1e épreuve agrégation interne 2012 - Corrigé

Michel Coste *

13 août 2012

A

1. (a) Si $M \in \mathcal{M}_n(\mathbf{Z})$ est inversible et $M^{-1} \in \mathcal{M}_n(\mathbf{Z})$ alors $\det(M)\,\det(M^{-1}) = 1$ et comme $\det(M)$ et $\det(M^{-1})$ sont entiers on a $\det(M) = \pm 1$.

   (b) Si $M \in \mathcal{M}_n(\mathbf{Z})$, tout mineur extrait de M est entier, donc la comatrice $\mathrm{com}(M)$ est à coeffcients entiers. Si de plus $\det(M) = \pm 1$, alors M est inversible et

$$M^{-1} = \frac{1}{\det(M)}\,{}^t\mathrm{com}(M)$$

   est à coefficients entiers, donc M appartient à $\mathrm{GL}_n(\mathbf{Z})$.

   (c) det est un homomorphisme de $(\mathrm{GL}_n(\mathbf{R}), \times)$ dans $(\mathbf{R}^*, \times)$ et $\mathrm{GL}_n(\mathbf{Z})$ qui est l'image réciproque par det du sous-groupe $\{\pm 1\}$ de $\mathbf{R}^*$ est un sous-groupe de $(\mathrm{GL}_n(\mathbf{R})$.

2. Λ contient 0, est stable par addition et passage à l'opposé.

3. Soit Λ' le réseau défini par $\mathcal{B}'$. La matrice de passage P de $\mathcal{B}$ à $\mathcal{B}'$ est à coefficients entiers si et seulement si $\Lambda' \subset \Lambda$. Comme la matrice de passage inverse est P^{-1}, on a $\Lambda' = \Lambda$ si et seulement si $P \in \mathrm{GL}_n(\mathbf{Z})$.

4. (a) D'après Bézout, il existe des entiers u, v tels que $au + bv = 1$. Posons $y = -v\varepsilon_1 + u\varepsilon_2$. Le déterminant de (x, y) dans la base canonique de $\mathbf{R}^2$ est 1, donc d'après la question 3 (x, y) est une $\mathbf{Z}$-base du réseau $\mathbf{Z}^2$.

   (b) La calcul d'une identité de Bézout par l'algorithme d'Euclide étendu donne $1 = 33\times 49 - 16\times 101$. Prendre $y = 33\,\varepsilon_1 + 16\,\varepsilon_2$.

   (c) L'algorithme d'Euclide étendu avec comme entrée a et b s'initialise avec $r_0 = a$, $r_1 = b$, $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$. Pour $n \geq 1$ et tant que $r_n \neq 0$ on pose r_{n+1} = le reste de la division euclidienne de r_{n-1} par r_n, soit

$$r_{n-1} = r_n q_n + r_{n+1} \quad \text{avec } 0 \leq r_{n+1} < |r_n|$$

   et $u_{n+1} = u_{n-1} - q_n u_n$, $v_{n+1} = v_{n-1} - q_n v_n$. L'algorithme s'arrête au bout d'un nombre fini N d'étapes avec $r_{N+1} = 0$. Alors r_N est le pgcd de a et b et on a $r_N = u_N a + v_N b$.

   (d) $(e_1 = \varepsilon_1 + \varepsilon_2,\ e_2 = 3\varepsilon_2)$ est une $\mathbf{Z}$-base de Λ. Les deux vecteurs forment une base de $\mathbf{R}^2$, sont dans Λ et si $x = x_1\varepsilon_1 + x_2\varepsilon_2 \in \Lambda$, alors $x = x_1 e_1 + \dfrac{x_2 - x_1}{3}\, e_2$ est bien combinaison linéaire à coefficients entiers de e_1 et e_2

5. Si $\mathcal{B}'$ est une autre $\mathbf{Z}$-base de Λ (ce qui entraîne $\det_{\mathcal{B}}(\mathcal{B}') = \pm 1$ d'après 3) et Ω' une autre b.o.n. de E (ce qui entraîne $\det_{\Omega'}(\Omega) = \pm 1$, la matrice de changement de base étant orthogonale), alors

$$\det_{\Omega'}(\mathcal{B}') = \det_{\mathcal{B}}(\mathcal{B}')\,\det_{\Omega}(\mathcal{B})\,\det_{\Omega'}(\Omega) = \pm \det_{\Omega}(\mathcal{B})\ ,$$

   ce qui montre que $|\det_{\Omega}(\mathcal{B})|$ ne dépend que de Λ.

