Agrégation Interne 2012

Corrigé de la première épreuve

Partie A

1.(a) On a $\det M \times \det M^{-1} = \det I_n = 1$ avec $\det M, \det M^{-1} \in \mathbb{Z}$ (ces deux matrices sont à coefficients dans $\mathbb{Z}$). Les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et -1, donc $\det M = \pm 1$.

1.(b) Comme $\det M \neq 0$, M est inversible dans $\mathcal{M}_n(\mathbb{R})$ et $M^{-1} = \frac{1}{\det M}\,{}^t\mathrm{Com}(M)$. Or $\mathrm{Com}(M) \in \mathcal{M}_n(\mathbb{Z})$ et $\det M = \pm 1$, donc $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$, i.e. $M \in GL_n(\mathbb{Z})$.

1.(c)
- $GL_n(\mathbb{Z}) \subset GL_n(\mathbb{R})$;
- $I_n \in GL_n(\mathbb{Z})$ donc $GL_n(\mathbb{Z}) \neq \emptyset$;
- si $M, N \in GL_n(\mathbb{Z})$, MN^{-1}et $\left(MN^{-1}\right)^{-1} = NM^{-1}$ sont à coefficients entiers (car M, M^{-1}, N et N^{-1} le sont) donc $MN^{-1} \in GL_n$

donc $GL_n(\mathbb{Z})$ est un sous-groupe de $GL_n(\mathbb{R})$.

2. Λ est un sous-groupe de E car c'est l'image du morphisme de groupe $\begin{array}{ccc} \mathbb{Z}^n & \longrightarrow & E \\ (x_i)_1^n & \longmapsto & \displaystyle\sum_{i=1}^n x_i e_i \end{array}$.

3. Notons Λ et Λ' les réseaux définis par $\mathcal{B}$ et $\mathcal{B}'$.

Si $\Lambda' \subset \Lambda$, les vecteurs de $\mathcal{B}'$ sont éléments de Λ et sont donc combinaisons linéaires à coefficients entiers de $\mathcal{B}$: la matrice P est donc à coefficients dans $\mathbb{Z}$. Par symétrie, si $\Lambda \subset \Lambda'$, $P^{-1} \in \mathcal{M}_n(\mathbb{Z})$. Ainsi, $P \in GL_n(\mathbb{Z})$ quand $\mathcal{B}$ et $\mathcal{B}'$ engendrent le même réseau.

Supposons que $P \in GL_n(\mathbb{Z})$. Soit $x \in E$ et notons X et X' les vecteurs coordonnés associés à x dans les bases $\mathcal{B}$ et $\mathcal{B}'$. Comme P et P^{-1} sont à coefficients entiers, nous avons :

$$\begin{cases} x \in \Lambda' \Longrightarrow X' \in \mathbb{Z}^n \Longrightarrow X = PX' \in \mathbb{Z}^n \Longrightarrow x \in \Lambda \\ x \in \Lambda \Longrightarrow X' \in \mathbb{Z}^n \Longrightarrow X' = P^{-1}X \in \mathbb{Z}^n \Longrightarrow x \in \Lambda \end{cases}$$

Deux bases engendrent donc le même réseau si et seulement si leur matrice de passage est élément de $GL_n(\mathbb{Z})$.

4.(a) D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Soit alors $y = -v\varepsilon_1 + u\varepsilon_2$. (x, y) est une base de $\mathbb{R}^2$ et la matrice de passage de $(\varepsilon_1, \varepsilon_2)$ à (x, y) est $P = \begin{pmatrix} a & -v \\ b & u \end{pmatrix}$: P est à coefficients entiers et son déterminant vaut ; on en déduit que $P \in GL_2(\mathbb{Z})$ (question 1.b) et que (x, y) est une $\mathbb{Z}$-base du réseau $\mathbb{Z}^2$ (question 3).

4.(b) Appliquons l'algorithme d'Euclide : $101 = 2 \times 49 + 3$ et $49 = 16 \times 3 + 1$, donc

$$1 = 49 - 16 \times 3 = 49 - 16 \times (101 - 2 \times 49) = -16 \times 101 + 33 \times 49$$

et $(101\varepsilon_1 + 49\varepsilon_2, -33\varepsilon_1 - 16\varepsilon_2)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^2$.

4.(c) On peut écrire un algorithme récursif qui, appliqué à un couple (a, b) d'entiers premiers entre eux, renvoie un couple d'entiers (c, d) tels que $ad - bc = \pm 1$:

- si $|a| < |b|$, on applique la fonction au couple (b, a) et on échange les deux éléments ainsi obtenus ;
- sinon, si $b = 0$, on envoie $(0, 1)$ (on a nécessairement $a = \pm 1$) ; si $b \neq 0$, on effectue la division euclidienne de a par b : $a = bq + r$ et on applique la fonction au couple (b, r), obtenant ainsi un couple (c', d') tel que $bd' - rc' = \pm 1$. On a alors $-ac' + b(d' + qc') = \pm 1$ et on renvoie le couple $(-d' - qc', -c')$.

En Maple, cela donne :

```
> calcul := proc(a,b)
  local r,q,L;
  if abs(a)<abs(b)then
     L := calcul(b,a);
     [L[2],L[1]]
  else
     if b=0 then
        [0,1]
     else
        r := a mod b;
        q := (a-r)/b;
        L := calcul(b,r);
        [-L[2]-q*L[1],-L[1]];
     fi;
  fi;
  end:

> calcul(101,49);
            [-33,-16]

>  calcul(-13645,2364553);
            [-2218, 384359]
```

4.(d) Nous avons $\Lambda = \{\alpha\varepsilon_1 + (\alpha + 3\beta)\varepsilon_2,\ \alpha, \beta \in \mathbb{Z}\} = \{x_1 e_1 + x_2 e_2, x_1, x_2 \in \mathbb{Z}\}$, en posant $e_1 = \varepsilon_1 + \varepsilon_2$ et $e_2 = 3\varepsilon_2$. Comme (e_1, e_2) est libre, Λ est un réseau de $\mathbb{R}^2$ associé à la base $(\varepsilon_1 + \varepsilon_2, 3\varepsilon_2)$.

