Trabalho apresentado no XLI CNMAC, Unicamp - Campinas - SP, 2022.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Corpos puros de grau 3 e aplicações

Livea Cichito Esteves[1], Antonio Aparecido de Andrade[2], Linara Stéfani Facini [3]
UNESP, São José do Rio Preto, SP

Resumo. Neste trabalho, apresentamos o anel de inteiros e o discriminante dos corpos puros cúbicos da forma $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[3]{d}$, $d \in \mathbb{Z}$, $d \neq 1$, d livre de cubos e da forma $d = m^2 n$ com $m, n \in \mathbb{Z}$ e $mdc(m, n) = 1$. Neste caso, $[\mathbb{K} : \mathbb{Q}] = 3$ e $p(x) = x^3 - d$ é o polinômio minimal de θ.

Palavras-chave. Corpos Puros, Corpo de Números, Anel de Inteiros, Discriminante

1 Introdução

Dado $\mathbb{K} = \mathbb{Q}(\sqrt[3]{d})$, com d inteiro livre de cubos, temos duas possibildades para d: d é livre de quadrados ou d não é livre de quadrados. O caso em que ocorre d livre de quadrados foi feito em detalhes em [3] e em [1]. O caso d não livre de quadrados é uma sugestão da lista de exercícios de [2], e neste trabalho, apresentamos sua resolução.

Assim, considerando a extensão $\mathbb{K} = \mathbb{Q}(\sqrt[3]{d})$, com d inteiro livre de cubos e não livre de quadrados, iremos determinar uma base integral e o discriminante a partir dessa base. Esta parte teórica é feita com o objetivo final de encontrar bons reticulados de grau 3 via essa extenção de corpos.

2 Resultados Básicos

Nesta seção, apresentamos alguns resultados básicos da Teoria dos Números úteis para o desenvolvimento do texto.

Definição 2.1. *Sejam $A \subseteq B$ anéis e $\alpha \in B$. O elemento α é chamado um **elemento inteiro** sobre A se α for raiz de um polinômio mônico não nulo $p(x)$ com coeficientes em A.*

Observação 2.1. *Quando $B \subseteq \mathbb{C}$ e $A = \mathbb{Z}$, o elemento α é chamado um **inteiro algébrico**.*

Definição 2.2. *Sejam $A \subseteq B$ anéis. O conjunto $\mathcal{O}_B = \{\alpha \in B \mid \alpha$ é inteiro sobre $A\}$, é chamado de **anel de inteiros** de B sobre A.*

Definição 2.3. *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão algébrica, com $\mathbb{K}$ um corpo finito ou de característica zero, $[\mathbb{L} : \mathbb{K}] = n$ e $\alpha \in \mathbb{L}$. Sejam $\alpha_1, \alpha_2, \ldots, \alpha_n$ as raízes do polinômio minimal de α sobre $\mathbb{K}$, cada uma repetida $[\mathbb{L} : \mathbb{K}(\alpha)]$-vezes.*

1. *O **traço** de α sobre $\mathbb{K}$ é definido por $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \alpha_i$.*

[1]liveacichito@gmail.com
[2]antonio.andrade@unesp.br
[3]linarafacini@gmail.com

2. A ***norma*** *de α sobre $\mathbb{K}$ é definida por $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.*

Definição 2.4. *Seja $\mathbb{K}$ um corpo de números. Uma base do $\mathbb{Z}$-módulo livre $\mathcal{O}_\mathbb{K}$ é chamada de* ***base integral*** *de $\mathbb{K}$.*

Definição 2.5. *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre finitamente gerado de posto n e $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ um conjunto de elementos de B. O* ***discriminante*** *de $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, é definido por*

$$\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(Tr_{B|A}(\alpha_i \alpha_j)) \in A,$$

onde $i, j = 1, 2, \ldots, n$.