6. (a) Soit M le maximum de la fonction continue $x \mapsto \max_i |x_i|$ sur la sphère unité de E (qui est compacte). Alors, en posant $A = 1/M > 0$ on a, pour tout x de E, $A \max_i |x_i| \leq \|x\|$.

   (b) On a donc $\{x \in \Lambda,\ \|x\| \leq R\} \subset \{x \in \Lambda,\ \max_i |x_i| \leq R/A\}$ et ce dernier ensemble a $(2\lfloor R/A \rfloor + 1)^n$ éléments.

*remarques et questions bienvenues à michel.coste@univ-rennes1.fr

(c) On choisit $x_1 \in \Lambda$. Alors $U = \{x \in \Lambda,\ \|x\| \leq \|x_1\|\}$ est fini d'après (b). Puisque $m(\Lambda) = \min_{x\in U, x\neq 0} \|x\|$, il existe $x_0 \in U \setminus \{0\}$ tel que $m(\Lambda) = \|x_0\|$.

(d) Comme $S(\Lambda) \subset U$ (avec la notation de (c)), $S(\Lambda)$ est fini. Il est non vide par (c) et puisque $x \in S(\Lambda) \Leftrightarrow -x \in S(\Lambda)$, le cardinal de $S(\Lambda)$ est pair.

7. Soit $L = \mathrm{Vect}_{\mathbf{Q}}(e_1, \ldots, e_n)$; c'est un espace vectoriel de dimension n sur $\mathbf{Q}$. Puisque $e_i \in \mathrm{Vect}_{\mathbf{Q}}(u_1, \ldots, u_k)$ pour $i = 1, \ldots, n$, $(u_1, \ldots, u_k)$ engendre L sur $\mathbf{Q}$ et aussi E sur $\mathbf{R}$.
Par ailleurs, supposons $\sum_{i=1}^{k} \lambda_i u_i = 0$ avec $\lambda_i \in \mathbf{Q}$ pour $i = 1, \ldots, k$. Soit d un dénominateur commun pour les λ_i ; alors les $d\lambda_i$ sont tous nuls par unicité de l'écriture de 0 comme combinaison linéaire à coefficients entiers des u_i et donc les λ_i sont tous nuls. Ainsi la famille $(u_1, \ldots, u_k)$ est libre sur $\mathbf{Q}$, c'est donc une base de L sur $\mathbf{Q}$, d'où $k = n$. Comme $(u_1, \ldots, u_n)$ engendre E qui est de dimension n, c'est une base de E et donc une $\mathbf{Z}$-base de Λ.

8. Soit $x \in D_1 \cap \Lambda$. Comme x est combinaison linéaire à coefficients entiers des $e_1, \ldots, e_n$ et que $(e_1, \ldots, e_n)$ est une base de E, on a $x = ae_1$ pour un certain entier a. Réciproquement, tout élément de $\mathbf{Z}e_1$ appartient à $D_1 \cap \Lambda$.
La projection p est une surjection de E sur F de noyau D_1. L'image par p de la base $(e_1, \ldots, e_n)$ engendre donc F et , comme $p(e_1) = 0$, $(p(e_2), \ldots, p(e_n))$ engendre F. Puisque F est de dimension $n-1$, $(p(e_2), \ldots, p(e_n))$ est une base de f. Comme

$$\Lambda' = \{p(\sum_{i=1}^{n} x_i e_i),\ (x_1, \ldots, x_n) \in \mathbf{Z}^n\} = \{\sum_{i=2}^{n} x_i p(e_i),\ (x_2, \ldots, x_n) \in \mathbf{Z}^{n-1}\}\ ,$$

