Réalisation de formes $\mathbb{Z}$-bilinéaires symétriques comme formes traces hermitiennes amplifiées

Grégory Berhuy

Introduction: Krüskemper a prouvé dans [2] que toute forme $\mathbb{Z}$-bilinéaire symétrique et non dégénérée peut se réaliser comme une forme trace amplifiée d'une algèbre $\mathbb{Z}[\alpha]$, où α est un entier algébrique. Le but de cet article est de montrer un résultat similaire concernant les formes traces hermitiennes amplifiées. Je remercie vivement Eva Bayer-Fluckiger, ma directrice de thèse, pour l'aide qu'elle m'a apporté dans la réalisation de ce travail.

Définitions et notations:

Dans ce qui suit, l'expression *forme $\mathbb{Z}$-bilinéaire* désigne un couple (M, b), où M est un $\mathbb{Z}$-module libre de type fini et où $b : M \times M \to \mathbb{Z}$ est une forme bilinéaire. On dit qu'elle est non dégénérée si elle est non dégénérée lorsqu'elle est vue comme forme $\mathbb{Q}$-bilinéaire.
Soit α un entier algébrique. Si I est un idéal de $\mathbb{Z}[\alpha]$, on note
$I^\sharp = \{x \in \mathbb{Q}(\alpha)/\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(xI) \subset \mathbb{Z}\}$. Soit $\mathfrak{I}$ un idéal de $\mathbb{Z}[\alpha]$, et soit λ un élément de $\mathbb{Q}(\alpha)$ tel que $\lambda \in (\mathfrak{I}^2)^\sharp$. La forme $\mathbb{Z}$-bilinéaire symétrique $\mathfrak{I} \times \mathfrak{I} \to \mathbb{Z}$, $(x, y) \mapsto \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\lambda xy)$ est appelée *forme trace amplifiée de* $\mathbb{Z}[\alpha]$ et est notée $(\mathfrak{I}, \mathrm{Tr}_\lambda)$.
Si de plus σ est une involution $\mathbb{Q}$-linéaire non triviale de $\mathbb{Q}(\alpha)$, et si μ est un élément de $\mathbb{Q}(\alpha)$ fixé par σ tel que $\mu \in (\mathfrak{I}\mathfrak{I}^\sigma)^\sharp$, la forme $\mathbb{Z}$-bilinéaire symétrique $\mathfrak{I} \times \mathfrak{I} \to \mathbb{Z}$ $(x, y) \mapsto \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\mu x y^\sigma)$ est appelée *forme trace hermitienne amplifiée de* $\mathbb{Z}[\alpha]$ par rapport à σ, et est notée $(\mathfrak{I}, \sigma, \mathrm{Tr}_\mu)$.
On notera $\mathbb{H}$ le plan hyperbolique $< 1, -1 >$. Enfin, si M est une matrice carrée, on note χ_M son polynôme caractéristique.

Réalisation de formes $\mathbb{Z}$-bilinéaires comme formes traces amplifiées:

Krüskemper a montré dans [2] le résultat suivant:

Théorème 1: Toute forme $\mathbb{Z}$-bilinéaire symétrique non dégénérée peut être réalisée comme forme trace amplifiée d'une algèbre $\mathbb{Z}[\alpha]$, pour un certain entier algébrique α.

Réalisation de formes $\mathbb{Z}$-bilinéaires comme formes traces hermitiennes amplifiées:

Dans la suite, on s'attachera à montrer le résultat suivant:

Théorème 2: Toute forme $\mathbb{Z}$-bilinéaire symétrique non dégénérée de rang pair, et non $\mathbb{Q}$-isomorphe à $\mathbb{H}$, peut être réalisée comme forme trace hermitienne amplifiée d'une algèbre $\mathbb{Z}[\alpha]$, où α est un entier algébrique.

Preuve: Dans ce qui suit, $S \in M_{2n}(\mathbb{Z})$ désignera la matrice de la forme bilinéaire considérée. On traite d'abord le cas $n = 1$, $\det S \in \mathbb{Q}^{*2}$, qui ne peut pas se résoudre par la méthode générale utilisée dans la suite. Remarquons qu'une forme trace hermitienne amplifiée d'une extension quadratique de $\mathbb{Q}$ est $\mathbb{Q}$-isométrique à $< 2\lambda, -2\lambda d >$, où $d \in \mathbb{Q}^* - \mathbb{Q}^{*2}$, et donc le discriminant de cette forme est différent de -1. Ainsi, une forme $\mathbb{Q}$-isomorphe à $\mathbb{H}$ ne peut se réaliser comme une forme trace hermitienne amplifiée.
Supposons maintenant que $n = 1$ et $\det S \in \mathbb{Q}^{*2}$. Alors S est congruente sur $\mathbb{Q}$ à sI_2 où $s \in \mathbb{Q}^*$, et donc il existe $U \in GL_n(\mathbb{Q})$ tel que $S = sU^tU$.
On peut supposer que U est à coefficients entiers. Sinon, il existe $r \in \mathbb{Z} - \{0\}$ tel que rU soit à coefficients entiers, et $S = \frac{s}{r^2}(rU)^t(rU)$.
Soit donc $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Posons alors $m = \det U$, $z_1 = m(ai + c)$, $z_2 = m(bi+d)$, et $\mathfrak{I} = \mathbb{Z}z_1 \oplus \mathbb{Z}z_2$. Montrons que $\mathfrak{I}$ est un idéal de $\mathbb{Z}[mi]$. Pour cela, il suffit de vérifier que $(mi)z_1$ et $(mi)z_2$ sont dans $\mathfrak{I}$. On vérifie aisément que $(mi)z_1 = (ab+cd)z_1 - (a^2+c^2)z_2$, et que $(mi)z_2 = (b^2+d^2)z_1 - (ab+cd)z_2$, et on a donc le résultat. Désignons maintenant par σ la conjugaison complexe, et posons $\lambda = \frac{s}{2m^2}$. On a alors $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(\lambda z_1 z_1^\sigma) = s(a^2 + c^2)$, $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(\lambda z_1 z_2^\sigma) = s(ab + cd)$, $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(\lambda z_2 z_2^\sigma) = s(b^2 + d^2)$, et donc S est la matrice de $(\mathfrak{I}, \sigma, \mathrm{Tr}_\lambda)$ relativement à la base z_1, z_2.

