Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 3, N. 1, 2015.
Trabalho apresentado no XXXV CNMAC, Natal-RN, 2014.

Uma nova construção do reticulado de Leech via reticulados ideais

Carina Alves
Depto de Matemática, IGCE, UNESP
13506-900, Rio Claro, SP
carina@rc.unesp.br

Jean-Claude Belfiore
TELECOM - ParisTech, Paris, França
75013, Rua Barrault 46, Paris, França
jean-claude.belfiore@telecom-paristech.fr

Resumo: *Neste trabalho, apresentamos novas construções algébricas de reticulados com densidade de empacotamento ótima em dimensões 8 e 24, onde estes reticulados são versões escalonadas do reticulado E_8 e do reticulado de Leech Λ_{24}, respectivamente. Mais especificamente, via a teoria de reticulado ideal propomos uma nova construção do reticulado de Leech Λ_{24} fazendo uma combinação das construções algébricas do reticulado E_8 e do reticulado de Barnes P_b. Além disso, verificamos que o reticulado Λ_{24} pode ser construído como o produto tensorial sobre $\mathbb{Z}[\alpha]$, onde $\alpha = (1+\sqrt{-7})/2$, de dois reticulados que quando vistos como um $\mathbb{Z}$-reticulado, são equivalentes a E_8 e a P_b.*

Palavras-chave: *Reticulado ideal, densidade de empacotamento, produto tensorial*

1 Introdução

Reticulados podem ser construídos via um corpo de números $\mathbb{K}$ considerando a representação geométrica de ideais no anel dos inteiros de $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$. Craig, em [4], mostrou que os reticulados D_4, E_8, K_{12}, Λ_{16} e Λ_{24} podem serem obtidos a partir de ideais devidamente escolhidos no anel dos inteiros de corpos ciclotômicos. A vantagem de obter reticulados por este método é que podemos identificar os pontos do reticulado no $\mathbb{R}^n$ como elementos de um corpo de números, e portanto, é possível utilizar algumas propriedades do corpo no estudo de tais reticulados.

Neste trabalho, focamos nos reticulados E_8 e Λ_{24}, sendo que ambos tem grupo de isometria finito e tem densidade de empacotamento ótimas em suas respectivas dimensões. Em [7] Λ_{24} foi construído usando o produto tensorial de dois reticulados sobre $\mathbb{Z}[\alpha]$, onde $\alpha = (1+\sqrt{-7})/2$, e que quando vistos como um $\mathbb{Z}$-reticulado, são equivalentes ao reticulado E_8 e ao reticulado de Barnes P_b. M. Hentschel [6] classificou todas as $\mathbb{Z}[\alpha]$ estruturas sobre os $\mathbb{Z}$-reticulados pares e unimodulares de dimensão 24. Em particular, existem exatamente nove estruturas sobre $\mathbb{Z}[\alpha]$ que produzem o reticulado de Leech Λ_{24}, sendo que uma delas é via o produto tensorial.

Tendo a construção de reticulados algébricos como motivação, apresentamos neste trabalho uma nova construção do reticulado E_8 e do reticulado de Leech Λ_{24} via reticulados ideais. A importância para este tipo de construção é que reticulados ideais tem muitas aplicações. Por exemplo, podemos usar reticulados ideais como uma ferramenta para construir códigos reticulados para camadas físicas e na área de criptografia, reticulados ideais podem ser usados

DOI: 10.5540/03.2015.003.01.0195

em esquemas de encriptação totalmente homomórficas, permitindo uma multiplicação de difícil decodificação [5].

Este trabalho é organizado como segue. Na seção 2, selecionamos alguns resultados básicos da teoria de reticulados ideais. Na Seção 3, mostramos como obter um $\mathbb{Z}$-reticulado a partir de um $\mathbb{Z}[\alpha]$-reticulado. Na Seção 4, apresentamos uma condição necessária para a construção de reticulados escalonados. Na Seção 5, uma nova construção do reticulado E_8 é apresentada. Na Seção 6, apresentamos uma nova construção do reticulado de Leech Λ_{24} via reticulado ideal. Nesta mesma seção, abordamos uma construção do reticulado de Barnes P_b. Finalmente, na Seção 7, apresentamos nossa conclusão.