Λ' est un réseau de F de $\mathbf{Z}$-base $(p(e_2), \ldots, p(e_n))$.
Soit $(u'_2, \ldots, u'_n)$ une $\mathbf{Z}$-base de Λ' et $u_2, \ldots, u_n \in \Lambda$ tels que $p(u_i) = u'_i$. Soit $x \in \Lambda$. Il existe un unique $(a_2, \ldots, a_n) \in \mathbf{Z}^{n-1}$ tels que $p(x) = \sum_{i=2}^{n} a_i u'_i$. Alors $x - \sum_{i=2}^{n} a_i u_i \in D_1 \cap \Lambda$ est de la forme $a_1 e_1$ avec $a_1 \in \mathbf{Z}$, et $x = a_1 e_1 + \sum_{i=2}^{n} a_i u_i$. Cette écriture est unique car si $x = b_1 e_1 + \sum_{i=2}^{n} b_i u_i$, alors $p(x) = \sum_{i=2}^{n} b_i u'_i$ d'où $b_i = a_i$ pour $i = 2, \ldots, , n$ et par suite $b_1 = a_1$. D'après 7, $(e_1, u_2, \ldots, u_n)$ est une $\mathbf{Z}$-base de Λ.

9. (a) φ_1 induit un morphisme de groupe additif de Λ dans $\mathbf{Z}$. L'image par φ_1 de G est donc un sous-groupe additif de $\mathbf{Z}$, de la forme $a_1\mathbf{Z}$ pour un certain entier a_1.

(b) Si $n = 1$, φ_1 est un isomorphisme linéaire, donc $a_1 \neq 0$ puisque $G \neq \{0\}$ et $\varphi_1^{-1}(a_1)$ est une base de E et une $\mathbf{Z}$-base de G, qui est un réseau de E.

(c) On a $\Lambda_1 = \Lambda \cap F_1$ et donc $H = G \cap F_1 = G \cap \Lambda_1$ est intersection de deux sous-groupes de Λ. C'est donc un sous-groupe de Λ_1 (et de G).

(d) Soit $x \in G$. Si $x = mb + v$ avec $m \in \mathbf{Z}$ et $v \in H$, alors $\varphi_1(x) = ma_1$. Puisque $a_1 \neq 0$, m est unique et $v = x - mb$ aussi. Par ailleurs si on prend pour m l'unique entier tel que $\varphi_1(x) = ma_1$ alors $v = x - mb \in \ker(\varphi_1) \cap G = H$. Il existe bien un unique couple $(m, v) \in \mathbf{Z} \times H$ tel que $x = mb + v$.

(e) Montrons par récurrence sur $n = \dim(E)$ que si G est un sous-groupe non nul de Λ, alors il existe un sous-espace vectoriel F de E tel que G soit un réseau de F. La cas $n = 1$ a été vu en (b). Supposons $n > 1$ et le résultat démontré pour $n - 1$. On utilise les notations de (c) et (d). Si $G \subset F_1$, alors G est un sous-groupe du réseau Λ_1 de F_1 et on peut appliquer l'hypothèse de récurrence. Si $G \not\subset F_1$, alors $a_1 \neq 0$. Si $H = \{0\}$ alors $G = \mathbf{Z}b$ est un réseau de la droite vectorielle engendrée par b. Si $H \neq \{0\}$, alors par l'hypothèse de récurrence c'est un réseau d'un sous-espace vectoriel L de F_1, de $\mathbf{Z}$-base $(f_2, \ldots, f_d)$; on en déduit que $(b, f_2, \ldots, f_d)$ est une base du sous-espace $F = \mathbf{R}b \oplus L$ et d'après (d) c'est une $\mathbf{Z}$-base du réseau G de F.
L'unicité de F est claire car $F = \mathrm{Vect}_{\mathbf{R}}(G)$.

10. (a) Puisque $0 < \|\frac{1}{k}\, b\| = \frac{1}{k}\|b\| < m(\Lambda)$, on a $\frac{1}{k}\, b \notin \Lambda$.

(b) Le (a) montre que $r_1, \ldots, r_n$ sont premiers dans leur ensemble, donc (Bézout) il existe $(s_1, \ldots, s_n) \in \mathbf{Z}^n$ tels que $\sum_{i=1}^{n} r_i s_i = 1$.