Pour traiter les autres cas, nous avons besoin du résultat suivant:

Proposition: Soit $D \in M_{2n}(\mathbb{Q})$ une matrice diagonale telle que $\det D \neq 0$ (avec $\det(D) \notin \mathbb{Q}^{*2}$ si $n = 1$). Alors il existe un entier algébrique α tel que $\alpha^2 \not\equiv -1 \pmod{\mathbb{Q}(\alpha^2)^{*2}}$, un élément $\lambda \in \mathbb{Q}(\alpha^2)$ et un idéal $\mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_{2n}$ de $\mathbb{Z}[\alpha]$, tels que $D = (\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\lambda v_i v_j))$.

Preuve de la proposition:

• On montre tout d'abord qu'il existe une matrice carrée de taille $2n$ A_{2n} à coefficients entiers, telle que $\chi_{A_{2n}}$ soit un polynôme pair irréductible sur $\mathbb{Q}$, et $D^{-1}A_{2n}D = A_{2n}^t$. Si $n = 1$, on peut supposer que $\det D \not\equiv \pm 1 \pmod{\mathbb{Q}^{*2}}$. Si $D = \begin{pmatrix} s_2 & 0 \\ 0 & s_1 \end{pmatrix}$, soit $m \in \mathbb{Z} - \{0\}$ tel que $ms_2^{-1}s_1$ soit un entier. La matrice $A_2 = \begin{pmatrix} 0 & m \\ ms_2^{-1}s_1 & 0 \end{pmatrix}$ convient alors.

Si $n \geq 2$, on a $D = \begin{pmatrix} s_{2n} & & \\ & \ddots & \\ & & s_1 \end{pmatrix}$

On construit des matrices tridiagonales de la manière suivante.

Soient $T_4, T_6, \cdots, T_{2n}$ et X des indéterminées indépendantes sur $\mathbb{Q}$ (remarquer que l'indice des T_i varie de 2 en 2).

Pour $2 \leq m \leq n$, on pose

$$B_{2m}(T_4, T_6, \cdots, T_{2m}) = \begin{pmatrix} 0 & T_{2m} & & & & & & & \\ T_{2m} & 0 & 1 & & & & & & \\ & 1 & 0 & T_{2m-2} & & & & & \\ & & T_{2m-2} & 0 & 1 & & & & \\ & & & 1 & 0 & \ddots & & & \\ & & & & \ddots & \ddots & T_4 & & \\ & & & & & T_4 & 0 & 1 & \\ & & & & & & 1 & 0 & 1 \\ & & & & & & & 1 & 0 \end{pmatrix}$$

On définit aussi $D_{2m} = diag < s_{2m}, \cdots, s_1 >$ pour $2 \leq m \leq 2n$. On pose alors $\Delta_{2m}(T_4, \cdots, T_{2m}, X) = \det(B_{2m} - XD_{2m}^{-1})$. On va montrer qu'il existe des spécialisations $T_{2j} = t_{2j}, 2 \leq j \leq n$ telles que $\Delta_{2n}(t_4, \cdots, t_{2n}, X)$ soit irréductible dans $\mathbb{Q}[X]$. Pour cela, on montre par récurrence que Δ_{2n} est irréductible dans $\mathbb{Q}[T_4, \cdots, T_{2n}, X]$, puis dans $\mathbb{Q}(T_4, \cdots, T_{2n})[X]$. On utilise alors le critère d'irréductibilité de Hilbert. Pour simplifier les notations, on omet les paramètres s_i.

