



UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
Câmpus de São José do Rio Preto

Maria Clara Lopes Taddone

Um estudo sobre bases integrais de corpos de
números

São José do Rio Preto
2023

Maria Clara Lopes Taddone

Um estudo sobre bases integrais de corpos de
números

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Financiadora: CAPES

São José do Rio Preto
2023

T121e

Taddone, Maria Clara Lopes

Um estudo sobre bases integrais de corpos de números / Maria Clara Lopes Taddone. -- , 2023

114 p. : tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto,

Orientador: Antonio Aparecido de Andrade

1. Matemática. 2. Corpos de números. 3. Inteiros mínimos. 4. Bases p-integrais. 5. Bases integrais. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Maria Clara Lopes Taddone

Um estudo sobre bases integrais de corpos de
números

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Prof. Dr. Antonio Aparecido de Andrade
Orientador

Prof. Dr. Trajano Pires da Nobrega Neto
UNESP – Câmpus de São José do Rio Preto

Prof. Dr. Agnaldo José Ferrari
UNESP – Câmpus de Bauru

São José do Rio Preto
28 de fevereiro de 2023

*À minha família e aos meus amigos,
dedico*

AGRADECIMENTOS

Muitas pessoas tiveram uma participação essencial na minha vida para que este trabalho fosse concluído. Com todo carinho e respeito, agradeço:

Aos meus pais Rita e Anderson, por todo amor, pela minha vida e pelo apoio essencial na minha trajetória.

Aos meus irmãos Patrícia e Pedro, por estarem perto mesmo estando longe.

À minha melhor amiga Maria Fernanda Zordan Bonini, com quem divido os melhores momentos, que me dá alegria e força para enfrentar os momentos mais difíceis e que é minha companheira de estudos e de vida.

À minha outra melhor amiga Thaís Cardoso, por estar ao meu lado há tantos anos com as melhores palavras de apoio, sorrisos e momentos incríveis.

Ao meu amigo Murillo Lozano, pela companhia nesses anos de Ibilce e por ser minha dupla em tantos momentos felizes.

Ao meu amigo Isaac Sanches, por me proporcionar as risadas mais sinceras que eu tanto valorizo.

Aos meus amigos Gabriel Leone, Neto Tofanin, Juliana Marques e Aldimir Bruzadin, pela companhia na “salinha do mestrado” e pelos cafés.

Às minhas amigas Maria Fernanda, Mayara Teixeira e Daiane Donegá, por serem as melhores companheiras de casa com quem eu poderia conviver. Nosso lar acolhedor foi o meu melhor refúgio.

Aos meus amigos Sérgio Verde, Pedro Melo, Ana Rossafa, Eduardo Martins, Milena Zacheo, Guilherme Zahra, Murillo e Maria Fernanda, pela amizade cultivada, nossos momentos de jogatina e por todas as conversas engraçadas e acolhedoras.

Aos queridos, Linara Faccini, por toda ajuda e apoio; Gabriel Scarlatti, por todas as vezes que ouviu meus desabafos e me incentivou; Luís Gustavo, pelo companheirismo e incentivo nos meus momentos de caos.

Ao meu orientador Prof. Dr. Antonio Aparecido de Andrade, pela confiança, pelos conselhos e por tudo que vem me ensinando ao longo desses anos.

Aos professores que fizeram parte da minha formação. Em especial, aos professores Weber Pereira, Juliana Precioso, Michelle Morgado, Márcio Gouveia e Maria Gorete.

Ao Programa de Educação Tutorial (PET Matemática), grupo pelo qual tenho imensa gratidão por cada momento vivido. Também a todos os amigos que fiz graças a ele, por terem sido uma segunda família durante a minha graduação e depois dela.

À Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto, Ibilce, por ter sido a minha segunda casa, lugar em que conheci pessoas incríveis que levarei comigo para sempre e onde descobri o meu amor pela matemática.

Aos membros titulares e suplentes da Banca, Prof. Dr. Trajano Pires da Nobrega Neto, Prof. Dr. Agnaldo José Ferrari, Prof. Dr. João Eloir Strapasson e Profa. Dra. Cintya Wink de Oliveira Benedito, por aceitarem fazer parte desse momento especial e por suas contribuições.

Enfim, a todos que estiveram ao meu lado e contribuíram direta ou indiretamente para este trabalho.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

*Um sorriso ainda é a única
língua que todos entendem.*
Emicida [1]

RESUMO

Neste trabalho, apresentamos alguns conceitos básicos da teoria algébrica dos números tais como números algébricos, anel de inteiros algébricos e discriminante. Analisamos a base integral de um corpo quadrático, o qual é um resultado bastante conhecido, e apresentamos o conceito de inteiros mínimos, elementos p -inteiros e bases p -inteiros de um corpo de números $\mathbb{K}$ sobre $\mathbb{Q}$. Estes conceitos são de extrema importância para determinar bases integrais para corpos cúbicos da forma $\mathbb{Q}(\theta)$, com θ uma raiz de um polinômio irreduzível sobre $\mathbb{Z}$ da forma $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, sob certas condições específicas sobre os coeficientes a e b .

Palavras-chave: Teoria algébrica dos números. Anel de inteiros. Discriminante. Elementos p -inteiros. Bases p -inteiros.

ABSTRACT

In this work, we present some basic concepts of the algebraic number theory such as algebraic numbers, ring of algebraic numbers and discriminant. We analyze the integral basis of a quadratic field, which is a well-known result, and we present the concept of minimal integers, p -integral elements and p -integral basis of a number field $\mathbb{K}$ over $\mathbb{Q}$. These concepts are extremely important to determine integral basis for cubic fields of the form $\mathbb{Q}(\theta)$, with θ a root of an irreducible polynomial over $\mathbb{Z}$ of the form $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, under certain specific conditions on the coefficients a and b .

Keywords: Algebraic number theory. Ring of integers. Discriminant. p -Integral elements. p -Integral basis.

Lista de Tabelas

5.1	Base 2-integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$	71
5.2	Base 3-integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$	84
5.3	Base p -integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$, com $p > 3$	101

Lista de Símbolos

$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{Q}$	Conjunto dos Números Racionais
$\mathbb{R}$	Conjunto dos Números Reais
$\mathbb{C}$	Conjunto dos Números Complexos
$\mathbb{K}$	Corpo
I	Ideal
$a \equiv b \pmod{m}$	a e b são congruentes módulo m
$a \not\equiv b \pmod{m}$	a e b não são congruentes módulo m
$m \nmid n$	m não divide n
$\mathbb{Q}(\alpha)$	Menor subcorpo de $\mathbb{C}$ contendo $\mathbb{Q}$ e α
$p(x)$	Polinômio na variável x
$\text{gr}(p(x))$	Grau do polinômio $p(x)$
$A[x]$	Conjunto dos polinômios na variável x e coeficientes em A
$\langle a \rangle$	Ideal gerado por a
$\det(M)$	Determinante da matriz M
$\mathcal{O}_B$	Anel de inteiros de A em B
$\mathcal{O}_{\mathbb{K}}$	Anel de inteiros do corpo $\mathbb{K}$
$m_{\alpha}(x)$	Polinômio minimal de α
$p_{\alpha}(x)$	Polinômio característico de α
$D(\alpha_1, \dots, \alpha_n)$	Discriminante do conjunto $\{\alpha_1, \dots, \alpha_n\}$
$D(\alpha)$	Discriminante do elemento α
$D(f(x))$	Discriminante do polinômio f

$D(\mathbb{K})$	Discriminante do corpo $\mathbb{K}$
$N(I)$	Norma do ideal I
$\text{ind}(\theta)$	Índice do elemento θ
$\alpha\mathcal{O}_{\mathbb{K}}$	Ideal gerado por α em $\mathcal{O}_{\mathbb{K}}$
$v_P(I)$	Valorização do ideal I no ideal primo P
$v_p(a)$	Valorização do inteiro a no número primo p
$[a]$	Parte inteira de a
$\text{gr}(\mathbb{K}(\alpha))$	Grau de α sobre o corpo $\mathbb{K}$
$\text{sgn}(x)$	Função sinal do elemento x

Sumário

1	Introdução	13
2	Conceitos Básicos	15
2.1	Anel de inteiros	15
2.2	Extensões algébricas	16
2.3	Corpo de números	20
2.4	Discriminante	22
2.5	Base de um ideal	23
3	Base Integral	24
3.1	Base integral de um corpo de números	24
3.2	Inteiros mínimos	34
3.3	Índice de um corpo de números	45
4	O anel de elementos p-integrals de um corpo de números	50
4.1	Elementos p -integrals de um corpo de números	50
4.2	Base p -integral de um corpo de números	55
5	Bases p-integrals de um corpo cúbico	66
5.1	Propriedades de elementos p -integrals em um corpo cúbico	66
5.2	Bases 2-integrals de um corpo cúbico	70
5.3	Bases 3-integrals de um corpo cúbico	83
5.4	Bases p -integrals de um corpo cúbico	100
5.5	Discriminante de um corpo cúbico	105
5.6	Base integral de um corpo cúbico	108
6	Conclusão	112
	Referências	113
	Índice Remissivo	114

1 Introdução

O presente texto tem como objetivo estudar bases p -integrais de um corpo de números $\mathbb{K}$, onde p representa um número primo, com o objetivo de que, a partir delas, encontramos uma base integral para o corpo $\mathbb{K}$. O nosso foco principal são os corpos cúbicos $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz de um polinômio irreduzível sobre $\mathbb{Z}$ da forma $f(t) = t^3 - at + b$. O desenvolvimento deste trabalho é baseado no artigo [2] e a principal referência é [3].

No Capítulo 2, apresentamos alguns conceitos básicos da Teoria Algébrica dos Números que são necessários para o entendimento deste trabalho. Nos Capítulos 2 e 3, as principais referências utilizadas foram [4], [5], [6] e [7]. Na Seção 2.1, apresentamos o conceito de elementos inteiros e apresentamos o anel de inteiros de uma extensão de anéis, que é um objeto essencial neste trabalho. Na Seção 2.2, tratamos das extensões algébricas de um corpo e encontramos o anel de inteiros de um corpo quadrático. Na Seção 2.3, apresentamos a definição de um corpo de números $\mathbb{K}$ e algumas propriedades do seu anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Na Seção 2.4, apresentamos o discriminante de um conjunto, de um elemento e de um polinômio. Por fim, na Seção 2.5, apresentamos uma base para um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$.

No Capítulo 3, apresentamos o conceito de bases integrais para um corpo de números. Na Seção 3.1, apresentamos a definição e alguns resultados de bases integrais, em especial de corpos quadráticos. Também é apresentado o discriminante de um corpo de números $\mathbb{K}$. Na Seção 3.2, introduzimos o conceito de inteiros mínimos e apresentamos sua representação. Por fim, na Seção 3.3, apresentamos o índice de um corpo de números e sua relação com uma base potente para o corpo $\mathbb{K}$.

No Capítulo 4, entramos no assunto que é o tema do presente trabalho, que são as bases p -integrais. A principal referência utilizada, e também no Capítulo 5 é [3]. Na Seção 4.1, apresentamos os elementos p -integrais de um corpo de números e algumas propriedades importantes. Na Seção 4.2, apresentamos resultados que fornecem condições para a existência de bases para o corpo $\mathbb{K}$ formadas por elementos p -integrais e apresentamos o conceito de uma base p -integral.

No Capítulo 5, apresentamos um estudo de bases p -integrais para um corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz de um polinômio irreduzível sobre $\mathbb{Z}$ da forma $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, sob certas condições específicas sobre os coeficientes a e b . Na Seção 5.1, apresentamos algumas propriedades dos elementos p -integrais de um corpo cúbico. Nas Seções 5.2, 5.3 e 5.4, analisamos os casos possíveis para encontrar uma base 2, 3 e p -integral para o corpo $\mathbb{K}$, respectivamente, onde p é um número primo maior que 3. Na Seção 5.5, avaliamos o discriminante do corpo $\mathbb{K}$. Por fim, na Seção 5.6, encontramos uma base integral para um corpo cúbico e para um corpo cúbico puro, finalizando com alguns exemplos numéricos.

No Capítulo 6, apresentamos a conclusão deste trabalho e algumas perspectivas futu-

ras.

2 Conceitos Básicos

Neste capítulo, apresentamos alguns resultados básicos, e importantes, da Teoria Algébrica dos Números que serão úteis para o entendimento dos próximos capítulos. Na Seção 2.1, apresentamos os elementos inteiros e o anel de inteiros de uma extensão de anéis. Na Seção 2.2, apresentamos uma breve introdução de extensões algébricas de um corpo. Na Seção 2.3, apresentamos alguns resultados básicos de corpos de números e algumas de suas propriedades. Na Seção 2.4, apresentamos o discriminante de um conjunto e de um elemento de uma extensão de corpos e, por fim, na Seção 2.5, apresentamos o conceito uma base de um ideal e algumas propriedades. Ao longo deste capítulo, foram usadas as referências [4] e [5]. A demonstração do Teorema 2.9 encontra-se no Capítulo 3 de [5] e os demais resultados encontram-se nos Capítulos 4, 5 e 6 de [4].

2.1 Anel de inteiros

Nesta seção, consideramos A , B e C anéis tais que $A \subseteq B \subseteq C$.

Definição 2.1. Um elemento $\alpha \in B$ é dito **inteiro sobre A** se α é raiz de um polinômio mônico com coeficientes em A , isto é, se existem $a_0, a_1, \dots, a_{n-1} \in A$, não todos nulos, tais que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0.$$

Quando $B = \mathbb{C}$ e $A = \mathbb{Q}$, o elemento α é chamado de **número algébrico**. Quando $A = \mathbb{Z}$, o elemento α é chamado **inteiro algébrico**.

Proposição 2.2. *Se $c \in C$ é inteiro sobre A , então c é inteiro sobre B .*

Definição 2.3. O anel B é chamado **inteiro sobre A** , quando b é inteiro sobre A , para todo $b \in B$.

Corolário 2.4. *Se C é inteiro sobre A , então C é inteiro sobre B .*

Teorema 2.5. *Um elemento $b \in B$ é inteiro sobre A se, e somente se, $A[b]$ é um A -módulo finitamente gerado.*

Teorema 2.6. *Seja $b \in B$. Se existe D um subanel de B , tal que $A[b] \subseteq D \subseteq B$ e D é um A -módulo finitamente gerado, então b é inteiro sobre A e $A[b]$ é um A -módulo finitamente gerado.*

Corolário 2.7. *Se B é um A -módulo finitamente gerado, então B é inteiro sobre A .*

Proposição 2.8. *Se B é um A -módulo finitamente gerado e C é um B -módulo finitamente gerado, então C é um A -módulo finitamente gerado.*

Teorema 2.9. *Seja B um domínio e inteiro sobre A . Assim, B é um corpo se, e somente se, A é um corpo.*

Proposição 2.10. *Se $b_1, b_2 \in B$ são elementos inteiros sobre A , então $b_1 + b_2$, $b_1 - b_2$ e $b_1 b_2$ são elementos inteiros sobre A .*

Proposição 2.11. *O conjunto dos elementos de B que são inteiros sobre A é um subanel de B contendo A .*

Definição 2.12. O conjunto dos elementos de B que são inteiros sobre A é definido por

$$\mathcal{O}_B = \{\alpha \in B : \alpha \text{ é inteiro sobre } A\},$$

e é chamado **anel de inteiros** de A em B .

Definição 2.13. O anel B é chamado **inteiro sobre A** quando $\mathcal{O}_B = B$

Proposição 2.14. *Se $b_1, \dots, b_n \in B$ são elementos inteiros sobre A , então $A[b_1, \dots, b_n]$ é um A -módulo finitamente gerado.*

Proposição 2.15. *Se $b_1, \dots, b_n \in B$ são elementos inteiros sobre A , então $A[b_1, \dots, b_n]$ é inteiro sobre A .*

Proposição 2.16. *Se B é inteiro sobre A e $c \in C$ é inteiro sobre B , então c é inteiro sobre A .*

Corolário 2.17. *Se C é inteiro sobre B e B é inteiro sobre A , então C é inteiro sobre A . Em outras palavras, a relação entre extensões inteiras é transitiva.*

Proposição 2.18. *Sejam A um domínio de fatoração única e $\mathbb{K}$ o seu corpo de frações. Assim, $c \in \mathbb{K}$ é inteiro sobre A se, e somente se $c \in A$.*

Corolário 2.19. *Se $\mathcal{O}_{\mathbb{Q}}$ é o anel de inteiros de $\mathbb{Z}$ em $\mathbb{Q}$, então $\mathbb{Q} \cap \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.*

Definição 2.20. O anel A é dito **integralmente fechado** em B quando $\mathcal{O}_B = A$. Sejam A um domínio e $\mathbb{K}$ o seu corpo de frações. O anel A é chamado integralmente fechado se $\mathcal{O}_{\mathbb{K}} = A$.

Observação 2.21. Sejam A um domínio de fatoração única e $\mathbb{K}$ o seu corpo de frações. Pela Proposição 2.18, segue que A é integralmente fechado.

Proposição 2.22. *Se α é um número algébrico, então $\alpha = \frac{a}{b}$, com a um inteiro algébrico e $b \in \mathbb{Z}$ não nulo.*

2.2 Extensões algébricas

Nesta seção, consideramos $\mathbb{K}$ um subcorpo de $\mathbb{C}$, ou seja, $\mathbb{K}$ um corpo tal que $\mathbb{K} \subseteq \mathbb{C}$.

Definição 2.23. Um elemento $\alpha \in \mathbb{C}$ é dito **algébrico** sobre o corpo $\mathbb{K}$ se for raiz de um polinômio mônico com coeficientes em $\mathbb{K}$. Caso contrário, α é chamado **transcendente** sobre o corpo $\mathbb{K}$.

Definição 2.24. Seja $\alpha \in \mathbb{C}$ algébrico sobre o corpo $\mathbb{K}$. O polinômio mônico $m_{\alpha}(x)$ de grau mínimo tal que $m_{\alpha}(\alpha) = 0$ é chamado **polinômio minimal** de α sobre $\mathbb{K}$.

Definição 2.25. Seja $\alpha \in \mathbb{C}$ algébrico sobre o corpo $\mathbb{K}$. O **grau de α sobre o corpo $\mathbb{K}$** é definido por

$$\text{gr}_{\mathbb{K}}(\alpha) = \text{gr}(m_{\alpha}(x)).$$

Quando $\mathbb{K} = \mathbb{Q}$, escrevemos apenas $\text{gr}(\alpha)$.

Proposição 2.26. Se $\alpha \in \mathbb{C}$ é algébrico sobre o corpo $\mathbb{K}$, então $m_{\alpha}(x)$ é irredutível em $\mathbb{K}[x]$.

Definição 2.27. Seja $\alpha \in \mathbb{C}$ algébrico sobre o corpo $\mathbb{K}$. Os **conjugados** de α sobre o corpo $\mathbb{K}$ são as raízes de $m_{\alpha}(x)$ em $\mathbb{C}$.

Proposição 2.28. Se $\alpha \in \mathbb{C}$ é algébrico sobre o corpo $\mathbb{K}$, então os conjugados de α sobre o corpo $\mathbb{K}$ são distintos.

Teorema 2.29. Se $\alpha \in \mathbb{C}$ é um inteiro algébrico, então os seus conjugados sobre $\mathbb{Q}$ também são inteiros algébricos.

Teorema 2.30. Se $\alpha \in \mathbb{C}$ é um inteiro algébrico, então $m_{\alpha}(x) \in \mathbb{Z}[x]$.

Corolário 2.31. Se $\alpha \in \mathbb{C}$ é um inteiro sobre $\mathbb{Z}$, então o polinômio mônico de menor grau em $\mathbb{Q}[x]$ do qual α é raiz, pertence a $\mathbb{Z}[x]$.

Seja $\alpha \in \mathbb{C}$ uma raiz de um polinômio $x^2 + ax + b \in \mathbb{Q}[x]$, irredutível em $\mathbb{Q}$. Mostra-se, na referência [4], que $\mathbb{Q}(\alpha) = \{x + y\alpha : x, y \in \mathbb{Q}\}$ é um corpo. Além disso, $\mathbb{Q}(\alpha)$ é o menor subcorpo de $\mathbb{C}$ contendo $\mathbb{Q}$ e α .

Definição 2.32. Seja $\alpha \in \mathbb{C}$ uma raiz de um polinômio irredutível $x^2 + ax + b \in \mathbb{Q}[x]$ em $\mathbb{Q}$. O corpo $\mathbb{Q}(\alpha)$ é chamado de **corpo quadrático** de $\mathbb{Q}$.

Teorema 2.33. Se $\mathbb{K}$ é um corpo quadrático, então existe um único $d \in \mathbb{Z}$, livre de quadrados, tal que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.

O próximo teorema encontra o anel de inteiros do corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados.

Teorema 2.34. Sejam $\mathbb{K}$ um corpo quadrático e $d \in \mathbb{Z}$ o único livre de quadrados tal que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. O anel de inteiros do corpo $\mathbb{K}$ em $\mathbb{Z}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}(\sqrt{d}), & \text{se } d \not\equiv 1 \pmod{4}, \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1 + \sqrt{d}}{2}\right), & \text{se } d \equiv 1 \pmod{4}. \end{cases}$$

Demonstração. Seja

$$A = \begin{cases} \mathbb{Z} + \mathbb{Z}(\sqrt{d}), & \text{se } d \not\equiv 1 \pmod{4}, \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1 + \sqrt{d}}{2}\right), & \text{se } d \equiv 1 \pmod{4}. \end{cases}$$

Se $\alpha \in A$, então $\alpha \in \mathbb{K}$.

1. Se $d \not\equiv 1 \pmod{4}$, então

$$\alpha \in \mathbb{Z} + \mathbb{Z}(\sqrt{d}) \Rightarrow \alpha = a + b\sqrt{d}, \text{ com } a, b \in \mathbb{Z}.$$

Assim,

$$\alpha^2 = a^2 + b^2d + 2ab\sqrt{d} + 2a^2 - 2a^2 = -a^2 + b^2d + 2a\alpha \Rightarrow \alpha^2 - 2a\alpha + (a^2 - b^2d) = 0.$$

Portanto, α é raiz do polinômio $x^2 - 2ax + (a^2 - b^2d) \in \mathbb{Z}[x]$, ou seja, $\alpha \in \mathcal{O}_{\mathbb{K}}$.

2. Se $d \equiv 1 \pmod{4}$, então

$$\alpha \in \mathbb{Z} + \mathbb{Z}\left(\frac{1 + \sqrt{d}}{2}\right) \Rightarrow \alpha = a + b\left(\frac{1 + \sqrt{d}}{2}\right), \text{ com } a, b \in \mathbb{Z}.$$

Assim,

$$\begin{aligned} \alpha^2 &= a^2 + 2ab\left(\frac{1 + \sqrt{d}}{2}\right) + \left(\frac{b + b\sqrt{d}}{2}\right)^2 = (2a + b)\alpha - a^2 - ab + b^2\left(\frac{d - 1}{4}\right) \\ &\Rightarrow \alpha^2 - (2a + b)\alpha + a^2 + ab - b^2\left(\frac{d - 1}{4}\right) = 0. \end{aligned}$$

Note que, como $d \equiv 1 \pmod{4}$, segue que $b^2\left(\frac{d - 1}{4}\right) \in \mathbb{Z}$. Assim, α é raiz do polinômio $x^2 - (2a + b)x - \left(a^2 + ab - b^2\left(\frac{d - 1}{4}\right)\right) \in \mathbb{Z}[x]$. Logo, $\alpha \in \mathcal{O}_{\mathbb{K}}$, e assim, $A \subseteq \mathcal{O}_{\mathbb{K}}$.

Por outro lado, se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\alpha \in \mathbb{K} \Rightarrow \alpha = a + b\sqrt{d}, \text{ com } a, b \in \mathbb{Q},$$

e α é raiz de um polinômio mônico em $\mathbb{Z}[x]$. Note que $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Q}$, ou seja, α é raiz de um polinômio mônico $x^2 - 2ax + (a^2 - db^2) \in \mathbb{Q}[x]$, que pode ser obtido da mesma maneira que foi feita na primeira parte da demonstração. Deste polinômio, segue que $\Delta = 4a^2 - 4(a^2 - db^2) = 4b^2d$. Dessa forma, como d é livre de quadrados, segue que este polinômio é redutível em $\mathbb{Q}[x]$ se $b = 0$ e irreduzível em $\mathbb{Q}[x]$ se $b \neq 0$. Assim, o polinômio minimal de α em $\mathbb{Q}[x]$ é dado por

$$m_{\mathbb{Q}}(\alpha) = \begin{cases} x - a, & \text{se } b = 0, \\ x^2 - 2ax + (a^2 - db^2), & \text{se } b \neq 0. \end{cases}$$

Por hipótese, $\alpha \in \mathcal{O}_{\mathbb{K}}$, e assim, $m_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. Logo,

$$\begin{cases} a \in \mathbb{Z}, & \text{se } b = 0, \\ 2a \in \mathbb{Z} \text{ e } a^2 - db^2 \in \mathbb{Z}, & \text{se } b \neq 0. \end{cases}$$

Se $b = 0$, então $\alpha = a \in \mathbb{Z} \subset \mathbb{Z} + \mathbb{Z}(\sqrt{d}) \subseteq A$. Se $b \neq 0$, então $2a \in \mathbb{Z}$ e $a^2 - db^2 \in \mathbb{Z}$. Dessa forma, se $2a$ é par, então $a \in \mathbb{Z}$ implica que $a^2 \in \mathbb{Z}$. Agora, uma vez que

$a^2 + db^2 \in \mathbb{Z}$, então devemos ter $db^2 \in \mathbb{Z}$. Assim, se $b = \frac{m}{n}$, com $m, n \in \mathbb{Z}$, $n \neq 0$ e $\text{mdc}(m, n) = 1$, então

$$db^2 = d \left(\frac{m}{n} \right)^2 \in \mathbb{Z} \Rightarrow n^2 \mid d \Rightarrow n^2 = 1,$$

pois d é livre de quadrados. Assim, $n = \pm 1 \Rightarrow b \in \mathbb{Z}$, e deste modo, $a + b\sqrt{d} \in \mathbb{Z} + \mathbb{Z}(\sqrt{d}) \subseteq A$. Mas, se $2a$ é ímpar, então $2a = 2k + 1$, com $k \in \mathbb{Z} \Rightarrow a = k + \frac{1}{2} \Rightarrow a^2 = k^2 + k + \frac{1}{4} \notin \mathbb{Z}$. Assim,

$$\begin{aligned} a^2 - db^2 \in \mathbb{Z} &\Rightarrow 4(a^2 - db^2) \in \mathbb{Z} \\ &\Rightarrow 4 \left[\left(k + \frac{1}{2} \right)^2 - db^2 \right] = 4k^2 + 4k + 1 - 4db^2 \in \mathbb{Z} \\ &\Rightarrow 4db^2 \in \mathbb{Z}. \end{aligned}$$

Agora, se $2b = \frac{r}{s}$, com $r, s \in \mathbb{Z}$, $s \neq 0$ e $\text{mdc}(r, s) = 1$, então

$$d(2b)^2 = d \left(\frac{r}{s} \right)^2 \in \mathbb{Z} \Rightarrow s^2 \mid d \Rightarrow s^2 = 1,$$

pois d é livre de quadrados. Portanto, $s = \pm 1 \Rightarrow 2b \in \mathbb{Z}$.

Neste caso, se $2b$ for par, então $b \in \mathbb{Z} \Rightarrow b^2 \in \mathbb{Z} \Rightarrow db^2 \in \mathbb{Z} \Rightarrow (a^2 - db^2) + db^2 \in \mathbb{Z} \Rightarrow a^2 \in \mathbb{Z}$, o que não ocorre. Logo, $2b$ é ímpar. Logo, $2b = 2q + 1$, com $q \in \mathbb{Z}$, e assim, $a = \frac{2k+1}{2}$ e $b = \frac{2q+1}{2}$, com $k, q \in \mathbb{Z}$. Assim,

$$\begin{aligned} a^2 - db^2 &= \left(\frac{2k+1}{2} \right)^2 - d \left(\frac{2q+1}{2} \right)^2 \\ &= \frac{1}{4} [(2k+1)^2 - d(2q+1)^2] \\ &= k^2 + k - dq^2 - dq + \frac{1-d}{4} \in \mathbb{Z}. \end{aligned}$$

Logo,

$$\frac{d-1}{4} = k^2 + k - d(q^2 - q) - (a^2 - db^2) \in \mathbb{Z} \Rightarrow d \equiv 1 \pmod{4}.$$

Com isso, segue que

$$\begin{aligned} \alpha &= a + b\sqrt{d} = \frac{2k+1}{2} + \frac{2q+1}{2}\sqrt{d} \\ &= \frac{2k+1}{2} + \frac{2q+1}{2}\sqrt{d} + \frac{2q+1}{2} - \frac{2q+1}{2} \\ &= (2q+1) \left(\frac{1+\sqrt{d}}{2} \right) + k - q \\ &= (k-q)(2q+1) \left(\frac{1+\sqrt{d}}{2} \right) \in \mathbb{Z} + \mathbb{Z} \left(\frac{1+\sqrt{d}}{2} \right) \subseteq A. \end{aligned}$$

Logo, $\alpha \in A$ e $\mathcal{O}_{\mathbb{K}} \subseteq A$, ou seja,

$$\mathcal{O}_{\mathbb{K}} = A = \begin{cases} \mathbb{Z} + \mathbb{Z}(\sqrt{d}), & \text{se } d \not\equiv 1 \pmod{4}, \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right), & \text{se } d \equiv 1 \pmod{4}, \end{cases}$$

o que prova o resultado. $\square$

Para os próximos resultados consideramos $\mathbb{K}$ um subcorpo de $\mathbb{C}$.