(c) f induit un homomorphisme du groupe additif Λ dans $\mathbf{Z}$, dont l'image est un sous-groupe de $\mathbf{Z}$ qui contient 1 par (b). Donc $f(\Lambda) = \mathbf{Z}$. Le noyau $H = \ker(f) \cap \Lambda$ de la restriction $f|_\Lambda$ est un sous groupe de Λ. Soit x un élément de Λ. Si $x = ab + u$ avec $a \in \mathbf{Z}$ et $u \in H$, alors $f(x) = a$ et $u = x - ab$, ce qui montre l'unicité. Comme $x - f(x)b$ appartient bien à H, tout $x \in \Lambda$ s'écrit de façon unique sous la forme $x = ab + u$ avec $u \in H$ et $a \in \mathbf{Z}$.

(d) Dans le cas $n = 1$ on utilise que $\Lambda = \mathbf{Z}b$. Supposons $n > 1$. Alors H est un sous-groupe non nul de Λ, et donc un réseau d'un sous-espace F de E d'après 9. Soit $b_2, \dots, b_k$ une $\mathbf{Z}$-base de H. D'après (c), tout élément de Λ est de manière unique combinaison linéaire à coefficients entiers de $b, b_2, \dots, b_k$. D'après 7, $k = n$ et $(b, b_2, \dots, b_n)$ est une $\mathbf{Z}$-base de Λ.

(e) Puisque F est un supplémentaire de $\mathbf{R}b$ et que p est la projection sur F parallèlement à $\mathbf{R}b$, $p(\Lambda)$ est un réseau de F par application directe de 8.

B Réseaux et matrices de Gram

1. $e_i \cdot e_j$ est bien le produit ligne-colonne de la i-ème ligne de ${}^tM$ par la j-ème colonne de M. Donc $G = {}^tM\,M$. Donc $\det(G) = \det(M)^2$, et $\mathcal{E}$ est une base de E si et seulement si $\det(M) \neq 0$ si et seulement si $\det(G) \neq 0$.
2. On a $\det(\Lambda)^2 = \det_\Omega(\mathcal{E})^2 = \det(G)$ par (a).
3. La matrice dont les colonnes sont les coeffcients de $b_1, \dots, b_n$ dans $\mathcal{E}$ est à coefficients entiers et
$$|\det_{\mathcal{E}}(\mathcal{B})| = |\det_\Omega(\mathcal{B})|/|\det_\Omega(\mathcal{E})| = |\det_\Omega(\mathcal{B})|/\det(\Lambda)\ .$$
D'après A.3, $\mathcal{B}$ est une $\mathbf{Z}$-base de Λ si et seulement si $|\det_{\mathcal{E}}(\mathcal{B})| = 1$, c.-à-d. si et seulement si $|\det_\Omega(\mathcal{B})| = \det(\Lambda)$.
4. (a) Soit $\mathcal{B} = (b_1, \dots, b_n)$ une $\mathbf{Z}$-base de Λ. Si u est une isométrie de E sur F qui envoie Λ sur Λ', alors $(u(b_1), \dots, u(b_n))$ est une $\mathbf{Z}$-base de Λ' qui a même matrice de Gram que $\mathcal{B}$.
Réciproquement, si $\mathcal{B}' = (b'_1, \dots, b'_n)$ est une $\mathbf{Z}$-base de Λ' qui a même matrice de Gram G que $\mathcal{B}$, alors l'isomorphisme linéaire $u : E \to F$ défini par $u(b_i) = b'_i$ pour $i = 1, \dots, n$ vérifie $u(\Lambda) = \Lambda'$ et est une isométrie. En effet si X est le vecteur colonne des coordonnées de $x \in E$ dans la base $\mathcal{B}$, c'est aussi le vecteur colonne des coordonnées de $u(x)$ dans $\mathcal{B}'$ et on a $\|x\|^2 = {}^tX\,G\,X = \|u(x)\|^2$.

   (b) Il existe une similitude de rapport $\lambda > 0$ envoyant Λ sur Λ' si et seulement s'il existe une isométrie envoyant $\lambda\Lambda$ sur Λ' si et seulement s'il existe une $\mathbf{Z}$-base de $\lambda\Lambda$ et une $\mathbf{Z}$-base de Λ' ayant des matrices de Gram égales (d'après (a)) si et seulement s'il existe une $\mathbf{Z}$-base $\mathcal{B}$ de Λ de matrice de Gram G et une $\mathbf{Z}$-base $\mathcal{B}'$ de Λ' de matrice de Gram G' telles que $G' = \lambda^2 G$.