Proposição 2.1. *[1] Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico e $\theta \in \mathbb{C}$ é um inteiro algébrico cujo polinômio minimal é $p(x) = x^3 + ax + b \in \mathbb{Z}[x]$. O polinômio característico do elemento $\alpha = a_0 + a_1\theta + a_2\theta^2 \in \mathbb{K}$, com $a_0, a_1, a_2 \in \mathbb{Q}$, é dado por*

$$\begin{aligned} f_\alpha(x) = x^3 - (3a_0 - 2a_2a)x^2 + (3a_0^2 - 4a_0a_2a + a_1^2a + 3a_1a_2b + a_2^2a^2)x - \\ - (a_0^3 - 2a_0^2a_2a + a_0a_1^2a + 3a_0a_1a_2b + a_0a_2^2a^2 - a_1^3b - a_1a_2^2ab + a_2^3b^2). \end{aligned} \tag{1}$$

Proposição 2.2. *[2] Seja $\mathbb{K}$ um corpo. Assim, $\alpha \in \mathbb{K}$ é um inteiro algébrico se, e somente se, seu polinômio característico tem coeficientes inteiros.*

Proposição 2.3. *[1] Se $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números, onde $\theta = \sqrt[3]{d}$ com $d \in \mathbb{Z}$ não livre de quadrados e livre de cúbicas, então*

$$Tr(\theta^k) = \begin{cases} 0, \text{ se } k = 1, 2, \\ 3d^s, \text{ se } k = 3s, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > 3 \text{ e } k \not\equiv 0 \pmod 3. \end{cases} \tag{2}$$

3 Anel de inteiros

Seja $\mathbb{K} = \mathbb{Q}(\theta)$,onde $\theta = \sqrt[3]{d}$, com $d \in \mathbb{Z}$, $d \neq 1$, não livre de quadrados e livre de cubos, ou seja, com $d = m^2n$, onde m e n são livres de quadrados e $mdc(m, n) = 1$.

Lema 3.1. *$d\mathbb{Z} \subseteq \theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} \subseteq mn\mathbb{Z}$, e assim, $\theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = k\mathbb{Z}$, para algum $k \in \mathbb{Z}$.*

Demonstração. Como $\theta \in \theta\mathcal{O}_\mathbb{K}$, segue que $\theta^3 = d \in \theta\mathcal{O}_\mathbb{K}$. Portanto, $d\mathbb{Z} \subseteq \theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z}$. Agora, se $\delta \in \theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z}$, então $\delta \in \theta\mathcal{O}_\mathbb{K}$ e $\delta \in \mathbb{Z}$. Logo, existem $\gamma \in \mathcal{O}_\mathbb{K}$ e $k \in \mathbb{Z}$ tal que $\delta = \theta\gamma = k$. Aplicando a norma, segue que

$$N_\mathbb{K}(\delta) = N_\mathbb{K}(\theta\gamma) = N_\mathbb{K}(k), \text{ ou seja, } N_\mathbb{K}(\theta\gamma) = \theta^3 N_\mathbb{K}(\gamma) = dN_\mathbb{K}(\gamma) = k^3.$$

Como $N_\mathbb{K}(\gamma) \in \mathbb{Z}$ e $d = m^2n$, segue que m e n dividem k^3. Como m e n são livres de quadrados, segue que m e n dividem k, e assim, mn divide k. Logo, $\theta\gamma \in mn\mathbb{Z}$, e desse modo, $d\mathbb{Z} \subseteq \theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} \subseteq mn\mathbb{Z}$. Como $\mathbb{Z}$ é principal, segue que $\theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = k\mathbb{Z}$, para algum $k \in \mathbb{Z}$. Assim, $d = kl_1$ e $d = kl_2$, para algum $l_1, l_2 \in \mathbb{Z}$. Portanto, $k = mnl_2$, onde $l_1l_2 = m$. □

Teorema 3.1. *O anel $\mathcal{O}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{K}$ é dado por*