5. Soit $\mathcal{B}'$ une autre $\mathbb{Z}$-base de Λ et Ω' une autre base orthonormale de E. Nous avons :

$$\det_{\Omega'} \mathcal{B}' = \det_{\Omega'} \Omega \times \det_{\Omega} \mathcal{B} \times \det_{\mathcal{B}} \mathcal{B}' = \pm \det_{Om} \mathcal{B}$$

car $\det_{\Omega'} \Omega \in O_n(\mathbb{R})$ et $\det_{\mathcal{B}} \mathcal{B}' \in GL_n(\mathbb{Z})$. La valeur absolue de $\det_{\Omega} \mathcal{B}$ ne dépend donc pas des deux bases choisis. Cette valeur est l'aire des pavés associés au réseau Λ (un réseau est associé à une infinité de pavages du plan, mais l'aire du pavé élémentaire de chacun de ces pavages ne dépend que du réseau).

6.(a) Notons $|| \, ||_\infty$ la norme $\sum_{i=1}^n x_i e_i \longmapsto \sup_{1\leq i\leq n} |x_i|$. Comme E est de dimension finie, les norme $|| \, ||$ et $|| \, ||_\infty$ sont équivalentes, d'où l'existence de la constante $A > 0$.

6.(b) Soit $x \in \Lambda$ tel que $||x|| \leq R$: x s'écrit donc $\sum_{i=1}^n x_i e_i$ avec $x_i \in \mathbb{Z}$ et $|x_i| \leq R/A$ pour tout i. Les x_i ne peuvent donc prendre qu'un nombre fini de valeurs et la boule fermée de centre 0 et de rayon R ne contient qu'un nombre fini de vecteurs de Λ.

6.(c) Posons $R = ||e_1||$. On a clairement : $\inf\limits_{x\in\Lambda, x\neq 0} ||x|| = \inf\limits_{x\in\Lambda, 0<||x||\leq R} ||x||$ et cette borne inférieure est atteinte, puisque $\{x \in \Lambda, 0 < ||x|| \leq R\}$ est fini (et non vide). On en déduit que $m(\Lambda)$ est strictement positif et qu'il existe $x_0 \in \Lambda$ tel que $m(\Lambda) = ||x_0||$.

6.(d) $S(\Lambda)$ est non vide (il contient x_0), fini (il est contenu dans $\{x \in \Lambda, \ ||x|| \leq m(\Lambda)\}$) et les parties de la forme $\{x, -x\}$, pour $x \in S(\Lambda)$, sont de cardinal 2 et partitionnent $S(\Lambda)$: le cardinal de $S(\Lambda)$ est donc pair.

7. Comme conseillé par l"énoncé, travaillons dans le $\mathbb{Q}$-espace vectoriel F engendré par les e_i.

Chaque vecteur e_i est élément de Λ, donc combinaison linéaire à coefficients dans $\mathbb{Z}$ (et donc dans $\mathbb{Q}$), des vecteurs $(u_1, \ldots, u_k)$. On en déduit que $(u_1, \ldots, u_k)$ est une famille génératrice de F.

Si $\alpha_1, \ldots, \alpha_k$ sont des rationnels tels que $\alpha_1 u_1 + \cdots + \alpha_k u_k = 0$, il existe un entier non nul β tel que $\beta\alpha_1, \ldots, \beta\alpha_k$ soient tous entiers. Nous avons alors

$$(\beta\alpha_1)u_1 + \cdots + (\beta\alpha_k)u_k = 0$$

ce qui impose $\beta\alpha_1 = \ldots = \beta\alpha_k = 0$ car $0 \in \Lambda$ admet une unique décomposition de la forme $x_1u_1 + \cdots + x_ku_k$ avec $x_1, \ldots, x_k \in \mathbb{Z}$. Ainsi, les α_i sont tous nuls et $(u_1, \ldots, u_k)$ est une famille libre, donc une base de F, ce qui prouve que $k = n$.

On en déduit que la matrice de passage de $(e_1, \ldots, e_n)$ à $(u_1, \ldots, u_n)$ est élément de $GL_n(\mathbb{Q})$, donc de $GL_n(\mathbb{R})$: $(u_1, \ldots, u_n)$ est une base de E.

On peut dès à présent remarquer que $(u_1, \ldots, u_n)$ est une $\mathbb{Z}$-base de Λ, puisque cette propriété sera utilisée à la question 10 (d) : le réseau engendré par les u_i est contenu dans Λ car les u_i sont éléments de Λ, et tout élément de Λ est par hypothèse combinaison à coefficients entiers des vecteurs u_i, ce qui donne bien

$$\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n.$$

8. Soit $x \in \Lambda$: x s'écrit de manière unique $x = x_1e_1 + \cdots + x_ne_n$ avec $x_1, \ldots, x_n \in \mathbb{Z}$. Comme $(e_1, \ldots, e_n)$ est libre, nous avons alors :

$$x \in D_1 \Longleftrightarrow x_2 = \ldots = x_n = 0$$

ce qui prouve que $D_1 \cap \Lambda = \mathbb{Z}e_1$.

Comme $E_1 = \mathrm{Vect}(e_2, \ldots, e_n)$ est un supplémentaire de $\mathrm{Ker}\, p$, la restriction de p à E_1 est un isomorphisme de E_1 sur $\mathrm{Im}\, p$, i.e. sur F. On en déduit que $(p(e_1), \ldots, p(e_n))$ est une base de F. On a ensuite :

$$\Lambda' = \{p(x_1e_1 + \cdots + x_ne_n), \ x_1, \ldots, x_n \in \mathbb{Z}\} = \{x_2p(e_2) + \cdots + x_np(e_n), \ x_2, \ldots, x_n \in \mathbb{Z}\}$$

donc Λ' est un réseau de F, de $\mathbb{Z}$-base $(p(e2), \ldots, p(e_n))$.

Soit $x \in \Lambda$. Comme $p(x) \in \Lambda'$, il existe $x_2, \dots, x_n \in \mathbb{Z}$ tels que $p(x) = x_2 u'_2 + \cdots + x_n u'_n$. Le vecteur $x - x_2 u_2 - \cdots - x_n u_n$ est alors élément de $\operatorname{Ker} p$, i.e. de D_1, et de Λ : il existe donc $x_1 \in \mathbb{Z}$ tel que

$$x = x_1 e_1 + x_2 u_2 + \cdots + x_n u_n.$$

Soit $x = y_1 e_1 + y_2 u_2 + \cdots + y_n e_n$, avec $y_1, \dots, y_n \in \mathbb{Z}$, une autre décomposition. Nous avons alors

$$x_2 u'_2 + \cdots + x_n u'_n = p(x) = y_2 u'_2 + \cdots + y_n u'_n,$$

donc $x_i = y_i$ pour tout $i \geq 2$ (les u'_i forment une base de F), puis $x_1 e_1 = y_1 e_1$, soit $x_1 = y_1$. La question 7 prouve donc que $(e_1, u_2, \dots, u_n)$ est une $\mathbb{Z}$-base de Λ.