   (c) S'il existe une similitude s de rapport $\lambda > 0$ envoyant Λ sur Λ', alors $m(\Lambda') = \lambda\, m(\Lambda)$ et $\det(\Lambda') = \lambda^n \det(\Lambda)$. Donc $\Gamma_n(\Lambda') = \Gamma_n(\Lambda)$. Par ailleurs s envoie $S(\Lambda)$ sur $S(\Lambda')$, et donc ces deux ensembles ont même cardinal.

C Quelques exemples de réseaux

1. On a $\det(\mathbf{Z}^n) = 1$, $m(\mathbf{Z}^n) = 1$, $S(\mathbf{Z}^n) = \{\pm\varepsilon_i,\ i = 1, \dots, n\}$ et $\mathrm{Card}(S(\mathbf{Z}^n)) = 2n$.
2. (a) D_n est le noyau du morphisme de groupes $\mathbf{Z}^n \to \mathbf{Z}/2\mathbf{Z}$ défini par $(x_1, \dots, x_n) \mapsto x_1 + \cdots + x_n \bmod 2$. C'est donc un sous-groupe de $\mathbf{Z}^n$.

   (b) Les vecteurs $e_1, \dots, e_n$ sont dans D_n. Par ailleurs, si $x = (x_1, \dots, x_n) \in \mathbf{R}^n$, alors
$$x = x_n e_n + (x_n + x_{n-1})e_{n-1} + \cdots + (x_n + \cdots + x_3)e_3 + \frac{x_n + \cdots + x_2 - x_1}{2}\, e_2 + \frac{x_n + \cdots + x_2 + x_1}{2}\, e_1\ .$$
Cette formule montre que $\mathcal{B} = (e_1, \dots, e_n)$ est un système générateur, et donc une base, de $\mathbf{R}^n$. Elle montre aussi que tout $x \in D_n$ est combinaison linéaire à coefficients entiers de $e_1, \dots, e_n$. Donc D_n est un réseau de $\mathbf{R}^n$ admettant $\mathcal{B}$ comme $\mathbf{Z}$-base.

   (c) Un vecteur non nul de D_n a au moins deux coordonnées entières non nulles et est donc de norme $\geq \sqrt{2}$. Comme $\|e_1\| = \sqrt{2}$, on a $m(D_n) = \sqrt{2}$. Les éléments de $S(D_n)$ sont les vecteurs ayant deux coordonnées de valeur absolue 1 et les autres nulles : $S(D_n) = \{\pm\varepsilon_i \pm \varepsilon_j,\ 1 \leq i < j \leq n\}$. Le cardinal de cet ensemble est $4 \times \binom{n}{2} = 2n(n-1)$.

   (d) Par développement suivant la première colonne,
$$\det_{\mathcal{E}_n} \mathcal{B} = \begin{vmatrix} 1 & -1 & 0 & \cdots & 0 \\ 1 & 1 & -1 & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & & \ddots & \ddots & -1 \\ 0 & \cdots & \cdots & 0 & 1 \end{vmatrix} = 1 + 1 = 2\ ,$$

donc $\det(D_n) = 2$.

(e) La matrice de Gram associée à $\mathcal{B}$ est $\begin{pmatrix} 2 & 0 & -1 & 0 & \cdots & 0 \\ 0 & 2 & -1 & 0 & & \vdots \\ -1 & -1 & 2 & -1 & \ddots & \vdots \\ 0 & 0 & -1 & 2 & \ddots & 0 \\ \vdots & & \ddots & \ddots & \ddots & -1 \\ 0 & \cdots & \cdots & 0 & -1 & 2 \end{pmatrix}$.

(f) D_2 admet pour $\mathbf{Z}$-base $(\varepsilon_1 + \varepsilon_2, -\varepsilon_1 + \varepsilon_2)$. La similitude directe d'angle $\pi/4$ et de rapport $\sqrt{2}$ envoie $\mathbf{Z}^2$ sur D_2.

(g) Pour $n \geq 3$, on a $2n(n-1) > 2n$ et donc $S(D_n)$ et $S(\mathbf{Z}^n)$ ont des cardinaux différents. Ceci entraîne que D_n n'est pas semblable à $\mathbf{Z}^n$.