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2}{m}) & se \quad d \not\equiv \pm 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2 + m\theta + m}{3m}) & se \quad d \equiv 1 (mod\ 9)\ e\ m \equiv 1, -2 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2 + 2m\theta + 2m}{3m}) & se \quad d \equiv 1 (mod\ 9)\ e\ m \not\equiv 1, -2 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2 + 2m\theta + m}{3m}) & se \quad d \equiv -1 (mod\ 9)\ e\ m \equiv 1, -2 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\frac{\theta^2 + m\theta + 2m}{3m}) & se \quad d \equiv -1 (mod\ 9)\ e\ m \not\equiv 1, -2 (mod\ 9). \end{cases}$$

Demonstração. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}} \subset \mathbb{K}$, e $\{1, \theta, \theta^2, \theta^2\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, então existem $a_i \in \mathbb{Q}$ tal que $\alpha = a_0 + a_1\theta + a_2\theta^2$. Além disso, como $d = m^2 n$ e

$$\begin{cases} Tr_{\mathbb{K}}(\alpha) = Tr_{\mathbb{K}}(a_0 + a_1\theta + a_2\theta^2) = 3a_0 \in \mathbb{Z} \\ Tr_{\mathbb{K}}(\alpha\theta) = Tr_{\mathbb{K}}(a_0\theta + a_1\theta^2 + a_2 d) = 3a_2 d \in mn\mathbb{Z} \\ Tr_{\mathbb{K}}(\alpha\theta^2) = Tr_{\mathbb{K}}(a_0\theta^2 + a_1 d + a_2\theta d) = 3a_1 d \in mn\mathbb{Z}, \end{cases}$$

segue que $b_0 = 3a_0,\ b_1 = 3a_1 m$ e $b_2 = 3a_2 m \in \mathbb{Z}$. Assim,

$$\alpha = \frac{b_0}{3} + \frac{b_1}{3m}\theta + \frac{b_2}{3m}\theta^2.$$

Pelo algoritmo da divisão, segue que $b_0 = 3c_0 + r_0$, $b_1 = 3mc_1 + r_1$ e $b_2 = 3c_2 + r_2$, com $c_i, r_i \in \mathbb{Z}$, $0 \leq r_0, r_2 \leq 2$ e $0 \leq r_1 \leq 3m - 1$. Logo,

$$\alpha = c_0 + \frac{r_0}{3} + (\frac{3mc_1 + r_1}{3m})\theta + (\frac{3c_2 + r_2}{3m})\theta^2 = c_0 + c_1\theta + \frac{r_0}{3} + \frac{r_1}{3m}\theta + (\frac{3c_2 + r_2}{3m})\theta^2,$$

onde $c_i \in \mathbb{Z}$, para $i = 0, 1, 2$, com $r_0, r_2 \in \{0, 1, 2\}$ e $r_1 \in \{0, 1, 2, \ldots, 3m - 1\}$, ou seja,

$$\alpha = c_0 + \frac{r_0}{3} + (c_1 + \frac{r_1}{3m})\theta + (\frac{3c_2 + r_2}{3m})\theta^2. \tag{3}$$

Agora, α é um inteiro algébrico se, e somente se,

$$\beta = \frac{r_0}{3} + \frac{r_1}{3m}\theta + (\frac{3c_2 + r_2}{3m})\theta^2$$

é um inteiro algébrico. Pelas Proposições 2.1 e 2.2, segue que

$$\alpha \in \mathcal{O}_{\mathbb{K}} \iff \begin{cases} 3(\frac{r_0}{3}) \in \mathbb{Z} \\ 3(\frac{r_0}{3})^2 - 3(\frac{r_1}{3m})(\frac{3c_2 + r_2}{3m})d \in \mathbb{Z} \\ (\frac{r_0}{3})^3 - 3(\frac{r_0}{3})(\frac{r_1}{3m})(\frac{3c_2 + r_2}{3m})d + d((\frac{r_1}{3m})^3 + (\frac{3c_2 + r_2}{3m})^3 d) \in \mathbb{Z} \end{cases}$$

ou seja, $\alpha \in \mathcal{O}_{\mathbb{K}}$ se, e somente se,

$$\begin{cases} r_0 \in \mathbb{Z} \\ \frac{r_0^2}{3} - \frac{1}{3m^2} 3r_1(3c_2 + r_2)d \in \mathbb{Z} \\ \frac{r_0^3}{27} - \frac{1}{9m^2} r_0 r_1(3c_2 + r_2)d + \frac{1}{27m^3} d(r_1^3 + (3c_2 + r_2)^3 d) \in \mathbb{Z}. \end{cases}$$