9.(a) φ_1 est un morphisme de groupe, donc l'image du sous-groupe G est un sous-groupe de $\mathbb{R}$, contenu dans $\varphi_1(\Lambda) = \mathbb{Z}$. Le théorème de caractérisation des sous-groupes de $\mathbb{Z}$ prouve qu'il existe un entier a_1 tel que $\varphi_1(G) = a_1\,\mathbb{Z}$.

9.(b) Quand $n = 1$, φ_1 est un isomorphisme d'espace vectoriel de E sur $\mathbb{R}$: sa restriction à G est alors un isomorphisme de groupe de G sur $a_1\,\mathbb{Z}$ (elle est surjective par définition de a_1 et injective comme restriction d'une injection). Comme $a_1\mathbb{Z}$ est engendré par a_1 (qui est non nul car $G \neq \{0\}$), G est engendré par $\varepsilon_1 = \varphi_1^{-1}(a_1)$: G est ainsi le réseau de E de $\mathbb{Z}$-base (ε_1).

9.(c) On a clairement $\Lambda_1 = \Lambda \cap F_1$, donc $H = G \cap F_1 = G \cap \Lambda \cap F_1 = G \cap \Lambda'$; H est donc un sous-groupe de E (intersection de deux sous-groupes de E) et il est contenu dans Λ' : c'est donc un sous-groupe de Λ'.

9.(d) Soit $x \in G$; $\varphi_1(x) \in a_1\mathbb{Z}$, donc il existe $m \in \mathbb{Z}$ tel que $\varphi_1(x) = m\,a_1 = \varphi_1(m\,b)$. Posons $v = x - m\,b$: $v \in F_1 \cap G = H$ et $x = v + m\,b$.

Supposons que $x = v' + m'\,b$ avec $v' \in H$ et $m' \in \mathbb{Z}$. Alors $m\,a_1 = \varphi(x) = m'\,a_1$, donc $m = m'$ (a_1 est non nul), puis $v = v'$: l'écriture est donc unique.

9.(e) Prouvons le résultat par récurrence sur n.

- si $n = 1$, le résultat a été prouvé à la question (b) ;
- soit $n \geq 2$ et supposons que le résultat ait été démontré pour tout réseau d'un espace de dimension $n - 1$. Soit G un sous-groupe non réduit à $\{0\}$ d'un réseau Λ d'un espace E de dimension n. En reprenant les notations précédentes, trois cas se présentent :
  - si $G \subset F_1$, l'hypothèse de récurrence s'applique : G est un sous-groupe non réduit à $\{0\}$ du réseau Γ_1 : il existe un sous-espace vectoriel F de F_1 (donc de E) tel que G soit un réseau de F ;
  - si $G \subset \mathbb{Z}e_1$, G est un réseau de $\operatorname{Vect}(e_1)$ d'après (b) ;
  - sinon, $H = G \cap F_1$ est un sous-groupe non réduit à $\{0\}$ de Λ_1 : il existe donc un sous-espace F_2 de F_1 tel que H soit un réseau de F_2. En fixant une $\mathbb{Z}$-base $(\varepsilon_2, \dots, \varepsilon_k)$ de ce réseau, la famille $(b, \varepsilon_2, \dots, \varepsilon_k)$ est libre (car $b \notin F_1$ et $(\varepsilon_2, \dots, \varepsilon_k)$ est un famille libre de F_1) : soit F le sous-espace qu'elle engendre. D'après le (d), tout élément de G s'écrit sous la forme $mb + x_2\varepsilon_2 + \cdots + x_k\varepsilon_k$ avec $m, x_2, \dots, x_k \in \mathbb{Z}$. Réciproquement, pour tout $m, x_2, \dots, x_k \in \mathbb{Z}$, $mb + x_2\varepsilon_2 + \cdots + m_k\varepsilon_k \in G$ car G est un sous-groupe contenant $b, \varepsilon_2, \dots, \varepsilon_k$. Ceci prouve que G est un réseau de F, admettant $(b, \varepsilon_2, \dots, \varepsilon_k)$ pour $\mathbb{Z}$-base.

10.(a) $\dfrac{1}{k}b \notin \Lambda$ car $0 < \left|\left|\dfrac{1}{k}b\right|\right| < ||b|| = \inf\limits_{x \in \Lambda,\, x \neq 0} ||x||$.

10.(b) Les r_i ne sont pas tous nuls, donc leur P.G.C.D. d est strictement positif. Comme $\frac{1}{d}b \in \Lambda$, la question précédente prouve que $d = 1$, i.e. que $r_1\mathbb{Z} + \cdots + r_n\mathbb{Z} = \mathbb{Z}$, d'où l'existence de la famille cherchée.

10.(c) f est un morphisme de groupe, donc $f(\Lambda)$ est un sous-groupe de Z : comme ce sous-groupe contient $f(b) = 1$, on a nécessairement $f(\Lambda) = \mathbb{Z}$.

$H = \Lambda \cap \mathrm{Ker}(f)$ est un sous-groupe (intersection de sous-groupes) contenu Λ : c'est un sous-groupe de Λ.

Soit $x \in \Lambda$.

- Analyse : supposons que $x = ab + u$ avec $a \in \mathbb{Z}$ et $u \in H$. Alors $f(x) = f(ab) + f(u) = af(b) = a$ et $u = x - ab$, ce qui prouve l'unicité de la décomposition cherchée.
- Synthèse : posons $a = f(x) \in \mathbb{Z}$ et $u = x - ab$. Comme $x, b \in \Lambda$, $u \in \Lambda$ et $f(u) = f(x) - af(b) = a - a = 0$: u est bien élément de H, ce qui prouve l'existence de la décomposition.