2 Reticulado ideal

Nesta seção, apresentamos alguns conceitos e resultados sobre reticulados ideais. Resultados sobre teoria algébrica dos números e reticulados algébricos usados neste trabalho podem ser encontrados em [2]. Por questão de conveniência, ao longo deste trabalho vamos considerar o corpo $\mathbb{F} = \mathbb{Q}(\alpha)$, onde $\alpha = (1 + \sqrt{-7})/2$, e seu anel dos inteiros $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\alpha]$.

Um *reticulado* m-dimensional $\Lambda \subseteq \mathbb{R}^m$ é um conjunto discreto de pontos do $\mathbb{R}^m$ gerado por combinações lineares inteiras de n vetores linearmente independentes $v_1, \cdots, v_n \in \mathbb{R}^m$. Chamamos de $\mathbb{Z}[\alpha]$-reticulado ao conjunto de pontos da forma

$$\Lambda_\alpha = \{\mathbf{x} = \lambda M \,:\, \lambda \in \mathbb{Z}[\alpha]^n\},$$

onde M é a *matriz geradora* e $M^\dagger M$ é a *matriz de Gram*, sendo que $\dagger$ denota a transposta conjugada. O reticulado $\mathbb{Z}[\alpha]$ pode ser obtido usando o mergulho canônico relativo de um corpo de números. Esta estrutura permite descrever com precisão alguns parâmetros do reticulado em termos de estruturas algébricas, de modo análogo ao caso de reticulados algébricos reais.

Seja $\mathbb{K}$ uma extensão de Galois de grau n sobre $\mathbb{Q}(\alpha)$. Denotamos por $Gal(\mathbb{K}/\mathbb{Q}(\alpha)) = \{\sigma_1, \cdots, \sigma_n\}$ o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}(\alpha)$. O *mergulho canônico relativo* de $\mathbb{K}$ em $\mathbb{C}^n$ é definido como

$$\begin{aligned} \sigma : \quad \mathbb{K} &\to \mathbb{C} \\ x &\mapsto \sigma(x) = (\sigma(x), \cdots, \sigma_n(x)) \end{aligned}$$

Seja $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$. Como $\mathbb{Z}[\alpha]$ é principal, segue que existe uma $\mathbb{Z}[\alpha]$-base $\mathcal{B}_{\mathbb{K}} = \{w_1, \cdots, w_n\}$. A matriz geradora do reticulado $\Lambda_\alpha(\mathcal{O}_{\mathbb{K}})$ é obtida aplicando o mergulho canônico relativo na base de $\mathcal{O}_{\mathbb{K}}$ e é dada por

$$M = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_1(w_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(w_1) & \cdots & \sigma_n(w_n) \end{pmatrix}. \tag{1}$$

A teoria de reticulados ideais apresenta uma estrutura geral para a construção de reticulados algébricos. Começaremos lembrando este conceito no caso de corpos de números totalmente reais.

DOI: 10.5540/03.2015.003.01.0195

Definição 2.1. *Sejam $\mathbb{K}$ um corpo de números totalmente real de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$. Um reticulado ideal é um reticulado $\Lambda = (\mathcal{I}, q_\gamma)$, onde $\mathcal{I}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ e $q_\gamma : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}$ definida por $q_\gamma(x, y) = Tr_{\mathbb{K}/\mathbb{Q}}(\gamma xy),\ \forall\, x,\, y \in \mathcal{I}$, com $\alpha \in \mathbb{K}$ totalmente positivo (isto é, $\sigma_i(\alpha) > 0,\ \forall i$).*

Vamos agora generalizar a definição de reticulado ideal para extensões relativas sobre $\mathbb{Q}(\alpha)$.

Definição 2.2. *Seja $\mathbb{K}/\mathbb{Q}(\alpha)$ uma extensão de Galois de grau n sobre $\mathbb{Q}(\alpha)$. Um $\mathbb{Z}[\alpha]$-reticulado ideal é um $\mathbb{Z}[\alpha]$-reticulado $\Lambda_\alpha = (\mathcal{I}, q)$, onde $\mathcal{I}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ e*

$$q : \mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z}[\alpha],\ q(x, y) = Tr_{\mathbb{K}/\mathbb{Q}(\alpha)}(x\overline{y}),\ \forall\, x, y \in \mathcal{I},$$

onde $-$ denota a conjugação complexa.