Como $d = m^2n$, segue que $\alpha \in \mathcal{O}_{\mathbb{K}}$ se, e somente se,

$$\begin{cases} r_0 \in \mathbb{Z} \\ \dfrac{r_0^2}{3} - \dfrac{1}{3}r_1(3c_2 + r_2)n \in \mathbb{Z} \\ \dfrac{r_0^3}{27} - \dfrac{1}{9}r_0r_1(3c_2 + r_2)n + \dfrac{1}{27m}n(r_1^3 + (3c_2 + r_2)^3m^2n) \in \mathbb{Z}. \end{cases}$$

Assim, $\alpha \in \mathcal{O}_{\mathbb{K}}$ se, e somente se,

$$r_0 \in \mathbb{Z}, \tag{4}$$

$$\frac{r_0^2 - r_1r_2n}{3} \in \mathbb{Z} \tag{5}$$

$$\frac{1}{27m}(r_0^3m - 9r_0r_1c_2mn - 3r_0r_1r_2mn + r_1^3n + 9c_2r_2^2m^2n^2 + r_2^3m^2n^2) \in \mathbb{Z}. \tag{6}$$

Assim, pela Equação (3) e pelas possibilidades para $r_0, r_2 \in \{0, 1, 2\}$ e $r_1 \in \{0, 1, 2, \ldots, 3m - 1\}$, obtemos os seguintes casos.

1. $\pm\frac{r_1n}{3} \in \mathbb{Z}$ se, e somente se, $r_1n = 3k$, para algum $k \in \mathbb{Z}$. Além disso, $\frac{1\pm r_1n}{3} \in \mathbb{Z}$ se, e somente se, $mdc(3, r_1) = 1$.

2. Se $\frac{r_1n}{3} \in \mathbb{Z}$, então $\frac{1\pm r_1n}{3} \notin \mathbb{Z}$.

3. Se $\frac{1\pm r_1n}{3} \in \mathbb{Z}$, então $\frac{r_1n}{3} \notin \mathbb{Z}$.

4. Se $r_0 = r_1 = r_2 = 0$, então as Equações (5) e (6) possuem solução para todo d e

$$\alpha = c_0 + c_1\theta + c_2\frac{\theta^2}{m}.$$

5. Se $r_0 = r_2 = 0$ e $r_1 \neq 0$, então $\frac{1}{27m}r_1^3n \notin \mathbb{Z}$, uma vez que se $\frac{r_1^3n}{m} = 27k_1$, onde $k_1 \in \mathbb{Z}$. Logo, m divide r_1^3n. Como $mdc(m, n) = 1$, segue que m divide r_1^3. Como m é livre de quadrados, segue que m divide r_1, ou seja, $r_1 = ml$, com $l \in \mathbb{Z}$. Como $1 \leq r_1 \leq 3m - 1$, segue que $l = 1, 2$. Se $l = 1$, então $\frac{1}{27m}m^3n = \frac{1}{27}d \in \mathbb{Z}$, ou seja, $d \equiv 0(mod\ 27)$ o que não ocorre. De modo análogo, se $l = 2$, então $\frac{1}{27m}8m^3n = \frac{1}{27}8d \in \mathbb{Z}$, ou seja, $8d \equiv 0(mod\ 27)$. Como $mdc(8, 27) = 1$, segue que $d \equiv 0(mod\ 27)$, o que não ocorre. Portanto, não existe d tal que $\frac{1}{27m}r_1^3n \in \mathbb{Z}$.