10.(d) Comme H est un sous-groupe de Λ, on peut appliquer le 9.(e) : il existe une sous-espace vectoriel F de E et une base $(u_2, \ldots, u_k)$ de F tels que H soit un réseau de f de $\mathbb{Z}$-base $(u_2, \ldots, u_k)$. Le (c) et la définition d'une $\mathbb{Z}$-base prouve que tout élément x de Λ s'écrit de façon unique sous la forme

$$x = ab + x_2u_2 + \cdots + x_ku_k$$

avec $a, x_2, \ldots, x_k \in \mathbb{Z}$: comme $b, u_2, \ldots, u_k$ sont des éléments de Λ, la question 7 prouve que $k = n$ et que $(b, u_2, \ldots, u_n)$ est une $\mathbb{Z}$-base de Λ (avec le complément démontré à la question 7).

10.(e) Travaillons dans la $\mathbb{Z}$-base $(b, u_2, \ldots, u_n)$ de Λ. En notant $D_1 = \mathbb{R}b$ et $F = D_1^{\perp}$, la question 8 prouve que $p(\Lambda)$ est un réseau de F admettant $(p(u_2), \ldots, p(u_n))$ pour $\mathbb{Z}$-base.

Partie B : Réseaux et matrices de Gram

1. Pour tous $i, j \in \{1, \ldots, n\}$, $G_{ij} = e_i.e_j = \sum_{k=1}^n m_{ki}m_{kj} = \sum_{k=1}^n M_{ki}M_{kj}$ donc $G = {}^tM\,M$. Si $\mathcal{E}$ est une base de E, M est la matrice de passage de Ω à $\mathcal{E}$, donc $\det G = (\det M)^2 \neq 0$.

2. Notons P la matrice de passage de Ω à $\mathcal{E}$: par définition, $\det \Lambda = |\det P|$, donc $\det G = (\det P)^2 = (\det \Lambda)^2$.

3. D'après la question A.3., nous avons :

$$\begin{aligned}
\mathcal{B} \text{ est une } \mathbb{Z}-\text{base de } \Lambda &\iff |\det_{\mathcal{E}}\mathcal{B}| = 1 \\
&\iff |\det_{\mathcal{E}}\Omega \times \det_{\Omega}\mathcal{B}| = 1 \\
&\iff |\det_{\Omega}\mathcal{B}| = |\det_{\Omega}\mathcal{E}| \\
&\iff |\det_{\Omega}\mathcal{B}| = \det\Lambda
\end{aligned}$$

4.(a) Supposons qu'il existe une telle isométrie, fixons une $\mathbb{Z}$-base $\mathcal{B} = (e_1, \ldots, e_n)$ de Λ et posons $\mathcal{B}' = (u(e_1), \ldots, u(e_n))$; u réalise alors un isomorphisme de groupe de Λ sur Λ', donc $\mathcal{B}'$ est une $\mathbb{Z}$-base de Λ', et

$$G' = (u(e_i).u(e_j))_{1 \leq i,j \leq n} = (e_i.e_j)_{1 \leq i,j \leq n} = G.$$

Supposons qu'il existe deux $\mathbb{Z}$-bases $\mathcal{B} = (e_1, \ldots, e_n)$ et $\mathcal{B}' = (e'_1, \ldots, e'_n)$ de Λ et Λ' telles que $G = G'$. Soit u l'isomorphisme de E qui envoie la base $\mathcal{B}$ sur la base $\mathcal{B}'$. Nous avons alors :

$$\forall\, x, y \in E,\ u(x).u(y) = \sum_{1 \le i,j \le n} x_i y_j u(e_i).u(e_j) = \sum_{1 \le i,j \le n} x_i y_j G'_{ij} = \sum_{1 \le i,j \le n} x_i y_j G_{ij} = \sum_{1 \le i,j \le n} x_i y_j e_i.e_j = x.y$$

u est ainsi une isométrie de E et $u(\Lambda) = \Lambda'$.

4.(b) Supposons que Λ et Λ' sont semblables : il existe alors une similitude f, de rapport $k > 0$, tel que $f(\Gamma) = \Gamma'$. Fixons une $\mathbb{Z}$-base $\mathcal{B} = (e_1, \ldots, e_n)$ de Λ et posons $\mathcal{B}' = (f(e_1), \ldots, f(e_n))$. f est encore un isomorphisme de groupe de Λ sur Λ', donc $\mathcal{B}'$ est une $\mathbb{Z}$-base de Λ' et

$$G' = (f(e_i).f(e_j))_{1 \le i,j \le n} = (k^2\, e_i.e_j)_{1 \le i,j \le n} = k^2\, G.$$

Supposons qu'il existe deux $\mathbb{Z}$-bases $\mathcal{B} = (e_1, \ldots, e_n)$ et $\mathcal{B}' = (e'_1, \ldots, e'_n)$ de Λ et Λ' et un réel $\mu > 0$ tels que $G = \mu\, G'$. L'isomorphisme f qui envoie $\mathcal{B}$ sur $\mathcal{B}'$ vérifie alors :

$$\forall\, x, y \in E,\ f(x).f(y) = \sum_{1 \le i,j \le n} x_i y_j f(e_i).f(e_j) = \sum_{1 \le i,j \le n} x_i y_j \mu(e_i.e_j) = \mu\, x.y$$

C'est donc une similitude qui envoie Λ sur Λ'.

4.(c) Comme Λ et Λ' sont semblables, il existe deux $\mathbb{Z}$-bases $\mathcal{B}$ et $\mathcal{B}'$ de Λ et Λ' et un réel $\mu > 0$ tels que $G' = \mu\, G$. On en déduit que $(\det \Lambda')^{2/n} = (\det G')^{1/n} = (\mu^n \det G)^{1/n} = \mu\, (\det \Lambda)^{2/n}$.

D'autre part, notons f une similitude qui envoie Γ sur Γ'. Nous avons :

$$m(\Lambda') = \inf_{x \in \Lambda, x \neq 0} ||f(x)|| = \sqrt{\mu} \inf_{x \in \Lambda, x \neq 0} ||x|| = \sqrt{\mu}\, m(\Lambda)$$

donc

$$\Gamma_n(\Lambda') = m(\Lambda')^2 (\det \Lambda')^{-2/n} = m(\Lambda)^2 (\det \Lambda)^{(} - 2/n) = \Gamma_n(\Lambda).$$

Nous avons d'autre part, pour tout $x \in E$, $x \in S(\Lambda)$ si et seulement si $f(x) \in S(\Lambda')$; f étant bijective, $\mathrm{Card}(S(\Lambda)) = \mathrm{Card}(S(\Lambda'))$.