Si $m = 2$, on a facilement
$\Delta_4(T_4, X) = -(s_2^{-1}s_1^{-1}X^2 - 1)T_4^2 + s_4^{-1}s_3^{-1}X^2(s_2^{-1}s_1^{-1}X^2 - 1) - s_4^{-1}s_1^{-1}X^2$.
On considère ce polynôme comme un élément de $\mathbb{Q}[X][T_4]$, et on montre qu'il est irréductible. Pour cela, il suffit de montrer son irréductibilité dans $\mathbb{Q}(X)[T_4]$. Supposons qu'il existe $R(X) \in \mathbb{Q}(X)$ tel que $\Delta_4(R(X), X) = 0$.
On a alors $-(s_2^{-1}s_1^{-1}X^2 - 1)R^2(X) + s_4^{-1}s_3^{-1}X^2(s_2^{-1}s_1^{-1}X^2 - 1) = s_4^{-1}s_1^{-1}X^2$.
Soit $I(X)$ un facteur irréductible de $s_2^{-1}s_1^{-1}X^2 - 1$. Si v_I désigne la valuation par rapport à I, on obtient
$v_I(s_2^{-1}s_1^{-1}X^2-1)+2v_I(R(X)) = v_I(s_4^{-1}s_1^{-1}X^2-s_4^{-1}s_3^{-1}X^2(s_2^{-1}s_1^{-1}X^2-1)) = 0$.
Il est clair que $s_2^{-1}s_1^{-1}X^2-1$ n'est pas un carré, et donc $v_I(s_2^{-1}s_1^{-1}X^2-1) = 1$.
On obtient donc $1 + 2v_I(R(X)) = 0$, ce qui est absurde, car $v_I(R(X)) \in \mathbb{Z}$.
Comme le degré en X de Δ_4 est égal à 2, cela montre son irréductibilité dans $\mathbb{Q}(X)[T_4]$, donc dans $\mathbb{Q}[X, T_4]$. Supposons avoir montré l'irréductibilité de $\Delta_{2m-2}(T_4, \cdots, T_{2m-2}, X)$ pour $m > 2$. Notons P_{2m-2} le déterminant de la matrice obtenue en ôtant la première ligne et la première colonne de $B_{2m-2} - XD_{2m-2}^{-1}$. Remarquons que $\deg P_{2m-2} < \deg\Delta_{2m-2}$, et donc Δ_{2m-2} ne divise pas P_{2m-2}. En développant le déterminant, on obtient
$\Delta_{2m} = -s_{2m}^{-1}XP_{2m} - T_{2m}^2\Delta_{2m-2}$.
On a ensuite $\Delta_{2m} = -s_{2m}^{-1}X(-s_{2m-1}^{-1}X\Delta_{2m-2} - P_{2m-2}) - T_{2m}^2\Delta_{2m-2}$. Considérons ce polynôme comme un élément de $\mathbb{Q}[T_4, \cdots, T_{2m-2}, X][T_{2m}]$. Il suffit de montrer son irréductibilité dans $\mathbb{Q}(T_4, \cdots, T_{2m-2}, X)[T_{2m}]$ pour avoir le résultat voulu. Supposons qu'il existe $R \in \mathbb{Q}(T_4, \cdots, T_{2m-2}, X)$ tel que $\Delta_{2m}(R, X) = 0$. On a alors $R^2\Delta_{2m-2} = -s_{2m}^{-1}X(-s_{2m-1}^{-1}X\Delta_{2m-2} - P_{2m-2})$.
Considérons la valuation $v_{\Delta_{2m-2}}$ par rapport à Δ_{2m-2}. Les propriétés élémentaires des valuations donnent immédiatement
$v_{\Delta_{2m-2}}(-s_{2m}^{-1}X(-s_{2m-1}^{-1}X\Delta_{2m-2} - P_{2m-2})) = v_{\Delta_{2m-2}}(P_{2m-2}) = 0$. En appliquant $v_{\Delta_{2m-2}}$ à l'égalité précédente, on obtient alors $1 + 2v_{\Delta_{2m-2}}(R) = 0$. Le même raisonnement que celui du cas précédent nous permet alors d'achever la récurrence. Bref, Δ_{2n} est irréductible dans $\mathbb{Q}[T_4, \cdots, T_{2n}, X]$. Montrons qu'il est irréductible dans $\mathbb{Q}(T_4, \cdots, T_{2n})[X]$. Pour cela, il suffit de le montrer pour $s_1 \cdots s_{2n}\Delta_{2n}$. Or ce dernier polynôme est unitaire en X et irréductible dans $\mathbb{Q}[T_4, \cdots, T_{2n}][X]$, donc dans $\mathbb{Q}(T_4, \cdots, T_{2n})[X]$. Le théorème d'irréductibilité de Hilbert nous donne alors le résultat voulu.
D'autre part, nous avons les relations $P_{2m} = -s_{2m-1}^{-1}X\Delta_{2m-2} - P_{2m-2}$ et $\Delta_{2m} = -s_{2m}^{-1}XP_{2m} - t_{2m}^2\Delta_{2m-2}$. Une récurrence immédiate nous montre alors que P_{2m} est impair et que Δ_{2m} est pair pour tout m.
Pour simplifier les notations, on note encore B_{2n} et Δ_{2n} la matrice et le polynôme obtenus en spécialisant.
Alors det $(DB_{2n} - XI_{2n}) = \det D \det(B_{2n} - XD_{2n}^{-1})$ est irréductible et pair, d'après ce qui précède. Soit $a_{2n} \in \mathbb{Z} - \{0\}$ tel que $A_{2n} = a_{2n}DB_{2n}$ soit à

coefficients entiers. Alors $\chi_{A_{2n}}(X) = a_{2n}^{2n}\chi_{DB_{2n}}(\dfrac{X}{a_{2n}})$ est encore irréductible pair. De plus, $D^{-1}A_{2n}D = a_{2n}B_{2n}D = a_{2n}B_{2n}^tD^t = (a_{2n}DB_{2n})^t = A_{2n}^t$.

• Soit $\alpha \in \mathbb{C}$ une valeur propre de A_{2n}. Par construction, c'est un entier algébrique. D'après [3], théorème 1, on peut choisir un vecteur propre $\mathbf{v}_\alpha = \begin{pmatrix} v_1 \\ \vdots \\ v_{2n} \end{pmatrix}$ de A_{2n} associé à α, avec $v_i \in \mathbb{Z}[\alpha]$ pour tout i, tel que $(v_1, \cdots, v_{2n})$ est une $\mathbb{Z}$-base d'un idéal de $\mathbb{Z}[\alpha]$. On prend en effet pour v_j le j-ième cofacteur de $A_{2n} - \alpha I_{2n}$ dans une ligne fixée. Le fait que l'on obtienne un vecteur propre provient de la formule de développement du déterminant par rapport à une ligne. Les relations $\alpha v_i = a_{i1}v_1 + \cdots + a_{in}v_{2n}$ suffisent à montrer que l'on obtient bien un idéal, car les coefficients a_{ij} sont entiers. De même, d'après [4], première preuve du théorème 1, il existe un vecteur propre $\mathbf{v}'_\alpha = \begin{pmatrix} v'_1 \\ \vdots \\ v'_{2n} \end{pmatrix}$ de A_{2n}^t associé à α, avec $v'_i \in \mathbb{Q}(\alpha)$, tel que $(v'_1, \cdots, v'_{2n})$ et $(v_1, \cdots, v_{2n})$ sont deux bases de $\mathbb{Q}(\alpha)$ duales par rapport à $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}$. Rappelons brièvement sa construction. Notons $\sigma_1, \cdots, \sigma_{2n}$ les $2n$ $\mathbb{Q}$-plongements de $\mathbb{Q}(\alpha)$ dans une clôture séparable, avec $\sigma_1 = \mathrm{Id}$. Posons $v_j^{(i)} = \sigma_i(v_j)$ et soit $M = (v_j^{(i)})$. Dans toute la suite, on notera μ_{ij} le mineur associé à $v_j^{(i)}$ et com(M) désignera la matrice des cofacteurs. Alors soit $v'_i = \dfrac{(-1)^{i+1}\mu_{i1}}{\det(M)}$. On peut montrer que c'est un élément de $\mathbb{Z}[\alpha]$. Le vecteur défini par ces $2n$ éléments possède alors les propriétés voulues (cela provient la formule de développement par rapport à une ligne, et de la relation $\det(M)I_{2n} = (\mathrm{com}(M))^tM$).
La relation $D^{-1}A_{2n}D = A_{2n}^t$ entraine que $D^{-1}\mathbf{v}_\alpha$ est un vecteur propre de A_{2n}^t, Puisque $\chi_{A_{2n}^t} = \chi_{A_{2n}}$ est irréductible sur $\mathbb{Q}$, il est séparable, et donc les sous-espaces propres associés à A_{2n}^t sont de dimension 1. et donc il existe $\lambda \in \mathbb{Q}(\alpha)$ tel que $\lambda D^{-1}\mathbf{v}_\alpha = \mathbf{v}'_\alpha$.