6. Se $r_0 = 0$, $r_1 \neq 0$ e $r_2 = 1$, então $\frac{-r_1n}{3} \notin \mathbb{Z}$ e $\frac{1}{27m}(r_1^3n + 9c_2m^2n^2 + m^2n^2) \notin \mathbb{Z}$, para qualquer d.

7. Se $r_0 = 0$, $r_1 \neq 0$ e $r_2 = 2$, então $\frac{-2r_1n}{3} \notin \mathbb{Z}$ e $\frac{1}{27m}(r_1^3n + 36c_2m^2n^2 + 8m^2n^2) \notin \mathbb{Z}$, uma vez que não existe solução.

8. Se $r_0 \neq 0$ e $r_1 = 0$ ou $r_2 = 0$, então $\frac{r_0^n}{3} \notin \mathbb{Z}$, uma vez que $r_0 = 1$ ou $r_0 = 1$.

Assim, as possibilidades para $r_i \in \{0, 1, 2\}$, com $i = 0, 1, 2$, são dadas por:

r_0	r_1	r_2	Equação (5)	Equação (6)	$d \equiv ?(mod\ 9)$ e $m \equiv ?(mod\ 9)$
0	0	0	0	0	para todo d
0	$r_1 \neq 0$	0	0	$\notin \mathbb{Z}$	não existe d
0	$r_1 \neq 0$	1	$\notin \mathbb{Z}$	$\notin \mathbb{Z}$	não existe d
0	$r_1 \neq 0$	2	$\notin \mathbb{Z}$	$\notin \mathbb{Z}$	não existe d
1	m	1	$\in \mathbb{Z}$	$\in \mathbb{Z}$	$d \equiv 1(mod\ 9)$ e $m \equiv 1, -2(mod\ 9)$
1	$2m$	1	$\in \mathbb{Z}$	$\in \mathbb{Z}$	$d \equiv -1(mod\ 9)$ e $m \equiv 1, -2(mod\ 9)$
1	m	2	$\in \mathbb{Z}$	$\in \mathbb{Z}$	$d \equiv 1(mod\ 9)$ e $m \not\equiv 1, -2(mod\ 9)$
1	$2m$	2	$\in \mathbb{Z}$	$\in \mathbb{Z}$	$d \equiv -1(mod\ 9)$ e $m \not\equiv 1, -2(mod\ 9)$
2	m	1	$\in \mathbb{Z}$	$\in \mathbb{Z}$	$d \equiv -1(mod\ 9)$ e $m \not\equiv 1, -2(mod\ 9)$
2	m	2	$\in \mathbb{Z}$	$\in \mathbb{Z}$	$d \equiv -1(mod\ 9)$ e $m \equiv 1, -2(mod\ 9)$
2	$2m$	2	$\in \mathbb{Z}$	$\in \mathbb{Z}$	$d \equiv 1(mod\ 9)$ e $m \equiv 1, -2(mod\ 9)$
2	$2m$	1	$\in \mathbb{Z}$	$\in \mathbb{Z}$	$d \equiv 1(mod\ 9)$ e $m \not\equiv 1, -2(mod\ 9)$

Logo,

1. Se $d \not\equiv \pm 1(mod\ 9)$, então $r_0 = r_1 = r - 2 = 0$, e portanto,

$$\alpha = c_0 + c_1\theta + c_2\frac{\theta^2}{m} \in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\frac{\theta^2}{m}.$$