Partie C : Quelques exemples de réseaux

1. On peut choisir $\Omega = \mathcal{E}_n$, donc $\det \mathbb{Z}^n = |\det I_n| = 1$. On a clairement :

$$m(\mathbb{Z}^n) = 1,\ S(\mathbb{Z}^n) = \{(1,0), (0,1), (-1,0), (0,-1)\} \text{ et } \mathrm{Card}(S(\mathbb{Z}^n)) = 4.$$

2.(a) L'application $\begin{array}{ccc} (\mathbb{Z}^n, +) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z}, +) \\ (x_i)_1^n & \longmapsto & \overline{x_1 + \cdots + x_n} \end{array}$, où $\overline{n}$ désigne la classe de n modulo 2, est un morphisme de groupe : son noyau D_n est donc un sous-groupe de $(\mathbb{Z}^n, +)$.

2.(b) La famille $\mathcal{B} = (e_i)$ est une base de $\mathbb{R}^n$, puisque la matrice de passage de $\mathcal{E}$ à $\mathcal{B}$ a un déterminant égal à 2. Soit Λ le réseau de $\mathbb{R}^n$ engendré par $\mathcal{B}$. Comme les e_i sont éléments du sous-groupe D_n, $\Lambda \subset D_n$.

Soit $x \in D_n$. x s'écrit donc sous les formes :

$$x = x_1\varepsilon_1 + \cdots + x_n\varepsilon_n = y_1e_1 + \cdots + y_ne_n$$

avec $x_1, \ldots, x_n \in \mathbb{Z}$, $x_1 + \cdots + x_n \equiv 0 \bmod 2$, les x_i et y_i étant liés par les relations :

$$\begin{cases} x_1 & = & y_1 - y_2 \\ x_2 & = & y_1 + y_2 - y_3 \\ x_3 & = & y_3 - y_4 \\ & \vdots & \\ x_{n-1} & = & y_{n-1} - y_n \\ x_n & = & y_n \end{cases}$$

Ce système s'inverse facilement :

$$\begin{cases} y_1 & = & \frac{1}{2}(x_1 + x_2 + \cdots + x_n) \\ y_2 & = & \frac{1}{2}(-x_1 + x_2 + \cdots + x_n) \\ y_3 & = & x_3 + \cdots + x_n \\ & \vdots & \\ y_{n-1} & = & x_{n-1} + x_n \\ y_n & = & x_n \end{cases}$$

Comme $-x_1 + x_2 + \cdots + x_n \equiv x_1 + x_2 + \cdots + x_n \equiv 0 \bmod 2$, tous les y_i sont entiers et $x \in \Lambda$. $D_n = \Lambda$ est donc le réseau de $\mathbb{R}^n$ engendré par la $\mathbb{Z}$-base $\mathcal{B}$.

2.(c) Soit $x = x_1\varepsilon_1 + \cdots x_n\varepsilon_n \in D_n \setminus \{0\}$. Si tous les x_i sont nuls sauf x_{i_0}, x_{i_0} est pair et $||x||^2 \geq 4$; sinon, au moins deux valeurs x_i sont nulles et $||x||^2 \geq 2$, avec égalité par exemple pour $x = \varepsilon_1 + \varepsilon_2$: on a donc $m(D_n) = \sqrt{2}$.

Le même argument prouve que $||x||^2 = 2$ si et seulement si $x = a\varepsilon_i + b\varepsilon_j$ avec $1 \leq i < j \leq n$ et $|a| = |b| = 1$, soit :

$$S(D_n) = \{a\varepsilon_i + b\varepsilon_j,\ 1 \leq i < j \leq n,\ a, b \in \{-1, 1\}\} \text{ et } \mathrm{Card}(S(D_n)) = 4 \times \binom{n}{2} = 2n(n-1).$$

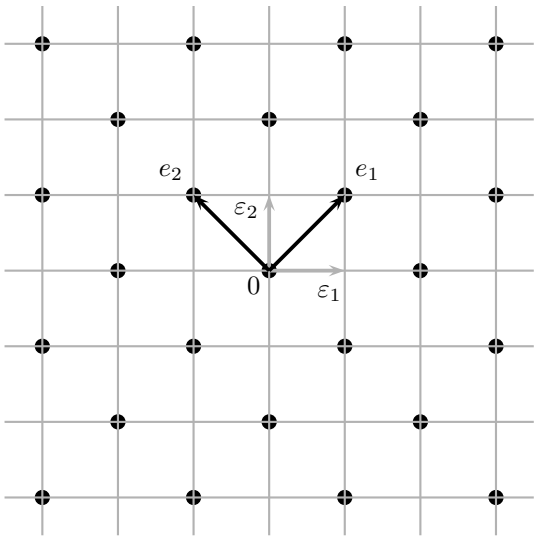
2.(d) $\mathcal{E}$ est une base orthonormale, donc :

$$\det D_n = |\det_{\mathcal{E}}\mathcal{B}| = \left| \det \begin{pmatrix} 1 & -1 & 0 & \ldots & \ldots & 0 \\ 1 & 1 & -1 & 0 & & \vdots \\ 0 & 0 & 1 & -1 & \ddots & \vdots \\ \vdots & & \ddots & 1 & \ddots & 0 \\ \vdots & & & \ddots & \ddots & -1 \\ 0 & \ldots & \ldots & \ldots & 0 & 1 \end{pmatrix} \right| = \left| \det \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \right| = 2$$

2.(e) On obtient facilement :

$$G(\mathcal{B}) = \begin{pmatrix} 2 & 0 & -1 & 0 & \dots & 0 \\ 0 & 2 & -1 & 0 & & \vdots \\ -1 & -1 & 2 & -1 & \ddots & \vdots \\ 0 & 0 & -1 & 2 & \ddots & 0 \\ \vdots & & \ddots & \ddots & \ddots & -1 \\ 0 & \dots & \dots & 0 & -1 & 2 \end{pmatrix}$$

2.(f) Quand $n = 2$, $\mathcal{B} = (e_1, e_2)$ est l'image de $\mathcal{E} = (\varepsilon_1, \varepsilon_2)$ par la similitude directe (vectorielle) d'angle $\pi/4$ et de rapport $\sqrt{2}$:



2.(g) Pour $n \geq 3$, on a $\Gamma_n(\mathbb{Z}^n) = 1$ et $\Gamma_n(D_n) = 2 \times 2^{-2/n} = 2^{1-2/n} \neq 1$ donc $\mathbb{Z}^n$ et D_n ne sont pas semblables, par contraposée du résultat B.4.(c).