3. (a) $\mathcal{B}$ est une base du plan H. Les vecteurs $e_1 = \varepsilon_2 - \varepsilon_1$ et $e_2 = \varepsilon_2 - \varepsilon_3$ sont dans A_2. Tout vecteur $x = x_1\varepsilon_1 + x_2\varepsilon_2 + x_3\varepsilon_3$ de A_2 est combinaison linéaire à coefficients entiers des vecteurs de $\mathcal{B}$: $x = -x_1 e_1 - x_3 e_2$. Donc A_2 est un réseau de H qui admet $\mathcal{B}$ pour $\mathbf{Z}$-base.

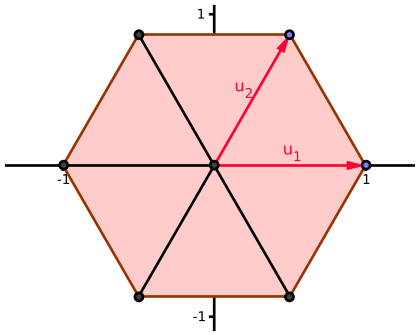
(b) La matrice de Gram associée à $\mathcal{B}$ est $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

(c) Un vecteur de A_2 non nul a au moins deux coordonnées entières non nulles et est donc de norme $\geq \sqrt{2}$. Comme $\|e_1\| = \sqrt{2}$, on a $m(A_2) = \sqrt{2}$. Les éléments de $S(A_2)$ ont deux coordonnées de valeur absolue 1 de signes opposés et la troisième nulle : $S(A_2) = \{\pm e_1, \pm e_2, \pm e_1 - e_2\}$, son cardinal est 6.

(d) i. A_2 et D_2 ne sont pas semblables car $S(A_2)$ et $S(D_2)$ n'ont pas même cardinal.

ii. La matrice de Gram de (u_1, u_2) est la moitié de la matrice de Gram de $\mathcal{B}$. Donc A_2 et Λ sont semblables, d'après B.4(b).

iii.



D

1. (a) Soit Ω la b.o.n. de E formé de $b_1/\|b_1\|$ et une b.o.n. Ω' de $(\mathbf{R}b_1)^\perp$. Puisque $p(u_i) = u_i - \frac{b_1 \cdot u_i}{\|b_1\|^2} b_1$, on a

$$\det_\Omega(b_1, u_2, \ldots, u_n) = \det_\Omega(b_1, p(u_2), \ldots, p(u_n)) = \|b_1\| \det_{\Omega'}(p(u_2), \ldots, p(u_n)) ,$$

d'où $\det(\Lambda) = \|b_1\| \det(\Lambda')$.

(b) Soit m un entier à distance minimum de α. On a $|m - \alpha| \leq \frac{1}{2}$, d'où $(m-\alpha)^2 \leq \frac{1}{4}$. Puisque $x_0, b_1 \in \Lambda$, $x = x_0 - mb_1$ appartient à Λ. On a $p(x) = p(x_0) - mp(b_1) = x'$ car $b_1 \in \ker(p)$. Par Pythagore,

$$\|x\|^2 - \|x'\|^2 = \|x - x'\|^2 = \|(\alpha - m)b_1\|^2 = (m-\alpha)^2\|b_1\|^2 .$$

En utilisant $(m-\alpha)^2 \leq \frac{1}{4}$ et $\|b_1\|^2 \leq \|x\|^2$ (car $x \in \Lambda$), il vient $\|x'\|^2 \geq \frac{3}{4}\|x\|^2$, c.-à-d. $\|x\|^2 \leq \frac{4}{3}\|x'\|^2$.