Proposição 2.35. *Se $\alpha \in \mathbb{C}$ é algébrico sobre o corpo $\mathbb{K}$ e $\text{gr}(m_{\alpha}(x)) = n$, então*

$$\mathbb{K}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \dots, a_{n-1} \in \mathbb{K}\}.$$

Observação 2.36. A Proposição 2.35 mostra que $\mathbb{K}(\alpha)$ pode ser visto como um espaço vetorial de dimensão n sobre o corpo $\mathbb{K}$, cuja base é dada por $\{1, \alpha, \dots, \alpha^{n-1}\}$.

Definição 2.37. Seja $\alpha \in \mathbb{C}$ algébrico sobre o corpo $\mathbb{K}$ e $\text{gr}(m_{\alpha}(x)) = n$. O **grau da extensão** $\mathbb{K}(\alpha)$ sobre o corpo $\mathbb{K}$ é n e escrevemos $[\mathbb{K}(\alpha) : \mathbb{K}] = n$.

Exemplo 2.38. Seja $d \in \mathbb{Z}$ livre de quadrados. O corpo $\mathbb{Q}(\sqrt{d})$ é uma extensão quadrática de $\mathbb{Q}$.

Definição 2.39. Sejam $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{C}$ algébricos sobre o corpo $\mathbb{K}$. O corpo $\mathbb{K}(\alpha_1, \dots, \alpha_k)$ é chamado de **extensão múltipla** do corpo $\mathbb{K}$ e é obtido através de uma sucessão de k junções simples:

$$\begin{aligned} \mathbb{K}(\alpha_1, \alpha_2) &= (\mathbb{K}(\alpha_1))(\alpha_2), \\ \mathbb{K}(\alpha_1, \alpha_2, \alpha_3) &= (\mathbb{K}(\alpha_1, \alpha_2))(\alpha_3), \\ &\vdots \\ \mathbb{K}(\alpha_1, \dots, \alpha_k) &= (\mathbb{K}(\alpha_1, \dots, \alpha_{k-1}))(\alpha_k). \end{aligned}$$

Proposição 2.40. *Se $\alpha, \beta \in \mathbb{C}$ são algébricos sobre o corpo $\mathbb{K}$, então existe $\gamma \in \mathbb{C}$ algébrico sobre o corpo $\mathbb{K}$ tal que $\mathbb{K}(\alpha, \beta) = \mathbb{K}(\gamma)$.*

Proposição 2.41. *Se $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ são algébricos sobre o corpo $\mathbb{K}$, então existe $\alpha \in \mathbb{C}$ algébrico sobre o corpo $\mathbb{K}$ tal que $\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha)$.*

Proposição 2.42. *Se $\alpha \in \mathbb{C}$ é algébrico sobre o corpo $\mathbb{K}$, então todo elemento $\beta \in \mathbb{K}(\alpha)$ é algébrico sobre o corpo $\mathbb{K}$ e o grau de β sobre o corpo $\mathbb{K}$ é menor ou igual ao grau de α sobre o corpo $\mathbb{K}$.*

2.3 Corpo de números

Nesta seção, apresentamos definições e propriedades envolvendo corpo de números.

Definição 2.43. Um **corpo de números** é um subcorpo de $\mathbb{C}$ da forma $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$, com $\alpha_1, \alpha_2, \dots, \alpha_n$ números algébricos. Em outras palavras, um corpo de números é uma extensão finita do corpo $\mathbb{Q}$.

Teorema 2.44. *Se $\mathbb{K}$ é um corpo de números, então existe um número algébrico θ tal que $\mathbb{K} = \mathbb{Q}(\theta)$.*

Observação 2.45. O elemento $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ é chamado de **elemento primitivo** do corpo $\mathbb{K}$.

Teorema 2.46. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, com θ um número algébrico, e $\alpha \in \mathbb{C}$ com $\text{gr}(m_{\alpha}(x)) = n$. Assim, $\alpha \in \mathbb{K}$ se, e somente se, existem únicos $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$ tais que $\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$.*

Observação 2.47. Um corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$ é um espaço vetorial sobre $\mathbb{Q}$ de dimensão finita $n = m_{\theta}(x)$. Se $n = 2$, dizemos que $\mathbb{K}$ é corpo quadrático. Se $n = 3$, $\mathbb{K}$ é um corpo cúbico. Se $n = 4$, então $\mathbb{K}$ é um corpo quártico.

Proposição 2.48. *Se $\mathbb{K}$ é um corpo de números, então $\mathcal{O}_{\mathbb{K}}$ é um domínio.*

Proposição 2.49. *Se $\mathbb{K}$ é um corpo de números, então o corpo de frações de $\mathcal{O}_{\mathbb{K}}$ é $\mathbb{K}$.*

Proposição 2.50. *Se $\mathbb{K}$ é um corpo de números, então $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado.*

Proposição 2.51. *Se $\mathbb{K}$ é um corpo de números, então todo ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ contém um número $b \in \mathbb{Z}$ não nulo.*

Proposição 2.52. *Seja $\mathbb{K}$ um corpo de números. Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então existe $\gamma \in I$ tal que $\mathbb{K} = \mathbb{Q}(\gamma)$.*

Teorema 2.53. *Se $\mathbb{K}$ é um corpo de números de grau n sobre $\mathbb{Q}$, então existem exatamente n monomorfismos $\sigma_k : \mathbb{K} \rightarrow \mathbb{C}$, $k = 1, \dots, n$.*

Sejam $\mathbb{K}$ um corpo de números de grau n sobre $\mathbb{Q}$, $\theta \in \mathbb{K}$, tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $\theta_1, \theta_2, \dots, \theta_n$ os conjugados de θ sobre $\mathbb{Q}$. Para $\alpha \in \mathbb{K}$, segue que existem únicos $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$, tais que $\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$. Para $k \in \{1, 2, \dots, n\}$, consideramos

$$\alpha_k = a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1} \in \mathbb{Q}(\theta_k).$$

Definição 2.54. Os elementos $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ são chamados de **$\mathbb{K}$ -conjugados de α** ou **conjugados de α relativos à $\mathbb{K}$** .

Observação 2.55. Os conjugados de α relativos à $\mathbb{K}$ são obtidos aplicando os monomorfismos $\sigma_k : \mathbb{K} \rightarrow \mathbb{C}$, $k = 1, \dots, n$ em α .

Definição 2.56. Sejam $\mathbb{K}$ um corpo de números de grau n , $\alpha \in \mathbb{K}$ e $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ os $\mathbb{K}$ -conjugados de α . O **polinômio característico** de α sobre o corpo $\mathbb{K}$ é definido como o polinômio

$$p_{\alpha}(x) = \prod_{k=1}^n (x - \alpha_k).$$

Proposição 2.57. *Seja $\mathbb{K}$ um corpo de números de grau n . Se $\alpha \in \mathbb{K}$, então $p_{\alpha}(x) \in \mathbb{Q}[x]$.*

Proposição 2.58. *Seja $\mathbb{K}$ um corpo de números de grau n . Se $\alpha \in \mathbb{K}$, então*

$$p_{\alpha}(x) = \left(m_{\alpha}(x)\right)^s,$$

$$\text{com } s = \frac{n}{\text{gr}(m_{\alpha}(x))} \in \mathbb{Z}_{+}^{*}.$$

Em outras palavras, os conjugados de α com respeito à $\mathbb{K}$ são as raízes de $m_{\alpha}(x)$ em $\mathbb{C}$, cada uma delas com multiplicidade $s = \frac{n}{\text{gr}(m_{\alpha}(x))}$

Proposição 2.59. *Seja $\mathbb{K}$ um corpo de números. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então os $\mathbb{K}$ -conjugados de α são inteiros algébricos.*

Proposição 2.60. *Sejam $\mathbb{K}$ um corpo de números e $\alpha \in \mathbb{K}$. Os $\mathbb{K}$ -conjugados de α com relação a $\mathbb{K}$ são iguais se, e somente se, $\alpha \in \mathbb{Q}$.*

Proposição 2.61. *Sejam $\mathbb{K}$ um corpo de números e $\alpha \in \mathbb{K}$. Os $\mathbb{K}$ -conjugados de α com relação a $\mathbb{K}$ são distintos se, e somente se, $\mathbb{K} = \mathbb{Q}(\alpha)$.*

2.4 Discriminante

Nesta seção, consideramos $\mathbb{K}$ um corpo de números de grau n .

Definição 2.62. Sejam $\omega_1, \omega_2, \dots, \omega_n \in \mathbb{K}$. Considere $\sigma_k : \mathbb{K} \rightarrow \mathbb{C}$, $k = 1, \dots, n$ os n monomorfismos distintos do corpo $\mathbb{K}$ em $\mathbb{C}$. Para $i = 1, 2, \dots, n$, denote por $\omega_i^{(j)} = \sigma_j(\omega_i)$, com $j = 1, \dots, n$, os $\mathbb{K}$ -conjugados de ω_i . O **discriminante** de $\{\omega_1, \dots, \omega_n\}$ é definido por

$$D(\omega_1, \dots, \omega_n) = \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2.$$

Definição 2.63. O discriminante de $\alpha \in \mathbb{K}$ é definido por $D(\alpha) = D(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$.

Proposição 2.64. *Se $\alpha \in \mathbb{K}$ e $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ são os $\mathbb{K}$ -conjugados de α , então*

$$D(\alpha) = \prod_{i \neq j} (\alpha_i - \alpha_j)^2.$$

Definição 2.65. Seja o polinômio $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$, com $n \in \mathbb{N}$ e $a_n \neq 0$, e sejam $x_1, x_2, \dots, x_n \in \mathbb{C}$ as raízes de $f(x)$. O discriminante de $f(x)$ é

$$D(f(x)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in \mathbb{C}.$$

Proposição 2.66. *Se $\alpha \in \mathbb{K}$, então $D(\alpha) = D(p_\alpha(x))$.*

Proposição 2.67. *Se $\alpha \in \mathbb{K}$, então $\mathbb{K} = \mathbb{Q}(\alpha)$ se, e somente se, $D(\alpha) \neq 0$.*

Teorema 2.68. *Seja $\mathbb{K}$ um corpo de números de grau n .*

1. *Se $\omega_1, \dots, \omega_n \in \mathbb{K}$, então $D(\omega_1, \dots, \omega_n) \in \mathbb{Q}$;*
2. *Se $\omega_1, \dots, \omega_n \in \mathcal{O}_{\mathbb{K}}$, então $D(\omega_1, \dots, \omega_n) \in \mathbb{Z}$;*
3. *Se $\omega_1, \dots, \omega_n \in \mathbb{K}$, então $D(\omega_1, \dots, \omega_n) \neq 0$ se, e somente se, $\omega_1, \dots, \omega_n$ são linearmente independentes sobre $\mathbb{Q}$.*

2.5 Base de um ideal

Nesta seção, consideramos $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o seu anel de inteiros algébricos.

Proposição 2.69. *Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então existem $\eta_1, \dots, \eta_n \in I$ tais que $D(\eta_1, \dots, \eta_n) \neq 0$.*

Proposição 2.70. *Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então existem $\eta_1, \dots, \eta_n \in I$ tais que para todo $\alpha \in I$, existem únicos $x_1, \dots, x_n \in \mathbb{Z}$ tais que $\alpha = x_1\eta_1 + \dots + x_n\eta_n$.*

Observação 2.71. Um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo finitamente gerado.

Proposição 2.72. *O anel $\mathcal{O}_{\mathbb{K}}$ é um domínio Noetheriano.*

Definição 2.73. Seja I um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Um subconjunto $\{\eta_1, \dots, \eta_n\}$ de I tal que para todo $\alpha \in I$ existem únicos $x_1, \dots, x_n \in \mathbb{Z}$ de modo que $\alpha = x_1\eta_1 + \dots + x_n\eta_n$ é chamado de **base do ideal I** .

Proposição 2.74. *Seja I um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$.*

1. *Se $\{\eta_1, \dots, \eta_n\}$ e $\{\lambda_1, \dots, \lambda_n\}$ são duas bases para I , então*

$$D(\eta_1, \dots, \eta_n) = D(\lambda_1, \dots, \lambda_n) \quad e \quad \eta_i = \sum_{j=1}^n c_{ij}\lambda_j, \quad \text{onde } i = 1, \dots, n,$$

com $c_{ij} \in \mathbb{Z}$ e $\det(c_{ij}) = \pm 1$;

2. *Seja $\{\eta_1, \dots, \eta_n\}$ uma base para I e $\lambda_1, \dots, \lambda_n \in I$ tais que*

$$D(\eta_1, \dots, \eta_n) = D(\lambda_1, \dots, \lambda_n),$$

então $\{\lambda_1, \dots, \lambda_n\}$ é uma base para I .

Definição 2.75. Sejam I um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ e $\{\eta_1, \dots, \eta_n\}$ uma base para I . O **discriminante do ideal I** é definido por $D(I) = D(\eta_1, \dots, \eta_n)$.

Teorema 2.76. *Sejam $\mathbb{K}$ um corpo quadrático e $d \in \mathbb{Z}$, livre de quadrados, tal que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.*

1. *Para $d \not\equiv 1 \pmod{4}$, sejam $a, b, c \in \mathbb{Z}$, com $a, c \neq 0$. Assim, $\{a, b + c\sqrt{d}\}$ é uma base para o ideal $I = \langle a, b + c\sqrt{d} \rangle$ se, e somente se, $c \mid a$, $c \mid b$ e $ac \mid b^2 - dc^2$;*
2. *Para $d \equiv 1 \pmod{4}$, sejam $a, b, c \in \mathbb{Z}$, com $a, b \neq 0$ e $b \equiv c \pmod{2}$. Assim, $\left\{a, \frac{b + c\sqrt{d}}{2}\right\}$ é uma base para o ideal $I = \left\langle a, \frac{b + c\sqrt{d}}{2} \right\rangle$ se, e somente se, $c \mid a$, $c \mid b$ e $4ac \mid b^2 - dc^2$.*

Proposição 2.77. *Seja $\mathbb{K}$ um corpo de números. Se P é um ideal primo de $\mathcal{O}_{\mathbb{K}}$, então P é um ideal maximal de $\mathcal{O}_{\mathbb{K}}$.*

Definição 2.78. Um anel A é chamado um anel (ou domínio) de **Dedekind** se A é um domínio Noetheriano, integralmente fechado e se todo ideal primo não nulo de A é um ideal maximal.

Observação 2.79. Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Pelas Proposições 2.50, 2.72 e 2.77, segue que $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado, é um domínio Noetheriano e todo ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$ é maximal. Com isso, concluímos que $\mathcal{O}_{\mathbb{K}}$ é um anel de Dedekind.

3 Base Integral

Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Neste capítulo, veremos que existe uma base da extensão $\mathbb{Q} \subseteq \mathbb{K}$ contida em $\mathcal{O}_{\mathbb{K}}$, chamada de base integral.

3.1 Base integral de um corpo de números

Nesta seção, consideramos $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros.

Definição 3.1. Uma base $\{u_1, \dots, u_n\}$ para $\mathcal{O}_{\mathbb{K}}$ é chamada uma **base integral** para o corpo $\mathbb{K}$.

Teorema 3.2. *Seja $\mathbb{K}$ um corpo quadrático. Se $d \in \mathbb{Z}$ é livre de quadrados tal que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, então $\{1, \sqrt{d}\}$ é uma base integral para o corpo $\mathbb{K}$, se $d \not\equiv 1 \pmod{4}$ e $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ é uma base integral para o corpo $\mathbb{K}$, se $d \equiv 1 \pmod{4}$.*

Demonstração. Segue diretamente do Teorema 2.34. □

O discriminante de uma base integral de um corpo de números está bem definida, ou seja, se $\{\eta_1, \dots, \eta_n\}$ e $\{\lambda_1, \dots, \lambda_n\}$ são duas bases integrais para um corpo de números $\mathbb{K}$ de grau n , então $D(\eta_1, \dots, \eta_n) = D(\lambda_1, \dots, \lambda_n)$ e se $\{\eta_1, \dots, \eta_n\}$ é uma base integral para o corpo $\mathbb{K}$ e $\lambda_1, \dots, \lambda_n \in \mathcal{O}_{\mathbb{K}}$ são tais que $D(\eta_1, \dots, \eta_n) = D(\lambda_1, \dots, \lambda_n)$, então $\{\lambda_1, \dots, \lambda_n\}$ é uma base integral para o corpo $\mathbb{K}$.

Definição 3.3. Seja $\{\eta_1, \dots, \eta_n\}$ uma base integral para o corpo $\mathbb{K}$. O número $D(\eta_1, \dots, \eta_n)$ é chamado **discriminante** do corpo $\mathbb{K}$ e denotado por $D(\mathbb{K})$.

Se $\mathbb{K}$ é um corpo de números de grau n e $\lambda_1, \dots, \lambda_n \in \mathcal{O}_{\mathbb{K}}$ são tais que $D(\lambda_1, \dots, \lambda_n) = D(\mathbb{K})$, então $\{\lambda_1, \dots, \lambda_n\}$ é uma base integral para o corpo $\mathbb{K}$. No próximo resultado, determinamos o discriminante de um corpo quadrático.

Teorema 3.4. *Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados, então o discriminante do corpo $\mathbb{K}$ é dado por*

$$D(\mathbb{K}) = \begin{cases} 4d, & \text{se } d \not\equiv 1 \pmod{4}, \\ d, & \text{se } d \equiv 1 \pmod{4}. \end{cases}$$

Demonstração. Seja $d \not\equiv 1 \pmod{4}$. Pelo Teorema 3.2, segue que $\{1, \sqrt{d}\}$ é uma base integral para o corpo $\mathbb{K}$. Assim,

$$D(\mathbb{K}) = D(1, \sqrt{d}) = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

Por outro lado, seja $d \equiv 1 \pmod{4}$. Pelo Teorema 3.2, segue que $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ é uma base integral para o corpo $\mathbb{K}$. Assim,

$$D(\mathbb{K}) = D\left(1, \frac{1+\sqrt{d}}{2}\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = (-\sqrt{d})^2 = d,$$

o que prova o resultado. $\square$

Proposição 3.5. *Se $\mathbb{K}$ é um corpo quadrático, então $\mathbb{K} = \mathbb{Q}(\sqrt{D(\mathbb{K})})$.*

Demonstração. Seja $d \in \mathbb{Z}$ livre de quadrados tal que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. Pelo Teorema 3.4, segue que $D(\mathbb{K}) = d$ ou $D(\mathbb{K}) = 4d$. Dessa forma, $\sqrt{D(\mathbb{K})} = \sqrt{d}$ ou $\sqrt{D(\mathbb{K})} = 2\sqrt{d}$, isto é, $\mathbb{Q}(\sqrt{D(\mathbb{K})}) = \mathbb{Q}(\sqrt{d}) = \mathbb{K}$. $\square$

Observação 3.6. Uma vez que um corpo quadrático é da forma $\mathbb{K} = \mathbb{Q}(\sqrt{D(\mathbb{K})})$, segue que $\mathbb{K}$ é um corpo real se, e somente se, $D(\mathbb{K}) > 0$.

Definição 3.7. Sejam $\mathbb{K}$ um corpo de números de grau n e I um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$.

A **norma do ideal** I é definida por $N(I) = \sqrt{\frac{D(I)}{D(\mathbb{K})}}$.

Proposição 3.8. *Seja $\mathbb{K}$ um corpo de números de grau n . Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(I) \in \mathbb{Z}$ e $N(I) > 0$.*

Demonstração. Considere $\{\eta_1, \dots, \eta_n\}$ uma base para I e $\{\omega_1, \dots, \omega_n\}$ uma base integral para o corpo $\mathbb{K}$. Uma vez que $\eta_1, \dots, \eta_n \in \mathcal{O}_{\mathbb{K}}$, segue que existem $c_{ij} \in \mathbb{Z}$, para $i, j = 1, \dots, n$, tais que $\eta_i = \sum_{j=1}^n c_{ij}\omega_j$, para todo $i = 1, 2, \dots, n$. Assim,

$$D(I) = D(\eta_1, \dots, \eta_n) = (\det(c_{ij}))^2 D(\omega_1, \dots, \omega_n) = (\det(c_{ij}))^2 D(\mathbb{K}).$$

Note que

$$I \neq \{0\} \Rightarrow D(I) \neq 0 \Rightarrow (\det(c_{ij}))^2 > 0.$$

Dessa forma,

$$N(I) = \sqrt{\frac{D(I)}{D(\mathbb{K})}} = \sqrt{\frac{(\det(c_{ij}))^2 D(\mathbb{K})}{D(\mathbb{K})}} = |\det(c_{ij})| \in \mathbb{Z} \text{ e } D(I) > 0,$$

o que prova a proposição. $\square$

Observação 3.9. Sejam $\mathbb{K}$ um corpo de números de grau n e I um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Considere $\{\eta_1, \dots, \eta_n\}$ uma base para I e $\{\omega_1, \dots, \omega_n\}$ uma base integral para o corpo $\mathbb{K}$. Note que, pela demonstração anterior, também podemos definir $N(I)$ por $N(I) = |\det(c_{ij})|$, com c_{ij} sendo os coeficientes na combinação linear dos ω_j para escrever η_i , para todo $i, j = 1, \dots, n$.

Exemplo 3.10. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$ e $I = \langle 2, 1 + \sqrt{-5} \rangle$ um ideal de $\mathcal{O}_{\mathbb{K}}$. Vamos determinar $N(I)$. Primeiramente, note que $-5 \not\equiv 1 \pmod{4}$. Assim, pelo Teorema 3.2, segue que $\{1, \sqrt{-5}\}$ é uma base para $\mathcal{O}_{\mathbb{K}}$. Além disso, pelo Teorema 3.4, segue que $D(\mathbb{K}) = 4 \cdot (-5) = -20$. Agora,

$$\begin{aligned} I = \langle 2, 1 + \sqrt{-5} \rangle &= \{(a + b\sqrt{-5}) \cdot 2 + (c + d\sqrt{-5})(1 + \sqrt{-5}) : a, b, c, d \in \mathbb{Z}\} \\ &= \{(2a + c - 5d) + (2b + c + d)\sqrt{-5} : a, b, c, d \in \mathbb{Z}\}. \end{aligned}$$

Chamando $y = 2b + c + d \in \mathbb{Z}$, segue que $c = y - 2b - d$ e

$$\begin{aligned} I &= \{(2a + c - 5d) + y\sqrt{-5} : a, c, d, y \in \mathbb{Z}\} \\ &= \{(2a + y - 2b - d - 5d) + y\sqrt{-5} : a, b, d, y \in \mathbb{Z}\} \\ &= \{2(a - b - 3d) + y + y\sqrt{-5} : a, b, d, y \in \mathbb{Z}\}. \end{aligned}$$

Agora, chamando $x = a - b - 3d \in \mathbb{Z}$, segue que $I = \{2x + y(1 + \sqrt{-5}) : x, y \in \mathbb{Z}\}$. Portanto, $\langle 2, 1 + \sqrt{-5} \rangle$ é uma base para I e

$$D(I) = \begin{vmatrix} 2 & 1 + \sqrt{-5} \\ 2 & 1 - \sqrt{-5} \end{vmatrix}^2 = (-4\sqrt{-5})^2 = -80.$$

$$\text{Logo, } N(I) = \sqrt{\frac{D(I)}{D(\mathbb{K})}} = \sqrt{\frac{-80}{-20}} = \sqrt{4} = 2.$$

Exemplo 3.11. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados e $d \not\equiv 1 \pmod{4}$, $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$ e $I = \langle \alpha \rangle$ um ideal de $\mathcal{O}_{\mathbb{K}}$. Vamos determinar $N(I)$. Agora,

$$\begin{aligned} I &= \langle \alpha \rangle = \langle a + b\sqrt{d} \rangle \\ &= \{(x + y\sqrt{d})(a + b\sqrt{d}) : x, y \in \mathbb{Z}\} \\ &= \{xa + xb\sqrt{d} + ya\sqrt{d} + ybd : x, y \in \mathbb{Z}\} \\ &= \{x(a + b\sqrt{d}) + y(bd + a\sqrt{d}) : x, y \in \mathbb{Z}\}. \end{aligned}$$

Portanto, $\{a + b\sqrt{d}, bd + a\sqrt{d}\}$ é uma base para o ideal I . Assim,

$$\begin{aligned} D(I) &= \begin{vmatrix} a + b\sqrt{d} & bd + a\sqrt{d} \\ a - b\sqrt{d} & bd - a\sqrt{d} \end{vmatrix}^2 \\ &= [(a + b\sqrt{d})(bd - a\sqrt{d}) - (a - b\sqrt{d})(bd + a\sqrt{d})]^2 \\ &= [2(b^2d\sqrt{d} - a^2\sqrt{d})]^2 = 4d(b^2d - a^2)^2. \end{aligned}$$

Além disso, uma vez que $d \not\equiv 1 \pmod{4}$, pelo Teorema 3.4, segue que $D(\mathbb{K}) = 4d$. Logo, $N(I) = \sqrt{\frac{D(I)}{D(\mathbb{K})}} = |b^2d - a^2|$.

Proposição 3.12. Sejam $\mathbb{K}$ um corpo quadrático e $d \in \mathbb{Z}$ livre de quadrados tal que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.

1. Se $d \not\equiv 1 \pmod{4}$, $a, b, c \in \mathbb{Z}$ tais que $a \neq 0$, $c \neq 0$, $c \mid a$ e $ac \mid b^2 - dc^2$, então $N(\langle a, b + c\sqrt{d} \rangle) = |ac|$.
2. Se $d \equiv 1 \pmod{4}$, $a, b, c \in \mathbb{Z}$ tais que $a \neq 0$, $c \neq 0$, $b \equiv c \pmod{2}$, $c \mid a$, $c \mid b$ e $4ac \mid b^2 - dc^2$, então $N\left(\left\langle a, \frac{b + c\sqrt{d}}{2} \right\rangle\right) = |ac|$.

Demonstração. Para o item 1, pelo Teorema 2.76, segue que $\{a, b + c\sqrt{d}\}$ é uma base para o ideal $\langle a, b + c\sqrt{d} \rangle$. Assim,

$$D(\langle a, b + c\sqrt{d} \rangle) = \begin{vmatrix} a & b + c\sqrt{d} \\ a & b - c\sqrt{d} \end{vmatrix}^2 = (-2ac\sqrt{d})^2 = 4a^2c^2d.$$

Além disso, pelo Teorema 3.2, segue que $d \not\equiv 1 \pmod{4} \Rightarrow D(\mathbb{K}) = 4d$. Assim,

$$N(\langle a, b + c\sqrt{d} \rangle) = \sqrt{\frac{D(\langle a, b + c\sqrt{d} \rangle)}{D(\mathbb{K})}} = \sqrt{\frac{4a^2c^2d}{4d}} = |ac|.$$

Agora, para o item 2, também pelo Teorema 2.76, segue que $\left\{a, \frac{b + c\sqrt{d}}{2}\right\}$ é uma base para o ideal $\left\langle a, \frac{b + c\sqrt{d}}{2} \right\rangle$. Assim,

$$D\left(\left\langle a, \frac{b + c\sqrt{d}}{2} \right\rangle\right) = \begin{vmatrix} a & \frac{b + c\sqrt{d}}{2} \\ a & \frac{b - c\sqrt{d}}{2} \end{vmatrix}^2 = \left(\frac{-2ac\sqrt{d}}{2}\right)^2 = a^2c^2d.$$

Além disso, pelo Teorema 3.4, se $d \equiv 1 \pmod{4}$, então $D(\mathbb{K}) = d$. Logo,

$$N\left(\left\langle a, \frac{b + c\sqrt{d}}{2} \right\rangle\right) = \sqrt{\frac{D(\langle a, \frac{b + c\sqrt{d}}{2} \rangle)}{D(\mathbb{K})}} = \sqrt{\frac{a^2c^2d}{d}} = |ac|,$$

o que prova a proposição. □

Proposição 3.13. *Sejam $\mathbb{K}$ um corpo de números de grau n e $c \in \mathbb{Q}$, com $c \neq 0$. Se $I = \langle c \rangle$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, então $N(\langle c \rangle) = |c|^n$.*

Demonstração. Seja $\{\omega_1, \dots, \omega_n\}$ uma base integral para o corpo $\mathbb{K}$. Assim, $\alpha \in \langle c \rangle$, isto é, $\alpha = c\beta$, para algum $\beta \in \mathcal{O}_{\mathbb{K}}$. Agora, se $\beta \in \mathcal{O}_{\mathbb{K}}$, então existem $x_1, \dots, x_n \in \mathbb{Z}$ tais que $\beta = \sum_{i=1}^n x_i \omega_i$. Logo,

$$\alpha = c\beta = c \left(\sum_{i=1}^n x_i \omega_i \right) = \sum_{i=1}^n x_i (c\omega_i), \quad x_1, \dots, x_n \in \mathbb{Z},$$

ou seja, $\{c\omega_1, \dots, c\omega_n\}$ é uma base do ideal principal $\langle c \rangle$. Dessa forma,

$$\begin{aligned} D(\langle c \rangle) &= D(c\omega_1, \dots, c\omega_n) = c^{2n} D(\omega_1, \dots, \omega_n) = c^{2n} D(\mathbb{K}) \\ \Rightarrow N(\langle c \rangle) &= \sqrt{\frac{D(\langle c \rangle)}{D(\mathbb{K})}} = \sqrt{c^{2n}} = |c|^n = |c|^n, \end{aligned}$$

o que prova a proposição. □

Se $\mathbb{K}$ é um corpo de números de grau n , então existe $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $D(\theta) \neq 0$. Sejam $\{\omega_1, \dots, \omega_n\}$ uma base integral para o corpo $\mathbb{K}$, então existem $c_{ij} \in \mathbb{Z}$, com $i, j = 1, \dots, n$, tais que

$$\begin{cases} 1 = c_{11}\omega_1 + \dots + c_{1n}\omega_n \\ \theta = c_{21}\omega_1 + \dots + c_{2n}\omega_n \\ \vdots \\ \theta^{n-1} = c_{n1}\omega_1 + \dots + c_{nn}\omega_n. \end{cases}$$

Assim,

$$D(\theta) = D(1, \theta, \dots, \theta^{n-1}) = (\det(c_{ij}))^2 D(\omega_1, \dots, \omega_n) = (\det(c_{ij}))^2 D(\mathbb{K}).$$

Portanto, $D(\theta) = m^2 D(\mathbb{K})$, com $m = (\det(c_{ij}))^2$ inteiro positivo.