3.(a) On a :

$$\begin{aligned} A_2 &= \{x_1\varepsilon_1 + x_2\varepsilon_2 + x_3\varepsilon_3,\ x_1, x_2, x_3 \in \mathbb{Z}, x_1 + x_2 + x_3 = 0\} \\ &= \{x_1\varepsilon_1 - (x_1 + x_3)x_2\varepsilon_2 + x_3\varepsilon_3,\ x_1, x_3 \in \mathbb{Z}\} \\ &= \{y_1(\varepsilon_2 - \varepsilon_1) + y_2(\varepsilon_2 - \varepsilon_3),\ y_1, y_2 \in \mathbb{Z}\} \end{aligned}$$

Comme $(\varepsilon_2 - \varepsilon_1, \varepsilon_2 - \varepsilon_3)$ est une base de H, A_2 est bien le réseau de H associé à la $\mathbb{Z}$-base $\mathcal{B}$.

3.(b) $G(\mathcal{B}) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

3.(c) Pour $x = -y_1\varepsilon_1 + (y_1+y_2)\varepsilon_2 - y_3\varepsilon_3 \in A_2 \setminus \{0\}$, on peut écrire :

$$||x||^2 = y_1^2 + (y_1+y_2)^2 + y_2^2 = 2\,(\underbrace{y_1^2 + y_1y_2 + y_2^2}_{\in\mathbb{N}^*}) \geq 2,$$

avec égalité pour $y_1 = 1$ et $y_2 = 0$: on a donc $m(A_2) = \sqrt{2}$.

Pour avoir $||x||^2 = 2$, il faut et il suffit que l'on ait $y_1^2 + y_1y_2 + y_2^2 = 1$, i.e. $3(y_1+y_2)^2 + (y_1-y_2)^2 = 4$. Il n'y a que deux façons d'écrire $4 = 3a + b$ avec $a, b \in \mathbb{N}$, à savoir $4 = 3\times 1 + 1$ et $4 = 3\times 0 + 4$. Nous avons donc :

$$x \in S(A_2) \iff \big((y_1+y_2)^2 = 1 \text{ et } (y_1-y_2)^2 = 1\big) \text{ ou } \big((y_1+y_2)^2 = 0 \text{ et } (y_1-y_2)^2 = 4\big)$$

$$\iff \begin{cases} y_1+y_2 = 1 \text{ et } y_1-y_2 = 1 \\ \text{ou} \\ y_1+y_2 = -1 \text{ et } y_1-y_2 = -1 \\ \text{ou} \\ y_1+y_2 = 1 \text{ et } y_1-y_2 = -1 \\ \text{ou} \\ y_1+y_2 = -1 \text{ et } y_1-y_2 = 1 \\ \text{ou} \\ y_2 = -y_1 \text{ et } y_1^2 = 1 \end{cases}$$

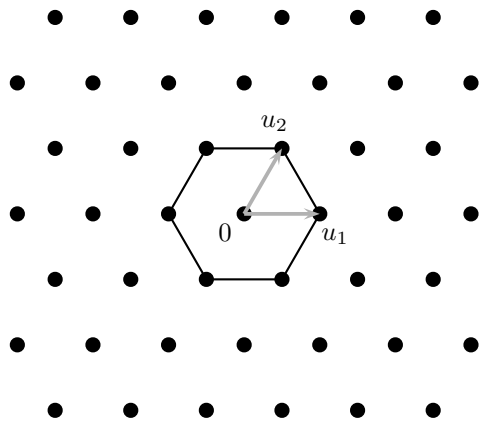
$$\iff (y_1, y_2) \in \big\{(1,0), (-1,0), (0,1), (0,-1), (1,-1), (-1,1)\big\}$$

soit $S(A_2) = \big\{-\varepsilon_1+\varepsilon_2, \varepsilon_1-\varepsilon_2, \varepsilon_2-\varepsilon_3, -\varepsilon_2+\varepsilon_3, -\varepsilon_1+\varepsilon_3, \varepsilon_1-\varepsilon_3\big\}$, qui est de cardinal 6.

3.(d) (i) $\Gamma_2(A_2) = 2\times(\det G(\mathcal{B}))^{-1/2} = \dfrac{2}{\sqrt{3}} \neq 1 = \Gamma_2(D_2)$ donc D_2 et A_2 ne sont pas semblables.

(ii) $G(u_1,u_2) = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix} = \mu\, G(\mathcal{B})$ avec $\mu = 1/4 > 0$: les réseaux Λ et A_2 sont donc semblables d'après la question B.4.(b).

(iii) Voici le dessin du réseau Λ :



Chaque élément du réseau a $m(\Lambda) = 6$ voisins, sommets d'un hexagone régulier, d'où la qualification de "réseau hexagonal".

Partie D

1.(a) Soit $\Omega = (e_1, \dots, e_n)$ une base orthonormale telle que $e_1 = b_1/||b_1||$ (Ω est par exemple la base orthonormale obtenue en appliquant le procédé d'orthonormalisation de Gram-Schmidt à $\mathcal{B} = (b_1, u_2, \dots, u_n)$). Nous pouvons écrire :

$$\forall\, i \in \{2, \dots, n\},\ u_i = a_{1,i}\, e_1 + \underbrace{a_{2,i}e_2 + \cdots + a_{n,i}e_n}_{=p(u_i)}$$

ce qui donne :

$$\det(\Lambda) = \left|\det \begin{pmatrix} ||b_1|| & a_{1,2} & \dots & a_{1,n} \\ 0 & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n,2} & \dots & a_{n,n} \end{pmatrix}\right| = ||b_1|| \left|\det \begin{pmatrix} a_{2,2} & \dots & a_{2,n} \\ \vdots & & \vdots \\ a_{n,2} & \dots & a_{n,n} \end{pmatrix}\right| = ||b_1||\, \det \Lambda'$$

car $(e_2, \dots, e_n)$ est une base orthonormale de $(\mathbb{R}b)^{\perp}$.

1.(b) Soit m l'entier (ou l'un des deux entiers) le plus proche de α : on a $|m - \alpha| \leq 1/2$, donc $(m - \alpha)^2 \leq 1/4$.

