R}^2$, on a $b'(x, y) \in \mathbf{Z}$ pour tout $(x, y) \in \mathcal{R}''^2$.

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

   On a l'égalité $\Delta_b(\mathcal{R}) = m_b(\mathcal{R})^2\, \Delta_{b'}(\mathcal{R}')$ et, si $\Delta_b(\mathcal{R})$ est fixé, l'entier $m_b(\mathcal{R})^2$ ne peut prendre qu'un nombre fini de valeurs d'après l'inégalité de Hermite-Minkowski. Donc $\Delta_{b'}(\mathcal{R}')$ ne peut prendre qu'un nombre fini de valeurs. Puisque $\mathcal{R}'' = m_b(\mathcal{R})^2\, \mathcal{R}'$, on a $\Delta_{b'}(\mathcal{R}'') = (m_b(\mathcal{R})^4)^{n-1}\, \Delta_{b'}(\mathcal{R}')$ (chacun des coefficients de la matrice dont le déterminant calcule le discriminant est multiplié par $m_b(\mathcal{R})^4$. Donc, si on fixe $\Delta_b(\mathcal{R})$, $\Delta_{b'}(\mathcal{R}'')$ ne peut prendre qu'un nombre fini de valeurs.

   Bien que ce ne soit pas demandé par l'énoncé, il est important pour la suite de remarquer que le résultat vaut aussi pour les formes b de signature $(0, q)$, c.-à-d. les formes définies négatives. En effet, on peut alors appliquer le raisonnement précédent aux formes définies positives $-b$ et $-b'$, en remarquant que $\Delta_{-b}(\mathcal{R}) = (-1)^n \Delta_b(\mathcal{R})$ et $\Delta_{-b'}(\mathcal{R}'') = (-1)^{n-1} \Delta_{b'}(\mathcal{R}'')$.

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*

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

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

   Soit $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathcal{R}_1$; on a $y \in \mathcal{C}(\mathcal{R}_1)$ si et seulement si $b(e_i, y) \in \mathbf{Z}$ pour tout $i \in \{1, \ldots, n\}$. Soit $e^* = (e_1^*, \ldots, e_n^*)$ la base duale de E^*. Puisque b est non dégénérée, pour tout $i \in \{1, \ldots, n\}$, il existe un unique vecteur f_i tel que la forme linéaire $b(\cdot, f_i)$ soit égale à e_i^*, et $f = (f_1, \ldots, f_n)$ est une base de E. Soit $y = \sum_{i=1}^n a_i f_i$ un vecteur de E. On a

$$b(x, y) = \sum_{i=1}^{n} a_i\, b(x, f_i) = \sum_{i=1}^{n} a_i\, e_i^*(x) \ ,$$

   et en particulier $b(e_j, y) = a_j$. Donc $\mathcal{C}(\mathcal{R}_1)$ est le réseau de E engendré par la $\mathbf{Z}$-base f.

   Pour toute extension $\mathcal{R}_2$ de $\mathcal{R}_1$, on a $b(x, y) \in \mathbf{Z}$ pour tout $x \in \mathcal{R}_1$ et tout $y_i n \mathcal{R}_2$. Donc $\mathcal{R}_2 \subset \mathcal{C}(\mathcal{R}_1)$.

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

Reprenons les notations de la solution de la question précédente. La matrice de passage de la base f à la base e est à coefficients entiers puisque $\mathcal{R}_1 \subset \mathcal{C}(\mathcal{R}_1)$. Donc son inverse est à coefficients rationnels ; soit d un dénominateur commun des coefficients de cet inverse. Alors $d\,\mathcal{C}(\mathcal{R}_1) \subset \mathcal{R}_1$, et l'ensemble des vecteurs $\sum_{i=1}^{n} a_i f_i$ avec $a_i \in \{0, \ldots, d-1\}$ contient un système de représentants de $\mathcal{C}(\mathcal{R}_1)/\mathcal{R}_1$. Par conséquent le cardinal de ce quotient est inférieur ou égal à d^n.

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

   Montrons la propriété par récurrence sur n. Pour $n = 1$, $\mathcal{R}$ est engendré par un vecteur e_1 et $b(e_1, e_1) = \Delta_b(\mathcal{R})$; si l'on fixe $\Delta \in \mathbf{Z}$, il n'y a qu'une seule classe d'équivalence de groupe libre quadratique de rang 1 et de discriminant Δ.

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.