Definição 3.14. Sejam $\mathbb{K}$ um corpo de números e $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. O **índice** de θ é o inteiro positivo $\text{ind}(\theta)$ tal que $D(\theta) = (\text{ind}(\theta))^2 D(\mathbb{K})$.

Proposição 3.15. Sejam $\mathbb{K}$ um corpo de números de grau n e $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Assim, $\{1, \theta, \dots, \theta^{n-1}\}$ é uma base integral para o corpo $\mathbb{K}$ se, e somente se, $\text{ind}(\theta) = 1$.

Demonstração. Segue do fato de que $\{1, \theta, \dots, \theta^{n-1}\}$ é uma base integral para $\mathbb{K}$ se, e somente se,

$$D(1, \theta, \dots, \theta^{n-1}) = D(\mathbb{K}) \Leftrightarrow D(\theta) = D(\mathbb{K}) \Leftrightarrow \text{ind}(\theta) = 1,$$

o que prova a proposição. $\square$

Proposição 3.16. Sejam $\mathbb{K}$ um corpo de números de grau n e $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Se $D(\theta)$ é livre de quadrados, então $\{1, \theta, \dots, \theta^{n-1}\}$ é uma base integral para o corpo $\mathbb{K}$.

Demonstração. Se $D(\theta) = (\text{ind}(\theta))^2 D(\mathbb{K})$, com $\text{ind}(\theta) \in \mathbb{Z}_+$, então $(\text{ind}(\theta)) = \sqrt{\frac{D(\theta)}{D(\mathbb{K})}} \in \mathbb{Z}_+$, o que implica que $\text{ind}(\theta) = 1$, pois $D(\theta)$ é livre de quadrados. Pela Proposição 3.15, segue que $\{1, \theta, \dots, \theta^{n-1}\}$ é uma base integral para o corpo $\mathbb{K}$. $\square$

Proposição 3.17. Seja θ um número algébrico de grau n . Se $\theta_1 = \theta, \theta_2, \dots, \theta_n$ são os conjugados de θ sobre $\mathbb{Q}$, ou seja, as raízes de $f(x) = m_{\theta}(x)$, então

$$D(\theta) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(\theta_i).$$

Demonstração. Se $f(x) = m_{\theta}(x) = \prod_{i=1}^n (x - \theta_i)$, então $f'(x) = \sum_{i=1}^n \prod_{j=1, j \neq i}^n (x - \theta_j)$. Assim,

$$f'(\theta_i) = \prod_{\substack{j=1 \\ j \neq i}}^n (\theta_i - \theta_j),$$

para $i = 1, 2, \dots, n$. Logo,

$$\begin{aligned}
 \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (\theta_i - \theta_j) &= \prod_{1 \leq i \leq j \leq n} (\theta_i - \theta_j) \prod_{1 \leq j \leq i \leq n} (\theta_i - \theta_j) \\
 &= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i \leq j \leq n} (\theta_i - \theta_j) \prod_{1 \leq j \leq i \leq n} (\theta_j - \theta_i) \\
 &= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i \leq j \leq n} (\theta_i - \theta_j) \prod_{1 \leq i \leq j \leq n} (\theta_i - \theta_j) \\
 &= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i \leq j \leq n} (\theta_i - \theta_j)^2 \\
 &= (-1)^{\frac{n(n-1)}{2}} D(\theta) \Rightarrow D(\theta) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(\theta_i),
 \end{aligned}$$

o que prova a proposição. $\square$

Teorema 3.18. *Sejam $a, b \in \mathbb{Z}$ tais que $x^3 + ax + b \in \mathbb{Z}[x]$ é irreduzível. Se $\theta \in \mathbb{C}$ é uma raiz de $x^3 + ax + b$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo cúbico e $\theta \in \mathcal{O}_{\mathbb{K}}$, então $D(\theta) = -4a^3 - 27b^2$.*

Demonstração. O elemento $\theta \in \mathbb{C}$ é uma raiz do polinômio irreduzível $x^3 + ax + b \in \mathbb{Z}[x]$, ou seja, $f(x) = m_{\alpha}(x) = x^3 + ax + b$ é o polinômio minimal de θ . Se $\theta_1 = \theta, \theta_2, \dots, \theta_n$ são os conjugados de θ sobre $\mathbb{Q}$, e assim, $(x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 + ax + b$. Logo,

$$\begin{cases} \theta_1 + \theta_2 + \theta_3 = 0 \\ \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = a \\ \theta_1\theta_2\theta_3 = -b. \end{cases}$$

Agora, $f'(x) = 3x^2 + a$, e assim,

$$\begin{aligned}
 f'(\theta_1)f'(\theta_2)f'(\theta_3) &= (3\theta_1^2 + a)(3\theta_2^2 + a)(3\theta_3^2 + a) \\
 &= a_3 + 3a^2(\theta_1^2 + \theta_2^2 + \theta_3^2) + 9a(\theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_1^2\theta_3^2) + 27\theta_1^2\theta_2^2\theta_3^2.
 \end{aligned}$$

Note que

$$\begin{cases} \theta_1^2 + \theta_2^2 + \theta_3^2 = (\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3) = -2a \\ \theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_1^2\theta_3^2 = (\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3)^2 - 2\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3) = a^2 \\ \theta_1^2\theta_2^2\theta_3^2 = (\theta_1\theta_2\theta_3)^3 = b^2. \end{cases}$$

Portanto, $f'(\theta_1)f'(\theta_2)f'(\theta_3) = a^2 + 3a^2(-2a) + 9aa^2 + 27b^2 = 4a^3 + 27b^2$. Dessa forma, pela Proposição 3.17, segue que $D(\theta) = (-1)^{\frac{3 \cdot 2}{2}} \prod_{i=1}^n f'(\theta_i) = -4a^3 - 27b^2$. $\square$

Exemplo 3.19. Considere $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz de $x^3 + x + 1 \in \mathbb{Z}[x]$. Vamos determinar uma base integral para o corpo $\mathbb{K}$. O polinômio $x^3 + x + 1 \in \mathbb{Z}[x]$ é irreduzível em $\mathbb{Z}$. Assim, $[\mathbb{K} : \mathbb{Q}] = 3$. Além disso, pelo Teorema 3.18, $\theta \in \mathcal{O}_{\mathbb{K}} \Rightarrow D(\theta) = -4(1)^3 - 27(1)^2 = -31$. E, uma vez que -31 é livre de quadrados segue, pela Proposição 3.16, que $\{1, \theta, \theta^2\}$ é uma base integral para o corpo $\mathbb{K}$.

Corolário 3.20. *Sejam $a, b \in \mathbb{Z}$, tais que $x^3 + ax + b \in \mathbb{Z}[x]$ é irreduzível e $-4a^3 - 27b^2$ é livre de quadrados. Se θ é uma raiz de $x^3 + ax + b$, então $\{1, \theta, \theta^2\}$ é uma base integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$.*

Demonstração. Se θ é uma raiz de $x^3 + ax + b \in \mathbb{Z}[x]$, então $\theta \in \mathcal{O}_{\mathbb{K}}$. Além disso, uma vez que esse polinômio é irreduzível, segue que $[\mathbb{K} : \mathbb{Q}] = 3$. Logo, pelo Teorema 3.18, segue que $D(\theta) = -4a^3 - 27b^2$ que, por hipótese, é livre de quadrados. Portanto, pela Proposição 3.16, segue que $\{1, \theta, \theta^2\}$ é uma base integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$. $\square$

Teorema 3.21. *Sejam $a, b \in \mathbb{Z}$ tais que $x^4 + ax + b \in \mathbb{Z}[x]$ é irreduzível. Se $\theta \in \mathbb{C}$ é uma raiz de $x^4 + ax + b$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo quártico, então $D(\theta) = -27a^4 + 256b^3$.*

Demonstração. A demonstração é feita de maneira análoga à que foi feita no Teorema 3.18. $\square$

Corolário 3.22. *Sejam $a, b \in \mathbb{Z}$ tais que $x^4 + ax + b \in \mathbb{Z}[x]$ é irreduzível e $-27a^4 + 256b^3$ é livre de quadrados. Se θ é uma raiz de $x^4 + ax + b$, então $\{1, \theta, \theta^2, \theta^3\}$ é uma base integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$.*

Demonstração. Se θ é uma raiz de $x^4 + ax + b \in \mathbb{Z}[x]$, então $\theta \in \mathcal{O}_{\mathbb{K}}$. Além disso, uma vez que esse polinômio é irreduzível, segue que $[\mathbb{K} : \mathbb{Q}] = 4$. Logo, pelo Teorema 3.21, segue que $D(\theta) = -27a^4 + 256b^3$ que, por hipótese é livre de quadrados. Portanto, pela Proposição 3.16, segue que $\{1, \theta, \theta^2, \theta^3\}$. $\square$

Exemplo 3.23. Seja θ uma raiz do polinômio irreduzível $x^4 + x + 1 \in \mathbb{Z}[x]$. Assim, $D(\theta) = -27(1)^4 + 256(1)^3 = 229$ é livre de quadrados. Portanto, $\{1, \theta, \theta^2, \theta^3\}$ é uma base integral para o corpo $\mathbb{Q}(\theta)$.

Proposição 3.24. *Se $\mathbb{K}$ é um corpo de números, então $D(\mathbb{K}) \equiv 0 \pmod{4}$ ou $D(\mathbb{K}) \equiv 1 \pmod{4}$.*

Demonstração. Sejam $\{\omega_1, \dots, \omega_n\}$ uma base integral para o corpo $\mathbb{K}$ e $\omega_i^{(1)} = \omega_i, \omega_i^{(2)}, \dots, \omega_i^{(n)}$ os $\mathbb{K}$ -conjugados de ω_i , com $i = 1, \dots, n$. Na expansão do determinante

$$\begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}$$

existem $n!$ termos, dos quais metade aparece com sinal positivo e a outra aparece com o sinal negativo. Considere λ a soma daqueles com sinal positivo e μ a soma daqueles com o sinal negativo. Assim, $\det(\omega_i^{(j)}) = \lambda - \mu$. Sejam $A = \lambda + \mu$ e $B = \lambda\mu$. Assim,

$$\begin{aligned} D(\mathbb{K}) &= \det(\omega_i^{(j)})^2 = (\lambda - \mu)^2 = \lambda^2 - 2\lambda\mu + \mu^2 = \lambda^2 + 2\lambda\mu - 4\lambda\mu + \mu^2 \\ &= (\lambda + \mu)^2 - 4\lambda\mu = A^2 - 4B. \end{aligned}$$

Como $\omega_i \in \mathcal{O}_{\mathbb{K}}$, $i = 1, \dots, n$, pela proposição 2.59, segue que seus $\mathbb{K}$ -conjugados $\omega_i^{(j)}$, $i, j = 1, \dots, n$ são inteiros algébricos. Portanto, λ e μ são inteiros algébricos e, dessa forma, A e B também são. Seja $\theta \in \mathcal{O}_{\mathbb{K}}$, tal que $\mathbb{K} = \mathbb{Q}(\theta)$, e sejam $\theta_1 = \theta, \theta_2, \dots, \theta_n$ os conjugados de θ sobre $\mathbb{Q}$. Se expressarmos cada ω_i como um polinômio em θ com coeficientes racionais, segue que A é uma função simétrica de $\omega_1, \dots, \omega_n$ com coeficientes

racionais. Assim, uma vez que A e B são inteiros algébricos, segue que se $A \in \mathbb{Q}$, então $A \in \mathbb{Z}$. Além disso,

$$B = \frac{A^2 - D(\mathbb{K})}{4} \in \mathbb{Q} \Rightarrow B \in \mathbb{Z}.$$

Agora, como $A, B \in \mathbb{Z}$, segue que $D(\mathbb{K}) = A^2 - 4B \equiv 0$ ou $1 \pmod{4}$. $\square$

Exemplo 3.25. Sejam $x^3 - x - 2 \in \mathbb{Z}[x]$ um polinômio cúbico irredutível, θ uma de suas raízes e $\mathbb{K} = \mathbb{Q}(\theta)$. Assim, $[\mathbb{K} : \mathbb{Q}] = 3$. Vamos calcular $D(\mathbb{K})$ e encontrar uma base integral para o corpo $\mathbb{K}$. Pelo Teorema 3.18, segue que $D(\theta) = -4a^3 - 27b^2 = -4(-1)^3 - 27(-2)^2 = 4 - 108 = -104 = -26 \cdot 2^2$, ou seja, não é livre de quadrados. Sabemos que $(\text{ind}(\theta))^2 = \frac{D(\theta)}{D(\mathbb{K})} \in \mathbb{Z}$. Dessa forma, devemos ter $\frac{D(\theta)}{D(\mathbb{K})} = 1$ ou $4 \Rightarrow D(\mathbb{K}) = -26$ ou -104 . Pela Proposição 3.24, segue que $D(\mathbb{K}) \equiv 0$ ou $1 \pmod{4} \Rightarrow D(\mathbb{K}) \neq -26 \Rightarrow D(\mathbb{K}) = -104$. Portanto, $\text{ind}(\theta) = 1$, e pela Proposição 3.15, segue que $\{1, \theta, \theta^2\}$ é uma base integral para o corpo $\mathbb{K}$.

Exemplo 3.26. Seja $\mathbb{K}$ o corpo quártico $\mathbb{K} = \mathbb{Q}(\sqrt{-1} + \sqrt{2}) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$. Vamos mostrar que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\sqrt{-1} + \mathbb{Z}\sqrt{2} + \mathbb{Z}\left(\frac{1}{2}(\sqrt{2} + \sqrt{-2})\right)$ e que $D(\mathbb{K}) = 256$. Note que

$$A = \mathbb{Z} + \mathbb{Z}\sqrt{2} + \mathbb{Z}\left(\frac{\sqrt{2} + \sqrt{-2}}{2}\right) \subseteq \mathcal{O}_{\mathbb{K}}.$$

Agora, seja $\theta \in \mathcal{O}_{\mathbb{K}}$. Note que os subcorpos do corpo $\mathbb{K}$ são $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{-2})$. Dessa forma,

1. se $\theta \in \mathbb{Q}$, então $\theta \in \mathbb{Z} \subseteq A$;
2. se $\theta \in \mathbb{Q}(\sqrt{-1})$, então $\theta \in \mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z} + \mathbb{Z}\sqrt{-1} \subseteq A$;
3. se $\theta \in \mathbb{Q}(\sqrt{2})$, então $\theta \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq A$;
4. se $\theta \in \mathbb{Q}(\sqrt{-2})$, então $\theta \in \mathcal{O}_{\mathbb{Q}(\sqrt{-2})} = \mathbb{Z} + \mathbb{Z}\sqrt{-2} \subseteq A$.

Vamos supor que θ não esteja em nenhum subcorpo do corpo $\mathbb{K}$. Assim,

$$\theta \in \mathbb{K} \Rightarrow \theta = a + b\sqrt{-1} + c\sqrt{2} + d\sqrt{-2}, \text{ com } a, b, c, d \in \mathbb{Q}.$$

Além disso, os conjugados de θ sobre $\mathbb{Q}$ são

$$\begin{aligned} \theta &= a + b\sqrt{-1} + c\sqrt{2} + d\sqrt{-2}, \\ \theta_1 &= a - b\sqrt{-1} + c\sqrt{2} - d\sqrt{-2}, \\ \theta_2 &= a + b\sqrt{-1} - c\sqrt{2} - d\sqrt{-2}, \\ \theta_3 &= a - b\sqrt{-1} - c\sqrt{2} + d\sqrt{-2}. \end{aligned}$$

Dessa forma,

- $\theta + \theta_1 = 2a + 2c\sqrt{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})}$,
- $\theta + \theta_2 = 2a + 2b\sqrt{-1} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$,
- $\theta + \theta_3 = 2a + 2d\sqrt{-2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-2})}$.

O que implica que $2a, 2b, 2c, 2d \in \mathbb{Z}$. Considere $a_1 = 2a, b_1 = 2b, c_1 = 2c, d_1 = 2d \in \mathbb{Z}$. Dessa forma,

$$\theta = \frac{1}{2}(a_1 + b_1\sqrt{-1} + c_1\sqrt{2} + d_1\sqrt{-2}).$$

Sejam $m = a_1^2 + 2d_1^2 \in \mathbb{Z}$, $n = a_1^2 + b_1^2 - 2c_1^2 - 2d_1^2 \in \mathbb{Z}$ e $r = a_1d_1 - b_1c_1 \in \mathbb{Z}$, então θ é raiz de

$$f(x) = x^4 - 2ax^3 = \left(m + \frac{n}{2}\right)x^2 + \left(-2d_1r - \frac{an}{2}\right)x + \left(\frac{n^2 + 8r^2}{16}\right) \in \mathbb{Q}[x].$$

Uma vez que θ não está em nenhum subcorpo do corpo $\mathbb{K}$. Assim, θ é de grau 4 e

$$\begin{aligned} f(x) = m_\theta(x) &\Rightarrow \theta \in \mathcal{O}_{\mathbb{K}} \Rightarrow f(x) \in \mathbb{Z}[x] \Rightarrow \frac{n}{2} \in \mathbb{Z} \text{ e } \frac{n^2 + 8r^2}{16} \in \mathbb{Z} \\ &\Rightarrow n \equiv 0 \pmod{2} \text{ e } n^2 + 8r^2 \equiv 0 \pmod{16} \Rightarrow n \equiv 0 \pmod{4} \text{ e } r \equiv 0 \pmod{2}. \end{aligned}$$

Logo,

$$a_1^2 + b_1^2 - 2c_1^2 - 2d_1^2 \equiv 0 \pmod{4} \text{ e} \quad (3.1)$$

$$a_1d_1 - b_1c_1 \equiv 0 \pmod{2}. \quad (3.2)$$

Seja a_1 ou b_1 ímpar. Pela Equação 3.1, segue que ambos serão ímpares. Assim, pela Equação 3.2, segue que

$$c_1 \equiv d_1 \pmod{2} \Rightarrow 2 \equiv 0 \pmod{4},$$

o que não ocorre. Logo, $a_1 \equiv b_1 \equiv 0 \pmod{2}$ e $c_1 \equiv d_1 \pmod{2}$. Vamos definir $v, y, z, w \in \mathbb{Z}$, tais que $a_1 = 2v, b_1 = 2y, c_1 = 2z + w$ e $d_1 = w$. Assim,

$$\begin{aligned} \theta &= \frac{1}{2}(a_1 + b_1\sqrt{-1} + c_1\sqrt{2} + d_1\sqrt{-2}) = \frac{1}{2}(2v + 2y\sqrt{-1} + (2z + w)\sqrt{2} + w\sqrt{-2}) \\ &= v + y\sqrt{-1} + z\sqrt{2} + w\left(\frac{\sqrt{2} + \sqrt{-2}}{2}\right), \text{ com } v, y, z, w \in \mathbb{Z} \Rightarrow \theta \in A. \end{aligned}$$

Portanto, $\left\{1, \sqrt{-1}, \sqrt{2}, \frac{\sqrt{2} + \sqrt{-2}}{2}\right\}$ é uma base integral para o corpo $\mathbb{K}$ e

$$D(\mathbb{K}) = \begin{vmatrix} 1 & \sqrt{-1} & \sqrt{2} & \frac{1}{2}(\sqrt{2} + \sqrt{-2}) \\ 1 & -\sqrt{-1} & \sqrt{2} & \frac{1}{2}(\sqrt{2} - \sqrt{-2}) \\ 1 & \sqrt{-1} & -\sqrt{2} & \frac{1}{2}(-\sqrt{2} - \sqrt{-2}) \\ 1 & -\sqrt{-1} & -\sqrt{2} & \frac{1}{2}(-\sqrt{2} + \sqrt{-2}) \end{vmatrix}^2 = 256.$$

Definição 3.27. Seja $\mathbb{K}$ um corpo de números de grau n . O corpo $\mathbb{K}$ é chamado **monogênico** se existir um elemento $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ é uma base integral para o corpo $\mathbb{K}$. Neste caso, a base integral $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ é chamada **base potente** para o corpo $\mathbb{K}$.

Exemplo 3.28. Considere o corpo quártico $\mathbb{K} = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ do Exemplo 3.26. Mostremos que $\mathbb{K}$ é monogênico. Para isso, seja $\theta = \frac{\sqrt{2} + i\sqrt{2}}{2}$. Logo, $\theta^2 = \frac{2 + 4i - 2}{4} = i$ e $\theta^3 = \frac{2\sqrt{2} + 6i\sqrt{2} - 6\sqrt{2} - 2i\sqrt{2}}{8} = \frac{-4\sqrt{2} + 4i\sqrt{2}}{8} = \frac{1}{2}(-\sqrt{2} + \sqrt{2}i)$. Assim, pelo Exemplo 3.26, segue que

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\sqrt{2} + \mathbb{Z}\left(\frac{\sqrt{2} + i\sqrt{2}}{2}\right) = \mathbb{Z} + \mathbb{Z}\theta^2 + \mathbb{Z}(\theta - \theta^3) + \mathbb{Z}\theta = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3.$$

Portanto, $\{1, \theta, \theta^2, \theta^3\}$ é uma base integral para o corpo $\mathbb{K}$, ou seja, $\mathbb{K}$ é monogênico.

Proposição 3.29. Sejam $\mathbb{K}$ um corpo de números de grau n e $\lambda_1, \dots, \lambda_n \in \mathcal{O}_{\mathbb{K}}$. Se $D(\lambda_1, \dots, \lambda_n) \neq 0$, então $|D(\mathbb{K})| \leq |D(\lambda_1, \dots, \lambda_n)|$. Além disso, se $D(\lambda_1, \dots, \lambda_n)$ é livre de quadrados, então $\{\lambda_1, \dots, \lambda_n\}$ é uma base integral para o corpo $\mathbb{K}$.

Demonstração. Se $\{\eta_1, \dots, \eta_n\}$ uma base integral para o corpo $\mathbb{K}$, então existem $c_{ij} \in \mathbb{Z}$, com $i, j = 1, \dots, n$, tais que

$$\begin{cases} \lambda_1 = c_{11}\eta_1 + \dots + c_{1n}\eta_n \\ \lambda_2 = c_{21}\eta_1 + \dots + c_{2n}\eta_n \\ \vdots \\ \lambda_n = c_{n1}\eta_1 + \dots + c_{nn}\eta_n. \end{cases}$$

Assim,

$$D(\lambda_1, \dots, \lambda_n) = \det(c_{ij})^2 D(\eta_1, \dots, \eta_n) = \det(c_{ij})^2 D(\mathbb{K}) \neq 0 \Rightarrow \det(c_{ij}) \neq 0.$$

Como $\det(c_{ij}) \in \mathbb{Z}$, segue que $\det(c_{ij})^2 \geq 1$ e, dessa forma, $|D(\lambda_1, \dots, \lambda_n)| \geq |D(\mathbb{K})|$. Se $D(\lambda_1, \dots, \lambda_n)$ é livre de quadrados, então

$$\det(c_{ij}) = \pm 1 \Rightarrow D(\lambda_1, \dots, \lambda_n) = D(\mathbb{K}).$$

Assim, $\{\lambda_1, \dots, \lambda_n\}$ é uma base integral para o corpo $\mathbb{K}$. □

Proposição 3.30. Sejam $\mathbb{K}$ um corpo de números de grau n , $\theta \in \mathcal{O}_{\mathbb{K}}$, tal que $\mathbb{K} = \mathbb{Q}(\theta)$, e $\theta_1 = \theta, \theta_2, \dots, \theta_n$ os conjugados de θ . Se r é o número de $\theta_1, \dots, \theta_n$ que são reais, então $\text{sgn}(D(\mathbb{K})) = (-1)^{\frac{n-r}{2}}$.

Demonstração. Como r é o número de conjugados de θ que são reais, segue que o número dos que não são reais é $n - r$. Dessa forma, uma vez que cada complexo acompanha seu conjugado, segue que $n - r$ é um número par. Assim, existe $s \in \mathbb{Z}$ tal que $n - r = 2s$, isto é, $n = 2s + r$. Seja $\{\omega_1, \dots, \omega_n\}$ uma base integral para o corpo $\mathbb{K}$ e sejam $\omega_k^{(j)}$, onde $j = 1, \dots, n$ os conjugados de ω_k , onde $k = 1, \dots, n$. Assim, $D(\mathbb{K}) = \det(\omega_k^{(j)})^2$. Seja $\det(\omega_k^{(j)}) = A + iB$, com $A, B \in \mathbb{R}$. Fazendo uma permutação de s pares de colunas, podemos mudar o sinal de i para $-i$, ficando $A - iB = (-1)^s \det(\omega_k^{(j)}) \Rightarrow A - iB = (-1)^s(A + iB)$.

- Se s é par, então $A - iB = A + iB \Rightarrow B = 0$. Assim, $\det(\omega_k^{(j)})^2 = A^2 > 0$.
- Se s é ímpar, então $A - iB = -A - iB \Rightarrow A = 0$. Assim, $\det(\omega_k^{(j)})^2 = (iB)^2 = -B^2 < 0$.

Portanto, $\text{sgn}(D(\mathbb{K})) = (-1)^s = (-1)^{\frac{n-r}{2}}$. □

3.2 Inteiros mínimos

Sejam $\mathbb{K}$ um corpo de números de grau n e $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Logo, para todo $\alpha \in \mathbb{K}$, segue que existem únicos $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$ tais que

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + \dots + a_{n-1}\theta^{n-1}.$$

Se $k = 1, 2, \dots, n$ é tal que

$$a_k \neq 0 \text{ e } a_{k+1} = a_{k+2} = \dots = a_{n-1} = 0,$$

então $\alpha = a_0 + a_1\theta + \dots + a_k\theta^k$ e dizemos que α é um inteiro de grau k em θ . Se $a_1 = a_2 = \dots = a_{n-1} = 0$, então $\alpha = a_0$ e dizemos que é um inteiro de grau 0 em θ . Observe que os inteiros de grau 0 em θ são os inteiros racionais. Vamos mostrar que os denominadores de a_j são limitados. Se $\{1, \theta, \dots, \theta^{n-1}\}$ é uma base potente para o corpo $\mathbb{K}$, então os denominadores são todos iguais a 1.

Proposição 3.31. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\omega_1, \dots, \omega_n \in \mathcal{O}_{\mathbb{K}}$. Se $D(\omega_1, \dots, \omega_n) \neq 0$, então para cada $\alpha \in \mathcal{O}_{\mathbb{K}}$, segue que existem únicos inteiros racionais $x_1, \dots, x_n$ tais que*

$$\alpha = \sum_{j=1}^n \frac{x_j}{D(\omega_1, \dots, \omega_n)} \omega_j \quad \text{e} \quad D(\omega_1, \dots, \omega_n) \mid x_j^2,$$

onde $j = 1, 2, \dots, n$.