Como $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) =< \sigma >$, com $\sigma(\alpha) = \overline{\alpha} = 1 - \alpha$, segue que σ coincide com a conjugação complexa. Como estamos considerando $\mathbb{Z}[\alpha]$-reticulados, segue que a matriz de Gram $M^\dagger M$ é uma forma traço hermitiana, e desse modo, dizemos também que Λ_α é um $\mathbb{Z}[\alpha]$-reticulado hermitiano. Um $\mathbb{Z}[\alpha]$-reticulado de posto n pode ser naturalmente considerado como um $\mathbb{Z}$-reticulado de posto $2n$ definindo $x \cdot y = \frac{1}{2} Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(q(x, y))$. A matriz geradora do reticulado $\Lambda_\alpha = (\mathcal{I}, q)$, onde $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$, é definida de modo análogo a matriz dada em (1).

3 Transformando Λ_α em um $\mathbb{Z}$-reticulado

Nesta seção, vamos transformar Λ_α em um $\mathbb{Z}$-reticulado com a métrica euclidiana usual. Considere $\{x_1 = 1,\, x_2 = \alpha\}$ uma base integral de $\mathbb{Q}(\alpha)$. O mergulho canônico envia o anel dos inteiros $\mathbb{Z}[\alpha]$ para um reticulado com matriz geradora dada por

$$A = \begin{pmatrix} \Re(x_1) & \Re(x_2) \\ \Im(x_1) & \Im(x_2) \end{pmatrix},$$

onde $\Re$ é a parte real e $\Im$ é a parte imaginária. Considere a matriz conversão complexa para real $ri(\cdot)$ que troca cada entrada complexa da matriz de Gram $G = (g_{i,j})_{i,j=1,\cdots,n}$ de Λ_α com uma matriz real 2×2.

$$ri((g_{i,j})) = \begin{pmatrix} \Re(g_{ij}) & -\Im(g_{ij}) \\ \Im(g_{ij}) & \Re(g_{ij}) \end{pmatrix}.$$

Defina a matriz $\Psi = (ri((g_{i,j})))_{i,j=1,\cdots,n}$ de ordem $2n \times 2n$. Assim, a partir do $\mathbb{Z}[\alpha]$-reticulado hermitiano Λ_α obtemos um $\mathbb{Z}$-reticulado Λ com matriz de Gram dada por

$$R^t \cdot \Psi^t \cdot \Psi \cdot R,$$

onde R é uma matriz diagonal tendo a matriz A na diagonal principal.

4 Condição necessária para obter reticulados escalonados

A seguir apresentamos uma proposição que diz como escolher um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ a fim de obter uma versão escalonada dos reticulados E_8, P_6 e Λ_{24}.

DOI: 10.5540/03.2015.003.01.0195

Primeiro consideramos o reticulado real Λ obtido de Λ_α pela vetorização das partes real e imaginária dos vetores do $\mathbb{Z}[\alpha]$-reticulado (ver Seção 3). Queremos que Λ seja isomorfo a uma versão escalonada de E_8, P_b e Λ_{24}, isto é, Λ seja isomorfo a $\sqrt{c}E_8$, $\sqrt{c}P_b$ e $\sqrt{c}\Lambda_{24}$, $c \in \mathbb{Z}$. Seja r_1 o número de mergulhos com imagem em $\mathbb{R}$ e $2r_2$ o número de mergulhos com imagem em $\mathbb{C}$ de modo que $r_1 + 2r_2 = n$.

Proposição 4.1. *[3] Seja $d_{\mathbb{K}}$ o discriminante de $\mathbb{K}$. O volume do paralelotopo fundamental de Λ é dado por $vol(\Lambda) = \sqrt{det(\Lambda)} = N(\mathcal{I})2^{-r_2}\sqrt{|d_{\mathbb{K}}|}$.*

A Proposição (4.1) fornece uma condição necessária para a escolha de $\mathcal{I}$. Observe que $det(\sqrt{c}E_8) = c^8$, $det(\sqrt{c}P_b) = c^6 7^3$ e $det(\sqrt{c}\Lambda_{24}) = c^{24}$.