• Rappelons que la j-ième composante de $\mathbf{v}_\alpha$ est
$v_j = (-1)^{j+1}\delta_{1j}(A_{2n} - \alpha I_{2n})$ où $\delta_{1j}(A_{2n} - \alpha I_{2n})$ est le déterminant obtenu en ôtant la première ligne et la j-ième colonne de $A_{2n} - \alpha I_{2n}$ (cf [3], preuve du théorème 1). On va montrer que v_{2j-1} est un polynôme impair en α et que v_{2j} est pair en α, pour $1 \leq j \leq n$. C'est vrai pour $n = 1$ et $n = 2$. Supposons maintenant $n \geq 3$. On voit facilement que $A_{2n} =$

$$a_{2n}\begin{pmatrix} 0 & s_{2n}t_{2n} & 0 & 0 & \cdots & 0 \\ s_{2n-1}t_{2n} & 0 & s_{2n-1} & 0 & \cdots & 0 \\ 0 & s_{2n-2} & & & & \\ 0 & 0 & & & a_{2n-2}^{-1}A_{2n-2} & \\ \vdots & \vdots & & & & \\ 0 & 0 & & & & \end{pmatrix}$$

On peut supposer sans perte de généralité que $a_{2m} = 1$ pour tout $m \geq 2$. Un simple calcul de déterminants nous donne alors
$\delta_{11}(A_{2n} - \alpha I_{2n}) = -\alpha \det(A_{2n-2} - \alpha I_{2n-2}) - s_{2n-1}s_{2n-2}\delta_{11}(A_{2n-2} - \alpha I_{2n-2})$.
Mais $\det(A_{2n-2} - \alpha I_{2n-2}) = \chi_{A_{2n-2}}(\alpha)$ est pair en α. Par hypothèse de récurrence, $\delta_{11}(A_{2n-2} - \alpha I_{2n-2})$ est impair en α. Le résultat est donc montré si $j = 1$. Si $j = 2$, on a $\delta_{12}(A_{2n} - \alpha I_{2n}) = s_{2n-1}t_{2n} \det(A_{2n-2} - \alpha I_{2n-2})$, et si $j > 2$, $\delta_{1j}(A_{2n} - \alpha I_{2n}) = s_{2n-1}t_{2n}\delta_{1(j-2)}(A_{2n-2} - \alpha I_{2n-2})$, et en utilisant l'hypothèse de récurrence, on a le résultat.

• On montre maintenant que $\lambda \in \mathbb{Q}(\alpha^2)$. On a $\mathbf{v}_\alpha = \begin{pmatrix} I_1(\alpha) \\ E_1(\alpha) \\ \vdots \\ I_n(\alpha) \\ E_n(\alpha) \end{pmatrix}$, où les E_i et les I_i sont des polynômes à coefficients entiers respectivement pairs et impairs. Comme $Irr(\alpha, \mathbb{Q}) = \chi_{A_{2n}}$ est pair, les conjugués de α s'écrivent $\pm\alpha, \pm\alpha_2, \cdots, \pm\alpha_n$.
Soient $\sigma_1 : \alpha \mapsto \alpha, \sigma_2 : \alpha \mapsto -\alpha, \cdots, \sigma_{2n-1} : \alpha \mapsto \alpha_n, \sigma_{2n} : \alpha \mapsto -\alpha_n$ les $2n$ $\mathbb{Q}$-plongements de $\mathbb{Q}(\alpha)$. Comme précédemment, notons M la matrice dont le coefficient à l'intersection de la ligne i et de la colonne j est le i-ème conjugué de v_j. Autrement dit, $M = (\sigma_i(v_j))$. On rappelle alors que $v_i' = (-1)^{i+1}\dfrac{\mu_{i1}}{\det M}$(cf.[4], première preuve du théorème 1). On va montrer que $\alpha v_1' \in \mathbb{Q}(\alpha^2)$. Pour cela, on montre que cette quantité est invariante par les éléments du groupe de Galois de la clôture galoisienne de $\mathbb{Q}(\alpha)$ qui fixent $\mathbb{Q}(\alpha^2)$. Ces automorphismes τ envoient α sur $\pm\alpha$ et induisent une permutation s_τ de l'ensemble $\{\pm\alpha_2, \cdots, \pm\alpha_n\}$.