Demonstração. Se $\omega_1, \dots, \omega_n \in \mathcal{O}_{\mathbb{K}}$, então pelo Teorema 2.68, segue que $D(\omega_1, \dots, \omega_n) \in \mathbb{Z}$. Como $D(\omega_1, \dots, \omega_n) \neq 0$, segue que $\{\omega_1, \dots, \omega_n\}$ é linearmente independente sobre $\mathbb{Q}$, e assim, $\{\omega_1, \dots, \omega_n\}$ é uma base para o corpo $\mathbb{K}$ sobre $\mathbb{Q}$. Deste modo, existem únicos $y_1, \dots, y_n \in \mathbb{Q}$ tais que $\alpha = \sum_{j=1}^n y_j \omega_j$. Sejam $\sigma_1 = id, \sigma_2, \dots, \sigma_n$ os n monomorfismos que $\mathbb{K}$ em $\mathbb{C}$. Assim,

$$\sigma_k(\alpha) = \sum_{j=1}^n y_j \sigma_j(\omega_j), \quad \text{onde } k = 1, \dots, n. \quad (3.3)$$

Logo, aplicando a Regra de Cramer no sistema formado pelas Equações 3.3 e considerando

$$A_j = \begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_{j-1}) & \sigma_1(\alpha) & \sigma_1(\omega_{j+1}) & \dots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \dots & \sigma_2(\omega_{j-1}) & \sigma_2(\alpha) & \sigma_2(\omega_{j+1}) & \dots & \sigma_2(\omega_n) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \dots & \sigma_n(\omega_{j-1}) & \sigma_n(\alpha) & \sigma_n(\omega_{j+1}) & \dots & \sigma_n(\omega_n) \end{vmatrix},$$

segue que $y_j = \frac{A_j}{\det(\sigma_j(\omega_j))}$, com $j = 1, \dots, n$. Assim,

$$y_j^2 D(\omega_1, \dots, \omega_n) = \begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_{j-1}) & \sigma_1(\alpha) & \sigma_1(\omega_{j+1}) & \dots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \dots & \sigma_2(\omega_{j-1}) & \sigma_2(\alpha) & \sigma_2(\omega_{j+1}) & \dots & \sigma_2(\omega_n) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \dots & \sigma_n(\omega_{j-1}) & \sigma_n(\alpha) & \sigma_n(\omega_{j+1}) & \dots & \sigma_n(\omega_n) \end{vmatrix}^2$$

é um inteiro algébrico para $j = 1, \dots, n$. Como

$$y_j^2 D(\omega_1, \dots, \omega_n) \in \mathbb{Q},$$

segue que $y_j^2 D(\omega_1, \dots, \omega_n) \in \mathbb{Z}$. Defina $y_j = \frac{r_j}{s_j}$, com $r_j \in \mathbb{Z}$, $s_j \in \mathbb{N}^*$ e $\text{mdc}(r_j, s_j) = 1$.

Assim, $\frac{r_j^2}{s_j^2} D(\omega_1, \dots, \omega_n) \in \mathbb{Z}$, para $j = 1, \dots, n$, ou seja, $s_j^2 \mid D(\omega_1, \dots, \omega_n)$. Se $x_j = y_j D(\omega_1, \dots, \omega_n) = \frac{r_j}{s_j} D(\omega_1, \dots, \omega_n) \in \mathbb{Z}$, para $j = 1, \dots, n$, então

$$\alpha = \sum_{j=1}^n y_j \omega_j = \sum_{j=1}^n \frac{x_j}{D(\omega_1, \dots, \omega_n)} \omega_j.$$

Agora, note que

$$\frac{x_j^2}{D(\omega_1, \dots, \omega_n)} = r_j^2 \frac{D(\omega_1, \dots, \omega_n)}{s_j^2} \in \mathbb{Z},$$

ou seja, $D(\omega_1, \dots, \omega_n) \mid x_j^2$, para $j = 1, \dots, n$. $\square$

Observação 3.32. Pela Proposição 3.31, se $D(\omega_1, \dots, \omega_n)$ é livre de quadrados, então $D(\omega_1, \dots, \omega_n) \mid x_j$, para $j = 1, \dots, n$. Dessa forma, para cada $\alpha \in \mathcal{O}_{\mathbb{K}}$, existem únicos inteiros $a_j = \frac{x_j}{D(\omega_1, \dots, \omega_n)}$, tais que $\alpha = \sum_{j=1}^n a_j \omega_j$, provando que $\{\omega_1, \dots, \omega_n\}$ é uma base integral para o corpo $\mathbb{K}$. Agora, usamos a Proposição 3.31 para limitar os denominadores de a_j .

Proposição 3.33. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então existem únicos racionais $\frac{r_j}{s_j}$, com $j = 1, \dots, n$, onde $\text{mdc}(r_j, s_j) = 1$ e $s_j > 0$ tais que*

$$\alpha = \sum_{j=1}^n \frac{r_j}{s_j} \theta^{j-1}, \quad 1 \leq s_j \leq |D(\theta)| \text{ e } s_j^2 \mid D(\theta).$$

Demonstração. Se $\theta \in \mathcal{O}_{\mathbb{K}}$, então $1, \theta, \theta^2, \dots, \theta^{n-1} \in \mathcal{O}_{\mathbb{K}}$. Pelo Teorema 2.68, segue que $D(\theta) = D(1, \theta, \dots, \theta^{n-1}) \in \mathbb{Z}$. Além disso, como $\mathbb{K} = \mathbb{Q}(\theta)$, sabemos, pela Proposição 2.67, que $D(\theta) \neq 0$. Dessa forma, pela Proposição 3.31, segue que existem únicos inteiros $x_1, \dots, x_n$ tais que $\alpha = \sum_{j=1}^n \frac{x_j}{D(\theta)} \theta^{j-1}$ e $D(\theta) \mid x_j^2$, onde $j = 1, \dots, n$. Para todo $j = 1, \dots, n$, vamos definir inteiros, primos entre si, $r_j, s_j > 0$ por

$$r_j = \frac{\text{sgn}(D(\theta))x_j}{\text{mdc}(x_j, D(\theta))} \text{ e } s_j = \frac{|D(\theta)|}{\text{mdc}(x_j, D(\theta))}.$$

Dessa forma,

$$\frac{r_j}{s_j} = \frac{\text{sgn}(D(\theta))x_j}{\text{mdc}(x_j, D(\theta))} \cdot \frac{\text{mdc}(x_j, D(\theta))}{|D(\theta)|} = \frac{x_j}{D(\theta)} \Rightarrow \alpha = \sum_{j=1}^n \frac{r_j}{s_j} \theta^{j-1} \text{ e } 1 \leq s_j \leq |D(\theta)|.$$

Além disso, para $j = 1, \dots, n$, segue que

$$\frac{r_j^2}{s_j^2} D(\theta) = \frac{x_j^2}{D(\theta)} \in \mathbb{Z} \Rightarrow s_j^2 \mid D(\theta),$$

uma vez que $\text{mdc}(r_j, s_j) = 1$. $\square$

Com isso, podemos definir o conceito de um "inteiro mínimo de grau k em θ ". Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n . Para $k \in \{0, 1, \dots, n-1\}$ defina o conjunto

$$S_k = \{a_k \in \mathbb{Q} : a_0 + a_1\theta + \dots + a_k\theta^k \in \mathcal{O}_{\mathbb{K}}, \text{ com } a_0, a_1, \dots, a_{k-1} \in \mathbb{Q}\}.$$

Assim, $S_0 = \{a_0 \in \mathbb{Q} : a_0 \in \mathcal{O}_{\mathbb{K}}\} = \mathbb{Z}$ e $\mathbb{Z} \subseteq S_k$, para $k = 0, 1, \dots, n-1$. Pela Proposição 3.33, segue que os denominadores dos racionais em S_k são limitados. Portanto, S_k tem um elemento menor positivo a_k^* . Neste caso, $a_0^* = 1$.

Definição 3.34. Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n ,

$$S_k = \{a_k \in \mathbb{Q} : a_0 + a_1\theta + \dots + a_k\theta^k \in \mathcal{O}_{\mathbb{K}}, \text{ com } a_0, a_1, \dots, a_{k-1} \in \mathbb{Q}\}, \quad k \in \{0, 1, \dots, n-1\}$$

e a_k^* o menor positivo de S_k . Um elemento inteiro do corpo $\mathbb{K}$ que é da forma

$$a_0 + a_1\theta + \dots + a_{k-1}\theta^{k-1} + a_k^*\theta^k,$$

com $a_0, \dots, a_{k-1} \in \mathbb{Q}$, é chamado de **inteiro mínimo de grau k em θ** .

Os próximos resultados apresentarão a estrutura de S_k , a forma de a_k^* e a forma dos inteiros de grau k em θ , com $k = 0, 1, \dots, n-1$.

Proposição 3.35. Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n e

$$S_k = \{a_k \in \mathbb{Q} : a_0 + a_1\theta + \dots + a_k\theta^k \in \mathcal{O}_{\mathbb{K}}, \text{ com } a_0, a_1, \dots, a_{k-1} \in \mathbb{Q}\},$$

para $k \in \{0, 1, \dots, n-1\}$. Se a_k^* é o menor positivo de S_k , então $S_k = a_k^*\mathbb{Z}$.

Demonstração. Sejam $a \in S_k$ e m o menor inteiro positivo tal que $ma \in \mathbb{Z}$ e $ma_k^* \in \mathbb{N}$. Pelo algoritmo da divisão, segue que existem $q, r \in \mathbb{Z}$, tais que $ma = qma_k^* + r$, onde $0 \leq r < ma_k^*$. Assim, $a = qa_k^* + \frac{r}{m}$, $0 \leq \frac{r}{m} < a_k^*$. Como $a, a_k^* \in S_k$, segue que existem $b_0, b_1, \dots, b_{k-1}, c_0, c_1, \dots, c_{k-1} \in \mathbb{Q}$ tais que

$$\alpha = b_0 + b_1\theta + \dots + b_{k-1}\theta^{k-1} + a\theta^k \in \mathcal{O}_{\mathbb{K}},$$

$$\beta = c_0 + c_1\theta + \dots + c_{k-1}\theta^{k-1} + a_k^*\theta^k \in \mathcal{O}_{\mathbb{K}}.$$

Assim,

$$\begin{aligned} \alpha - q\beta &\in \mathcal{O}_{\mathbb{K}} \Rightarrow (b_0 - qc_0) + (b_1 - qc_1)\theta + \dots + (b_{k-1} - qc_{k-1})\theta^{k-1} + (a - qa_k^*)\theta^k \\ &= (b_0 - qc_0) + (b_1 - qc_1)\theta + \dots + (b_{k-1} - qc_{k-1})\theta^{k-1} + \frac{r}{m}\theta^k \in \mathcal{O}_{\mathbb{K}} \Rightarrow \frac{r}{m} \in S_k. \end{aligned}$$

Agora, se $\frac{r}{m} \neq 0$, então teríamos $0 < \frac{r}{m} < a_k^*$, mas isso contradiz a minimalidade de a_k^* em S_k . Portanto, $\frac{r}{m} = 0$, ou seja, $a = qa_k^*$. Logo, $S_k = a_k^*\mathbb{Z}$. $\square$

Proposição 3.36. Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n e

$$S_k = \{a_k \in \mathbb{Q} : a_0 + a_1\theta + \dots + a_k\theta^k \in \mathcal{O}_{\mathbb{K}}, \text{ com } a_0, a_1, \dots, a_{k-1} \in \mathbb{Q}\},$$

para $k \in \{0, 1, \dots, n-1\}$. Se a_k^* é o menor positivo de S_k , então existe $d_k \in \mathbb{N}$ tal que $a_k^* = \frac{1}{d_k}$.

Demonstração. A demonstração será feita por indução sobre $k \in \{0, 1, \dots, n-1\}$. Para $k = 0$, segue que $S_0 = \mathbb{Z}$ e $a_0^* = 1$. Logo, $d_0 = 1$ e o resultado é válido. Suponhamos que o resultado seja válido para k , com $0 \leq k < l \leq n-1$, ou seja, $a_k^* = \frac{1}{d_k}$ e $d_k \in \mathbb{N}$, para $k = 0, 1, \dots, l-1$, com $1 \leq l \leq n-2$. Mostremos que é válido para $k = l$. Pela hipótese de indução, segue que $a_{l-1}^* \in S_{l-1}$. Assim, existem $a_0, a_1, \dots, a_{l-2} \in \mathbb{Q}$ tais que $a_0 + a_1\theta + \dots + a_{l-1}\theta^{l-2} + \frac{1}{d_{l-1}}\theta^{l-1} \in \mathcal{O}_{\mathbb{K}}$. Logo,

$$a_0\theta + a_1\theta^2 + \dots + a_{l-2}\theta^{l-1} + \frac{1}{d_{l-1}}\theta^l \in \mathcal{O}_{\mathbb{K}} \Rightarrow \frac{1}{d_{l-1}} \in S_l.$$

Dessa forma, pela Proposição 3.35, segue que existe $m \in \mathbb{Z}$ tal que $\frac{1}{d_{l-1}} = a_l^*m \Rightarrow a_l^* = \frac{1}{d_{l-1}m}$, com $d_{l-1} \in \mathbb{N}$. Assim, chamando $d_l = d_{l-1}m$, segue que $a_l^* = \frac{1}{d_l}$, com $d_l \in \mathbb{N}$, ou seja, o resultado é válido para $l = k$. Portanto, por indução, segue que para todo $k = 0, 1, \dots, n-1$, existe $d_k \in \mathbb{N}$ tal que $a_k^* = \frac{1}{d_k}$. $\square$

Proposição 3.37. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n ,*

$$S_k = \{a_k \in \mathbb{Q} : a_0 + a_1\theta + \dots + a_k\theta^k \in \mathcal{O}_{\mathbb{K}}, \text{ com } a_0, a_1, \dots, a_{k-1} \in \mathbb{Q}\},$$

para $k \in \{0, 1, \dots, n-1\}$, e $a_k^ = \frac{1}{d_k}$, com $d_k \in \mathbb{N}$, o menor positivo de S_k . Assim, para $k = 1, \dots, n-1$, segue que $d_{k-1} \mid d_k$.*

Demonstração. Sejam $k \in \{1, 2, \dots, n-1\}$ e $a_k^* \in S_{k-1}$. Assim, existem $a_0, a_1, \dots, a_{k-2} \in \mathbb{Q}$ tais que

$$\begin{aligned} a_0 + a_1\theta + \dots + a_{k-2}\theta^{k-2} + a_{k-1}^*\theta^{k-1} &\in \mathcal{O}_{\mathbb{K}} \\ \Rightarrow a_0\theta + a_1\theta^2 + \dots + a_{k-2}\theta^{k-1} + a_{k-1}^*\theta^k &\in \mathcal{O}_{\mathbb{K}} \\ \Rightarrow a_{k-1}^* &\in S_k. \end{aligned}$$

Assim, pela Proposição 3.35, segue que existe $m \in \mathbb{Z}$ tal que $a_{k-1}^* = a_k^*m$. Agora, pela Proposição 3.36, segue que

$$\frac{1}{d_{k-1}} = \frac{1}{d_k}m, \quad d_{k-1}, d_k \in \mathbb{N} \Rightarrow d_k = d_{k-1}m \Rightarrow d_{k-1} \mid d_k,$$

onde $k = 1, 2, \dots, n-1$. $\square$

Proposição 3.38. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n . Se α é um inteiro de grau k em θ , então existem $a_0, a_1, \dots, a_k \in \mathbb{Z}$ tais que*

$$\alpha = \frac{a_0 + a_1\theta + \dots + a_{k-1}\theta^{k-1} + a_k\theta^k}{d_k}.$$

Em particular, se α é um inteiro mínimo de grau k em θ , então existem $a_0, a_1, \dots, a_{k-1} \in \mathbb{Z}$ tais que

$$\alpha = \frac{a_0 + a_1\theta + \dots + a_{k-1}\theta^{k-1} + \theta^k}{d_k}.$$

Demonstração. A prova será feita por indução sobre $k \in \{0, 1, \dots, n-1\}$. Para $k = 0$, seja α um inteiro de grau 0 em θ . Assim, $\alpha = a_0 \in \mathbb{Z}$, ou seja, $d_0 = 1$ e o resultado é válido. Agora, suponhamos que o resultado seja válido para todo inteiro de grau $l-1$ em θ , com $l \in \{0, 1, \dots, n-1\}$. Seja α um inteiro de grau l em θ . Pelas Proposições 3.35 e 3.36, segue que existem $r_0, \dots, r_{l-1} \in \mathbb{Q}$, com $a_l \in \mathbb{Z}$ e $d_l \in \mathbb{N}$ tais que $\alpha = r_0 + r_1\theta + \dots + r_{l-1}\theta^{l-1} + \frac{a_l}{d_l}\theta^l$. Agora, seja β um inteiro mínimo de grau $l-1$ em θ . Pela hipótese de indução, segue que existem $s_0, s_1, \dots, s_{l-2} \in \mathbb{Z}$ e $d_{l-1} \in \mathbb{N}$ tais que $\beta = \frac{s_0 + s_1\theta + \dots + s_{l-2}\theta^{l-2} + \theta^{l-1}}{d_{l-1}}$.

Além disso, pela Proposição 3.37, segue que $d_{l-1} \mid d_l$. Assim, $\frac{d_l}{d_{l-1}} \in \mathbb{Z}$ e, uma vez que

$\frac{d_l}{d_{l-1}}\alpha \in \mathcal{O}_{\mathbb{K}}$ e $a_l\theta\beta \in \mathcal{O}_{\mathbb{K}}$, segue que

$$\begin{aligned} \frac{d_l}{d_{l-1}}\alpha - a_l\theta\beta \in \mathcal{O}_{\mathbb{K}} &\Rightarrow \frac{d_l}{d_{l-1}}r_0 + \frac{d_l}{d_{l-1}}r_1\theta + \dots + \frac{d_l}{d_{l-1}}r_{l-1}\theta^{l-1} + \frac{d_l}{d_{l-1}}r_l\theta^l - \\ &\left(\frac{a_ls_0\theta + a_ls_1\theta^2 + \dots + a_ls_{l-2}\theta^{l-1} + a_l\theta^l}{d_{l-1}} \right) \in \mathcal{O}_{\mathbb{K}} \Rightarrow \frac{d_l}{d_{l-1}}r_0 + \sum_{j=1}^{l-1} \left(\frac{d_lr_j - a_ls_{j-1}}{d_{l-1}} \right) \theta^j \in \mathcal{O}_{\mathbb{K}}. \end{aligned}$$

Portanto, $\frac{d_l}{d_{l-1}}r_0 + \sum_{j=1}^{l-1} \left(\frac{d_lr_j - a_ls_{j-1}}{d_{l-1}} \right) \theta^j$ é um inteiro de grau $l-1$ em θ . Pela hipótese de indução, segue que existem $c_0, c_1, \dots, c_{l-1} \in \mathbb{Z}$ tais que

$$\frac{d_l}{d_{l-1}}r_0 + \sum_{j=1}^{l-1} \left(\frac{d_lr_j - a_ls_{j-1}}{d_{l-1}} \right) \theta^j = \sum_{j=0}^{l-1} \frac{c_j}{d_{l-1}} \theta^j,$$

e assim,

$$\begin{cases} \frac{d_l}{d_{l-1}}r_0 = \frac{c_0}{d_{l-1}} \\ \frac{d_lr_j - a_ls_{j-1}}{d_{l-1}} = \frac{c_j}{d_{l-1}}, \end{cases}$$

onde $j = 1, \dots, l-1$. Logo,

$$\begin{cases} r_0 = \frac{c_0}{d_l} \\ r_j = \frac{c_j + a_ls_{j-1}}{d_l}, \end{cases}$$

onde $j = 1, \dots, l-1$. Agora, sejam $a_0 = c_0$, $a_j = c_j + a_ls_{j-1}$, onde $j = 1, \dots, l-1$. Assim, $a_j \in \mathbb{Z}$ e $r_j = \frac{a_j}{d_l}$, onde $j = 0, 1, \dots, l-1$. Portanto, $\alpha = \frac{r_0 + r_1\theta + \dots + r_{l-1}\theta^{l-1} + a_l\theta^l}{d_l}$. Logo, por indução, o resultado é válido para todo $k = 0, 1, \dots, n-1$. $\square$

No próximo teorema, mostramos que se α_k , com $k \in \{0, 1, \dots, n-1\}$, é um inteiro mínimo de grau k em θ , então $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ é uma base integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$.

Teorema 3.39. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Se α_k é um inteiro mínimo de grau k em θ , para $k = 0, 1, \dots, n-1$, então $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ é uma base integral para o corpo $\mathbb{K}$.*

Demonstração. Em qualquer base integral de $\mathbb{K} = \mathbb{Q}(\theta)$, pelo menos um dos elementos é da forma $a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$, com $a_{n-1} \neq 0$ (caso contrário, não seria possível representar o elemento θ^{n-1}). Além disso, podemos considerar $a_{n-1} > 0$. Dessa forma, escolhemos uma base integral $\{\omega_1, \dots, \omega_n\}$ para o corpo $\mathbb{K}$ com $\omega_n = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$, com $a_{n-1} > 0$ e a_{n-1} sendo o menor coeficiente positivo que acompanha o θ^{n-1} entre os demais elementos da base. Seja $k \in \{1, 2, \dots, n-1\}$ e suponha que

$$\omega_k = b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1}, \text{ com } b_0, b_1, \dots, b_{n-1} \in \mathbb{Q}.$$

Trocando ω_k por $-\omega_k$, se necessário, podemos supor que $b_{n-1} \geq 0$. Assim, pela forma como tomamos a_{n-1} , no caso em que $b_{n-1} \neq 0$, segue que $b_{n-1} \geq a_{n-1}$. Seja m o único inteiro não negativo tal que $0 \leq \frac{b_{n-1}}{a_{n-1}} - 1 < m < \frac{b_{n-1}}{a_{n-1}}$, então

$$b_{n-1} - a_{n-1} < ma_{n-1} < b_{n-1} \Rightarrow 0 \leq b_{n-1} - ma_{n-1} < a_{n-1} < b_{n-1}.$$

Vamos definir $\omega'_k = \omega_k - m\omega_n$. Se $b_{n-1} - ma_{n-1} \neq 0$, então $\{\omega_1, \dots, \omega_{k-1}, \omega'_k, \omega_{k+1}, \dots, \omega_n\}$ é uma base integral do corpo $\mathbb{K}$. Note que, neste caso, o coeficiente que acompanha θ^{n-1} no elemento ω'_k é $b_{n-1} - ma_{n-1} < a_{n-1}$. Mas isso contradiz a minimalidade de a_{n-1} como coeficiente de θ^{n-1} . Portanto,

$$b_{n-1} - ma_{n-1} = 0 \Rightarrow b_{n-1} = ma_{n-1},$$

ou seja, b_{n-1} é um múltiplo de a_{n-1} . Com isso, observe que para todo $k \in \{1, 2, \dots, n-1\}$, considerando $\omega_k = b_{k0} + b_{k1}\theta + \dots + b_{k,n-1}\theta^{n-1}$, segue que existem $m_1, m_2, \dots, m_{n-1}$ tais que $b_{k,n-1} = m_k a_{n-1}$. Assim, $\omega'_k = \omega_k - m_k \omega_n$ e o coeficiente que acompanha θ^{n-1} é $b_{k,n-1} - m_k a_{n-1} = 0$. Portanto, ω'_k é um inteiro de grau no máximo $n-2$ em θ . Além disso, $\{\omega'_1, \omega'_2, \dots, \omega'_{n-1}, \omega_n\}$ é uma base integral para o corpo $\mathbb{K}$. Entre todas as bases $\{\omega_1, \dots, \omega_n\}$, para as quais os elementos $\omega_1, \dots, \omega_{n-1}$ são inteiros mínimos de grau no máximo $n-2$ em θ , vamos escolher um elemento em que o coeficiente de θ^{n-2} seja positivo e mínimo. Assim, continuamos dessa construção até chegarmos a uma base integral $\{\alpha_0, \dots, \alpha_{n-1}\}$, em que cada α_i é de grau i em θ , com $i = 1, \dots, n-1$. Seja $\alpha_i = \sum_{k=0}^i a_{ik}\theta^k$, com $a_{ik} \in \mathbb{Q}$. Assim,

$$D(\mathbb{K}) = D(\alpha_0, \dots, \alpha_{n-1}) = (a_{00}a_{11} \dots a_{n-1,n-1})^2 D(\theta).$$

Para $i = 0, 1, \dots, n-1$, seja β_i o inteiro de grau i em θ . Logo, $D(\beta_0, \dots, \beta_{n-1}) = (a_0^* a_1^* \dots a_{n-1}^*) D(\theta)$. Pela Proposição 3.29, segue que

$$\begin{aligned} |D(\mathbb{K})| &\leq |D(\beta_0, \dots, \beta_{n-1})| \\ \Rightarrow a_{00}a_{11} \dots a_{n-1,n-1} &\leq a_0^* a_1^* \dots a_{n-1}^* \\ \Rightarrow \frac{a_{00}a_{11} \dots a_{n-1,n-1}}{a_0^* a_1^* \dots a_{n-1}^*} &\leq 1 \\ \Rightarrow \frac{a_{00}}{a_0^*} \dots \frac{a_{n-1,n-1}}{a_{n-1}^*} &\leq 1. \end{aligned}$$

Como $a_{ii} \in S_i$, para todo $i = 0, 1, \dots, n-1$, pela Proposição 3.35, segue que $\frac{a_{ii}}{a_i^*} \in \mathbb{Z}_+^*$, para todo $i = 0, 1, \dots, n-1$. Logo, como $\frac{a_{00}}{a_0^*} \dots \frac{a_{n-1,n-1}}{a_{n-1}^*} \leq 1$, segue que $a_{ii} = a_i^*$,

para todo $k = 0, 1, \dots, n-1$. Portanto, α_i é um inteiro mínimo de grau i em θ , para todo $i = 0, 1, \dots, n-1$ e $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ é a base integral para o corpo $\mathbb{K}$, o prova o resultado. $\square$

O Teorema 3.39 fornece um método para obter uma base integral para um corpo de números $\mathbb{K}$ de grau n . Segundo esse teorema, é preciso apenas encontrar um inteiro mínimo de cada grau até $n-1$. No próximo teorema, apresentamos algumas informações úteis sobre os denominadores dos inteiros mínimos.

Teorema 3.40. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Para $k = 0, 1, \dots, n-1$, se $\alpha_k = \frac{a_{k0} + a_{k1}\theta + \dots + a_{kk-1}\theta^{k-1} + \theta^k}{d_k}$, com $a_{ki} \in \mathbb{Z}$, para $i = 1, \dots, k-1$, é um inteiro mínimo de grau k em θ , tal que $\alpha_0 = d_0 = 1$, então $d_0 d_1 \dots d_{n-1} = \text{ind}(\theta)$ e $d_i^{2(n-i)} \mid D(\theta)$, com $i = 0, 1, \dots, n-1$.*

Demonstração. Pelo Teorema 3.39, segue que $\{\alpha_0, \dots, \alpha_{n-1}\}$ é uma base integral para o corpo $\mathbb{K}$. Portanto, $D(\alpha_0, \dots, \alpha_{n-1}) = D(\mathbb{K})$. Além disso,

$$D(\alpha_0, \dots, \alpha_{n-1}) = \frac{D(\theta)}{(d_0 \dots d_{n-1})^2} = \frac{(\text{ind}(\theta))^2 D(\mathbb{K})}{(d_0 \dots d_{n-1})^2}.$$

Agora, como $d_0, \dots, d_{n-1}, \text{ind}(\theta) \in \mathbb{Z}_+^*$, então $\text{ind}(\theta) = d_0 \dots d_{n-1}$. Note que,

$$\frac{D(\theta)}{(d_0 \dots d_{n-1})^2} = D(\mathbb{K}) \in \mathbb{Z} \Rightarrow (d_0 \dots d_{n-1})^2 \mid D(\theta).$$

Pela Proposição 3.37, segue que $d_i \mid d_j$, para todo $j = i+1, \dots, n-1$, $i = 0, 1, \dots, n-1$, e assim, $d_i^{2(n-i)} \mid D(\theta)$. $\square$

Os Teoremas 3.39 e 3.40 podem ser utilizados para determinar bases integrais para alguns corpos cúbicos. O próximo resultado também é uma ferramenta útil neste processo.