5 Uma nova construção do reticulado E_8 via reticulados ideais

O reticulado E_8 é definido por $E_8 = \{(x_1, \cdots, x_8);\ x_i \in \mathbb{Z},\ \forall i = 1, \cdots, 8$ ou $x_i \in \mathbb{Z} + 1/2,\ \forall i = 1, \cdots, 8$ e $\sum_{i=1}^{8} x_i$ é par$\}$, sendo o reticulado de maior densidade de empacotamento em dimensão 8 e é o único reticulado par e unimodular nesta dimensão. Apresentamos, a seguir, uma nova construção do reticulado E_8 via reticulados ideais.

Considere $\mathbb{K} = \mathbb{Q}(\alpha, i, \zeta_5 + \zeta_5^{-1})$ como uma extensão relativa de $\mathbb{F} = \mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$, com polinômio minimal $x^4 + 3x^2 + 1$ e base integral $\{1, \theta, \theta^2, \theta^3\}$. Como o discriminante absoluto de $\mathbb{K}$ é $d_{\mathbb{K}} = 2^8 \cdot 5^4 \cdot 7^4$, segue que uma condição necessária para obter uma versão escalonada de E_8 é que exista um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ com norma $5^2 \cdot 7^2$. Na tentativa de encontrarmos os ideais com a norma desejada, consideramos as seguintes fatorações de ideais

$$\begin{array}{cc} \mathfrak{p}_5\mathcal{O}_{\mathbb{K}} = (\mathfrak{B}_5\overline{\mathfrak{B}}_5)^2 & \mathfrak{p}_7\mathcal{O}_{\mathbb{K}} = \mathfrak{B}_7\overline{\mathfrak{B}}_7 \\ | & | \\ 5\mathcal{O}_{\mathbb{F}} = \mathfrak{p}_5 = (5) & 7\mathcal{O}_{\mathbb{F}} = \mathfrak{p}_7^2 \end{array}$$

Pela transitividade da norma, segue que $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{B}_7) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(\mathfrak{B}_7)) = N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{p}_7^2) = 7^2$ e $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{B}_5) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(\mathfrak{B}_5)) = N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{p}_5) = 5^2$. Portanto, o ideal $\mathcal{I} = \mathfrak{B}_5 \cdot \mathfrak{B}_7 = (\gamma)\mathcal{O}_{\mathbb{K}}$ com $\gamma = (\alpha - 1)\theta^3 + (-\alpha + 3)\theta^2 + (w - 2)\theta - 2w + 4$ tem a norma desejada. O mergulho relativo de $\mathbb{K}$ definido é por $\sigma : \mathbb{K} \to \mathbb{C}^4$, onde $\sigma(x) = (\sigma_1(x), \sigma_2(x), \sigma_3(x), \sigma_4(x))$ sendo que $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = -\theta$, $\sigma_3(\theta) = -3\theta - \theta^3$ e $\sigma_4(\theta) = 3\theta + \theta^3$.

Uma $\mathbb{Z}[\alpha]$-base de $\mathcal{I}$ é dada por $\{\alpha\theta^i\}_{i=0}^3$. Aplicando o mergulho canônico nesta base obtemos que a matriz de Gram do reticulado de posto 4 sobre $\mathbb{Z}[\alpha]$ é dada por

$$G = M^\dagger M = \begin{pmatrix} 7 & -3 - 6\alpha & -14 & 8 + 16\alpha \\ 3 + 6\alpha & 14 & -8 - 16\alpha & -35 \\ -14 & 8 + 16\alpha & 35 & -21 - 42\alpha \\ -8 - 16\alpha & -35 & 21 + 42\alpha & 91 \end{pmatrix}.$$

Aplicando os passos da Seção 3 obtemos um $\mathbb{Z}$-reticulado Λ que é unimodular e par em dimensão 8. Como E_8 é o único reticulado par e unimodular em sua dimensão, concluímos que Λ é isomorfo ao reticulado $\sqrt{35}E_8$.