2. (a) Pour $n = 1$, $\Lambda = \mathbf{Z}u_1$ pour un vecteur non nul u_1 de la droite E et $\|u_1\|^2 = \det(\Lambda)^2$. Supposons $n > 1$ et le résultat établi pour $n-1$. Avec les notations de 1, par l'hypothèse de récurrence il existe une $\mathbf{Z}$-base $(u'_2, \ldots, u'_n)$ de Λ' telle que

$$\prod_{i=2}^{n} \|u'_i\|^2 \leq \left(\frac{4}{3}\right)^{(n-1)(n-2)/2} \det(\Lambda')^2 .$$

D'après 1(b), il existe des vecteurs $u_2, \dots, u_n$ de λ tels que $p(u_i) = u_i'$ et $\|u_i\|^2 \leq \frac{4}{3}\|u_i'\|^2$. D'après A.8, en posant $u_1 = b_1$, $(u_1, u_2, \dots, u_n)$ est une base de Λ et d'après 1(a) elle vérifie

$$\prod_{i=1}^{n} \|u_i\|^2 \leq \left(\frac{4}{3}\right)^{((n-1)(n-2)/2)+n-1} \|b_1\|^2 \det(\Lambda')^2 = \left(\frac{4}{3}\right)^{n(n-1)/2} \det(\Lambda)^2 .$$

3. (a) D'après C.3(b), le déterminant de la matrice de Gram pour A_2 est 3, donc d'après B.2 $\det(A_2) = \sqrt{3}$. On a $\Gamma_2(A_2) = m(A_2)^2/\det(A_2) = 2/\sqrt{3}$. Comme $\gamma_2 \leq \left(\frac{4}{3}\right)^{1/2} = 2/\sqrt{3}$, on en déduit $\gamma_2 = 2/\sqrt{3}$.

   (b) i. Transformer le réseau par une homothétie (cas particulier de similitude) ne change pas Γ_2. On peut choisir l'homothétie de rapport $1/m(\Lambda)$, ce qui permet de se ramener au cas où $m(\Lambda) = 1$.

   ii. Vu que $\Gamma_2(\Lambda) = 2/\sqrt{3}$, ceci entraîne $\det(\Lambda) = \sqrt{3}/2$. D'après 2(a), on a une $\mathbf{Z}$-base (u_1, u_2) de Λ telle que $\|u_1\|^2 \|u_2\|^2 \leq 1$. Comme $\|u_i\| \geq 1$ puisque $m(\Lambda) = 1$, ceci impose $\|u_1\| = \|u_2\| = 1$.

   iii. Choisissons une b.o.n. Ω de E dont le premier vecteur est u_1. Puisque $|\det_\Omega(u_1, u_2)| = \sqrt{3}/2$ et que u_2 est unitaire, les coordonnées de u_2 dans Ω sont $(\pm 1/2, \pm\sqrt{3}/2)$ (avec les signes indépendants). Le dessin de C.3(d) montre que Λ est isométrique au réseau qui y est représenté, et donc semblable à A_2.

E

1. (a) Si $y \in f_m(K^*)$, alors il existe $x \in K^*$ tel que $y = x^m$ et donc $y^{(p-1)/m} = x^{p-1} = 1$ d'après le théorème de Lagrange appliqué au groupe K^* de cardinal $p-1$.

   (b) Tout élément de $f_m(K^*)$ est racine du polynôme $X^{(p-1)/m} - 1$ qui a au plus $(p-1)/m$ racines dans K. Donc Card $f_m(K^*) \leq (p-1)/m$. Puisque Card $f_m(K^*) \times$ Card $\ker(f_m) =$ Card $K^* = p-1$, on en déduit Card $\ker(f_m) \geq m$.

   (c) $x \in \ker(f_m)$ si et seulement si x est racine de $X^m - 1$ dans K. D'après (b) ce polynôme de degré m a au moins m racines dans K. Il est donc scindé dans $K[X]$.

2. (a) D'après 1, $X^4 - 1 = (X^2-1)(X^2+1)$ est sindé dans $K[X]$, donc X^2+1 est scindé dans $K[X]$ et en particulier a une racine dans K ; ceci entraîne qu'il existe $u \in \mathbf{Z}$ tel que $u^2 + 1 \equiv 0 \bmod p$.

   (b) Soit $x = ape_1 + b(ue_1 + e_2) \in \Lambda$ (a et b sont entiers). Alors

$$\|x\|^2 = (ap + bu)^2 + b^2 = (a^2p + 2abu)p + b^2(u^2+1) \equiv 0 \bmod p .$$

   Donc, pour tout x de Λ, $\|x\|^2$ est un entier divisible par p.