Proposição 3.41. *Se θ é uma raiz da equação cúbica $x^3 + ax + b = 0$, com $a, b \in \mathbb{Q}$, então $y_0 + y_1\theta + y_2\theta^2$, com $y_0, y_1, y_2 \in \mathbb{Q}$, é uma raiz da equação cúbica $x^3 + Ax^2 + Bx + C = 0$, com*

$$A = -3y_0 + 2ay_2,$$

$$B = 3y_0^2 + ay_1^2 + a^2y_2^2 - 4ay_0y_2 + 3by_1y_2,$$

$$C = -y_0^3 + by_1^3 - b^2y_2^3 - ay_0y_1^2 - a^2y_0y_2^2 + 2ay_0^2y_2 + aby_1y_2^2 - 3by_0y_1y_2.$$

Demonstração. Sejam θ, θ' e $\theta'' \in \mathbb{C}$ as raízes da equação cúbica $x^3 + ax + b = 0$. Assim,

$$\begin{cases} \theta + \theta' + \theta'' = 0 \\ \theta\theta' + \theta\theta'' + \theta'\theta'' = a \\ \theta\theta'\theta'' = -b. \end{cases}$$

Assim,

- $\theta^2 + \theta'^2 + \theta''^2 = (\theta + \theta' + \theta'')^2 - 2(\theta\theta' + \theta\theta'' + \theta'\theta'') = -2a;$
- $\theta^2\theta'^2 + \theta^2\theta''^2 + \theta'^2\theta''^2 = (\theta\theta' + \theta\theta'' + \theta'\theta'')^2 - 2\theta\theta'\theta''(\theta + \theta' + \theta'') = a^2;$
- $\theta\theta'^2 + \theta^2\theta' + \theta\theta''^2 + \theta^2\theta'' + \theta'\theta''^2 + \theta'^2\theta'' = \theta\theta'(\theta' + \theta) + \theta\theta''(\theta'' + \theta) + \theta'\theta''(\theta'' + \theta') = -3\theta\theta'\theta'' = 3b.$

Agora, sejam

$$\begin{cases} \alpha = y_0 + y_1\theta + y_2\theta^2, \\ \alpha' = y_0 + y_1\theta' + y_2\theta'^2, \\ \alpha'' = y_0 + y_1\theta'' + y_2\theta''^2. \end{cases}$$

Com isso,

- $\alpha + \alpha' + \alpha'' = 3y_0 - 2y_2a;$
- $\alpha\alpha' + \alpha\alpha'' + \alpha'\alpha'' = 3y_0^2 + y_1^2a - y_2^2a^2 - 4y_0y_2a + 3y_1y_2b;$
- $\alpha\alpha'\alpha'' = y_0^3 - y_1^3b + y_2^3b^2 + y_0y_1^2a + y_0y_2^2a^2 - 2y_0^2y_2a - y_1y_2^2ab + 3y_0y_1y_2b.$

Agora, sejam

$$\begin{aligned} A &= -3y_0 + 2ay_2 \\ B &= 3y_0^2 + ay_1^2 + a^2y_2^2 - 4ay_0y_2 + 3by_1y_2 \\ C &= -y_0^3 + by_1^3 - b^2y_2^3 - ay_0y_1^2 - a^2y_0y_2^2 + 2ay_0^2y_2 + aby_1y_2^2 - 3by_0y_1y_2. \end{aligned}$$

Assim,

$$\begin{cases} \alpha + \alpha' + \alpha'' = -A \\ \alpha\alpha' + \alpha\alpha'' + \alpha'\alpha'' = B \\ \alpha\alpha'\alpha'' = -C. \end{cases}$$

Logo, $\alpha = y_0 + y_1\theta + y_2\theta^2$ é raiz de $x^3 + Ax^2 + Bx + C = 0$. □

Exemplo 3.42. Seja θ uma raiz do polinômio $x^3 - 3x + 9 = 0$. Vamos determinar um polinômio para o qual $\frac{\theta^2}{3}$ é uma raiz. Com a notação da Proposição 3.41, no polinômio $x^3 - 3x + 9$, segue que $a = -3$ e $b = 9$. Chamando $\frac{\theta^2}{3} = y_0 + y_1\theta + y_2\theta^2$, segue $y_0 = y_1 = 0$ e $y_2 = \frac{1}{3}$. Considere

$$\begin{aligned} A &= -3y_0 + 2ay_2 = 2 \cdot \left(\frac{1}{3}\right) \cdot (-3) = -2, \\ B &= 3y_0^2 + ay_1^2 + a^2y_2^2 - 4ay_0y_2 + 3by_1y_2 = \left(\frac{1}{3}\right)^2 \cdot (-3)^2 = 1, \\ C &= y_0^3 + by_1^3 - b^2y_2^3 - ay_0y_1^2 - a^2y_0y_2^2 + 2ay_0^2y_2 + aby_1y_2^2 - 3by_0y_1y_2 \\ &= -9^2 \cdot \left(\frac{1}{3}\right)^3 = -3. \end{aligned}$$

Pela Proposição 3.41, segue que $\frac{\theta^2}{3}$ é uma raiz do polinômio $x^3 + Ax^2 + Bx + C = x^3 - 2x^2 + x - 3 \in \mathbb{Z}[x]$.

Exemplo 3.43. Seja θ uma raiz do polinômio $x^3 - 21x - 236 = 0$. Vamos determinar um polinômio para o qual $\frac{1+\theta}{3}$ é uma raiz. Com a notação da Proposição 3.41, no polinômio $x^3 - 21x - 236$, segue que $a = -21$ e $b = -236$. Chamando $\frac{1+\theta}{3} = y_0 + y_1\theta + y_2\theta^2$, segue

que $y_0 = y_1 = \frac{1}{3}$ e $y_2 = 0$. Considere

$$\begin{aligned} A &= -3y_0 + 2ay_2 = -3\left(\frac{1}{3}\right) = -1, \\ B &= 3y_0^2 + ay_1^2 + a^2y_2^2 - 4ay_0y_2 + 3by_1y_2 = 3\cdot\left(\frac{1}{3}\right)^2 + (-21)\cdot\left(\frac{1}{3}\right)^2 = -2, \\ C &= y_0^3 + by_1^3 - b^2y_2^3 - ay_0y_1^2 - a^2y_0y_2^2 + 2ay_0^2y_2 + aby_1y_2^2 - 3by_0y_1y_2 \\ &= \left(\frac{1}{3}\right)^3 - 236\cdot\left(\frac{1}{3}\right)^3 - (-21)\cdot\left(\frac{1}{3}\right)^3 = -8. \end{aligned}$$

Pela Proposição 3.41, segue que $\frac{1+\theta}{3}$ é uma raiz do polinômio $x^3 + Ax^2 + Bx + C = x^3 - x^2 - 2x - 8 \in \mathbb{Z}[x]$.

Exemplo 3.44. Seja θ uma raiz do polinômio $x^3 - 21x - 236 = 0$. Vamos determinar um polinômio para o qual $\frac{-2-\theta+\theta^2}{18}$ é uma raiz. Com a notação da Proposição 3.41, no polinômio $x^3 - 21x - 236$, segue que $a = -21$ e $b = -236$. Chamando $\frac{-2-\theta+\theta^2}{18} = y_0 + y_1\theta + y_2\theta^2$, segue que $y_0 = -\frac{1}{9}$, $y_1 = -\frac{1}{18}$ e $y_2 = \frac{1}{18}$. Considere

$$\begin{aligned} A &= -3y_0 + 2ay_2 = -3\cdot\left(-\frac{1}{9}\right) + 2\cdot(-21)\cdot\left(\frac{1}{18}\right) = -2, \\ B &= 3y_0^2 + ay_1^2 + a^2y_2^2 - 4ay_0y_2 + 3by_1y_2 = 3\cdot\left(-\frac{1}{9}\right)^2 + (-21)\cdot\left(-\frac{1}{18}\right)^2 \\ &\quad + (-21)\cdot\left(-\frac{1}{18}\right)^2 + (-21)^2\cdot\left(\frac{1}{18}\right)^2 - 4\cdot(-21)\cdot\left(-\frac{1}{9}\right)\cdot\left(\frac{1}{18}\right) \\ &\quad + 3\cdot(-236)\cdot\left(-\frac{1}{18}\right)\cdot\left(\frac{1}{18}\right) = 3, \\ C &= y_0^3 + by_1^3 - b^2y_2^3 - ay_0y_1^2 - a^2y_0y_2^2 + 2ay_0^2y_2 + aby_1y_2^2 - 3by_0y_1y_2 \\ &= \left(-\frac{1}{9}\right)^3 + (-236)\cdot\left(-\frac{1}{18}\right)^3 - (-236)^2\cdot\left(\frac{1}{18}\right)^3 - (-21)\cdot\left(-\frac{1}{9}\right)\cdot\left(-\frac{1}{18}\right)^2 \\ &\quad - (-21)^2\cdot\left(-\frac{1}{9}\right)\cdot\left(\frac{1}{18}\right)^2 + 2\cdot(-21)\cdot\left(-\frac{1}{9}\right)\cdot\left(\frac{1}{18}\right) \\ &\quad + (-21)\cdot(-236)\cdot\left(-\frac{1}{18}\right)\cdot\left(\frac{1}{18}\right)^2 - 3\cdot(-236)\cdot\left(-\frac{1}{9}\right)\cdot\left(-\frac{1}{18}\right)\cdot\left(\frac{1}{18}\right) = -10. \end{aligned}$$

Pela Proposição 3.41, segue que $\frac{-2-\theta+\theta^2}{18}$ é uma raiz do polinômio $x^3 + Ax^2 + Bx + C = x^3 - 2x^2 + 3x - 10 \in \mathbb{Z}[x]$.

Nos próximos exemplos, usamos os Teoremas 3.39 e 3.40 para determinar bases integrais para alguns corpos cúbicos.

Exemplo 3.45. Seja θ uma raiz do polinômio cúbico $x^3 - 3x + 9$. Vamos determinar uma base integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$. Primeiramente, observe que o polinômio

$x^3 - 3x + 9 \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Z}$. Portanto, $\mathbb{K}$ é um corpo cúbico. Dessa forma, pelo Teorema 3.18, segue que $D(\theta) = -4.(-3)^2 - 27.9^2 = -3^3.7.11$. Agora, pelo Teorema 3.40, segue que os inteiros mínimos de grau k em θ , com $k = 0, 1, 2$, são da forma $\alpha_k = \frac{a_{k_0} + a_{k_1}\theta + \dots + a_{k_{k-1}}\theta^{k-1} + \theta^k}{d_k}$ e $d_i^{2(3-i)} \mid D(\theta)$. Assim,

- $\alpha_0 = 1$ e $d_0 = 1$;
- $d_1^{2(3-1)} = d_1^4 \mid D(\theta) = -3^3.7.11 \Rightarrow d_1 = 1 \Rightarrow \alpha_1 = \theta$;
- $d_2^{2(3-2)} = d_2^2 \mid D(\theta) = -3^3.7.11 \Rightarrow d_2 = 1$ ou 3 . Pelo Exemplo 3.42, segue que $\frac{\theta^2}{3}$ é um inteiro do corpo $\mathbb{K}$, uma vez que é raiz do polinômio $x^3 - 2x^2 + x - 3 \in \mathbb{Z}[x]$. Portanto, como satisfaz a forma dos inteiros mínimos, segue que $\frac{\theta^2}{3}$ é um inteiro mínimo de grau 2 em θ . Logo, $d_2 = 3$ e $\alpha_2 = \frac{\theta^2}{3}$.

Com isso, pelo Teorema 3.39, segue que $\left\{1, \theta, \frac{\theta^2}{3}\right\}$ é uma base integral para o corpo $\mathbb{K}$. Além disso, pelo Teorema 3.40, segue que $\text{ind}(\theta) = d_0 d_1 d_2 = 3$. Assim,

$$D(\mathbb{K}) = \frac{D(\theta)}{(\text{ind}(\theta))^2} = \frac{-3^3.7.11}{3^2} = -231.$$

Exemplo 3.46. Seja θ uma raiz do polinômio cúbico $x^3 - 21x - 236$. Vamos determinar uma base integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$. Primeiramente, observe que o polinômio $x^3 - 21x - 236 \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Z}$. Portanto, $\mathbb{K}$ é um corpo cúbico. Dessa forma, pelo Teorema 3.18, segue que $D(\theta) = -4.(-21)^2 - 27.(-236)^2 = -2^2.3^6.503$. Agora, pelo Teorema 3.40, segue que os inteiros mínimos de grau k em θ , com $k = 0, 1, 2$, são da forma $\alpha_k = \frac{a_{k_0} + a_{k_1}\theta + \dots + a_{k_{k-1}}\theta^{k-1} + \theta^k}{d_k}$ e $d_i^{2(3-i)} \mid D(\theta)$. Assim,

- $\alpha_0 = 1$ e $d_0 = 1$;
- $d_1^{2(3-1)} = d_1^4 \mid D(\theta) = -2^2.3^6.503 \Rightarrow d_1 = 1$ ou 3 . Note que, pelo Exemplo 3.43, segue que $\frac{1+\theta}{3}$ é um inteiro do corpo $\mathbb{K}$, uma vez que é raiz do polinômio $x^3 - x^2 - 2x - 8 \in \mathbb{Z}[x]$. Portanto, como satisfaz a forma dos inteiros mínimos, segue que $\frac{1+\theta}{3}$ é um inteiro mínimo de grau 1 em θ . Logo, $d_1 = 3$ e $\alpha_1 = \frac{1+\theta}{3}$;
- $d_2^{2(3-2)} = d_2^2 \mid D(\theta) = -2^2.3^6.503 \Rightarrow d_2 = 1, 2, 3, 2.3$ ou 2.3^2 . Note que, pelo Exemplo 3.44, segue que $\frac{-2-\theta+\theta^2}{18}$ é um inteiro do corpo $\mathbb{K}$, uma vez que é raiz do polinômio $x^3 - 2x^2 + 3x - 10 \in \mathbb{Z}[x]$. Portanto, como satisfaz a forma dos inteiros mínimos, segue que $\frac{-2-\theta+\theta^2}{18}$ é um inteiro mínimo de grau 2 em θ . Logo, $d_2 = 2.3^2 = 18$ e $\alpha_2 = \frac{-2-\theta+\theta^2}{18}$.

Com isso, pelo Teorema 3.39, segue que $\left\{1, \frac{1+\theta}{3}, \frac{-2-\theta+\theta^2}{18}\right\}$ é uma base integral para o corpo $\mathbb{K}$. Além disso, pelo Teorema 3.40, segue que $\text{ind}(\theta) = d_0 d_1 d_2 = 2 \cdot 3^3$. Assim,

$$D(\mathbb{K}) = \frac{D(\theta)}{(\text{ind}(\theta))^2} = \frac{-2^2 \cdot 3^6 \cdot 503}{2^2 \cdot 3^6} = -503.$$

Definição 3.47. Um corpo cúbico $\mathbb{K}$ é dito um **corpo cúbico puro**, se existe $d \in \mathbb{Z}$, que não é um cubo perfeito, tal que $\mathbb{K} = \mathbb{Q}(\sqrt[3]{d})$.

Exemplo 3.48. Seja $\theta \in \mathbb{R}$ uma raiz do polinômio $x^3 + 6x + 2$. Vamos mostrar que o corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$ é o corpo cúbico puro $\mathbb{Q}(\sqrt[3]{2})$ e determinar uma base integral para o corpo $\mathbb{K}$. Primeiramente, note que

$$(-1)^3 + 6 \cdot (-1) + 2 = -5 < 0 \text{ e } 0^3 + 6 \cdot 0 + 2 = 2 > 0.$$

Portanto, $-1 < \theta < 0$. Além disso, para $-2 < x < -\sqrt{2}$, segue que $-1 < x - \frac{2}{x} < 0$.

Assim, existe um único $a \in \mathbb{R}$ tal que $-2 < a < -\sqrt{2}$ e $\theta = a - \frac{2}{a}$. Logo,

$$\begin{aligned} \theta^3 + 6\theta + 2 = 0 &\Rightarrow \left(a - \frac{2}{a}\right)^3 + 6 \cdot \left(a - \frac{2}{a}\right) + 2 = 0 \\ &\Rightarrow a^3 - 3a^2 \cdot \frac{2}{a} + 3a \cdot \frac{4}{a^2} - \frac{8}{a^3} + 6a - \frac{12}{a} + 2 = 0 \\ &\Rightarrow a^3 - \frac{8}{a^3} + 2 = 0 \Rightarrow a^3 = 2 \text{ ou } a^3 = -4. \end{aligned}$$

Como $-2 < a < -\sqrt{2}$, segue que

$$a^3 < 0 \Rightarrow a^3 = -4 \Rightarrow a^3 = -2^2 \Rightarrow a = -2^{\frac{2}{3}} \Rightarrow \theta = -2^{\frac{2}{3}} - \left(\frac{2}{-2^{\frac{2}{3}}}\right) = 2^{\frac{1}{3}} - 2^{\frac{2}{3}} \in \mathbb{Q}(\sqrt[3]{2}).$$

Portanto, $\mathbb{K} = \mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[3]{2})$. Por outro lado, $\theta^2 = (2^{\frac{1}{3}} - 2^{\frac{2}{3}})^2 = -4 + 2 \cdot 2^{\frac{1}{3}} + 2^{\frac{2}{3}}$. Assim,

$$\begin{aligned} \theta + \theta^2 &= 2^{\frac{1}{3}} - 2^{\frac{2}{3}} - 4 + 2 \cdot 2^{\frac{1}{3}} + 2^{\frac{2}{3}} = -4 + 3 \cdot 2^{\frac{1}{3}} \\ &\Rightarrow \sqrt[3]{2} = \frac{4 + \theta + \theta^2}{3} \in \mathbb{Q}(\theta) \\ &\Rightarrow \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{K}. \end{aligned}$$

Portanto, $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$. Agora, como $2^{\frac{1}{3}} = \frac{4 + \theta + \theta^2}{3}$ e $2^{\frac{2}{3}} = 2^{\frac{1}{3}} - \theta = \frac{4 - 2\theta + \theta^2}{3}$, pela Proposição 3.13, segue que $\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}\}$ é uma base integral para o corpo $\mathbb{K}$. Dessa forma, $\left\{1, \frac{4 + \theta + \theta^2}{3}, \frac{4 - 2\theta + \theta^2}{3}\right\}$ é uma base integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$. Agora,

$$\frac{4 + \theta + \theta^2}{3} - \frac{4 - 2\theta + \theta^2}{3} = 0 \text{ e } \frac{4 + \theta + \theta^2}{3} - 1 = \frac{1 + \theta + \theta^2}{3} \Rightarrow \left\{1, \theta, \frac{1 + \theta + \theta^2}{3}\right\}$$

é uma base integral mais simples para o corpo $\mathbb{K}$.

Mais adiante, apresentando um resultado generalizado para bases integrais de corpos cúbicos puros.

3.3 Índice de um corpo de números

Seja $\mathbb{K}$ um corpo de números de grau n sobre $\mathbb{Q}$. Um elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ é dito um gerador do corpo $\mathbb{K}$ quando $\mathbb{K} = \mathbb{Q}(\alpha)$. Além disso, pela Proposição 2.67, sabemos que $\alpha \in \mathcal{O}_{\mathbb{K}}$ é um gerador do corpo $\mathbb{K}$ se, e somente se, $D(\alpha) \neq 0$.

Para um gerador α de $\mathbb{K}$, o índice de α é o inteiro positivo $\text{ind}(\alpha)$, dado por $D(\alpha) = (\text{ind}(\alpha))^2 \cdot D(\mathbb{K})$.

Definição 3.49. Seja $\mathbb{K}$ um corpo de números, o **índice do corpo** $\mathbb{K}$ é dado por

$$i(\mathbb{K}) = \text{mdc}\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\}.$$

Definição 3.50. Seja $\mathbb{K}$ um corpo de números, o **índice minimal do corpo** $\mathbb{K}$ é definido por

$$m(\mathbb{K}) = \min\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\}.$$

Observe que $i(\mathbb{K}) \mid m(\mathbb{K})$.

Proposição 3.51. *Seja $\mathbb{K}$ um corpo de números de grau n . Assim, $m(\mathbb{K}) = 1$ se, e somente se, $\mathbb{K}$ possui uma base potente.*

Demonstração. Se $m(\mathbb{K}) = 1$, então existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ um gerador do corpo $\mathbb{K}$ tal que $i(\mathbb{K}) = 1$. Dessa forma,

$$D(1, \alpha, \dots, \alpha^{n-1}) = D(\alpha) = (\text{ind}(\alpha))^2 \cdot D(\mathbb{K}) = D(\mathbb{K}) \Rightarrow D(\mathbb{K}) = D(1, \alpha, \dots, \alpha^{n-1}).$$

Portanto, $\{1, \alpha, \dots, \alpha^{n-1}\}$ é uma base integral para o corpo $\mathbb{K}$, ou seja, $\mathbb{K}$ possui uma base potente. Reciprocamente, se $\mathbb{K}$ possui uma base potente $\{1, \alpha, \dots, \alpha^{n-1}\}$, então

$$D(\mathbb{K}) = D(1, \alpha, \dots, \alpha^{n-1}) = D(\alpha).$$

Agora, como $D(\alpha) = (\text{ind}(\alpha))^2 \cdot D(\mathbb{K})$, segue que $\text{ind}(\alpha) = 1$. Logo, $m(\mathbb{K}) = 1$. $\square$

Proposição 3.52. *Seja $\mathbb{K}$ um corpo de números. Se $\mathbb{K}$ possui uma base potente, então $i(\mathbb{K}) = 1$.*

Demonstração. Seja $\mathbb{K}$ um corpo que possui uma base potente, pela Proposição 3.51, segue que $m(\mathbb{K}) = 1$. Logo, uma vez que $i(\mathbb{K}) \mid m(\mathbb{K})$, segue que $i(\mathbb{K}) = 1$. $\square$

Note que, segundo a Proposição 3.52, quando $i(\mathbb{K}) \geq 1$, segue que $\mathbb{K}$ não possui uma base potente. Além disso, vale observar que $i(\mathbb{K}) = 1$ não implica que $\mathbb{K}$ possui uma base potente.

Proposição 3.53. *Seja $\mathbb{K}$ um corpo quadrático, então $i(\mathbb{K}) = m(\mathbb{K}) = 1$.*

Demonstração. Como $\mathbb{K}$ é um corpo quadrático, pelo Teorema 2.33, segue que existe um único $d \in \mathbb{Z}$, livre de quadrados, tal que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.

- Seja $d \equiv 1 \pmod{4}$. Pelos Teoremas 3.2 e 3.4, segue que $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ é uma base integral para o corpo $\mathbb{K}$ e $D(\mathbb{K}) = d$. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$, então existem $a, b \in \mathbb{Z}$ tais que $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right)$. Dessa forma,

$$D(\alpha) = \begin{vmatrix} 1 & a + b\left(\frac{1+\sqrt{d}}{2}\right) \\ 1 & a + b\left(\frac{1-\sqrt{d}}{2}\right) \end{vmatrix}^2 = b^2d.$$

Agora, α é um gerador de $\mathbb{K} \Leftrightarrow D(\alpha) \neq 0 \Leftrightarrow b^2d \neq 0 \Leftrightarrow b \neq 0$. Assim,

$$\text{ind}(\alpha) = \sqrt{\frac{D(\alpha)}{D(\mathbb{K})}} = \sqrt{\frac{b^2d}{d}} = \sqrt{b^2} = |b|.$$

Logo, $i(\mathbb{K}) = \text{mdc}\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\} = \text{mdc}\{|b| : b \in \mathbb{Z}, b \neq 0\} = 1$ e $m(\mathbb{K}) = \min\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\} = \text{mdc}\{|b| : b \in \mathbb{Z}, b \neq 0\} = 1$.

- Seja $d \not\equiv 1 \pmod{4}$. Pelos Teoremas 3.2 e 3.4, segue que $\{1, \sqrt{d}\}$ é uma base integral para o corpo $\mathbb{K}$ e $D(\mathbb{K}) = 4d$. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então existem $a, b \in \mathbb{Z}$ tais que $\alpha = a + b\sqrt{d}$. Dessa forma,

$$D(\alpha) = \begin{vmatrix} 1 & a + b\sqrt{d} \\ 1 & a - b\sqrt{d} \end{vmatrix}^2 = 4b^2d.$$

Agora, α é um gerador de $\mathbb{K} \Leftrightarrow D(\alpha) \neq 0 \Leftrightarrow 4b^2d \neq 0 \Leftrightarrow b \neq 0$. Assim,

$$\text{ind}(\alpha) = \sqrt{\frac{D(\alpha)}{D(\mathbb{K})}} = \sqrt{\frac{4b^2d}{4d}} = |b|.$$

Logo, $i(\mathbb{K}) = \text{mdc}\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\} = \text{mdc}\{|b| : b \in \mathbb{Z}, b \neq 0\} = 1$ e $m(\mathbb{K}) = \min\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\} = \text{mdc}\{|b| : b \in \mathbb{Z}, b \neq 0\} = 1$,

o que prova a proposição. $\square$

Exemplo 3.54. Seja θ uma raiz do polinômio cúbico $f(x) = x^3 - 3x + 9$. Vamos determinar o índice e o índice minimal do corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$. Sejam θ' e θ'' as outras raízes de $f(x)$, então $x^3 - 3x + 9 = (x - \theta)(x - \theta')(x - \theta'')$. No Exemplo 3.43, vimos que $\left\{1, \theta, \frac{\theta^2}{3}\right\}$ é uma base integral para o corpo $\mathbb{K}$, $D(\theta) = -3^3 \cdot 7 \cdot 11$ e $D(\mathbb{K}) = -3 \cdot 7 \cdot 11$. Se

$\alpha \in \mathcal{O}_{\mathbb{K}}$, então existem $a, b, c \in \mathbb{Z}$, tais que $\alpha = a + b\theta + c\frac{\theta^2}{3}$. Dessa forma, os conjugados de α são $\alpha = a + b\theta + c\frac{\theta^2}{3}$, $\alpha' = a + b\theta' + c\frac{\theta'^2}{3}$ e $\alpha'' = a + b\theta'' + c\frac{\theta''^2}{3}$. Assim, como $\theta + \theta' + \theta'' = 0$, segue que

$$\begin{aligned} \bullet \quad \alpha - \alpha' &= a + b\theta + c\frac{\theta^2}{3} - \left(a + b\theta' + c\frac{\theta'^2}{3}\right) = b(\theta - \theta') + c\left(\frac{\theta^2 - \theta'^2}{3}\right) = b(\theta - \theta') + \\ &\quad \frac{c}{3}(\theta - \theta')(\theta + \theta') = (\theta - \theta')\left(b + \frac{c}{3}(\theta + \theta')\right) = (\theta - \theta')\left(b - \frac{c}{3}\theta''\right); \end{aligned}$$

- $\alpha - \alpha'' = (\theta - \theta'') \left(b - \frac{c}{3}\theta' \right);$
- $\alpha' - \alpha'' = (\theta' - \theta'') \left(b - \frac{c}{3}\theta \right).$

Agora, pela Proposição 2.64, segue que

$$\begin{aligned}
 D(\alpha) &= (\alpha - \alpha')^2(\alpha - \alpha'')^2(\alpha' - \alpha'')^2 \\
 &= (\theta - \theta')^2(\theta - \theta'')^2(\theta' - \theta'')^2 \left(b - \frac{c}{3}\theta \right)^2 \left(b - \frac{c}{3}\theta' \right)^2 \left(b - \frac{c}{3}\theta'' \right)^2 \\
 &= D(\theta) \left[\left(b - \frac{c}{3}\theta \right) \left(b - \frac{c}{3}\theta' \right) \left(b - \frac{c}{3}\theta'' \right) \right]^2 \\
 &= D(\theta) \left[b^3 + \frac{bc^2}{9}(\theta\theta' + \theta'\theta'' + \theta'\theta'') - \frac{b^2c}{3}(\theta + \theta' + \theta'') - \frac{c^3}{27}\theta\theta'\theta'' \right]^2.
 \end{aligned}$$

Pelas relações de Girard, segue que

$$\begin{cases} \theta + \theta' + \theta'' = 0 \\ \theta\theta' + \theta\theta'' + \theta'\theta'' = -3 \\ \theta\theta'\theta'' = -9. \end{cases}$$

Dessa forma, $D(\alpha) = D(\theta) \left(b^3 + \frac{bc^2}{9} \cdot (-3) - \frac{c^3}{27} \cdot (-9) \right)^2 = -3^3 \cdot 7 \cdot 11 \left(\frac{3b^3 - bc^2 + c^3}{3} \right)^2$, ou seja, $D(\alpha) = -3 \cdot 7 \cdot 11 (3b - bc^2 + c^3)^2$. Agora, α é um gerador de $\mathbb{K} \Leftrightarrow D(\alpha) \neq 0 \Leftrightarrow 3b - bc^2 + c^3 \neq 0$. Assim,

$$\text{ind}(\alpha) = \sqrt{\frac{D(\alpha)}{D(\mathbb{K})}} = \sqrt{\frac{-3 \cdot 7 \cdot 11 (3b - bc^2 + c^3)^2}{-3 \cdot 7 \cdot 11}} = |3b - bc^2 + c^3|.$$

Logo,

$$\begin{aligned}
 m(\mathbb{K}) &= \min\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\} \\
 &= \min\{|3b - bc^2 + c^3| : 3b - bc^2 + c^3 \neq 0, b, c \in \mathbb{Z}\}.
 \end{aligned}$$

Note que, para $b = 1$ e $c = -1$, segue que $3b - bc^2 + c^3 = 0$. Portanto, $m(\mathbb{K}) = 1$. Por fim, $i(\mathbb{K}) \mid m(\mathbb{K}) \Rightarrow i(\mathbb{K}) = 1$. Pela Proposição 3.51, segue que $\mathbb{K}$ possui uma base potente, uma vez que $m(\mathbb{K}) = 1$. Assim,

$$f(\theta) = 0 \Rightarrow \theta^3 - 3\theta + 9 = 0 \Rightarrow \theta^3 = 3\theta - 9 \Rightarrow \theta^4 = 3\theta^2 - 9\theta,$$

e assim,

$$\frac{\theta^4}{9} = \frac{\theta^2}{3} - \theta \Rightarrow -\theta = \frac{\theta^4}{9} - \frac{\theta^2}{2}.$$

Assim,

$$\begin{aligned}
 D(\mathbb{K}) &= D\left(1, \theta, \frac{\theta^2}{3}\right) = D\left(1, \frac{\theta^2}{3}, -\theta\right) = D\left(1, \frac{\theta^2}{3}, \frac{\theta^2}{3} - \theta\right) = D\left(1, \frac{\theta^2}{3}, \frac{\theta^4}{9}\right) \\
 &= D\left(1, \frac{\theta^2}{3}, \left(\frac{\theta^2}{3}\right)^2\right).
 \end{aligned}$$

Portanto, $\left\{1, \frac{\theta^2}{3}, \left(\frac{\theta^2}{3}\right)^2\right\}$ é uma base potente para o corpo $\mathbb{K}$.