2. Se $d \equiv 1(mod\ 9)$ e $m \equiv 1, -2(mod\ 9)$, então $r_0 = 1$, $r_1 = m$ e $r_2 = 1$, e portanto,

$$\begin{aligned} \alpha &= c_0 + \tfrac{1}{3} + (c_1 + \tfrac{1}{3})\theta + (\tfrac{3c_2+1}{3m})\theta^2 \\ &= (c_0 - c_2) + (c_1 - c_2)\theta + (3c_2 + 1)(\tfrac{\theta^2+m\theta+m}{3m}) \\ &\in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\tfrac{\theta^2+m\theta+m}{3m}). \end{aligned}$$

   ou $r_0 = 2$, $r_1 = 2m$ e $r_2 = 2$, e portanto,

$$\begin{aligned} \alpha &= c_0 + \tfrac{2}{3} + (c_1 + \tfrac{2}{3})\theta + (\tfrac{3c_2+2}{3m})\theta^2 \\ &= (c_0 - c_2) + (c_1 - c_2)\theta + (3c_2 + 2)(\tfrac{\theta^2+m\theta+m}{3m}) \\ &\in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\tfrac{\theta^2+m\theta+m}{3m}). \end{aligned}$$

3. Se $d \equiv 1(mod\ 9)$ e $m \not\equiv 1, -2(mod\ 9)$, então $r_0 = 1$, $r_1 = m$ e $r_2 = 2$, e portanto,

$$\begin{aligned} \alpha &= c_0 + \tfrac{1}{3} + (c_1 + \tfrac{1}{3})\theta + (\tfrac{3c_2+2}{3m})\theta^2 \\ &= (c_0 - 2c_2 - 1) + (c_1 - 2c_2 - 1)\theta + (3c_2 + 2)(\tfrac{\theta^2+2m\theta+2m}{3m}) \\ &\in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\tfrac{\theta^2+2m\theta+2m}{3m}). \end{aligned}$$

   or $r_0 = 2$, $r_1 = 2m$ e $r_2 = 1$, e portanto,

$$\begin{aligned} \alpha &= c_0 + \tfrac{2}{3} + (c_1 + \tfrac{2}{3})\theta + (\tfrac{3c_2+1}{3m})\theta^2 \\ &= (c_0 - 2c_2) + (c_1 - 2c_2)\theta + (3c_2 + 1)(\tfrac{\theta^2+2m\theta+2m}{3m}) \\ &\in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\tfrac{\theta^2+2m\theta+2m}{3m}). \end{aligned}$$

4. Se $d \equiv -1(mod\ 9)$, $m \equiv 1, -2(mod\ 9)$, então $r_0 = 1$, $r_1 = 2m$ e $r_2 = 1$, e portanto,

$$\begin{aligned} \alpha &= c_0 + \tfrac{1}{3} + (c_1 + \tfrac{2}{3})\theta + (\tfrac{3c_2+1}{3m})\theta^2 \\ &= (c_0 - c_2) + (c_1 - 2c_2)\theta + (3c_2 + 1)(\tfrac{\theta^2+2m\theta+m}{3m}) \\ &\in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\tfrac{\theta^2+2m\theta+m}{3m}). \end{aligned}$$

or $r_0 = 2$, $r_1 = m$ e $r_2 = 2$, e portanto,

$$\begin{aligned}\alpha &= c_0 + \tfrac{2}{3} + (c_1 + \tfrac{1}{3})\theta + (\tfrac{3c_2+2}{3m})\theta^2 \\ &= (c_0 - c_2) + (c_1 - 2c_2 - 1)\theta + (3c_2 + 2)(\tfrac{\theta^2+2m\theta+m}{3m}) \\ &\in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\tfrac{\theta^2+2m\theta+m}{3m}).\end{aligned}$$

5. Se $d \equiv -1(mod\ 9)$, $m \not\equiv 1, -2(mod\ 9)$, então $r_0 = 1$, $r_1 = 2m$ e $r_2 = 2$, e portanto,

$$\begin{aligned}\alpha &= c_0 + \tfrac{1}{3} + (c_1 + \tfrac{2}{3})\theta + (\tfrac{3c_2+2}{3m})\theta^2 \\ &= (c_0 - 2c_2 - 1) + (c_1 - c_2)\theta + (3c_2 + 2)(\tfrac{\theta^2+m\theta+2m}{3m}) \\ &\in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\tfrac{\theta^2+m\theta+2m}{3m}).\end{aligned}$$