On a $\det M = \begin{vmatrix} I_1(\alpha) & E_1(\alpha) & I_2(\alpha) & E_2(\alpha) & \cdots & I_n(\alpha) & E_n(\alpha) \\ -I_1(\alpha) & E_1(\alpha) & -I_2(\alpha) & E_2(\alpha) & \cdots & -I_n(\alpha) & E_n(\alpha) \\ \vdots & & & & & & \vdots \\ \vdots & & & & & & \vdots \\ I_1(\alpha_n) & E_1(\alpha_n) & I_2(\alpha_n) & E_2(\alpha_n) & \cdots & I_n(\alpha_n) & E_n(\alpha_n) \\ -I_1(\alpha_n) & E_1(\alpha_n) & -I_2(\alpha_n) & E_2(\alpha_n) & \cdots & -I_n(\alpha_n) & E_n(\alpha_n) \end{vmatrix}$

Notons $\varepsilon(s_\tau)$ la signature de la permutation s_τ. Par échange des lignes deux à deux, on voit que $\tau(\det M) = \varepsilon(s_\tau)\det M$ si $\tau(\alpha) = \alpha$, et
$\tau(\det M) = -\varepsilon(s_\tau)\det M$ si $\tau(\alpha) = -\alpha$, d'où $\tau(\alpha^{-1} \det M) = \varepsilon(s_\tau)\alpha^{-1}\det M$, pour tout τ. On veut montrer que la valeur de μ_{11} ne change pas lorsque l'on remplace α par $-\alpha$. Or on a

$$\mu_{11}(-\alpha) = \begin{vmatrix} E_1(\alpha) & I_2(\alpha) & E_2(\alpha) & \cdots & I_n(\alpha) & E_n(\alpha) \\ E_1(\alpha_2) & I_2(\alpha_2) & E_2(\alpha_2) & \cdots & I_n(\alpha_2) & E_n(\alpha_2) \\ E_1(\alpha_2) & -I_2(\alpha_2) & E_2(\alpha_2) & \cdots & I_n(\alpha_2) & E_n(\alpha_2) \\ \vdots & & & & & \vdots \\ \vdots & & & & & \vdots \\ E_1(\alpha_n) & I_2(\alpha_n) & E_2(\alpha_n) & \cdots & I_n(\alpha_n) & E_n(\alpha_n) \\ E_1(\alpha_n) & -I_2(\alpha_n) & E_2(\alpha_n) & \cdots & -I_n(\alpha_n) & E_n(\alpha_n) \end{vmatrix}$$

$$= (-1)^{n-1} \begin{vmatrix} E_1(\alpha) & -I_2(\alpha) & E_2(\alpha) & \cdots & -I_n(\alpha) & E_n(\alpha) \\ E_1(\alpha_2) & -I_2(\alpha_2) & E_2(\alpha_2) & \cdots & -I_n(\alpha_n) & E_n(\alpha_n) \\ E_1(\alpha_2) & I_2(\alpha_2) & E_2(\alpha_2) & \cdots & I_n(\alpha_2) & E_n(\alpha_n) \\ \vdots & & & & & \vdots \\ \vdots & & & & & \vdots \\ E_1(\alpha_n) & -I_2(\alpha_n) & E_2(\alpha_n) & \cdots & -I_n(\alpha_n) & E_n(\alpha_n) \\ E_1(\alpha_n) & I_2(\alpha_n) & E_2(\alpha_n) & \cdots & I_n(\alpha_n) & E_n(\alpha_n) \end{vmatrix}$$

En procédant à l'échange des lignes deux à deux, on en déduit que ce déterminant est égal à μ_{11}, ce qu'on voulait montrer. On obtient donc $\tau(\mu_{11}) = \varepsilon(s_\tau)\mu_{11}$ pour tout τ. Finalement, $\tau(\alpha\dfrac{\mu_{11}}{\det M}) = \alpha\dfrac{\mu_{11}}{\det M}$, donc $\alpha v_1' \in \mathbb{Q}(\alpha^2)$ et $\lambda = s_{2n}\dfrac{v_1'}{I_1(\alpha)} = s_{2n}\dfrac{\alpha v_1'}{\alpha I_1(\alpha)} \in \mathbb{Q}(\alpha^2)$.

Puisqu'on a $\lambda D^{-1}\mathbf{v}_\alpha = \mathbf{v}'_\alpha$, on a alors $\lambda\mathbf{v}_\alpha = D\mathbf{v}'_\alpha$, soit $\lambda v_j = s_{2n+1-j}v_j'$ et donc $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\lambda v_i v_j) = s_{2n+1-j}\delta_{ij}$. On en déduit que $D = (\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\lambda v_i v_j))$.

• On montre enfin que l'on peut choisir α tel que $\alpha^2 \not\equiv -1 \pmod{\mathbb{Q}(\alpha^2)^{*2}}$. Puisque Δ_{2m} est pair, on peut écrire
$\Delta_{2m}(T_4, \cdots, T_{2m}, X) = U_{2m}(T_4, \cdots, T_{2m}, X^2)$. On peut aisément montrer (comme pour Δ_{2m}) que le polynôme
$F_{2m}(T_4, \cdots, T_{2m}, X) = U_{2m}(T_4, \cdots, T_{2m}, -X^2)$ est irréductible pour tout m. D'après le critère d'irréductibilité de Hilbert, on peut trouver une spécialisation

des T_i telle que les polynômes spécialisés Δ_{2n} et F_{2n} sont irréductibles.
Soit alors $\alpha \in \mathbb{C}$ une racine de Δ_{2n}.
Par définition, $F_{2n}(\sqrt{-\alpha^2}) = \Delta_{2n}(\alpha) = 0$. Puisque $(-1)^n \det DF_{2n}$ est irréductible et unitaire, on obtient $Irr(\sqrt{-\alpha^2}, \mathbb{Q}) = (-1)^n \det DF_{2n}$. Ainsi $[\mathbb{Q}(\sqrt{-\alpha^2}) : \mathbb{Q}] = 2n$ et $[\mathbb{Q}(\sqrt{-\alpha^2}) : \mathbb{Q}(\alpha^2)] = 2$, ce qui signifie que $-\alpha^2$ n'est pas un carré dans $\mathbb{Q}(\alpha^2)$. Ceci achève la preuve de la proposition.