Exemplo 3.55. Seja θ uma raiz do polinômio cúbico $f(x) = x^3 - 21x - 236$. Vamos determinar o índice e o índice minimal do corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$. Sejam θ' e θ'' as outras raízes de $f(x)$, então $x^3 - 21x - 236 = (x - \theta)(x - \theta')(x - \theta'')$. No Exemplo 3.44, vimos que $\left\{1, \frac{1 + \theta}{3}, \frac{-2 - \theta + \theta^2}{18}\right\}$ é uma base integral para o corpo $\mathbb{K}$, $D(\theta) = -2^2 \cdot 3^6 \cdot 503$ e $D(\mathbb{K}) = -503$. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então existem $a, b, c \in \mathbb{Z}$, tais que $\alpha = a + b \left(\frac{1 + \theta}{3}\right) + c \left(\frac{-2 - \theta + \theta^2}{18}\right)$. Dessa forma, os conjugados de α são

$$\begin{aligned}\alpha &= a + b \left(\frac{1 + \theta}{3}\right) + c \left(\frac{-2 - \theta + \theta^2}{18}\right), \\ \alpha' &= a + b \left(\frac{1 + \theta'}{3}\right) + c \left(\frac{-2 - \theta' + \theta'^2}{18}\right) \quad \text{e} \\ \alpha'' &= a + b \left(\frac{1 + \theta''}{3}\right) + c \left(\frac{-2 - \theta'' + \theta''^2}{18}\right).\end{aligned}$$

Pelas relações de Girard, segue que

$$\begin{cases} \theta + \theta' + \theta'' = 0 \\ \theta\theta' + \theta\theta'' + \theta'\theta'' = -21 \\ \theta\theta'\theta'' = 236. \end{cases}$$

Dessa forma,

$$\begin{aligned}\alpha - \alpha' &= a + b \left(\frac{1 + \theta}{3}\right) + c \left(\frac{-2 - \theta + \theta^2}{18}\right) \\ &\quad - \left(a + b \left(\frac{1 + \theta'}{3}\right) + c \left(\frac{-2 - \theta' + \theta'^2}{18}\right)\right) \\ &= b \left(\frac{\theta - \theta'}{3}\right) + c \left(\frac{\theta^2 - \theta - \theta'^2 + \theta'}{18}\right) = \frac{b}{3}(\theta - \theta') + \frac{c}{18}(\theta^2 - \theta'^2 - \theta + \theta') \\ &= \frac{b}{3}(\theta - \theta') + \frac{c}{18}((\theta - \theta')(\theta + \theta') - (\theta - \theta')) \\ &= (\theta - \theta') \left(\frac{b}{3} - \frac{c}{18} + \frac{c}{18}(\theta + \theta')\right) \\ &= (\theta - \theta') \left(\frac{b}{3} - \frac{c}{18} - \frac{c}{18}\theta''\right). \\ \alpha - \alpha'' &= (\theta - \theta'') \left(\frac{b}{3} - \frac{c}{18} - \frac{c}{18}\theta'\right). \\ \alpha' - \alpha'' &= (\theta' - \theta'') \left(\frac{b}{3} - \frac{c}{18} - \frac{c}{18}\theta\right).\end{aligned}$$

Agora,

$$\begin{aligned}
D(\alpha) &= [(\alpha - \alpha')(\alpha - \alpha'')(\alpha' - \alpha'')]^2 \\
&= [(\theta - \theta')(\theta - \theta'')(\theta' - \theta'')]^2 \left[\left(\frac{b}{3} - \frac{c}{18} - \frac{c}{18}\theta \right) \left(\frac{b}{3} - \frac{c}{18} - \frac{c}{18}\theta' \right) \left(\frac{b}{3} - \frac{c}{18} - \frac{c}{18}\theta'' \right) \right] \\
&= D(\theta) \left[\frac{b^3}{27} - \frac{b^2c}{18 \cdot 3} - \frac{bc^2}{18^2} + \frac{bc^2}{18^2 \cdot 3} \cdot (-21) - \frac{c^3}{18^3}(-21) - \frac{c^3}{18^3}(236) - \frac{c^3}{18^3} \right]^2 \\
&= D(\theta) \frac{1}{2^6 \cdot 3^{12}} (216b^3 - 108b^2c - 108bc^2 - 216c^3)^2 \\
&= (-2^2 \cdot 3^6 \cdot 503) \frac{2^4 \cdot 3^6}{2^6 \cdot 3^{12}} (2b^3 - b^2c - bc^2 - 2c^3)^2,
\end{aligned}$$

e assim, $D(\alpha) = -503(2b^3 - b^2c - bc^2 - 2c^3)^2$. Agora, α é um gerador de $\mathbb{K} \Leftrightarrow D(\alpha) \neq 0 \Leftrightarrow 2b^3 - b^2c - bc^2 - 2c^3 \neq 0$. Assim,

$$\text{ind}(\alpha) = \sqrt{\frac{D(\alpha)}{D(\mathbb{K})}} = |2b^3 - b^2c - bc^2 - 2c^3| = |2(b^3 - c^3) - bc(b + c)|.$$

Agora, para todo $b, c \in \mathbb{Z}$, segue que $2(b^3 - c^3)$ é par. Se b ou c é par, então bc é par. E se b e c são ímpares, então $b + c$ é ímpar. Dessa forma, para todo $b, c \in \mathbb{Z}$, segue que $2(b^3 - c^3) - bc(b + c) \equiv 0 \pmod{2}$. Além disso, para $b = 1$ e $c = 0$, segue que $2(b^3 - c^3) - bc(b + c) = 2$. Logo,

$$\begin{aligned}
m(\mathbb{K}) &= \min\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\} \\
&= \min\{|2(b^3 - c^3) - bc(b + c)| : 2(b^3 - c^3) - bc(b + c) \neq 0, b, c \in \mathbb{Z}\} = 2 \\
i(\mathbb{K}) &= \text{mdc}\{\text{ind}(\alpha) : \alpha \text{ é um gerador de } \mathbb{K}\} \\
&= \text{mdc}\{|2(b^3 - c^3) - bc(b + c)| : 2(b^3 - c^3) - bc(b + c) \neq 0, b, c \in \mathbb{Z}\} = 2,
\end{aligned}$$

uma vez que $2(b^3 - c^3) - bc(b + c) \equiv 0 \pmod{2}$. Note que, $m(\mathbb{K}) = 2$ implica que $\mathbb{K}$ não possui uma base potente.

Definição 3.56. Seja $\mathbb{K}$ um corpo de números de grau n sobre $\mathbb{Q}$. Um primo p é chamado de **divisor discriminante não essencial** ou **divisor de índice comum**, se $p \mid \text{ind}(\alpha)$, para todo α gerador de $\mathbb{K}$.

Observe que os discriminantes não essenciais de um corpo de números $\mathbb{K}$ são, precisamente, os fatores primos do índice $i(\mathbb{K})$.

4 O anel de elementos p -inteiros de um corpo de números

O presente capítulo tem como objetivo introduzir o tema principal deste trabalho, que são as bases p -inteiros. A principal referência utilizada, e também no Capítulo 5, é [3]. Na Seção 4.1, apresentamos os elementos p -inteiros de um corpo de números e algumas propriedades importantes. Na Seção 4.2, veremos a existência de bases para o corpo $\mathbb{K}$ formadas por elementos p -inteiros e apresentamos o conceito de uma base p -integral.

4.1 Elementos p -inteiros de um corpo de números

Dado um corpo de números $\mathbb{K}$ de grau n , vimos, na Observação 2.79, que o seu anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é um domínio de Dedekind, ou seja, é Noetheriano, integralmente fechado e todo ideal primo de $\mathcal{O}_{\mathbb{K}}$ é um ideal maximal. Portanto, todo ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ contém um produto de ideais primos, uma vez que este fato é verdadeiro para domínios Noetherianos [5]. Além disso, todo ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ é um produto de ideais primos e essa fatoração é única, ou seja, dado $I \subseteq \mathcal{O}_{\mathbb{K}}$ um ideal não nulo, então I é expresso de maneira única como $\prod_{i=1}^r P_i^{m_i}$, com P_i ideais primos distintos de $\mathcal{O}_{\mathbb{K}}$ e $m_i \in \mathbb{Z}$ [5].

Definição 4.1. Sejam D um domínio e $\mathbb{K}$ o seu corpo de frações, então um ideal não vazio $I \subseteq \mathbb{K}$ é dito um **ideal fracionário de D** se satisfaz:

1. Se $\alpha \in I$ e $\beta \in I$, então $\alpha \pm \beta \in I$;
2. Se $\alpha \in I$ e $r \in D$, então $r\alpha \in I$;
3. Existe $\gamma \in D$, $\gamma \neq 0$, tal que $\gamma I \subseteq D$. Neste caso, γ é chamado de denominador comum.

Definição 4.2. Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Um ideal não vazio $I \subseteq \mathbb{K}$ é dito um **ideal fracionário de $\mathcal{O}_{\mathbb{K}}$** se satisfaz:

1. Se $\alpha \in I$ e $\beta \in I$, então $\alpha \pm \beta \in I$;
2. Se $\alpha \in I$ e $r \in \mathcal{O}_{\mathbb{K}}$, então $r\alpha \in I$;
3. Existe $\gamma \in \mathcal{O}_{\mathbb{K}}$, $\gamma \neq 0$, tal que $\gamma I \subseteq \mathcal{O}_{\mathbb{K}}$.

Definição 4.3. Sejam $\mathbb{K}$ um corpo de números de grau n , $\mathcal{O}_{\mathbb{K}}$ o seu anel de inteiros e $I \subseteq \mathcal{O}_{\mathbb{K}}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, ou seja, $I = \prod_{i=1}^r P_i^{m_i}$, com P_i ideais primos distintos de

$\mathcal{O}_{\mathbb{K}}$ e $m_i \in \mathbb{Z}$. Para todo $i = 1, \dots, r$, a **valorização** de I em P_i é definida como potência do ideal primo P_i na decomposição de I em ideais primos e denotamos $v_{P_i}(I) = m_i$. Se $I = \alpha\mathcal{O}_{\mathbb{K}}$ é um ideal principal, então usamos a notação $v_{P_i}(I) = v_{P_i}(\alpha)$. Também, consideramos $v_P(0) = +\infty$, para todo ideal primo P de $\mathcal{O}_{\mathbb{K}}$.

Definição 4.4. Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o seu anel de inteiros, então

1. Seja P um ideal primo de $\mathcal{O}_{\mathbb{K}}$ e $\alpha \in \mathbb{K}$. Se $v_P(\alpha) \geq 0$, então α é chamado de **elemento P -integral do corpo $\mathbb{K}$** ;
2. Seja p um número primo, se $\alpha \in \mathbb{K}$ é P -integral para todo ideal primo P de $\mathcal{O}_{\mathbb{K}}$, tal que $P \mid p\mathcal{O}_{\mathbb{K}}$, então α é chamado de **elemento p -integral do corpo $\mathbb{K}$** .

Em outras palavras, α é dito um elemento P -integral do corpo $\mathbb{K}$ se o ideal primo P aparece na decomposição do ideal $\alpha\mathcal{O}_{\mathbb{K}}$ em ideais primos de $\mathcal{O}_{\mathbb{K}}$ com expoente não negativo e α é dito um elemento p -integral do corpo $\mathbb{K}$ se todo ideal primo na decomposição de $p\mathcal{O}_{\mathbb{K}}$ aparece na decomposição de $\alpha\mathcal{O}_{\mathbb{K}}$ em ideais primos de $\mathcal{O}_{\mathbb{K}}$ com expoente não negativo.

Exemplo 4.5. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$ um corpo quadrático e $\mathcal{O}_{\mathbb{K}} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ o seu anel de inteiros. Considere $\alpha = 6 \in \mathbb{K}$. Como

$$\alpha = 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

com $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ elementos irredutíveis não associados de $\mathcal{O}_{\mathbb{K}}$, segue que $\mathcal{O}_{\mathbb{K}}$ não é um domínio de fatoração única. Considere os ideais primos de $\mathcal{O}_{\mathbb{K}}$ dados por $P = \langle 2, 1 + \sqrt{-5} \rangle$, $P_1 = \langle 3, 1 + \sqrt{-5} \rangle$ e $P_2 = \langle 3, 1 - \sqrt{-5} \rangle$. Agora,

- $P = \langle 2, 1 + \sqrt{-5} \rangle = \langle 2, 1 + \sqrt{-5}, 2 - (1 + \sqrt{-5}) \rangle = \langle 2, 1 + \sqrt{-5}, 1 - \sqrt{-5} \rangle$
 $= \langle 2, 2 - (1 - \sqrt{-5}), 1 - \sqrt{-5} \rangle = \langle 2, 1 - \sqrt{-5} \rangle$;
- $P^2 = \langle 2, 1 + \sqrt{-5} \rangle^2 = \langle 2, 1 + \sqrt{-5} \rangle \langle 2, 1 + \sqrt{-5} \rangle = \langle 2, 1 + \sqrt{-5} \rangle \langle 2, 1 - \sqrt{-5} \rangle$
 $= \langle 4, 2(1 - \sqrt{-5}), 2(1 + \sqrt{-5}), 2 \cdot 3 \rangle = \langle 2 \rangle \langle 2, 1 - \sqrt{-5}, 1 + \sqrt{-5}, 3 \rangle = \langle 2 \rangle \langle 1 \rangle = \langle 2 \rangle$;
- $P_1 P_2 = \langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle = \langle 9, 3(1 - \sqrt{-5}), 3(1 + \sqrt{-5}), 2 \cdot 3 \rangle$
 $= \langle 3 \rangle \langle 3, 1 - \sqrt{-5}, 1 + \sqrt{-5}, 2 \rangle = \langle 3 \rangle \langle 1 \rangle = \langle 3 \rangle$;
- $PP_1 = \langle 2, 1 + \sqrt{-5} \rangle \langle 3, 1 + \sqrt{-5} \rangle = \langle 6, 2(1 + \sqrt{-5}), 3(1 + \sqrt{-5}), (1 + \sqrt{-5})^2 \rangle$
 $= \langle (1 + \sqrt{-5})(1 - \sqrt{-5}), 2(1 + \sqrt{-5}), 3(1 + \sqrt{-5}), (1 + \sqrt{-5})^2 \rangle$
 $= \langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{-5}, 2, 3, (1 + \sqrt{-5}) \rangle = \langle 1 + \sqrt{-5} \rangle \langle 1 \rangle = \langle 1 + \sqrt{-5} \rangle$;
- $PP_2 = \langle 2, 1 - \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle = \langle 6, 2(1 - \sqrt{-5}), 3(1 - \sqrt{-5}), (1 - \sqrt{-5})^2 \rangle$
 $= \langle (1 + \sqrt{-5})(1 - \sqrt{-5}), 2(1 - \sqrt{-5}), 3(1 - \sqrt{-5}), (1 - \sqrt{-5})^2 \rangle$
 $= \langle 1 - \sqrt{-5} \rangle \langle 1 + \sqrt{-5}, 2, 3, (1 - \sqrt{-5}) \rangle = \langle 1 - \sqrt{-5} \rangle \langle 1 \rangle = \langle 1 - \sqrt{-5} \rangle$.

Assim, em $\mathcal{O}_{\mathbb{K}}$, segue que $\langle 2 \rangle = P^2$, ou seja, 2 é um elemento P -integral do corpo $\mathbb{K}$; $\langle 3 \rangle = P_1 P_2$, ou seja, 3 é um elemento P_1 -integral e P_2 -integral do corpo $\mathbb{K}$; $\langle 1 + \sqrt{-5} \rangle = PP_1$, ou seja, $1 + \sqrt{-5}$ é um elemento P -integral e P_1 -integral do corpo $\mathbb{K}$; e $\langle 1 - \sqrt{-5} \rangle = PP_2$, ou seja, $1 - \sqrt{-5}$ é um elemento P -integral e P_2 -integral do corpo $\mathbb{K}$. Além disso, $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = \langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{-5} \rangle = P^2 P_1 P_2$, ou seja, 6 é um elemento P -integral, P_1 -integral, P_2 -integral, 2-integral e 3-integral do corpo $\mathbb{K}$.

Observação 4.6. Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o seu anel de inteiros. Dados P um ideal primo de $\mathcal{O}_{\mathbb{K}}$ e $\alpha, \beta \in \mathbb{K}$, então:

1. $v_P(\alpha + \beta) \geq \min\{v_P(\alpha), v_P(\beta)\}$;
2. $v_P(\alpha\beta) = v_P(\alpha) + v_P(\beta)$;
3. $v_P(\alpha^{-1}) = -v_P(\alpha)$.

Teorema 4.7. Sejam $\mathbb{K}$ um corpo de números de grau n sobre $\mathbb{Q}$ e $\mathcal{O}_{\mathbb{K}}$ o seu anel de inteiros.

1. Se P é um ideal primo de $\mathcal{O}_{\mathbb{K}}$, então os elementos P -inteiros do corpo $\mathbb{K}$ formam um domínio $\mathcal{D}_P$;
2. Se $p \in \mathbb{Z}$ um número primo, então os elementos p -inteiros do corpo $\mathbb{K}$ formam um domínio $\mathcal{D}_p$;
3. Se $p \in \mathbb{Z}$ um número primo, então $\mathcal{D}_p = \bigcap_{P|p\mathcal{O}_{\mathbb{K}}} \mathcal{D}_P$.

Demonstração. Para o primeiro item, seja P um ideal primo de $\mathcal{O}_{\mathbb{K}}$, considere

$$\mathcal{D}_P = \{\alpha \in \mathbb{K} : \alpha \text{ é um elemento } P\text{-integral de } \mathbb{K}\} = \{\alpha \in \mathbb{K} : v_P(\alpha) \geq 0\}.$$

Se $\alpha, \beta \in \mathcal{D}_P$, então $v_P(\alpha) \geq 0$ e $v_P(\beta) \geq 0$. Dessa forma,

$$v_P(\alpha + \beta) \geq \min\{v_P(\alpha), v_P(\beta)\} \geq 0 \Rightarrow \alpha + \beta \in \mathcal{D}_P.$$

Além disso,

$$v_P(\alpha\beta) = v_P(\alpha) + v_P(\beta) \geq 0 \Rightarrow \alpha\beta \in \mathcal{D}_P.$$

Portanto, $\mathcal{D}_P$ é um domínio. Para o segundo item, seja $p \in \mathbb{Z}$ um número primo, considere

$$\begin{aligned} \mathcal{D}_p &= \{\alpha \in \mathbb{K} : \alpha \text{ é um elemento } p\text{-integral de } \mathbb{K}\} \\ &= \{\alpha \in \mathbb{K} : v_P(\alpha) \geq 0, \text{ para todo } P \text{ ideal primo de } \mathcal{O}_{\mathbb{K}}, P | p\mathcal{O}_{\mathbb{K}}\}. \end{aligned}$$

Sejam $\alpha, \beta \in \mathcal{D}_p$. Para todo ideal primo P de $\mathcal{O}_{\mathbb{K}}$ tal que $P | p\mathcal{O}_{\mathbb{K}}$, segue que $v_P(\alpha) \geq 0$ e $v_P(\beta) \geq 0$. Dessa forma, segue que

$$v_P(\alpha + \beta) \geq \min\{v_P(\alpha), v_P(\beta)\} \geq 0 \text{ e } v_P(\alpha\beta) = v_P(\alpha) + v_P(\beta) \geq 0,$$

para todo P ideal primo de $\mathcal{O}_{\mathbb{K}}$ com $P | p\mathcal{O}_{\mathbb{K}}$, ou seja, $\alpha + \beta \in \mathcal{D}_p$ e $\alpha\beta \in \mathcal{D}_p$. Portanto, $\mathcal{D}_p$ é um domínio. Finalmente, para o terceiro item, sejam $p \in \mathbb{Z}$ um número primo e $\alpha \in \mathcal{D}_p$, então $v_P(\alpha) \geq 0$, para todo P ideal primo de $\mathcal{O}_{\mathbb{K}}$ com $P | p\mathcal{O}_{\mathbb{K}} \Rightarrow \alpha \in \mathcal{D}_P$, para todo P ideal primo de $\mathcal{O}_{\mathbb{K}}$ com $P | p\mathcal{O}_{\mathbb{K}}$. Assim,

$$\alpha \in \bigcap_{P|p\mathcal{O}_{\mathbb{K}}} \mathcal{D}_P.$$

Por outro lado, seja $\alpha \in \bigcap_{P|p\mathcal{O}_{\mathbb{K}}} \mathcal{D}_P$, então $\alpha \in \mathcal{D}_P$, para todo P ideal primo de $\mathcal{O}_{\mathbb{K}}$ com $P | p\mathcal{O}_{\mathbb{K}}$. Assim, $v_P(\alpha) \geq 0$, para todo P ideal primo de $\mathcal{O}_{\mathbb{K}}$ com $P | p\mathcal{O}_{\mathbb{K}}$, o que implica que $\alpha \in \mathcal{D}_p$. Portanto, $\mathcal{D}_p = \bigcap_{P|p\mathcal{O}_{\mathbb{K}}} \mathcal{D}_P$. $\square$

Para os próximos resultados, considere o anel $\mathbb{Z}$ e $\mathbb{Q}$ o seu corpo de frações. Dado um número primo $p \in \mathbb{Z}$, apresentamos alguns resultados de elementos p -integrais de $\mathbb{Q}$.

Proposição 4.8. *Seja $p \in \mathbb{Z}$ um número primo. Se $m \in \mathbb{Z}$, então m é um elemento p -integral de $\mathbb{Q}$.*

Demonstração. Para todo $m \in \mathbb{Z} \subseteq \mathbb{Q}$, segue que $m = 1 \cdot m = p^0 \cdot m$. Se $p \mid m$, então $v_p(m) > 0$ e se $p \nmid m$, então $v_p(m) = 0$. Portanto, m é um elemento p -integral de $\mathbb{Q}$. $\square$

Proposição 4.9. *Se m é um elemento p -integral de $\mathbb{Q}$, para todo $p \in \mathbb{Z}$ primo, então $m \in \mathbb{Z}$.*

Demonstração. Se $m \in \mathbb{Q}$, então existem $a, b \in \mathbb{Z}$, com $b \neq 0$, tais que

$$m = \frac{a}{b} \Rightarrow m = ab^{-1} \Rightarrow v_p(m) = v_p(a) + v_p(b^{-1}) \Rightarrow v_p(m) = v_p(a) - v_p(b).$$

Como, por hipótese, m é um elemento p -integral de $\mathbb{Q}$, segue que

$$v_p(m) = v_p(a) - v_p(b) \geq 0 \Rightarrow v_p(a) \geq v_p(b),$$

para todo $p \in \mathbb{Z}$ primo. Assim, todos os primos nas decomposições de a e b aparecem com maior expoente em a . Portanto, $b \mid a \Rightarrow m \in \mathbb{Z}$. $\square$

Proposição 4.10. *Seja $\frac{a}{b} \in \mathbb{Q}$, com $a, b \in \mathbb{Z}$, $b \neq 0$ e $p \in \mathbb{Z}$ um número primo. Se $p \nmid b$, então $\frac{a}{b}$ é um elemento p -integral de $\mathbb{Q}$.*

Demonstração. Pela Proposição 4.9, segue que $a, b \in \mathbb{Z}$ são elementos p -integrais de $\mathbb{Q}$, ou seja, $v_p(a) \geq 0$ e $v_p(b) \geq 0$. Dessa forma, como $p \nmid b$, segue que $v_p(b) = 0$. Agora,

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b) = v_p(a) \geq 0.$$

Logo, $v_p\left(\frac{a}{b}\right) \geq 0$, ou seja, $\frac{a}{b}$ é um elemento p -integral de $\mathbb{Q}$. $\square$

Lema 4.11. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n e $p \in \mathbb{Z}$ um número primo. Se $\alpha \in \mathbb{K}$ é um elemento p -integral do corpo $\mathbb{K}$, então $\alpha = \frac{\gamma}{d}$, com $\gamma \in \mathcal{O}_{\mathbb{K}}$, $d \in \mathbb{Z}$, $d \neq 0$ e $p \nmid d$.*

Demonstração. Como $\alpha \in \mathbb{K} = \mathbb{Q}(\theta)$, segue que existem únicos $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$ tais que $\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$. Para cada $i = 0, 1, \dots, n-1$, segue que $a_i = \frac{b_i}{c_i}$, com $b_i, c_i \in \mathbb{Z}$, $c_i \neq 0$. Assim,

$$\alpha = \frac{b_0}{c_0} + \frac{b_1}{c_1}\theta + \dots + \frac{b_{n-1}}{c_{n-1}}\theta^{n-1} \Rightarrow \alpha = \frac{A_0 + A_1\theta + \dots + A_{n-1}\theta^{n-1}}{\text{mdc}\{c_i : i = 0, 1, \dots, n-1\}}.$$

Chamando $\gamma = A_0 + A_1\theta + \dots + A_{n-1}\theta^{n-1} \in \mathcal{O}_{\mathbb{K}}$ e $d = \text{mdc}\{c_i : i = 0, 1, \dots, n-1\}$, segue que $\alpha = \frac{\gamma}{d}$, com $\gamma \in \mathcal{O}_{\mathbb{K}}$ e $d \in \mathbb{Z}$, $d \neq 0$. Além disso, note que nenhum número inteiro diferente de ± 1 divide γ e d . Agora, como α é um elemento p -integral do corpo $\mathbb{K}$, então todo ideal primo de $\mathcal{O}_{\mathbb{K}}$ na decomposição de $p\mathcal{O}_{\mathbb{K}}$, com expoente não negativo, aparece na decomposição de $\alpha\mathcal{O}_{\mathbb{K}}$ em ideais primos de $\mathcal{O}_{\mathbb{K}}$, também com expoente não

negativo. Vamos supor que $p \mid d$. Assim, $d = p^l t$, com $l, t \in \mathbb{Z}$, $l \geq 1$ e $p \nmid t$. Considere a fatoração de $p\mathcal{O}_{\mathbb{K}}$ em ideais primos:

$$p\mathcal{O}_{\mathbb{K}} = \prod_{j=1}^k P_j^{m_j} = P_1^{m_1} P_2^{m_2} \dots P_k^{m_k}.$$

Dessa forma,

$$\begin{aligned} \alpha\mathcal{O}_{\mathbb{K}} &= \left(\frac{\gamma}{d}\right)\mathcal{O}_{\mathbb{K}} = (d^{-1}\gamma)\mathcal{O}_{\mathbb{K}} = (p^l t)^{-1}\gamma\mathcal{O}_{\mathbb{K}} = (p^{-l}t^{-1}\gamma)\mathcal{O}_{\mathbb{K}} \\ &= (p^{-l}\mathcal{O}_{\mathbb{K}})(t^{-1}\gamma)\mathcal{O}_{\mathbb{K}} = (P_1^{-lm_1}P_2^{-lm_2}\dots P_k^{-lm_k})(t^{-1}\mathcal{O}_{\mathbb{K}})(\gamma\mathcal{O}_{\mathbb{K}}). \end{aligned}$$

Como α é um elemento p -integral do corpo $\mathbb{K}$, segue que para todo $j = 1, 2, \dots, k$, $v_{P_j}(\alpha) \geq 0$. Assim,

$$v_{P_j}(\alpha) = v_{P_j}(\gamma d^{-1}) = v_{P_j}(\gamma) + v_{P_j}(d^{-1}) = v_{P_j}(\gamma) + v_{P_j}(p^{-l}t) = v_{P_j}(\gamma) + v_{P_j}(p^{-l}) + v_{P_j}(t) \geq 0.$$

Note que, como $p \nmid t$, então para todo $j = 1, 2, \dots, k$, $v_{P_j}(t) = 0$. Assim,

$$v_{P_j}(\alpha) = v_{P_j}(\gamma) + v_{P_j}(p^{-l}) = v_{P_j}(\gamma) - lm_j \geq 0 \Rightarrow v_{P_j}(\gamma) \geq lm_j \geq m_j,$$

ou seja, p é um fator de γ , o que é um absurdo. Portanto, $p \nmid d$, o que completa a demonstração. $\square$

O último teorema desta seção, afirma que se $p \in \mathbb{Z}$ é um número primo e α é um elemento p -integral do corpo $\mathbb{K}$, então α satisfaz um polinômio mônico com coeficientes sendo elementos p -integrais de $\mathbb{Q}$.

Teorema 4.12. *Sejam $\mathbb{K}$ um corpo de números de grau n e $p \in \mathbb{Z}$ um número primo. Se $\alpha \in \mathbb{K}$ e $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ são os conjugados de α com respeito a $\mathbb{K}$, então α é um elemento p -integral do corpo $\mathbb{K}$ se, e somente se, as funções simétricas elementares*

$$\begin{cases} \alpha_1 + \alpha_2 + \dots + \alpha_n \\ \alpha_1\alpha_2 + \dots + \alpha_{n-1}\alpha_n \\ \vdots \\ \alpha_1 \dots \alpha_n \end{cases}$$

são elementos p -integrais de $\mathbb{Q}$.