DOI: 10.5540/03.2015.003.01.0195

6 Construção do reticulado de Leech Λ_{24}

O reticulado de Leech é o reticulado de maior densidade de empacotamento em dimensão 24. Muitas tentativas tem sido feitas para encontrar construções mais simples de Λ_{24}. Apresentamos, a seguir, uma nova construção do reticulado de Leech via reticulado ideal. Para isso fizemos uma combinação das construções algébricas do reticulado E_8 apresentado na Seção 5 e do reticulado de Barnes P_b que apresentamos a seguir.

6.1 Reticulado de Barnes P_b

O reticulado de Barnes P_b é um reticulado hermitiano de posto 3 sobre $\mathbb{Z}[\alpha]$ e unimodular sobre $\mathbb{Z}[\alpha]$. Considerando-o com um $\mathbb{Z}$-reticulado, segue que P_b é um reticulado de dimensão 6 e tem norma mínima 4. Além disso, P_b é o reticulado mais denso $\mathbb{Z}[\alpha]$-reticulado em dimensão 3 [7].

Considere $\mathbb{K} = \mathbb{Q}(\zeta_7)$ como uma extensão relativa de $\mathbb{F} = \mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$, com polinômio minimal $x^3 - \alpha x^2 + (-\alpha - 1)x - 1$ e com base integral $\{1, \theta, \theta^2\}$. Como o discriminante absoluto de $\mathbb{K}$ é $d_{\mathbb{K}} = 7^5$, segue que uma condição necessária para obter uma versão escalonada de P_b é que exista um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ com norma 7^2. Na tentativa de encontrarmos um ideal com a norma desejada, observe que $7\mathcal{O}_{\mathbb{F}} = \mathfrak{p}_7^2$ e $\mathfrak{p}_7\mathcal{O}_{\mathbb{K}} = \mathcal{I}_7^3$. Pela transitividade da norma, segue que $N_{\mathbb{K}/\mathbb{Q}}(\mathcal{I}_7) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(\mathcal{I}_7)) = N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{p}_7) = 7$. Portanto, o ideal $\mathcal{I} = \mathcal{I}_7^2 = (\gamma)\mathcal{O}_{\mathbb{K}}$, com $\gamma = (-\theta^2 + \alpha\theta + \alpha + 2)^2$, tem a norma desejada.

O mergulho relativo de $\mathbb{K}$ é definido por $\sigma : \mathbb{K} \to \mathbb{C}^3$, onde $\sigma(x) = (\sigma_1(x), \sigma_2(x), \sigma_3(x))$ com $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \theta^2$ e $\sigma_3(\theta) = \alpha - \theta - \theta^2$. Uma $\mathbb{Z}[\alpha]$-base de $\mathcal{I}$ é dada por $\{\alpha\theta^i\}_{i=0}^2$. Aplicando o mergulho canônico nesta base obtemos que a matriz de Gram do reticulado de posto 3 sobre $\mathbb{Z}[\alpha]$ é dada por

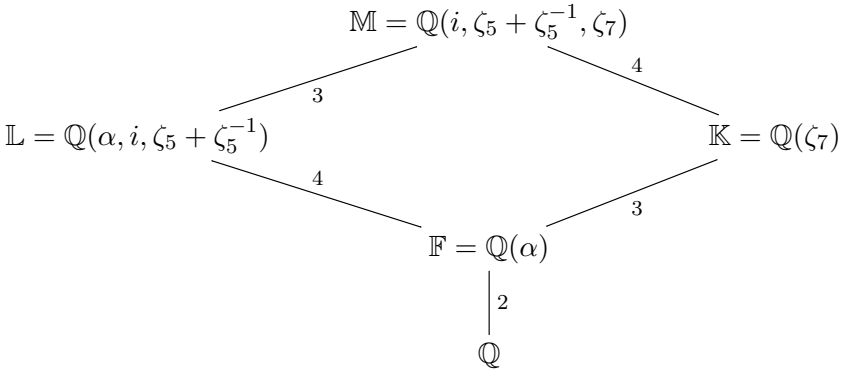
$$G = M^\dagger M = \begin{pmatrix} 3 & -2 & 1+w \\ -2 & 3 & -2 \\ -w & -2 & 3 \end{pmatrix}.$$

Observe que $det(G) = 1$. Aplicando os passos da Seção 3, obtemos um $\mathbb{Z}$-reticulado Λ com determinante 7^3 e norma mínima 4. Estas são exatamente as mesmas características do reticulado de Barnes P_b, e portanto, Λ é isomorfo a $\sqrt{7}P_b$.