Fin de la preuve du théorème 2:

• Soit $S \in M_{2n}(\mathbb{Z})$, telle que $\det S \neq 0$. Si $n = 1$, on suppose de plus que $\det S \not\equiv \pm 1 \pmod{\mathbb{Q}^{*2}}$. On a $S = U^t D U$, où $U \in GL_{2n}(\mathbb{Q})$ et D vérifie les hypothèses de la proposition. On peut supposer U à coefficients dans $\mathbb{Z}$, sinon il existe $a \in \mathbb{Z} - \{0\}$ tel que aU est à coefficients entiers, et $S = (aU)^t \dfrac{1}{a^2} D(aU)$.
On considère alors les éléments $A_{2n}, \mathbf{v}_\alpha, \mathbf{v}'_\alpha$ et λ associés à D grâce à la proposition précédente. On a $D = (U^t)^{-1} S U^{-1}$, et donc $D^{-1} = U S^{-1} U^t$.
Alors $\lambda U S^{-1} U^t \mathbf{v}_\alpha = \mathbf{v}'_\alpha$, c'est-à-dire $\lambda S^{-1} U^t \mathbf{v}_\alpha = U^{-1} \mathbf{v}'_\alpha$.
Posons $C = m U^t A_{2n} (U^t)^{-1}$, avec $m \in \mathbb{Z} - \{0\}$ tel que C est à coefficients entiers, $\mathbf{w}_\alpha = m^{2n-1} U^t \mathbf{v}_\alpha = \begin{pmatrix} w_1 \\ \vdots \\ w_{2n} \end{pmatrix}$, $\mathbf{w}'_\alpha = \dfrac{1}{m^{2n-1}} U^{-1} \mathbf{v}'_\alpha = \begin{pmatrix} w'_1 \\ \vdots \\ w'_{2n} \end{pmatrix}$.
On a alors $m^{-4n+2} \lambda S^{-1} \mathbf{w}_\alpha = \mathbf{w}'_\alpha$. On va montrer que $\mathfrak{A} = \mathbb{Z} w_1 \oplus \cdots \oplus \mathbb{Z} w_{2n}$ est un idéal de $\mathbb{Z}[m\alpha]$. On voit facilement que $w_i \in \mathbb{Z}[m\alpha]$ pour tout i. On a d'autre part $m\alpha \mathbf{w}_\alpha = C \mathbf{w}_\alpha$. Comme C est à coefficients entiers, cela suffit à montrer que $\mathbb{Z} w_1 \oplus \cdots \oplus \mathbb{Z} w_{2n}$ est un idéal. De plus, on a
$m^{-4n+2} \lambda \mathbf{w}_\alpha = S \mathbf{w}'_\alpha = (\sum_{j=1}^{2n} s_{ij} w'_j)_{1 \leq 1 \leq n}$, et donc $m^{-4n+2} \lambda w_i w_k = \sum_{j=1}^{2n} s_{ij} w_k w'_j$.
Notons $U = (u_{ij})$ et $U^{-1} = (u'_{ij})$. Alors $w_i = m^{2n-1} \sum_{j=1}^{2n} u_{ji} v_j$ et
$w'_i = \dfrac{1}{m^{2n-1}} \sum_{j=1}^{2n} u'_{ij} v'_j$. Donc $w_k w'_j = \sum_{i,l} u_{ik} u'_{jl} v_i v'_l$. On a alors
$\mathrm{Tr}_{\mathbb{Q}(m\alpha)/\mathbb{Q}}(w_k w'_j) = \sum_{i,l} u_{ik} u'_{jl} \delta_{il} = \sum_{i=1}^{2n} u_{ik} u'_{ji} = \delta_{kj}$.
D'où $s_{ik} = \mathrm{Tr}_{\mathbb{Q}(m\alpha)/\mathbb{Q}}(m^{-4n+2} \lambda w_i w_k)$. De plus, $m^{-4n+2} \lambda \in \mathbb{Q}(\alpha^2) = \mathbb{Q}((m\alpha)^2)$.

On vient donc de montrer que $S = (\mathrm{Tr}_{\mathbb{Q}(m\alpha)/\mathbb{Q}}(m^{-4n+2} \lambda w_i w_j))$, où α est un entier algébrique α tel que $\alpha^2 \not\equiv -1 \pmod{\mathbb{Q}(\alpha^2)}$, $\lambda \in \mathbb{Q}((m\alpha)^2)$, m est un entier, égal à 1 si S est diagonale, et $\mathbb{Z} w_1 \oplus \cdots \oplus \mathbb{Z} w_{2n}$ est un idéal de $\mathbb{Z}[m\alpha]$.