Demonstração. Seja α um elemento p -integral do corpo $\mathbb{K}$. Pelo Lema 4.11, segue que α pode ser escrito como $\frac{\gamma}{d}$, com $\gamma \in \mathcal{O}_{\mathbb{K}}$, $d \in \mathbb{Z}$, $d \neq 0$ e $p \nmid d$. Agora, como $\gamma \in \mathcal{O}_{\mathbb{K}}$, então existem $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$ tais que $a_0 + a_1\gamma + \dots + a_{n-1}\gamma^{n-1} + \gamma^n$, com n o menor possível. Dessa forma, as funções simétricas elementares são

$$\begin{cases} \gamma_1 + \dots + \gamma_n = -a_{n-1} \in \mathbb{Z} \\ \gamma_1\gamma_2 + \dots + \gamma_{n-1}\gamma_n = a_{n-2} \in \mathbb{Z} \\ \vdots \\ \gamma_1 \dots \gamma_n = (-1)^n a_0 \in \mathbb{Z}. \end{cases}$$

Note que, pela Proposição 4.8, para cada $i = 0, 1, \dots, n-1$, segue que $a_i \in \mathbb{Z} \Rightarrow a_i$ é um elemento p -integral de $\mathbb{Q}$. Além disso, para todo $j = 0, 1, \dots, n-1$, segue que $\alpha_j = \frac{\gamma_j}{d}$, então

$$\begin{cases} \alpha_1 + \dots + \alpha_n = -\frac{a_{n-1}}{d} \in \mathbb{Q} \\ \alpha_1\alpha_2 + \dots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{d^2} \in \mathbb{Q} \\ \vdots \\ \alpha_1 \dots \alpha_n = \frac{(-1)^n a_0}{d^n} \in \mathbb{Q}. \end{cases}$$

Como $p \nmid d$, pela Proposição 4.10, segue que $\frac{(-1)^{n-j} a_j}{d^{n-j}}$ é um elemento p -integral de $\mathbb{Q}$, para todo $j = 0, 1, \dots, n-1$, ou seja, as funções simétricas elementares são elementos p -integrals de $\mathbb{Q}$. Reciprocamente, sejam $\alpha \in \mathbb{K}$ e $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ seus $\mathbb{K}$ -conjugados. Considere as funções simétricas elementares

$$\begin{cases} \alpha_1 + \alpha_2 + \dots + \alpha_n \\ \alpha_1\alpha_2 + \dots + \alpha_{n-1}\alpha_n \\ \vdots \\ \alpha_1 \dots \alpha_n \end{cases}$$

e considere cada função simétrica elementar um elemento p -integral de $\mathbb{Q}$, ou seja, é um número de $\mathbb{Q}$ em que p aparece na fatoração com expoente não negativo. Suponhamos que α não seja um elemento p -integral do corpo $\mathbb{K}$. Assim, existe um ideal primo P de $\mathcal{O}_{\mathbb{K}}$, com $P \mid p\mathcal{O}_{\mathbb{K}}$ tal que $v_P(\alpha) < 0$. Agora, uma vez que as funções simétricas elementares são coeficientes de um polinômio mônico, digamos $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, e que $\alpha = \alpha_1$ é raiz deste polinômio, segue que

$$\alpha_n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0 \Rightarrow a^n = -(a_{n-1}x^{n-1} + \dots + a_1\alpha + a_0).$$

Dessa forma,

$$v_P(\alpha^n) = n.v_P(\alpha) \Rightarrow v_P(a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0) = n.v_P(\alpha).$$

Assim,

$$\begin{aligned} n.v_P(\alpha) &\geq \min\{v_P(a_{n-1}\alpha^{n-1}), \dots, v_P(a_1\alpha), v_P(a_0)\} \\ &= \min\{v_P(a_{n-1}) + v_P(\alpha^{n-1}), \dots, v_P(a_1) + v_P(\alpha), v_P(a_0)\} \\ &\geq \min\{v_P(\alpha^{n-1}), v_P(\alpha^{n-2}), \dots, v_P(\alpha), 0\} \\ &= v_P(\alpha^{n-1}), \text{ pois } v_P(\alpha) < 0. \end{aligned}$$

Logo,

$$n.v_P(\alpha) \geq (n-1).v_P(\alpha) \Rightarrow (n-n+1).v_P(\alpha) \geq 0 \Rightarrow v_P(\alpha) \geq 0,$$

o que é um absurdo. Portanto, α é um elemento p -integral do corpo $\mathbb{K}$. $\square$

4.2 Base p -integral de um corpo de números

Nesta seção, iremos definir o conceito de base p -integral de um corpo de números $\mathbb{K}$. Mas, para isso, iremos dar alguns resultados que garantem a existência dessas bases.

Proposição 4.13. *Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o seu anel de inteiros. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então para todo $p \in \mathbb{Z}$ primo, α é um elemento p -integral.*

Demonstração. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$, então existem $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$ tais que $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$. Seja $p \in \mathbb{Z}$ primo, vamos supor que $v_p(\alpha) < 0$. Assim,

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n = 0 \Rightarrow \alpha^n = -(a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}).$$

Dessa forma,

$$\begin{aligned} v_p(\alpha^n) &= v_p(a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}) \\ &\geq \min\{v_p(a_0), v_p(a_1\alpha), \dots, v_p(a_{n-1}\alpha^{n-1})\} \\ &= \min\{v_p(a_0), v_p(a_1) + v_p(\alpha), \dots, v_p(a_{n-1}) + v_p(\alpha^{n-1})\} \\ &\geq \min\{0, v_p(\alpha), \dots, v_p(\alpha^{n-1})\} = v_p(\alpha^{n-1}). \end{aligned}$$

pois $v_p(\alpha) < 0$. Dessa forma,

$$v_p(\alpha^n) \geq v_p(\alpha^{n-1}) \Rightarrow n.v_p(\alpha) \geq (n-1).v_p(\alpha) \Rightarrow (n-n+1).v_p(\alpha) \geq 0 \Rightarrow v_p(\alpha) \geq 0,$$

o que é um absurdo. Portanto, α é um elemento p -integral do corpo $\mathbb{K}$, para qualquer $p \in \mathbb{Z}$ primo. $\square$

Corolário 4.14. *Sejam $\mathbb{K}$ um corpo de números de grau n e $p \in \mathbb{Z}$ um número primo. Se $\{\omega_1, \dots, \omega_n\}$ é uma base integral do corpo $\mathbb{K}$, então é uma base formada por elementos p -inteiros do corpo $\mathbb{K}$.*

Demonstração. Segue da Proposição 4.13, pelo fato de cada ω_i , para $i = 1, \dots, n$, ser um elemento de $\mathcal{O}_{\mathbb{K}}$. $\square$

O Corolário 4.14 garante a existência de bases formadas por elementos p -inteiros do corpo $\mathbb{K}$, e assim, possibilitando enunciar e demonstrar o seguinte teorema.

Teorema 4.15. *Sejam $\mathbb{K}$ um corpo de números de grau n e $p \in \mathbb{Z}$ um número primo. Seja $\{\omega_1, \dots, \omega_n\}$ uma base do corpo $\mathbb{K}$ sobre $\mathbb{Q}$ formada por elementos p -inteiros do corpo $\mathbb{K}$ tal que $v_p(D(\omega_1, \dots, \omega_n))$ seja mínimo. Se $\alpha = a_1\omega_1 + \dots + a_n\omega_n$, com $a_1, \dots, a_n \in \mathbb{Q}$, é um elemento p -integral do corpo $\mathbb{K}$, então os coeficientes $a_1, \dots, a_n$ são elementos p -inteiros de $\mathbb{Q}$.*

Demonstração. Primeiramente, observe que para toda base de $\mathbb{K}$ sobre $\mathbb{Q}$, $\{\omega_1, \dots, \omega_n\}$, formada por elementos p -inteiros do corpo $\mathbb{K}$, segue que seu discriminante $D(\omega_1, \dots, \omega_n)$ é um número inteiro. Portanto, a valorização $v_p(D(\omega_1, \dots, \omega_n))$ é um número inteiro não negativo, o que torna possível considerar a base cuja valorização em p seja a menor possível. Dito isso, seja $\alpha \in \mathbb{K}$ um elemento p -integral do corpo $\mathbb{K}$, existem $a_1, \dots, a_n \in \mathbb{Q}$ tais que $\alpha = a_1\omega_1 + \dots + a_n\omega_n$. Suponhamos que, para algum $i = 1, \dots, n$, o coeficiente a_i não seja p -integral. Sem perda de generalidade, vamos considerar $i = 1$. Assim,

$$v_p(a_1) < 0 \Rightarrow a_1 = p^{-k}a = \frac{a}{p^k}, \text{ com } a \in \mathbb{Q}, v_p(a) = 0, k \in \mathbb{Z}, k \geq 1.$$

Como $\alpha \in \mathbb{K}$ é p -integral, segue que o conjunto

$$\{\alpha, \omega_2, \dots, \omega_n\} = \{a_1\omega_1 + \dots + a_n\omega_n, \omega_2, \dots, \omega_n\}$$

é uma base do corpo $\mathbb{K}$ sobre $\mathbb{Q}$ formada por elementos p -integrais do corpo $\mathbb{K}$. Dessa forma,

$$\begin{aligned}
 v_p(D(\alpha, \omega_2, \dots, \omega_n)) &= v_p(D(a_1\omega_1 + \dots + a_n\omega_n, \omega_2, \dots, \omega_n)) \\
 &= v_p\left(D\left(\frac{a}{p^k}\omega_1 + \dots + a_n\omega_n, \omega_2, \dots, \omega_n\right)\right) \\
 &= v_p\left(\left(\frac{a}{p^k}\right)^2 D(\omega_1, \dots, \omega_n)\right) \\
 &= v_p\left(\left(\frac{a}{p^k}\right)^2\right) v_p(D(\omega_1, \dots, \omega_n)) \\
 &= -2k + v_p(D(\omega_1, \dots, \omega_n)) < v_p(D(\omega_1, \dots, \omega_n)),
 \end{aligned}$$

o que contradiz a minimalidade de $v_p(D(\omega_1, \dots, \omega_n))$. Logo, segue que a_i é um elemento p -integral de $\mathbb{Q}$, para todo $i = 1, \dots, n$. $\square$

Agora, podemos definir uma base p -integral do corpo $\mathbb{K}$.

Definição 4.16. Sejam $\mathbb{K}$ um corpo de números de grau n , $p \in \mathbb{Z}$ um número primo e $\{\omega_1, \dots, \omega_n\}$ uma base do corpo $\mathbb{K}$ sobre $\mathbb{Q}$ formada por elementos p -integrais do corpo $\mathbb{K}$. Diremos que $\{\omega_1, \dots, \omega_n\}$ é uma **base p -integral do corpo $\mathbb{K}$** , se todo elemento $\alpha \in \mathbb{K}$ que for p -integral puder ser escrito como $\alpha = a_1\omega_1 + \dots + a_n\omega_n$, com a_i sendo um elemento p -integral de $\mathbb{Q}$, para todo $i = 1, \dots, n$.

Exemplo 4.17. Considere o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ e o número primo $p = 3$. Vamos mostrar que o conjunto $\{1, \sqrt{5}\}$ forma uma base 3-integral para o corpo $\mathbb{K}$. Sabemos que o conjunto $\{1, \sqrt{5}\}$ é uma base do corpo $\mathbb{K}$ sobre $\mathbb{Q}$ (que não é integral). Além disso, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$, pois $5 \equiv 1 \pmod{4}$. Seja $\alpha \in \mathbb{K}$ um elemento 3-integral, pelo Lema 4.11, sabemos que podemos escrever α como $\frac{\gamma}{d}$, com $\gamma \in \mathcal{O}_{\mathbb{K}}$, $d \in \mathbb{Z}$, $d \neq 0$ e $3 \nmid d$. Agora,

$$\gamma \in \mathcal{O}_{\mathbb{K}} \Rightarrow \gamma = a + b\left(\frac{1+\sqrt{5}}{2}\right), \text{ com } a, b \in \mathbb{Q}.$$

Dessa forma,

$$\alpha = \frac{a}{d} + \frac{b}{d}\left(\frac{1+\sqrt{5}}{2}\right) = \frac{a}{d} + \frac{b}{2d} + \frac{b}{2d}\sqrt{5} = \frac{2a+b}{2d} + \frac{b}{2d}\sqrt{5},$$

com $a, b, d \in \mathbb{Z}$, $d \neq 0$ e $3 \nmid d$. Uma vez que $3 \nmid 2$ e $3 \nmid d$, segue que $3 \nmid 2d$. Portanto, pela Proposição 4.10, segue que os coeficientes $\frac{2a+b}{2d}$ e $\frac{b}{2d}$ são elementos 3-integrais de $\mathbb{Q}$. Logo, $\{1, \sqrt{5}\}$ é uma base 3-integral para o corpo $\mathbb{K}$.

Lema 4.18. Sejam $\mathbb{K}$ um corpo de números de grau n sobre $\mathbb{Q}$, $p \in \mathbb{Z}$ um número primo e $\{\omega_1, \dots, \omega_n\}$ uma base p -integral do corpo $\mathbb{K}$. Se $\{\alpha_1, \dots, \alpha_n\}$ é um conjunto formado por n elementos p -integrais do corpo $\mathbb{K}$, então $v_p(D(\alpha_1, \dots, \alpha_n)) \geq v_p(D(\omega_1, \dots, \omega_n))$.

Demonstração. Para todo $i = 1, 2, \dots, n$, como α_i é um elemento p -integral do corpo $\mathbb{K}$ e $\{\omega_1, \dots, \omega_n\}$ é uma base p -integral do corpo $\mathbb{K}$, segue que existem c_{ij} , $j = 1, \dots, n$, elementos p -integrais de $\mathbb{Q}$ tais que $\alpha_i = \sum_{j=1}^n c_{ij}\omega_j$. Além disso, como cada $c_{ij} \in \mathbb{Q}$ é p -integral, segue que $\det(c_{ij})^2$ é um elemento p -integral de $\mathbb{Q}$, ou seja, $v_p(\det(c_{ij})) \geq 0$. Dessa forma,

$$D(\alpha_1, \dots, \alpha_n) = \det(c_{ij})^2 D(\omega_1, \dots, \omega_n),$$

e assim,

$$\begin{aligned} v_p(D(\alpha_1, \dots, \alpha_n)) &= v_p(\det(c_{ij})^2 D(\omega_1, \dots, \omega_n)) \\ &= v_p(\det(c_{ij})^2) + v_p(D(\omega_1, \dots, \omega_n)), \end{aligned}$$

e deste modo,

$$v_p(D(\alpha_1, \dots, \alpha_n)) \geq v_p(D(\omega_1, \dots, \omega_n)),$$

o que prova o lema. $\square$

Proposição 4.19. *Sejam $\mathbb{K}$ um corpo de números de grau n e $p \in \mathbb{Z}$ um número primo. Se $\{\omega_1, \dots, \omega_n\}$ e $\{\mu_1, \dots, \mu_n\}$ são duas bases p -integrais do corpo $\mathbb{K}$, então $v_p(D(\omega_1, \dots, \omega_n)) = v_p(D(\mu_1, \dots, \mu_n))$.*

Demonstração. Como $\{\mu_1, \dots, \mu_n\}$ é uma base p -integral do corpo $\mathbb{K}$ e $\{\omega_1, \dots, \omega_n\}$ é um conjunto formado por n elementos p -integrais do corpo $\mathbb{K}$, pelo Lema 4.18, segue que

$$v_p(D(\omega_1, \dots, \omega_n)) \geq v_p(D(\mu_1, \dots, \mu_n)).$$

Por outro lado, como $\{\omega_1, \dots, \omega_n\}$ é uma base p -integral do corpo $\mathbb{K}$ e $\{\mu_1, \dots, \mu_n\}$ é um conjunto formado por n elementos p -integrais do corpo $\mathbb{K}$, pelo Lema 4.18, segue que

$$v_p(D(\mu_1, \dots, \mu_n)) \geq v_p(D(\omega_1, \dots, \omega_n)),$$

o que prova a proposição. $\square$

Teorema 4.20. *Sejam $\mathbb{K}$ um corpo de números de grau n . Assim, $\{\omega_1, \dots, \omega_n\}$ é uma base integral para o corpo $\mathbb{K}$ se, e somente se, é uma base p -integral do corpo $\mathbb{K}$, para todo $p \in \mathbb{Z}$ primo.*

Demonstração. Considere $\mathcal{B} = \{\omega_1, \dots, \omega_n\}$ uma base integral para o corpo $\mathbb{K}$. Pelo Corolário 4.14, segue que para qualquer $p \in \mathbb{Z}$ primo, $\mathcal{B}$ é uma base formada por elementos p -integrais do corpo $\mathbb{K}$. Seja $\alpha \in \mathbb{K}$ um elemento p -integral. Pelo Lema 4.11, segue que α pode ser escrito como $\frac{\gamma}{d}$, com $\gamma \in \mathcal{O}_{\mathbb{K}}$, $d \in \mathbb{Z}$, $d \neq 0$ e $p \nmid d$. Assim, existem $b_1, \dots, b_n \in \mathbb{Z}$ tais que $\gamma = b_1\omega_1 + \dots + b_n\omega_n$ e $\alpha = \frac{b_1}{d}\omega_1 + \dots + \frac{b_n}{d}\omega_n$, com $b_1, \dots, b_n, d \in \mathbb{Z}$, $d \neq 0$ e $p \nmid d$.

Como $p \nmid d$, pela Proposição 4.10, segue que para todo $i = 1, \dots, n$, $a_i = \frac{b_i}{d}$ é um elemento p -integral de $\mathbb{Q}$. Portanto, $\mathcal{B} = \{\omega_1, \dots, \omega_n\}$ é uma base p -integral do corpo $\mathbb{K}$, para todo $p \in \mathbb{Z}$ primo. Reciprocamente, se para todo $p \in \mathbb{Z}$ primo tivermos $\mathcal{B} = \{\omega_1, \dots, \omega_n\}$ uma base p -integral do corpo $\mathbb{K}$, então pelo Teorema 4.12, cada ω_i , com $i = 1, \dots, n$, é raiz de um polinômio mônico com coeficientes que são elementos p -integrais de $\mathbb{Q}$. Assim, os coeficientes destes polinômios mônicos são elementos integrais do corpo $\mathbb{K}$. Além disso, seja $\alpha \in \mathcal{O}_{\mathbb{K}}$, então α é um elemento p -integral do corpo $\mathbb{K}$, para todo $p \in \mathbb{Z}$ primo, e pode ser escrito como $a_1\omega_1 + \dots + a_n\omega_n$, com $a_0, \dots, a_n$ elementos p -integrais de $\mathbb{Q}$, para todo $p \in \mathbb{Z}$ primo. Logo, pela Proposição 4.9, segue que $a_0, \dots, a_n \in \mathbb{Z}$, ou seja, $\{\omega_1, \dots, \omega_n\}$ é uma base integral para o corpo $\mathbb{K}$. $\square$

Exemplo 4.21. Considere o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{7})$. Uma vez que $7 \not\equiv 1 \pmod{4}$, segue que $\{1, \sqrt{7}\}$ é uma base integral para o corpo $\mathbb{K}$. Vamos mostrar que para todo primo $p \in \mathbb{Z}$, $\{1, \sqrt{7}\}$ é uma base p -integral do corpo $\mathbb{K}$. Como $1, \sqrt{7} \in \mathcal{O}_{\mathbb{K}}$, segue que são elementos 1 e $\sqrt{7}$ são p -integrais, para todo $p \in \mathbb{Z}$ primo. Seja $\alpha \in \mathbb{K}$ um elemento p -integral. Assim, pelo Lema 4.11, segue que podemos escrever α como $\frac{\gamma}{d}$, com $\gamma \in \mathcal{O}_{\mathbb{K}}$, $d \in \mathbb{Z}$, $d \neq 0$ e $p \nmid d$. Agora,

$$\gamma \in \mathcal{O}_{\mathbb{K}} \Rightarrow \gamma = a + b\sqrt{7}, \text{ com } a, b \in \mathbb{Z}.$$

Dessa forma, $\alpha = \frac{a}{d} + \frac{b}{d}\sqrt{7}$, com $a, b, d \in \mathbb{Z}$, $d \neq 0$ e $p \nmid d$. Como $p \nmid d$, pela Proposição 4.10, segue que os coeficientes $\frac{a}{d}$ e $\frac{b}{d}$ são elementos p -integrais de $\mathbb{Q}$. Logo, $\{1, \sqrt{7}\}$ é uma base p -integral do corpo $\mathbb{K}$, para qualquer que seja $p \in \mathbb{Z}$ primo.

Teorema 4.22. (Teorema do divisor discriminante) *Sejam $\mathbb{K}$ um corpo de números de grau n e $p \in \mathbb{K}$ um número primo. Se $\{\omega_1, \dots, \omega_n\}$ do corpo $\mathbb{K}$ é uma base p -integral, então $v_p(D(\mathbb{K})) = v_p(D(\omega_1, \dots, \omega_n))$.*

Demonstração. Seja $\{\mu_1, \dots, \mu_n\}$ uma base integral para o corpo $\mathbb{K}$. Assim, $D(\mathbb{K}) = D(\mu_1, \dots, \mu_n)$, ou seja, $v_p(D(\mathbb{K})) = v_p(D(\mu_1, \dots, \mu_n))$. Pelo Teorema 4.20, segue que $\{\mu_1, \dots, \mu_n\}$ é uma base p -integral do corpo $\mathbb{K}$. Assim, dada $\{\omega_1, \dots, \omega_n\}$ uma base p -integral do corpo $\mathbb{K}$, pela Proposição 4.19, segue que $v_p(D(\omega_1, \dots, \omega_n)) = v_p(D(\mu_1, \dots, \mu_n)) = v_p(D(\mathbb{K}))$. $\square$

Lema 4.23. *Sejam $\mathbb{K}$ um corpo de números de grau n , $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $p \in \mathbb{Z}$ primo e $i \in \mathbb{Z}$, com $1 \leq i \leq n-1$. Se $x_0, x_1, \dots, x_{i-1}, j \in \mathbb{Z}$ são tais que*

$$x = \frac{x_0 + x_1\theta + \dots + x_{i-1}\theta^{i-1} + \theta^i}{p^j}$$

é um elemento p -integral do corpo $\mathbb{K}$, então $j \leq \frac{1}{2}(v_p(D(\theta)) - v_p(D(\mathbb{K})))$.

Demonstração. Como $\theta \in \mathcal{O}_{\mathbb{K}}$, segue que os elementos

$$1, \theta, \theta^2, \dots, \theta^{i-1}, x = \frac{x_0 + x_1\theta + \dots + x_{i-1}\theta^{i-1} + \theta^i}{p^j}, \theta^{i+1}, \dots, \theta^{n-1}$$

são p -integrais. Logo, formam um conjunto de n elementos p -integrais do corpo $\mathbb{K}$. Seja $\{\omega_1, \dots, \omega_n\}$ uma base p -integral do corpo $\mathbb{K}$. Pelo Lema 4.18, segue que

$$\begin{aligned} & v_p(D(1, \theta, \theta^2, \dots, \theta^{i-1}, x, \theta^{i+1}, \dots, \theta^{n-1})) \\ &= v_p\left(D\left(1, \theta, \theta^2, \dots, \theta^{i-1}, \frac{x_0 + x_1\theta + \dots + x_{i-1}\theta^{i-1} + \theta^i}{p^j}, \theta^{i+1}, \dots, \theta^{n-1}\right)\right) \\ &\geq v_p(D(\omega_1, \dots, \omega_n)) = v_p(D(\mathbb{K})) \\ &\Rightarrow v_p\left(\frac{D(\theta)}{p^{2j}}\right) \geq v_p(D(\mathbb{K})) \\ &\Rightarrow v_p(D(\theta)) - 2j \geq v_p(D(\mathbb{K})), \end{aligned}$$

e assim,

$$2j \leq v_p(D(\theta)) - v_p(D(\mathbb{K})) \Rightarrow j \leq \frac{1}{2}(v_p(D(\theta)) - v_p(D(\mathbb{K}))),$$

o que prova o lema. $\square$

Lema 4.24. *Sejam $\mathbb{K}$ um corpo de números de grau n , $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $p \in \mathbb{Z}$ um número primo. Se*

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{d_1}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{d_2}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + \theta^{n-1}}{d_{n-1}} \right\}$$

é uma base integral do corpo $\mathbb{K}$ formada por inteiros mínimos, então

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{m_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{m_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + \theta^{n-1}}{p^{m_{n-1}}} \right\}$$

é uma base p -integral do corpo $\mathbb{K}$, com $p^{m_i} | d_i$ e $p^{m_i+1} \nmid d_i$, para todo $i \in \{1, \dots, n-1\}$, $m_1 \leq m_2 \leq \dots \leq m_{n-1}$ e $v_p(\text{ind}(\theta)) = m_1 + m_2 + \dots + m_{n-1}$.

Demonstração. Para facilitar a notação, para cada $i \in \{1, \dots, n-1\}$, considere

$$x^{(i)} = x_0^{(i)} + x_1^{(i)}\theta + \dots + x_{i-1}^{(i)}\theta^{i-1} + \theta^i.$$

Como $\left\{ 1, \frac{x^{(1)}}{d_1}, \frac{x^{(2)}}{d_2}, \dots, \frac{x^{(n-1)}}{d_{n-1}} \right\}$ é uma base integral para o corpo $\mathbb{K}$ formada por inteiros mínimos, segue que também é uma base p -integral do corpo $\mathbb{K}$. Para cada $i \in \{1, \dots, n-1\}$, considere $v_p(d_i) = m_i$, ou seja, $d_i = p^{m_i}q_i$, com $p \nmid q_i$. Dessa forma, para cada $i \in \{1, \dots, n-1\}$, segue que

$$\frac{x^{(i)}}{d_i} = \frac{x^{(i)}}{p^{m_i}q_i} = \frac{1}{q_i} \cdot \frac{x^{(i)}}{p^{m_i}}.$$

Note que, como $p \nmid q_i$, pela Proposição 4.10, segue que $\frac{1}{q_i}$ é um elemento p -integral de $\mathbb{Q}$. Logo, $\left\{ 1, \frac{x^{(1)}}{p^{m_1}}, \dots, \frac{x^{(n-1)}}{p^{m_{n-1}}} \right\}$ é uma base p -integral do corpo $\mathbb{K}$. Além disso, pelo Teorema 3.40, sabemos que $d_{i-1} | d_i$, para todo $i = 1, \dots, n-1$. Portanto, para todo $i \in \{1, \dots, n-1\}$, segue que

$$p^{m_{i-1}}q_{i-1} \mid p^{m_i}q_i \Rightarrow m_i \geq m_{i-1},$$

ou seja, $m_1 \leq m_2 \leq \dots \leq m_{n-1}$. Por fim, como $\text{ind}(\theta) = d_1 d_2 \dots d_{n-1}$, segue que

$$v_p(\text{ind}(\theta)) = v_p(d_1 d_2 \dots d_{n-1}) = v_p(d_1) + v_p(d_2) + \dots + v_p(d_{n-1}) = m_1 + m_2 + \dots + m_{n-1},$$

o que prova o lema. $\square$

Teorema 4.25. *Sejam $\mathbb{K}$ um corpo de números de grau n , $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $p \in \mathbb{Z}$ um número primo. Para cada $i \in \{1, 2, \dots, n-1\}$, seja k_i o maior inteiro para o qual existem $x_0^{(i)}, x_1^{(i)}, \dots, x_{i-1}^{(i)} \in \mathbb{Z}$ tais que*

$$x = \frac{x_0^{(i)} + x_1^{(i)}\theta + \dots + x_{i-1}^{(i)}\theta^{i-1} + \theta^i}{p^{k_i}}$$

é p -integral.

$$1. 0 \leq k_1 \leq k_2 \leq \dots \leq k_{n-1};$$

$$2. \left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-1} + \theta^{n-1}}{p^{k_{n-1}}} \right\} \text{ é uma base } p\text{-integral do corpo } \mathbb{K};$$

$$3. v_p(D(\mathbb{K})) = v_p(D(\theta)) - 2(k_1 + k_2 + \dots + k_{n-1}).$$

Demonstração. Primeiramente, note que para todo $i \in \{1, 2, \dots, n-1\}$ o inteiro k_i existe, é não negativo e, pelo Lema 4.23, segue que $k_i \leq \frac{1}{2}(v_p(D(\theta)) - v_p(D(\mathbb{K})))$. Para o item (1), considere

$$\left\{ 1, \frac{y_0^{(1)} + \theta}{d_1}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{d_{n-1}} \right\}$$

uma base integral para o corpo $\mathbb{K}$ formada por inteiros mínimos do corpo $\mathbb{K}$. Pelo Lema 4.24, segue que $\mathbb{K}$ tem uma base p -integral da forma

$$\left\{ 1, \frac{y_0^{(1)} + \theta}{p^{m_1}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{m_{n-1}}} \right\}$$

com $m_1, \dots, m_{n-1} \in \mathbb{Z}$ tais que

$$\begin{cases} p^{m_i} \mid d_i, \quad i = 1, \dots, n-1; \\ p^{m_i+1} \nmid d_i, \quad i = 1, \dots, n-1; \\ m_1 \leq m_2 \leq \dots \leq m_{n-1} \end{cases}$$

e $v_p(\text{ind}(\theta)) = m_1 + m_2 + \dots + m_{n-1}$. Pela maximalidade de k_i , segue que $k_i \geq m_i$, para todo $i \in \{1, 2, \dots, n-1\}$. Assim, $k_1 + \dots + k_{n-1} \geq m_1 + \dots + m_{n-1}$. Por outro lado, uma vez que