6.2 Uma nova construção do reticulado de Leech Λ_{24} via reticulados ideais

Considere extensões de corpos $\mathbb{L}, \mathbb{K}, \mathbb{F}$ e $\mathbb{M}$ como no diagrama abaixo.

DOI: 10.5540/03.2015.003.01.0195



Como o discriminante absoluto de $\mathbb{M}$ é $d_{\mathbb{M}} = 2^{24} \cdot 5^{12} \cdot 7^{20}$, segue que uma condição necessária para obter uma versão escalonada de Λ_{24} é que exista um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{M}}$ com norma $5^6 \cdot 7^{14}$. Na tentativa de encontrarmos um ideal com a norma desejada, observe as seguintes fatorações de ideais:

$$\begin{array}{ccc} \mathfrak{B}_5\mathcal{O}_{\mathbb{M}} = \mathcal{I}_{5_1}\mathcal{I}_{5_2}\mathcal{I}_{5_3} & \mathfrak{B}_7\mathcal{O}_{\mathbb{M}} = \mathcal{I}_7^3 & \mathcal{Q}_7\mathcal{O}_{\mathbb{M}} = \mathcal{I}_7\overline{\mathcal{I}_7} \\ | & | & | \\ \mathfrak{p}_5\mathcal{O}_{\mathbb{L}} = (\mathfrak{B}_5\overline{\mathfrak{B}}_5)^2 & \mathfrak{p}_7\mathcal{O}_{\mathbb{L}} = \mathfrak{B}_7\overline{\mathfrak{B}}_7 & \mathfrak{p}_7\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_7^3 \\ | & | & | \\ 5\mathcal{O}_{\mathbb{F}} = \mathfrak{p}_5 = (5) & 7\mathcal{O}_{\mathbb{F}} = \mathfrak{p}_7^2 & 7\mathcal{O}_{\mathbb{F}} = \mathfrak{p}_7^2 \end{array}$$

Pela transitividade da norma, segue que

$$N_{\mathbb{M}/\mathbb{Q}}(\mathcal{I}_{5_i}) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{L}/\mathbb{F}}(N_{\mathbb{M}/\mathbb{L}}(\mathcal{I}_{5_i}) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{L}/\mathbb{F}}(\mathfrak{B}_5)) = N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{p}_5) = 5^2,\ i = 1,\ 2,\ 3$$

$$N_{\mathbb{M}/\mathbb{Q}}(\mathcal{I}_7) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{L}/\mathbb{F}}(N_{\mathbb{M}/\mathbb{L}}(\mathcal{I}_7))) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{L}/\mathbb{F}}(\mathfrak{B}_7)) = N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{p}_7^2) = 7^2$$

$$N_{\mathbb{M}/\mathbb{Q}}(\mathcal{I}_7) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(N_{\mathbb{M}/\mathbb{K}}(\mathcal{I}_7))) = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(\mathcal{Q}_7^2)) = N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{p}_7^2) = 7^2$$

O ideal $\mathcal{I} = \mathcal{I}_{5_1} \cdot \mathcal{I}_{5_2} \cdot \mathcal{I}_{5_3} \cdot \mathcal{I}_7^3 \cdot (\mathcal{I}_7\overline{\mathcal{I}_7})^2$ tem a norma desejada. De fato, $N_{\mathbb{M}/\mathbb{Q}}(\mathcal{I}) = 5^2 \cdot 5^2 \cdot 5^2 \cdot (7^2)^3 \cdot (7^2)^2 \cdot (7^2)^2 = 5^6 7^{14}$. A fatoração do ideal $\mathcal{I}$ em $\mathbb{M}$, base integral e mergulho canônico podem ser encontrados usando o software "*Sage*".