• Par construction de α, $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^2)] = 2$, et w_i s'écrit alors de manière unique sous la forme $w_i = x_i + m\alpha y_i$, où $x_i, y_i \in \mathbb{Z}[(m\alpha)^2]$.
Posons $z_i = x_i + my_i\beta$, avec $\beta = \sqrt{-\alpha^2}$, et notons $\mathbf{z}_\beta$ le vecteur de composantes z_i.
Soit enfin σ l'involution $\mathbb{Q}$-linéaire de $\mathbb{Q}(m\beta)$ définie par $\beta \mapsto -\beta$, $\sigma|_{\mathbb{Q}(\alpha^2)} = \mathrm{Id}$. On vérifie que $\mathrm{Tr}_{\mathbb{Q}(m\alpha)/\mathbb{Q}}(m^{-4n+2}\lambda w_i w_j)$
$= \mathrm{Tr}_{\mathbb{Q}(\alpha^2)/\mathbb{Q}}(2\lambda(x_ix_j + m^2\alpha^2 y_iy_j)) = \mathrm{Tr}_{\mathbb{Q}(m\beta)/\mathbb{Q}}(m^{-4n+2}\lambda z_i z_j^\sigma)$.
Il reste à montrer que $\mathfrak{I} = \mathbb{Z}z_1 \oplus \cdots \mathbb{Z}z_{2n}$ est un idéal de $\mathbb{Z}[m\beta]$. Rappelons tout d'abord que la i-ème composante de $\mathbf{v}_\alpha$ est un polynôme en α de la parité de i. On peut donc poser $v_{2i} = x'_{2i}$ et $v_{2i-1} = \alpha y'_{2i-1}$, où $x'_{2i}, y'_{2i-1} \in \mathbb{Z}[\alpha^2]$, pour $i = 1, \cdots, n$. Soit $\mathbf{t}_\beta$ le vecteur défini par $t_{2i} = x'_{2i}$, et $t_{2i-1} = \beta y'_{2i-1}$ pour $i = 1, \cdots, n$. On va montrer l'existence d'une matrice à coefficients entiers, qui admet $\mathbf{t}_\beta$ comme vecteur propre associé à la valeur propre β. Par définition, $\mathbf{v}_\alpha$ est un vecteur propre de A_{2n}. Par construction même de $A_{2n} = (a_{ij})$, on a $a_{2i-1,2j-1} = a_{2i,2j} = 0$ pour $1 \le i, j \le n$.
On a $\alpha v_{2i-1} = \sum_{j=1}^{n} a_{2i-1,2j}v_{2j}$, et $\alpha v_{2i} = \sum_{j=1}^{n} a_{2i,2j-1}v_{2j-1}$.
On en déduit $\alpha^2 y'_{2i-1} = \sum_{j=1}^{n} a_{2i-1,2j}x'_{2j}$ et $x'_{2i} = \sum_{j=1}^{n} a_{2i,2j-1}y'_{2j-1}$.
On a alors $\beta t_{2i-1} = \beta^2 y'_{2i-1} = -\alpha^2 y'_{2i-1} = -\sum_{j=1}^{n} a_{2i-1,2j}x'_{2j} = -\sum_{j=1}^{n} a_{2i-1,2j}t_{2j}$.
On a aussi
$\beta^2 t_{2i} = \beta^2 x'_{2i} = \beta^2 \sum_{j=1}^{n} a_{2i,2j-1}y_{2j-1}\prime = \sum_{j=1}^{n} a_{2i,2j-1}\beta^2 y'_{2j-1} = \sum_{j=1}^{n} a_{2i,2j-1}\beta t_{2j-1}$.
D'où $\beta t_{2i} = \sum_{j=1}^{n} a_{2i,2j-1}t_{2j-1}$. Les relations précédentes nous assurent l'existence d'une matrice $B \in M_{2n}(\mathbb{Z})$ telle que $B\mathbf{t}_\beta = \beta\mathbf{t}_\beta$. Il est clair que $\mathbf{z}_\beta = m^{2n-1}U^tB\mathbf{t}_\beta$, car $\mathbf{t}_\beta$ a été défini à partir de $\mathbf{v}_\alpha$ de la même manière que $\mathbf{z}_\beta$ a été défini à partir de $\mathbf{w}_\alpha$, c'est-à-dire en laissant fixe les polynômes en α^2, et en remplaçant α par β (on peut également faire un calcul pour s'en convaincre). Par construction de $B = (b_{ij})$, on a $b_{ij} = \pm a_{ij}$, ce qui entraîne facilement que $m^{2n-1}U^tB$ est à coefficients entiers. Comme précédemment, cela suffit pour conclure. Remarquons que $m^{-4n+2}\lambda \in (\mathfrak{I}\mathfrak{I}^\sigma)^\sharp$, puisque la matrice de la forme trace hermitienne amplifiée dans la base $(z_1, \cdots, z_{2n})$ est par construction la matrice S, qui est à coefficients entiers. Enfin, il est bien clair que β est un entier algébrique. On a finalement montré que S est la matrice de $(\mathfrak{I}, \sigma, \mathrm{Tr}_{m^{-4n+2}\lambda})$.

On remarque que le théorème et sa démonstration restent valables si on remplace $\mathbb{Q}$ et $\mathbb{Z}$ par un corps de nombres et son anneau des entiers, puisque tout corps de nombres est hilbertien.

Remarques sur l'effectivité de la méthode et calcul pratique:

La méthode décrite dans la preuve permet de trouver explicitement les éléments définissant la forme trace hermitienne amplifiée. En effet, on diagonalise S en s'arrangeant pour avoir une matrice de changement de base à coefficients entiers. Ensuite, on calcule A_{2n}. Il n'y a aucune difficulté à trouver une matrice de polynôme caractéristique irréductible, car en choisissant $t_2, \cdots, t_{2n}$ au hasard, on trouve presque surement une matrice qui convient. On calcule ensuite les v_i. Ce sont des polynômes en α de degrés inférieurs ou égaux à $2n-1$.
Il n'est donc pas nécessaire d'utiliser la relation $\chi_{A_{2n}}(\alpha) = 0$ pour calculer l'expression finale, et donc cela ne dépend pas de la nature de α. Autrement dit, α peut être considéré dans ce calcul comme une indéterminée, et donc un logiciel de calcul formel effectuera ceci sans aucun problème. La difficulté réside a priori dans la détermination des v'_i (indispensable pour calculer λ), car l'expression donnée dans la preuve dépend des conjugués de α, et une fois le calcul des déterminants effectués, il faut manipuler l'expression obtenue de manière à obtenir un résultat ne dépendant que de α, ce qui est loin d'être aisé, et ne se fait pas de manière algorithmique. Ce qui suit donne une méthode qui permet de calculer v'_i de manière systématique. On sait que $(v_1, \cdots, v_{2n})$ et $(v'_1, \cdots, v'_{2n})$ forment deux bases de $\mathbb{Q}(\alpha)$. On montre facilement que $v_i = \sum_{j=1}^{2n} \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(v_i v_j) v'_j$.
Soit $G = (\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{i-1}\alpha^{j-1}))_{1 \leq i,j \leq 2n}$. Grâce aux relations de Newton, on s'aperçoit que le calcul des coefficients de cette matrice revient à l'inversion d'une matrice triangulaire, ce qui est simple. Soit V la matrice des coordonnées de $(v_1, \cdots, v_{2n})$ dans la base $(1, \alpha, \cdots, \alpha^{2n-1})$. La relation précédente nous montre alors que les coordonnées des v'_i dans la base $(1, \alpha, \cdots, \alpha^{2n-1})$ sont données par les vecteurs colonnes de $G^{-1}V^t = (m_{ij})_{1 \leq i,j \leq 2n}$. Autrement dit, $v'_j = \sum_{\imath=1}^{2n} m_{ij}\alpha^{i-1}$. On achève ensuite le calcul en trouvant m et en explicitant les w_i, puis les z_i.