or $r_0 = 2$, $r_1 = m$ e $r_2 = 1$, e portanto,

$$\begin{aligned}\alpha &= c_0 + \tfrac{2}{3} + (c_1 + \tfrac{1}{3})\theta + (\tfrac{3c_2+1}{3m})\theta^2 \\ &= (c_0 - 2c_2) + (c_1 - c_2)\theta + (3c_2 + 1)(\tfrac{\theta^2+m\theta+2m}{3m}) \\ &\in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\tfrac{\theta^2+m\theta+2m}{3m}),\end{aligned}$$

o que prova o teorema. □

4 Discriminante

Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[3]{d}$, com $d \in \mathbb{Z}$, $d \neq 1$ livre de cubos e não livre de quadrados, ou seja, $d = m^2 n$ e $mdc(m, n) = 1$.

Proposição 4.1. *O discriminante de* $\mathbb{K}$ *é dado por*

$$D(\mathbb{K}) = \begin{cases} -27m^2n^2, \text{ se } d \not\equiv \pm 1(mod\ 9) \\ -3m^2n^2, \text{ se } d \equiv \pm 1(mod\ 9). \end{cases}$$

Demonstração. Usando a Proposição 2.3, segue que $Tr(1) = 3$, $Tr(\theta) = 0$, $Tr(\theta^2) = 0$, $Tr(d) = 3d$ e $Tr(\theta^4) = 0$. Agora,

1. Se $d \not\equiv \pm 1(mod\ 9)$, então

$$\begin{aligned}D(1, \theta, \tfrac{\theta^2}{m}) &= \det \begin{pmatrix} Tr(1) & Tr(\theta) & Tr(\frac{\theta^2}{m}) \\ Tr(\theta) & Tr(\theta^2) & Tr(\frac{d}{m}) \\ Tr(\frac{\theta^2}{m}) & Tr(\frac{d}{m}) & Tr(\frac{\theta^4}{m^2}) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & \frac{3d}{m} \\ 0 & \frac{3d}{m} & 0 \end{pmatrix} \\ &= \tfrac{-27d^2}{m^2} = \tfrac{-27m^4n^2}{m^2} = -27m^2n^2.\end{aligned}$$

2. Se $d \equiv 1(mod\ 9)$ e $m \equiv 1, -2(mod\ 9)$, então $D\left(1, \theta, \frac{m+m\theta+\theta^2}{3m}\right)$ é dado por

$$\begin{aligned}&\det \begin{pmatrix} Tr(1) & Tr(\theta) & Tr\left(\frac{m+m\theta+\theta^2}{3m}\right) \\ Tr(\theta) & Tr(\theta^2) & Tr\left(\frac{m\theta+m\theta^2+d}{3m}\right) \\ Tr\left(\frac{m+m\theta+\theta^2}{3m}\right) & Tr\left(\frac{m\theta+m\theta^2+d}{3m}\right) & Tr\left(\frac{m^2+2m^2\theta+(2m+m^2)\theta^2+2md+\theta^4}{9m^2}\right) \end{pmatrix} \\ &= \det \begin{pmatrix} 3 & 0 & 1 \\ 0 & 0 & \frac{d}{m} \\ 1 & \frac{d}{m} & \frac{m+2d}{3m} \end{pmatrix} = \tfrac{-3d^2}{m^2} = \tfrac{-3m^4n^2}{m^2} = -3m^2n^2.\end{aligned}$$