   (c) D'après D.2(b), on a $m(\Lambda)^2 \leq \frac{2}{\sqrt{3}} \det(\Lambda)$. Comme $\det(\Lambda)$ est la valeur absolue de $\begin{vmatrix} p & u \\ 0 & 1 \end{vmatrix} = p$, on en déduit qu'il existe $x \in \Lambda$ non nul tel que $\|x\|^2 \leq \frac{2}{\sqrt{3}} p < 2p$. Puisque $\|x\|^2$ est un entier > 0 et divisible par p, ceci impose $\|x\|^2 = p$.

   (d) Si $p \equiv 1 \bmod 4$, d'après ce qui précède il existe $x \in \Lambda \subset \mathbf{Z}^2$ tel que $\|x\|^2 = p$. Donc il existe $a, b \in \mathbf{Z}$ tels que $p = a^2 + b^2$.

3. (a) D'après 1, $X^8 - 1 = (X^4-1)(X^4+1)$ est scindé dans $K[X]$, donc X^4+1 est scindé dans $K[X]$ et en particulier a une racine z (forcément $\neq 0$) dans K. Alors

$$\left(z - \frac{1}{z}\right)^2 = \frac{z^4+1}{z^2} - 2 = -2 ,$$

   donc $X^2 + 2$ a une racine dans K, ce qui veut dire qu'il existe $u \in \mathbf{Z}$ tel que $u^2 + 2 \equiv 0 \bmod p$.

   (b) Soit Λ le réseau de base $(pe_1, ue_1 + \sqrt{2}\, e_2)$. On montre comme ci-dessus que pour tout x de Λ, $\|x\|^2$ est un entier divisible par p. Ici $\det(\Lambda) = \sqrt{2}p$, donc il existe $x \in \Lambda$ non nul tel que $\|x\|^2 \leq \frac{2\sqrt{2}}{\sqrt{3}} p < 2p$; forcément $\|x\|^2 = p$. Comme $\Lambda \subset \mathbf{Z}e_1 + \mathbf{Z}\sqrt{2}\, e_2$, il existe $a, b \in \mathbf{Z}$ tels que $p = a^2 + 2b^2$.

4. (a) D'après 1, $X^3-1=(X-1)(X^2+X+1)$ est scindé dans $K[X]$, donc (X^2+X+1) est scindé dans $K[X]$ et en particulier a une racine z (forcément $\neq 0$) dans K. Alors

$$\left(z-\frac{1}{z}\right)^2=\frac{z^4+z^2+1}{z^2}-3=\frac{(z^2+z+1)(z^2-z+1)}{z^2}-3=-3\,,$$

donc X^2+3 a une racine dans K, ce qui veut dire qu'il existe $u\in\mathbf{Z}$ tel que $u^2+3\equiv 0 \bmod p$.

(b) Soit Λ le réseau de base $(pe_1, ue_1+\sqrt{3}\,e_2)$. Si $x=ape_1+b(ue_1+\sqrt{3}\,e_2)\in\Lambda$ (a et b entiers), on a

$$\|x\|^2=(ap+bu)^2+3b^2=p(a^2p+2abu)+b^2(u^2+3)\equiv 0 \bmod p\,.$$

Par ailleurs, ou bien $ap+bu$ et b sont de parités différentes, auquel cas $\|x\|^2$ est impair, ou bien ils ont même parité et alors $\|x\|^2$ est divisible par 4. Le seul cas non évident est celui où $ap+bu=2k+1$ et $b=2\ell+1$ sont tous les deux impairs ; alors $(2k+1)^2+3(2\ell+1)^2=4(k^2+k+3\ell^2+3\ell+1)$.

(c) Ici $\det(\Lambda)=\sqrt{3}\,p$, et on en déduit qu'il existe $x\in\Lambda$ non nul tel que $\|x\|^2\leq 2p$. Le cas $2p$ est à exclure car $2p$ n'est ni impair ni divisible par 4 (remarquer que $p\neq 2$). Donc il existe $x\in\Lambda\subset\mathbf{Z}e_1+\mathbf{Z}\sqrt{3}\,e_2$ tel que $\|x\|^2=p$. Ceci montre que pour tout premier $p\equiv 1 \bmod 3$, il existe $a,b\in\mathbf{Z}$ tels que $p=a^2+3b^2$.