Comme $x_0, b_1 \in \Lambda$ et $m \in \mathbb{Z}$, $x = x_0 + mb_1 \in \Lambda$ et $p(x) = p(x_0) = x'$.

Si $x = 0$, $x' = 0$ et l'inégalité demandée est vérifiée. Sinon, $||b_1|| \leq ||x||$ car x est un élément non nul de Λ, et comme b_1 et x' sont orthogonaux :

$$||x||^2 = ||(\alpha - m)b_1 + x'||^2 = (\alpha - m)^2||b_1||^2 + ||x'||^2 \leq \frac{||b_1||^2}{4} + ||x'||^2 \leq \frac{||x||^2}{4} + ||x'||^2$$

d'où l'inégalité demandée.

2.(a) Procédons par récurrence sur n.

- si $n = 1$, $\Gamma = \mathbb{Z}\, b_1$ et $\Omega = (\varepsilon_1) = (b_1/||b_1||)$ est une base orthonormale de E ; le vecteur $u_1 = b_1$ est alors solution du problème :

$$\left(\frac{4}{3}\right)^0 (\det \Lambda)^2 = (\det_\Omega(||b_1||\varepsilon_1))^2 = ||b_1||^2.$$

- supposons que $n \geq 2$ et que le résultat ait été démontré pour tout réseau de dimension $n - 1$. Soit Λ un réseau de E où E est de dimension n. En reprenant les notations précédentes, il existe donc une $\mathbb{Z}$-base $(w_2, \dots, w_n)$ du réseau Λ' telle que

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

  En appliquant le (b) aux vecteurs w_i, on construit des vecteurs v_i de Λ tels que

$$\forall\, i \in \{2, \dots, n\}\ ||v_i||^2 \leq \frac{4}{3}||w_i|| \text{ et } p(v_i) = w_i.$$

D'après la question A.8, $(b_1, v_2, \ldots, v_n)$ est une $\mathbb{Z}$-base de Λ qui vérifie l'inégalité (1) :

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

ce qui achève la preuve par récurrence.

2.(b) Fixons donc une $\mathbb{Z}$-base (u_i) de Λ vérifiant (1). Comme les u_i sont des vecteurs non nuls de Λ, $||u_i|| \geq m(\Lambda)$, d'où :

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

3.(a) On a $\dfrac{2}{\sqrt{3}} = \Gamma_2(A_2) \leq \gamma_2 \leq \left(\dfrac{4}{3}\right)^{1/2} = \dfrac{2}{\sqrt{3}}$, donc $\gamma_2 = \dfrac{2}{\sqrt{3}}$.

3.(b) (i) L'image de Λ pat l'homothétie $x \longmapsto \frac{1}{m(\Lambda)} x$ est un réseau Λ', semblable à Λ, tel que $m(\Lambda') = 1$ et $\Gamma_2(\Lambda') = \Gamma_2(\Lambda) = \frac{2}{\sqrt{3}}$. Il suffit donc de montrer que Λ' est semblable à A_2 pour démontrer que Λ l'est également : cela revient à supposer que $m(\Lambda) = 1$.

(ii) $||u_1||^2 \geq 1$, $||u_2||^2 \geq 1$ et $||u_1||^2 \, ||u_2||^2 \leq \dfrac{4}{3} (\det \Lambda)^2 = \dfrac{4}{3} \left(\dfrac{m(\lambda)^2}{\Gamma_2(\Lambda)}\right)^2 = 1$, donc $||u_1|| = ||u_2|| = 1$.

D'autre part, le déterminant de (u_1, u_2) dans une base orthonormale est, au signe près, $\det \Lambda = \dfrac{m(\lambda)^2}{\Gamma_2(\Lambda)} = \dfrac{\sqrt{3}}{2}$.

(iii) $G(u_1, u_2)$ est donc de la forme $\begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix}$ avec $1 - a^2 = \det G(u_1, u_2) = (\det \Lambda)^2 = 3/4$, i.e. $a = \pm 1/2$. Quitte à changer u_2 en $-u_2$, nous pouvons supposer que $a = 1/2$: (u_1, u_2) a la même matrice de Gram que la $\mathbb{Z}$-base qui définit A_2, donc Λ est semblable à A_2 d'après B.4.a.

Partie E

1.(a) Soit $y \in f_m(K^*)$. Il existe donc $x \in K^*$ tel que $y = x^m$. On a donc $y^{(p-1)/m} = x^{p-1} = 1$. En effet, x est élément du groupe multiplicatif K^*, qui est de cardinal $p-1$ et le théorème de Lagrange prouve que l'ordre de x divise ce cardinal.

1.(b) $f_m(K^*)$ est donc contenu dans l'ensemble des racines du polynôme $X^{(p-1)/m} - 1$: comme K est un corps commutatif, ce polynôme possède au plus $(p-1)/m$ racines, d'où $\mathrm{Card}(f_m(K^*)) \leq \dfrac{p-1}{m}$.

Pour chaque $y = f_m(x) \in f_m(K^*)$, $f_m^{-1}(\{y\}) = \{xu,\ u \in \ker f_m\}$ est de même cardinal que $\ker f_m$. Comme K^* est la réunion disjointe de ces images réciproques, on obtient :

$$p - 1 = \mathrm{Card}(K^*) = \sum_{y \in f_m(K^*)} \mathrm{Card}(f_m^{-1}(\{y\}) = \mathrm{Card}(f_m(K^*)) \times \mathrm{Card}(\ker f_m) \leq \frac{p-1}{m} \times \mathrm{Card}(\ker f_m)$$

soit $\mathrm{Card}(\ker f_m) \geq m$.

1.(c) Ceci prouve que le polynôme $X^m - 1$ admet au moins m racines dans K^* : comme il est de degré m et que K est un corps commutatif, il est scindé (et même à racines simples) dans $K[X]$.

2.(a) Si $m = 4$, $X^m - 1 = (X^2 - 1)(X^2 + 1)$ est scindé sur K ; il existe donc $x \in K$ tel que $x^2 + 1 = 0$. Si u est un entier représentant x, nous avons alors $u^2 + 1 \equiv 0 \bmod p$.