DOI: 10.5540/03.2022.009.01.0244

3. Se $d \equiv 1(mod\ 9)$ e $m \not\equiv 1, -2(mod\ 9)$, então $D\left(1, \theta, \frac{2m+2m\theta+\theta^2}{3m}\right)$ é dado por

$$\det\begin{pmatrix} Tr(1) & Tr(\theta) & Tr\left(\frac{2m+2m\theta+\theta^2}{3m}\right) \\ Tr(\theta) & Tr(\theta^2) & Tr\left(\frac{2m\theta+2m\theta^2+d}{3m}\right) \\ Tr\left(\frac{2m+2m\theta+\theta^2}{3m}\right) & Tr\left(\frac{2m\theta+2m\theta^2+d}{3m}\right) & Tr\left(\frac{4m^2+8m^2\theta+(4m+4m^2)\theta^2+4md+\theta^4}{9m^2}\right) \end{pmatrix}$$
$$= \det\begin{pmatrix} 3 & 0 & 2 \\ 0 & 0 & \frac{d}{m} \\ 2 & \frac{d}{m} & \frac{4m+4d}{3m} \end{pmatrix} = \frac{-3d^2}{m^2} = \frac{-3m^4n^2}{m^2} = -3m^2n^2.$$

4. Se $d \equiv -1(mod\ 9)$ e $m \equiv 1, -2(mod\ 9)$, então $D\left(1, \theta, \frac{m+2m\theta+\theta^2}{3m}\right)$ é dado por

$$\det\begin{pmatrix} Tr(1) & Tr(\theta) & Tr\left(\frac{m+2m\theta+\theta^2}{3m}\right) \\ Tr(\theta) & Tr(\theta^2) & Tr\left(\frac{m\theta+2m\theta^2+d}{3m}\right) \\ Tr\left(\frac{m+2m\theta+\theta^2}{3m}\right) & Tr\left(\frac{m\theta+2m\theta^2+d}{3m}\right) & Tr\left(\frac{m^2+4m^2\theta+(2m+4m^2)\theta^2+4md+\theta^4}{9m^2}\right) \end{pmatrix}$$
$$= \det\begin{pmatrix} 3 & 0 & 1 \\ 0 & 0 & \frac{d}{m} \\ 1 & \frac{d}{m} & \frac{m+4d}{3m} \end{pmatrix} = \frac{-3d^2}{m^2} = \frac{-3m^4n^2}{m^2} = -3m^2n^2.,$$

5. Se $d \equiv -1(mod\ 9)$ e $m \not\equiv 1, -2(mod\ 9)$, então $D\left(1, \theta, \frac{2m+m\theta+\theta^2}{3m}\right)$ é dado por

$$\det\begin{pmatrix} Tr(1) & Tr(\theta) & Tr\left(\frac{2m+m\theta+\theta^2}{3m}\right) \\ Tr(\theta) & Tr(\theta^2) & Tr\left(\frac{2m\theta+m\theta^2+d}{3m}\right) \\ Tr\left(\frac{2m+m\theta+\theta^2}{3m}\right) & Tr\left(\frac{2m\theta+m\theta^2+d}{3m}\right) & Tr\left(\frac{4m^2+4m^2\theta+(m^2+4m)\theta^2+2md+\theta^4}{9m^2}\right) \end{pmatrix}$$
$$= \det\begin{pmatrix} 3 & 0 & 2 \\ 0 & 0 & \frac{d}{m} \\ 2 & \frac{d}{m} & \frac{2d+4m}{3m} \end{pmatrix} = \frac{-3d^2}{m^2} = \frac{-3m^4n^2}{m^2} = -3m^2n^2.$$

o que prova o resultado. □

5 Considerações Finais

Neste trabalho, nosso objetivo foi determinar uma base e o discriminante para corpos cúbicos da forma $\mathbb{Q}(\sqrt[3]{d})$, com $d \in \mathbb{Z}$, $d \neq 1$ não livre de quadrados e livre de cubos. Agora, o próximo passo, como aplicação, é usar essa construção para obter bons reticulados de dimensão 3 via o homomorfismo de Minkowski.

Referências

[1] L. S. Facini. "Uma introdução aos corpos não abelianos de grau menor ou igual a 6". Dissertação de mestrado. Unesp, 2021.

[2] D. A. Marcus. **Number fields**. New York: Springer-Verlag, 1977. ISBN: 9780387902791.

[3] J. P. G. Vicente. "Reticulados de posto 3 sobre corpos de números". Dissertação de mestrado. Unesp, 2000.