Exemple:

On conserve dans la suite les notations précédentes. On va appliquer la méthode précédente pour réaliser le réseau $\mathbb{A}_4$.

La forme bilinéaire associée à ce réseau a pour matrice $S = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}$.

On trouve alors par réduction de Gauss $D = \begin{pmatrix} \frac{1}{72} & 0 & 0 & 0 \\ 0 & \frac{1}{96} & 0 & 0 \\ 0 & 0 & \frac{1}{108} & 0 \\ 0 & 0 & 0 & \frac{5}{576} \end{pmatrix}$

et $U = \begin{pmatrix} 12 & 6 & 6 & 6 \\ 0 & 12 & 4 & 4 \\ 0 & 0 & 12 & 3 \\ 0 & 0 & 0 & 12 \end{pmatrix}$ (On s'est arrangé pour avoir U à coefficients entiers).

En prenant $t_4 = 1$ dans B_4 et en multipliant par un entier convenable pour avoir des coefficients entiers, on trouve

$A_4 = \begin{pmatrix} 0 & 24 & 0 & 0 \\ 18 & 0 & 18 & 0 \\ 0 & 16 & 0 & 16 \\ 0 & 0 & 15 & 0 \end{pmatrix}$

0n a $\chi_{A_4}(X) = X^4 - 960X^2 + 103680$, qui est irréductible sur $\mathbb{Q}$ car c'est un polynôme d'Einsenstein pour $p = 5$. Soit $\alpha \in \mathbb{C}$ une racine de ce polynôme.

On obtient alors $\mathbf{v}_\alpha = \begin{pmatrix} 528\alpha - \alpha^3 \\ 4320 - 18\alpha^2 \\ -288\alpha \\ -4320 \end{pmatrix}$, c'est-à-dire

$V = \begin{pmatrix} 0 & 4320 & 0 & -4320 \\ 528 & 0 & -288 & 0 \\ 0 & -18 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$

Posons $\sigma_i = \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^i)$.

Les relations de Newton donnent alors immédiatement $\sigma_0 = 4$, $\sigma_2 = 1920$, $\sigma_4 = 1428480$, $\sigma_6 = 1172275200$ et $\sigma_1 = \sigma_3 = \sigma_5 = 0$.

On a donc $G = \begin{pmatrix} 4 & 0 & 1920 & 0 \\ 0 & 1920 & 0 & 1428480 \\ 1920 & 0 & 1428480 & 0 \\ 0 & 1428480 & 0 & 1172275200 \end{pmatrix}$

La dernière colonne de $G^{-1}V^t$ nous donne $v'_4 = -\frac{7}{63360} + \frac{\alpha^2}{9123840}$.
La relation $\lambda \mathbf{v}_\alpha = D\mathbf{v}'_\alpha$ appliquée à la dernière coordonnée nous donne alors $\lambda = \frac{7}{31531991040} - \frac{\alpha^2}{4540606709760}$. On vérifie par simple calcul que $m = 1$.

On a alors $\mathbf{w}_\alpha = \begin{pmatrix} (6336 - 12\alpha^2)\alpha \\ (51840 - 216\alpha^2) + (3168 - 6\alpha^2)\alpha \\ (17280 - 72\alpha^2) - (288 + 6\alpha^2)\alpha \\ -(34560 + 72\alpha^2) + (2304 - 6\alpha^2)\alpha \end{pmatrix}$.

Posons $\beta = \sqrt{-\alpha^2}$. Alors $\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} (6336 + 12\beta^2)\beta \\ (51840 + 216\beta^2) + (3168 + 6\beta^2)\beta \\ (17280 + 72\beta^2) + (6\beta^2 - 288)\beta \\ (72\beta^2 - 34560) + (2304 + 6\beta^2)\beta \end{pmatrix}$.

S se réalise donc comme la forme trace hermitienne amplifiée de l'algèbre $\mathbb{Z}[\beta]$ $(\mathfrak{I}, \sigma, \mathrm{Tr}_\lambda)$ avec $Irr(\beta, \mathbb{Q}) = X^4 + 960X^2 + 103680$, $\mathfrak{I} = \mathbb{Z}z_1 \oplus \mathbb{Z}z_2 \oplus \mathbb{Z}z_3 \oplus \mathbb{Z}z_4$, $\lambda = \frac{7}{31531991040} + \frac{\beta^2}{4540606709760}$ et $\sigma : \mathbb{Q}(\beta) \to \mathbb{Q}(\beta), \beta \mapsto -\beta$.

Remarquons que ce n'est pas la construction la plus simple de $\mathbb{A}_4$ en tant que forme trace hermitienne amplifiée. En effet on peut obtenir $\mathbb{A}_4$ à partir des racines 5-ièmes de l'unité (cf. par exemple [1], §4).

References

[1] Eva Bayer-Fluckiger, Jacques Martinet. *Formes quadratiques liées aux algèbres semi-simples.* J. reine angew. Math. 451, 51-69 (1994).

[2] Martin Krüskemper. *Algebraic construction of bilinear forms over $\mathbb{Z}$.* Pub. Math. de Besançon, Théorie des nombres (96/97-97/98).

[3] Olga Taussky. *On a theorem of Latimer and MacDuffee.* Canad. J. Math. 1, 300-302 (1949).

[4] Olga Taussky. *On matrix classes corresponding to an ideal and its inverse.* Illinois Math. J. 1, 108-113 (1957).

e-mail:berhuy@math.univ-fcomte.fr