2.(b) Soit $x \in \Lambda$. En écrivant $x = ape_1 + b(ue_1 + e_2)$ avec $a, b \in \mathbb{Z}$, nous avons :

$$\begin{aligned} ||x||^2 &= (ap + bu)^2 + b^2 \in \mathbb{Z} \\ &\equiv b^2\,(u^2 + 1)b^2 \bmod p \\ &\equiv 0 \bmod p \end{aligned}$$

donc $||x||^2$ est un entier divisible par p.

2.(c) Il existe $x_0 \in \Lambda$ tel que $||x_0|| = m(\Lambda)$. D'après (2), nous avons alors :

$$0 < ||x_0||^2 = m(\Lambda)^2 \leq \frac{2}{\sqrt{3}}\,p < 2p$$

Comme $||x_0||^2$ est un multiple de p, ceci impose $||x_0||^2 = p$.

2.(d) Si p est premier congru à 1 modulo 4, la construction précédente s'applique puisque 4 divise $p - 1$; on peut alors écrire $x_0 = \alpha pe_1 + \beta(ue_1 + e_2)$ avec $\alpha, \beta \in \mathbb{Z}$, ce qui donne :

$$p = ||x_0||^2 = (\alpha\,p + \beta\,u)^2 + \beta^{\,2} = a^2 + b^2$$

avec $a = \alpha\,p + \beta\,u \in \mathbb{Z}$ et $b = \beta \in \mathbb{Z}$.

3.(a) On a cette fois $X^m - 1 = (X^4 - 1)(X^4 + 1)$ donc $X^4 + 1$ est scindé dans $K[X]$. Soit donc $z \in K$ une racine de $X^4 + 1$ et $x = z - 1/z$. On a :

$$x^2 = \frac{z^4 - 2z^2 + 1}{z^2} = -2$$

En choisissant un entier u représentant x, nous avons donc $u^2 + 2 \equiv 0 \bmod p$.

3.(b) Si p est un nombre premier congru à 1 modulo 8, on peut définir u comme à la question précédente et considérer le réseau $\Lambda = \mathbb{Z}(pe_1) + \mathbb{Z}(ue_1 + \sqrt{3}e_2)$. En choisissant $x_0 = \alpha\,pe_1 + \beta(ue_1 + \sqrt{2}e_2) \in \Lambda$ tel que $||x_0|| = m(\Lambda)$, on a comme dans la partie 2 :

$$\begin{cases} ||x_0||^2 = (\alpha p + \beta u)^2 + 2\beta^2 \equiv (u^2 + 2)\beta^2 \equiv 0 \bmod p \\ 0 < ||x_0||^2 = m(\Lambda_2) \leq \dfrac{2}{\sqrt{3}}\,\det\Lambda = \dfrac{2}{\sqrt{3}}\begin{vmatrix} p & u \\ 0 & \sqrt{2} \end{vmatrix} = 2p\,\dfrac{\sqrt{2}}{\sqrt{3}} < 2p \end{cases}$$

donc $p = a^2 + 2b^2$ avec $a = \alpha p + \beta u \in \mathbb{Z}$ et $b = \beta \in \mathbb{Z}$.

4.(a) La preuve est encore identique : quand $m = 3$, $X^m - 1 = (X - 1)(X^2 + X + 1)$ donc $X^2 + X + 1$ est scindé dans $K[X]$.

Le lien existant entre les racines de X^2+X+1 et de X^2+3 ne semble pas évident. On peut le deviner expérimentalement, en utilisant Maple : l'instruction ci-dessous calcule et affiche, pour les premières valeurs possibles de p, les listes des racines des deux polynômes :

```
> for q from 2 to 30 do
      p := 1+3*q;
         if isprime(p) then
            L1 := NULL; L2 := NULL;
            for x to p-1 do
               if x^2+x+1 mod p = 0 then L1 := L1,x fi;
               if x^2+3 mod p = 0 then L2 := L2,x fi;
            od;
            print(p,[L1],[L2])
         fi;
   od:
```

$$7, [2,4], [2,5]$$
$$13, [3,9], [6,7]$$
$$19, [7,11], [4,15]$$
$$31, [5,25], [11,20]$$
$$37, [10,26], [16,21]$$
$$43, [6,36], [13,30]$$
$$61, [13,47], [27,34]$$
$$67, [29,37], [8,59]$$
$$73, [8,64], [17,56]$$
$$79, [23,55], [32,47]$$

On peut conjecturer que les racines de X^2+3 sont $x-y$ et $y-x$, où x et y sont les deux racines de X^2+X+1, ce qui se vérifie facilement. En effet, les relations entre racines et coefficients donnent $x+y=-1$ et $xy=1$, donc

$$(x-y)^2 = x^2-2xy+y^2 = -x-1-2-y-1 = -3$$

En choisissant un entier u représentant $x-y$, nous avons donc $u^2+3 \equiv 0 \bmod p$.

4.(b) Soit $x = \alpha\, pe_1 + \beta(ue_1 + \sqrt{3}e_2) \in \Lambda$. Nous avons

$$||x||^2 = (\alpha p + \beta u)^2 + 3\beta^2 \equiv (u^2+3)\,\beta^2 \equiv 0 \bmod p$$

D'autre part, pour $a \in \mathbb{Z}/4\mathbb{Z}$, $a^2 = 0$ ou 1, donc pour $a, b \in \mathbb{Z}/4\mathbb{Z}$, $a^2+3b^2 \neq 2$; on en déduit que $||x||^2$ n'est pas congru à 2 modulo 4, ce qui revient à dire qu'il est ou impair, ou divisible par 4.

4.(c) Comme 3 divise $p-1$, on peut appliquer les résultats (a) et (b). En choisissant $x_0 = \alpha\, pe_1 + \beta(ue_1 + \sqrt{3}e_2) \in \Lambda$ tel que $||x_0|| = m(\Lambda)$, $||x_0||^2$ est un multiple de p qui est soit pair, soit divisible par 4. Or :

$$0 < ||x_0||^2 = m(\Lambda_2) \leq \frac{2}{\sqrt{3}} \det \Lambda = \frac{2}{\sqrt{3}} \begin{vmatrix} p & u \\ 0 & \sqrt{3} \end{vmatrix} = 2p$$

donc $||x_0||^2 = p$, puisque $2p$ n'est ni impair, ni multiple de 4, ce qui donne $p = a^2+3b^2$ avec $a = \alpha p + \beta u \in \mathbb{Z}$ et $b = \beta \in \mathbb{Z}$.