Desse modo obtemos um $\mathbb{Z}$-reticulado Λ na dimensão 24 com determinante 1 e norma mínima 4. Como Λ_{24} é o único com tais características em dimensão 24, concluímos que Λ é isomorfo a $7\sqrt{5}\Lambda_{24}$. Observe que neste caso $\mathcal{I}$ é o produto dos ideais usados na construção dos reticulados E_8 e P_b movidos para a extensão $\mathbb{M}/\mathbb{L}$ e $\mathbb{M}/\mathbb{K}$, respectivamente. Como E_8 e P_b são construídos usando o mesmo corpo base $\mathbb{Q}(\alpha)$, segue que considerar o produto dos dois ideais em $\mathbb{M}$ é equivalente a fazer o produto tensorial sobre $\mathbb{Z}[\alpha]$. Portanto, Λ_{24} também pode ser obtido via o produto tensorial das matrizes da seguinte forma

$$\begin{pmatrix} 7 & -3-6\alpha & -14 & 8+16\alpha \\ 3+6\alpha & 14 & -8-16\alpha & -35 \\ -14 & 8+16\alpha & 35 & -21-42\alpha \\ -8-16\alpha & -35 & 21+42\alpha & 91 \end{pmatrix} \otimes_{\mathbb{Z}[\alpha]} \begin{pmatrix} 3 & -2 & 1+w \\ -2 & 3 & -2 \\ -w & -2 & 3 \end{pmatrix}.$$

DOI: 10.5540/03.2015.003.01.0195

Ao contrário do produto tensorial sobre $\mathbb{Z}$, o produto tensorial sobre corpos quadráticos totalmente imaginário mostrou-se bem sucedido na construção de reticulados extremos [1]. No entanto, isso acontece apenas excepcionalmente. Em geral, o produto tensorial de reticulados hermitianos não consegue produzir reticulados com boa densidade de empacotamento (como faz o produto tensorial sobre $\mathbb{Z}$).

7 Conclusão

Neste trabalho, apresentamos uma nova construção de Λ_{24} via reticulados ideais. Usando a estrutura da construção, é possível obter Λ_{24} via o produto tensorial sobre $\mathbb{Z}[\alpha]$. Este reticulado ocupa um lugar especial em matemática devido as suas propriedades e por isso possui inúmeras aplicações. Finalmente, o uso de reticulados ideais tem se tornado importantes devido as suas recentes aplicações, uma vez que podem ser usados em esquemas de encriptação totalmente homomórficas. Estima-se que essa técnica pode revolucionar as áreas de segurança e privacidade, por permitir processamentos seguro em ambientes não confiáveis como computação em nuvens, grades distribuídas e *testbeds* compartilhados. Esse processamento seguro possui aplicações em diversas áreas, como o processamento de extratos bancários, votações eletrônicas e prontuários médicos [5].

Referências

[1] C. Bachoc, G. Nebe, Extremal lattices of minimum 8 related to the Mathieu group M_{22}, J.reine angew, *Math.,* 494 (1998) 155-171.

[2] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, Algebraic Lattice Constellations: Bounds on Performance, *IEEE Trans. on Inform. Theory*, 52 (1) (2006) 319-327.

[3] J, Boutros, E. Viterbo, C. Rastello, J-C. Belfiore, Good Lattice Constellation for Both Rayleigh Fading and Gaussian Channels, *IEE Trans. on Inform. Theory*, 42 (1996) 502-518.

[4] M. Craig, Extreme forms and cyclotomic, *Mathematicka*, 25 (1978b) 44-56.

[5] M. V. Dijk, M., C. Gentry, S. Halevi, et al., Fully homomorphic encryption over the integers, *Advances in Cryptology-EUROCRYPT*, (2010) 24-43.

[6] M. Hentschel, On Hermitian theta series and modular forms, Thesis RWTH Aachen 2009.

[7] G. Nebe, An even unimodular 72-dimensional lattice of minimum, *Journal für die reine und angewandte Mathematik*, 673 (2012) 237-247.

DOI: 10.5540/03.2015.003.01.0195