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-1} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

é um conjunto formado por n elementos p -integrais do corpo $\mathbb{K}$, pelo Lema 4.18, segue que

$$\begin{aligned} & v_p \left(D \left(1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-1} + \theta^{n-1}}{p^{k_{n-1}}} \right) \right) \\ & \geq v_p \left(D \left(1, \frac{y_0^{(1)} + \theta}{p^{m_1}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{m_{n-1}}} \right) \right) \\ & \Rightarrow v_p \left(\frac{D(\theta)}{p^{2(k_1 + \dots + k_{n-1})}} \right) \geq v_p \left(\frac{D(\theta)}{p^{2(m_1 + \dots + m_{n-1})}} \right) \\ & \Rightarrow v_p(D(\theta)) - 2(k_1 + \dots + k_{n-1}) \geq v_p(D(\theta)) - 2(m_1 + \dots + m_{n-1}) \\ & \Rightarrow k_1 + \dots + k_{n-1} \leq m_1 + \dots + m_{n-1}. \end{aligned}$$

Portanto, $k_1 + \dots + k_{n-1} = m_1 + \dots + m_{n-1}$ e concluímos que $m_i = k_i$, para todo $i \in \{1, 2, \dots, n-1\}$. Logo, $k_1 \leq k_2 \leq \dots \leq k_{n-1}$. Para o item (2), como $\frac{x_0^{(1)} + \theta}{p^{k_1}}$ e $\frac{y_0^{(1)} + \theta}{p^{k_1}}$ são elementos p -integrais do corpo $\mathbb{K}$, segue que

$$\frac{y_0^{(1)} + \theta}{p^{k_1}} - \frac{x_0^{(1)} + \theta}{p^{k_1}} = \frac{y_0^{(1)} - x_0^{(1)}}{p^{k_1}}$$

também é um elemento p -integral do corpo $\mathbb{K}$. Como $y_0^{(1)}, x_0^{(1)} \in \mathbb{Z}$, segue que

$$\begin{aligned} p^{k_1} &\mid y_0^{(1)} - x_0^{(1)} \\ \Rightarrow y_0^{(1)} &\equiv x_0^{(1)} \pmod{p^{k_1}} \\ \Rightarrow y_0^{(1)} &= x_0^{(1)} + p^{k_1} \cdot l, \text{ para algum } l \in \mathbb{Z} \\ \Rightarrow \frac{y_0^{(1)} + \theta}{p^{k_1}} &= \frac{x_0^{(1)} + \theta}{p^{k_1}} + l. \end{aligned}$$

Dessa forma, o conjunto

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{m_2}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{m_{n-1}}} \right\}$$

é uma base p -integral do corpo $\mathbb{K}$. Agora, como $\frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}$ e $\frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{k_2}}$ são elementos p -integrais do corpo $\mathbb{K}$, então

$$\frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{k_2}} - \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}} = \frac{(y_0^{(2)} - x_0^{(2)}) + (y_1^{(2)} - x_1^{(2)})\theta}{p^{k_2}}$$

também é um elemento p -integral do corpo $\mathbb{K}$. Assim, existem $a_0, a_1 \in \mathbb{Q}$ elementos p -integrais de $\mathbb{Q}$, tais que

$$\begin{aligned} \frac{(y_0^{(2)} - x_0^{(2)}) + (y_1^{(2)} - x_1^{(2)})\theta}{p^{k_2}} &= a_0 \cdot 1 + a_1 \cdot \left(\frac{x_0^{(1)} + \theta}{p^{k_1}} \right) \\ \Rightarrow (y_0^{(2)} - x_0^{(2)}) + (y_1^{(2)} - x_1^{(2)})\theta &= a_0 p^{k_2} + a_1 p^{k_2-k_1} (x_0^{(1)} + \theta) \\ \Rightarrow y_0^{(2)} + y_1^{(2)}\theta &= (a_0 p^{k_2} + x_0^{(2)} + a_1 p^{k_2-k_1} x_0^{(1)}) + (a_1 p^{k_2-k_1} + x_1^{(2)})\theta \\ \Rightarrow \begin{cases} y_0^{(2)} = x_0^{(2)} + p^{k_2} a_0 + p^{k_2-k_1} a_1 x_0^{(1)} \\ y_1^{(2)} = x_1^{(2)} + p^{k_2-k_1} a_1 \end{cases} \end{aligned}$$

e, dessa forma,

$$\begin{aligned} \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{k_2}} &= \frac{x_0^{(2)} + p^{k_2} a_0 + p^{k_2-k_1} a_1 x_0^{(1)} + (x_1^{(2)} + p^{k_2-k_1} a_1)\theta + \theta^2}{p^{k_2}} \\ &= \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}} + a_0 + a_1 \left(\frac{x_0^{(1)} + \theta}{p^{k_1}} \right). \end{aligned}$$

Portanto, o conjunto

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \frac{y_0^{(3)} + y_1^{(3)}\theta + y_2^{(3)}\theta^2 + \theta^3}{p^{m_3}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{m_{n-1}}} \right\}$$

é uma base p -integral do corpo $\mathbb{K}$. Repetindo esse processo, concluímos que

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

é uma base p -integral do corpo $\mathbb{K}$. Por fim, para o item (3), uma vez que

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

é uma base p -integral para o corpo $\mathbb{K}$ (pois $k_i = m_i$, para todo $i = 1, \dots, n-1$), segue que

$$D(\mathbb{K}) = \frac{D(\theta)}{p^{2(k_1 + \dots + k_{n-1})}} \Rightarrow v_p(D(\mathbb{K})) = v_p(D(\theta)) - 2(k_1 + \dots + k_{n-1}),$$

o que prova o teorema. $\square$

Corolário 4.26. *Seja $\mathbb{K}$ um corpo de números de grau n , $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $p \in \mathbb{Z}$ um número primo. Se, para algum $i \in \{1, 2, \dots, n-1\}$, tivermos que*

$$\frac{x_0^{(i)} + x_1^{(i)}\theta + \dots + x_{i-1}^{(i)}\theta^{i-1} + \theta^i}{p}$$

não é um elemento p -integral do corpo $\mathbb{K}$, para todo $x_j^{(i)} \in \mathbb{Z}$, com $j \in \{0, 1, \dots, i-1\}$ então

$$\frac{y_0^{(l)} + y_1^{(l)}\theta + \dots + y_{l-1}^{(l)}\theta^{l-1} + \theta^k}{p}$$

não é um elemento p -integral do corpo $\mathbb{K}$, para todo $x_j^{(i)} \in \mathbb{Z}$, com $j \in \{0, 1, \dots, l-1\}$ e $l \in \{0, 1, \dots, i-1\}$.

Demonstração. Segue do item (1) do Teorema 4.25, pois como $k_1 \leq \dots \leq k_{n-1}$, com cada k_i , onde $i \in \{0, 1, \dots, n-1\}$ sendo a potência de p no denominador do elemento, segue que se $k_i = 0$, para algum $i \in \{0, 1, \dots, n-1\}$, então $k_0 = k_1 = \dots = k_{i-1} = k_i = 0$. $\square$

Teorema 4.27. *Sejam $\mathbb{K}$ um corpo de números de grau n , $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $p, q \in \mathbb{Z}$ dois primos distintos. Sejam*

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \dots, \frac{x_0^{(n-1)} + \dots + x_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

uma base p -integral do corpo $\mathbb{K}$ e

$$\left\{ 1, \frac{y_0^{(1)} + \theta}{q^{l_1}}, \dots, \frac{y_0^{(n-1)} + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{q^{l_{n-1}}} \right\}$$

uma base q -integral do corpo $\mathbb{K}$. Defina $X_i^{(j)} \in \mathbb{Z}$, com $i \in \{0, 1, \dots, j-1\}$ e $j \in \{1, 2, \dots, n-1\}$ por

$$\begin{cases} X_i^{(j)} \equiv x_i^{(j)} \pmod{p^{k_j}} \\ X_i^{(j)} \equiv y_i^{(j)} \pmod{q^{l_j}}. \end{cases}$$

Assim,

$$\mathcal{B} = \left\{ 1, \frac{X_0^{(1)} + \theta}{p^{k_1} q^{l_1}}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{p^{k_2} q^{l_2}}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \dots + X_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}} q^{l_{n-1}}} \right\}$$

é uma base p -integral e q -integral do corpo $\mathbb{K}$.

Demonstração. Para cada $j \in \{1, 2, \dots, n-1\}$, segue que

$$X_i^{(j)} \equiv x_i^{(j)} \pmod{p^{k_j}}, \text{ para todo } i \in \{0, 1, \dots, j-1\}.$$

Dessa forma, existem $t_i^{(j)} \in \mathbb{Z}$ tais que $X_i^{(j)} = x_i^{(j)} + p^{k_j} t_i^{(j)}$. Como $p \neq q$, segue que $v_p(p^{k_j} q^{l_j}) = k_j$, para todo $j \in \{1, 2, \dots, n\}$, ou seja, $\mathcal{B}$ é uma base p -integral do corpo $\mathbb{K}$ se, e somente se,

$$\left\{ 1, \frac{X_0^{(1)} + \theta}{p^{k_1}}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \dots + X_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

é uma base p -integral do corpo $\mathbb{K}$. Note que, para cada $j \in \{1, 2, \dots, n-1\}$, segue que

$$\begin{aligned} & \frac{X_0^{(j)} + X_1^{(j)}\theta + \dots + X_{j-1}^{(j)}\theta^{j-1} + \theta^j}{p^{k_{n-1}}} \\ &= \frac{(x_0^{(j)} + p^{k_j} t_0^{(j)}) + (x_1^{(j)} + p^{k_j} t_1^{(j)})\theta + \dots + (x_{j-1}^{(j)} + p^{k_j} t_{j-1}^{(j)})\theta^{j-1} + \theta^j}{p^{k_{n-1}}} \\ &= \left(\frac{x_0^{(j)} + x_1^{(j)}\theta + \dots + x_{j-1}^{(j)}\theta^{j-1} + \theta^j}{p^{k_j}} \right) + (t_0^{(j)} + t_1^{(j)} + \dots + t_{j-1}^{(j)}). \end{aligned}$$

Portanto,

$$\left\{ 1, \frac{X_0^{(1)} + \theta}{p^{k_1}}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \dots + X_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

é uma base p -integral do corpo $\mathbb{K}$. Logo, $\mathcal{B}$ é uma base p -integral do corpo $\mathbb{K}$. De maneira análoga, mostra-se que $\mathcal{B}$ também é uma base q -integral do corpo $\mathbb{K}$. $\square$

O Teorema 4.27 pode ser estendido para um número finito de primos distintos, e assim, fornece uma ferramenta para encontrar bases integrais para um corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$ a partir de bases p -integrais, com $p \in \mathbb{Z}$ primo. Se um número primo p não divide $\text{ind}(\theta)$, então $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ é uma base p -integral do corpo $\mathbb{K}$. Agora, suponha que p divide $\text{ind}(\theta)$. Neste caso, o Teorema 4.25 garante a existência de uma base p -integral do corpo $\mathbb{K}$. O próximo teorema fornece essa generalização.

Teorema 4.28. *Sejam $\mathbb{K}$ um corpo de números de grau n , $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $p_1, p_2, \dots, p_s \in \mathbb{Z}$ todos os primos, distintos dois a dois, que dividem $\text{ind}(\theta)$. Se $r \in \{1, 2, \dots, s\}$, então*

$$\left\{ 1, \frac{x_{r_0}^{(1)} + \theta}{p_r^{k_{r_1}}}, \frac{x_{r_0}^{(2)} + x_{r_1}^{(2)}\theta + \theta^2}{p_r^{k_{r_2}}}, \dots, \frac{x_{r_0}^{(n-1)} + x_{r_1}^{(n-1)}\theta + \dots + x_{r_{n-2}}^{(n-1)}\theta^{n-1} + \theta^{n-2}}{p_r^{k_{r_{n-1}}}} \right\}$$

é uma base p_r -integral do corpo $\mathbb{K}$. Para cada $j \in \{1, 2, \dots, n-1\}$ e $i \in \{0, 1, \dots, j-1\}$, define $X_i^{(j)}$ por

$$X_i^{(j)} \equiv x_{r_i}^{(j)} \pmod{p_r^{k_{r_j}}}, \text{ com } r \in \{1, 2, \dots, s\}$$

e considere

$$T_j = \prod_{r=1}^s p_r^{k_{r_j}}, \text{ com } j \in \{1, 2, \dots, n-1\}.$$

Assim,

$$\left\{ 1, \frac{X_0^{(1)} + \theta}{T_1}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{T_2}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \dots + X_{n-2}^{(n-1)}\theta^{n-1} + \theta^{n-1}}{T_{n-1}} \right\}$$

é uma base integral para o corpo $\mathbb{K}$.

Demonstração. É suficiente repetir o processo feito na demonstração do Teorema 4.27. $\square$

5 Bases p -integrais de um corpo cúbico

Neste capítulo, iremos encontrar bases p -integrais para um corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$ e $p \in \mathbb{Z}$ primo. Nosso objetivo é que, a partir das bases p -integrais, utilizando o Teorema 4.28, nós encontremos uma base integral para o corpo $\mathbb{K}$. Na seção 5.1, veremos algumas condições para que um elemento do corpo $\mathbb{K}$ seja p -integral. Esses resultados irão ser usados nas Seções 5.2, 5.3 e 5.4, onde encontramos bases 2, 3 e p -integrais, com $p > 3$, para o corpo $\mathbb{K}$, respectivamente. Na seção 5.5 avaliamos o discriminante do corpo $\mathbb{K}$ e, finalmente, na seção 5.6, explicitamos uma base integral para o corpo $\mathbb{K}$ e finalizamos encontrando uma base integral para um corpo cúbico puro.

5.1 Propriedades de elementos p -integrais em um corpo cúbico

Considere o polinômio mônico irreduzível $f(t) = t^3 - at + b$, com $a, b \in \mathbb{Z}$, θ uma raiz de f e $\mathbb{K} = \mathbb{Q}(\theta)$. Uma vez que $\theta \in \mathcal{O}_{\mathbb{K}}$, segue que $v_p(\theta) \geq 0$, para todo número primo $p \in \mathbb{Z}$. Se tivermos, para um primo $p \in \mathbb{Z}$, que $v_p(a) \geq 2$ e $v_p(b) \geq 3$, então $\frac{a}{p^2}, \frac{b}{p^3} \in \mathbb{Z}$, o polinômio $g(t) = t^3 - \frac{a}{p^2}t + \frac{b}{p^3}$ é mônico com coeficientes em $\mathbb{Z}$ e

$$g\left(\frac{\theta}{p}\right) = \left(\frac{\theta}{p}\right)^3 - \left(\frac{a}{p^2}\right)\left(\frac{\theta}{p}\right) + \frac{b}{p^3} = \frac{\theta^3 - a\theta + b}{p^3} = \frac{f(\theta)}{p^3} = 0,$$

ou seja, $\frac{\theta}{p} \in \mathcal{O}_{\mathbb{K}}$.

Com isso, podemos considerar $v_p(a) < 2$ ou $v_p(b) < 3$, para todo número primo $p \in \mathbb{Z}$. Além disso, o discriminante de θ , ou de $f(t)$, é

$$\Delta = D(\theta) = 4a^3 - 27b^2 \neq 0 \text{ e } \Delta = \text{ind}(\theta)^2 D(\mathbb{K}).$$

Para cada primo $p \in \mathbb{Z}$, vamos definir

$$s_p = v_p(\Delta) \text{ e } \Delta_p = \frac{\Delta}{p^{s_p}}. \quad (5.1)$$

Além disso, $p \nmid \Delta_p$.

Nesta seção, apresentamos alguns resultados importantes sobre elementos p -inteiros de um corpo cúbico da forma $\mathbb{K} = \mathbb{Q}(\theta)$. Esses resultados serão muito utilizados para encontrar bases p -inteiros para o corpo $\mathbb{K}$, e conseqüentemente, para encontrar bases inteiros.

O próximo teorema fornece uma condição necessária e suficiente para que um elemento $\alpha \in \mathbb{K}$ seja um elemento p -integral.

Teorema 5.1. *Sejam $p \in \mathbb{Z}$ um número primo, $f(t) = t^3 - at + b$, com $a, b \in \mathbb{Z}$, $v_p(a) < 2$ ou $v_p(b) < 3$, θ uma raiz de $f(t)$ e $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico. Seja $\alpha = \frac{x + y\theta + z\theta^2}{p^m}$, com $x, y, z, m \in \mathbb{Z}$ e $m \geq 0$, considere*

$$\begin{cases} X = 3x + 2az, \\ Y = 3x^2 + 4axz - ay^2 + a^2z^2 + 3byz, \\ Z = x^3 + 2ax^2z - axy^2 + 3bxyz + a^2xz^2 - by^3 + b^2z^3 + aby^2z. \end{cases}$$

Assim, α é um elemento p -integral do corpo $\mathbb{K}$ se, e somente se,

$$X \equiv 0 \pmod{p^m}, Y \equiv 0 \pmod{p^{2m}} \text{ e } Z \equiv 0 \pmod{p^{3m}}.$$

Demonstração. Considere $\alpha = \alpha_1, \alpha_2$ e α_3 os conjugados de α com respeito à $\mathbb{K}$. Pelo Teorema 4.12, segue que α é um elemento p -integral do corpo $\mathbb{K}$ se, e somente se, $\alpha_1 + \alpha_2 + \alpha_3$, $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$ e $\alpha_1\alpha_2\alpha_3$ são elementos p -inteiros de $\mathbb{Q}$. Portanto, para mostrar o que queremos, basta mostrar que

$$\alpha_1 + \alpha_2 + \alpha_3 = \frac{X}{p^m}, \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \frac{Y}{p^{2m}} \text{ e } \alpha_1\alpha_2\alpha_3 = \frac{Z}{p^{3m}},$$

pois, se isso ocorre, então α é um elemento p -integral do corpo $\mathbb{K}$ se, e somente se,

$$\frac{X}{p^m}, \frac{Y}{p^{2m}} \text{ e } \frac{Z}{p^{3m}} \text{ são } p\text{-inteiros de } \mathbb{K} \Leftrightarrow$$

$$X \equiv 0 \pmod{p^m}, Y \equiv 0 \pmod{p^{2m}} \text{ e } Z \equiv 0 \pmod{p^{3m}}.$$

Sejam $\theta = \theta_1, \theta_2, \theta_3$ as raízes de $f(t) = t^3 - at + b$. Logo,

$$\begin{cases} \theta_1 + \theta_2 + \theta_3 = 0, \\ \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = -a, \\ \theta_1\theta_2\theta_3 = -b. \end{cases}$$

Assim,

$$\theta_1^2 + \theta_2^2 + \theta_3^2 = (\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3) = 2a,$$

$$\theta_1^2\theta_2^2 + \theta_1^2\theta_3^2 + \theta_2^2\theta_3^2 = (\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3)^2 - 2\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3) = a^2,$$

$$\begin{aligned} \theta_1\theta_2^2 + \theta_1^2\theta_2 + \theta_1\theta_3^2 + \theta_1^2\theta_3 + \theta_2\theta_3^2 + \theta_2^2\theta_3 &= \theta_1\theta_2(\theta_2 + \theta_1) + \theta_1\theta_3(\theta_3 + \theta_1) + \theta_2\theta_3(\theta_3 + \theta_2) \\ &= -3\theta_1\theta_2\theta_3 = 3b. \end{aligned}$$

Agora, uma vez que $\alpha = \alpha_1, \alpha_2$ e α_3 são conjugados de α com respeito à $\mathbb{K}$, segue que

$$\alpha = \alpha_1 = \frac{x + y\theta_1 + z\theta_1^2}{p^m}, \alpha_2 = \frac{x + y\theta_2 + z\theta_2^2}{p^m} \text{ e } \alpha_3 = \frac{x + y\theta_3 + z\theta_3^2}{p^m}.$$

Dessa forma,

- $\alpha_1 + \alpha_2 + \alpha_3 = \frac{1}{p^m} [3x + y(\theta_1 + \theta_2 + \theta_3) + z(\theta_1^2 + \theta_2^2 + \theta_3^2)] = \frac{1}{p^p} (3x + 2az) = \frac{X}{p^m},$
- $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \frac{1}{p^{2m}} [3x^2 + 2xy(\theta_1 + \theta_2 + \theta_3) + 2xy(\theta_1^2 + \theta_2^2 + \theta_3^2) + y^2(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3) + yz(\theta_1\theta_2^2 + \theta_1^2\theta_2 + \theta_1\theta_3^2 + \theta_1^2\theta_3 + \theta_2\theta_3^2 + \theta_2^2\theta_3) + z^2(\theta_1^2\theta_2^2 + \theta_1^2\theta_3^2 + \theta_2^2\theta_3^2)]$
 $= \frac{1}{p^{2m}} [3x^2 + 2xy(\theta_1 + \theta_2 + \theta_3) + 2xz(\theta_1^2 + \theta_2^2 + \theta_3^2) + y^2(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3) + yz(\theta_1\theta_2^2 + \theta_1^2\theta_2 + \theta_1\theta_3^2 + \theta_1^2\theta_3 + \theta_2\theta_3^2 + \theta_2^2\theta_3) + z^2(\theta_1^2\theta_2^2 + \theta_1^2\theta_3^2 + \theta_2^2\theta_3^2)]$
 $= \frac{1}{p^{2m}} (3x^2 + 4axz - ay^2 + 3byz + a^2z^2) = \frac{Y}{p^{2m}},$
- $\alpha_1\alpha_2\alpha_3 = \frac{1}{p^{3m}} [x^3 + x^2y(\theta_1 + \theta_2 + \theta_3) + x^2z(\theta_1^2 + \theta_2^2 + \theta_3^2) + xy^2(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3) + xyz(\theta_1\theta_2^2 + \theta_1^2\theta_2 + \theta_1\theta_3^2 + \theta_1^2\theta_3 + \theta_2\theta_3^2 + \theta_2^2\theta_3) + xz^2(\theta_1^2\theta_2^2 + \theta_1^2\theta_3^2 + \theta_2^2\theta_3^2) + y^3\theta_1\theta_2\theta_3 + y^2z\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3) + yz^2\theta_1\theta_2\theta_3(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3) + z^3\theta_1^2\theta_2^2\theta_3^2]$
 $= \frac{1}{p^{3m}} (x^3 + 2ax^2z - axy^2 + 3bxyz + a^2xz^2 - by^3 + aby^2z + b^2z^3) = \frac{Z}{p^{3m}},$

o que completa a demonstração. $\square$

O próximo teorema fornece uma outra representação para os inteiros Y e Z , definidos no Teorema 5.1.

Teorema 5.2. *Sejam $p \in \mathbb{Z}$ um número primo, $f(t) = t^3 - at + b$, com $a, b \in \mathbb{Z}$, $v_p(a) < 2$ ou $v_p(b) < 3$, θ uma raiz de $f(t)$ e $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico. Sejam*

$$\begin{cases} X = 3x + 2az \\ Y = 3x^2 + 4axz - ay^2 + a^2z^2 + 3byz \\ Z = x^3 + 2ax^2z - axy^2 + 3bxyz + a^2xz^2 - by^3 + b^2z^3 + aby^2z \end{cases}$$

como definidos no Teorema 5.1. Se $U = 9by - 2a^2z$ e $V = 2ay - 3bz$, então

$$\begin{aligned} Y &= \frac{1}{2^2 3 a^2} (2^2 a^2 X^2 - U^2 - 3 \Delta y^2) \quad e \\ Z &= \frac{1}{2^2 3^3 a^3} (2^2 a^3 X^3 - 3aXU^2 - 3^2 a \Delta X y^2 - 3U^3 - 3^2 \Delta U y^2 + 2a \Delta U z^2 \\ &\quad + 3^3 b V^3 + 2 \cdot 3^2 b \Delta V z^2 + \Delta^2 z^3), \end{aligned}$$

com $\Delta = D(\theta) = 4a^3 - 27b^2$.

Demonstração.

$$\begin{aligned} &\bullet \frac{1}{2^2 3 a^2} (2^2 a^2 X^2 - U^2 - 3 \Delta y^2) \\ &= \frac{1}{2^2 3 a^2} [2^2 a^2 (3x + 2az)^2 - (9by - 2a^2z)^2 - 3(4a^3 - 27b^2)y^2] \\ &= \frac{1}{2^2 3 a^2} [2^2 a^2 (3^2 x^2 + 2^2 3axz + 2^2 a^2 z^2) - (3^4 b^2 y^2 - 2^2 3^2 a^2 byz + 2^2 a^4 z^2) - 2^2 3a^3 y^2 + 3^4 b^2 y^2] \\ &= \frac{1}{2^2 3 a^2} (2^2 3^2 a^2 x^2 + 2^4 3a^3 xz + 2^4 a^4 z^2 - 3^4 b^2 y^2 + 2^2 3^2 a^2 byz - 2^2 a^4 z^2 - 2^2 3a^3 y^2 + 3^4 b^2 y^2) \\ &= 3x^2 + 4axz + a^2z^2 + 3byz - ay^2 = Y, \end{aligned}$$

e portanto, $Y = \frac{1}{2^2 3 a^2} (2^2 a^2 X^2 - U^2 - 3 \Delta y^2)$ e

$$\begin{aligned}
& \bullet \frac{1}{2^2 3^3 a^3} (2^2 a^3 X^3 - 3aXU^2 - 3^2 a \Delta X y^2 - 3U^3 - 3^2 \Delta U y^2 + 2a \Delta U z^2 + 3^3 b V^3 \\
& \quad + 2 \cdot 3^2 b \Delta V z^2 + \Delta^2 z^3) \\
&= \frac{1}{2^2 3^3 a^3} [2^2 a^3 (3x + 2az)^3 - 3a(3x + 2az)(9by - 2a^2 z)^2 - 3^2 a(4a^3 - 27b^2)(3x + 2az)y^2 \\
& \quad - 3(9by - 2a^2 z)^3 - 3^2(4a^3 - 27b^2)(9by - 2a^2 z)y^2 + 2a(4a^3 - 27b^2)(9by - 2a^2 z)z^2 \\
& \quad + 3^3 b(2ay - 3bz)^3 + 2 \cdot 3^2 b(4a^3 - 27b^2)(2ay - 3bz)z^2 + (4a^3 - 27b^2)^2 z^3] \\
&= \frac{1}{2^2 3^3 a^3} [2^2 a^3 (2^3 a^3 z^3 + 2^2 3^2 a^2 x z^2 + 2 \cdot 3^3 a x^2 z + 3^3 x^3) \\
& \quad - 3a(-2^2 a^3 z^2 - 2 \cdot 3 a^2 x z + 2 \cdot 3^2 a b y z + 3^3 b x y) \\
& \quad - 3^2 a y^2 (2^3 a^4 z + 2^2 3 a^3 x - 2 \cdot 3^3 a b^2 z - 3^4 b^2 x) \\
& \quad - 3(-2^3 a^6 z^3 + 2^2 3^3 a^4 b y z^2 - 2 \cdot 3^5 a^2 b^2 y^2 z + 3^6 b^3 y^3) \\
& \quad - 3^2 y^2 (-2^3 a^5 z + 2^2 3^2 a^3 b y + 2 \cdot 3^3 a^2 b^2 z - 3^5 b^3 y) \\
& \quad + 2a z^2 (-2^3 a^5 z + 2^2 3^2 a^3 b y + 2 \cdot 3^3 a^2 b^2 z - 3^5 b^3 y) \\
& \quad + 3^3 b(2^3 a^3 y^3 - 2^2 3^2 a^2 b y^2 z + 2 \cdot 3^3 a b^2 y z^2 - 3^3 b^3 z^3) \\
& \quad + 2 \cdot 3^2 b z^2 (2^3 a^4 y - 2^2 3 a^3 b z - 2 \cdot 3^3 a b^2 y + 3^4 b^3 z) - z^3 (2^2 a^3 - 3^3 b^2) \\
&= \frac{1}{2^2 3^3 a^3} (2^5 a^6 z^3 + 2^4 3^2 a^5 x z^2 + 2^3 3^3 a^4 x^2 z + 2^2 3^3 a^3 x^3 + 2^2 3 a^4 z^2 + 2 \cdot 3^2 a^3 x z - 2 \cdot 3^3 a^2 b y z \\
& \quad - 3^4 a b x y - 2^3 3^2 a^5 y^2 z - 2^2 3^3 a^4 x y^2 + 2 \cdot 3^5 a^2 b^2 y^2 z + 3^6 a b^2 x y^2 + 2^3 3 a^6 z^3 - 2^2 3^4 a^4 b y z^2 \\
& \quad + 2 \cdot 3^6 a^2 b^2 y^2 z - 3^7 b^3 y^3 + 2^3 3^2 a^5 y^2 z - 2^2 3^4 a^3 b y^3 - 2 \cdot 3^5 a^2 b^2 y^2 z + 3^7 b^3 y^3 - 2^4 a^6 z \\
& \quad + 2^3 3^2 a^4 b y + 2^2 3^3 a^3 b^2 z - 2 \cdot 3^5 a b^3 y + 2^3 3^3 a^3 b y^3 - 2^2 3^5 a^2 b^2 y^2 z + 2 \cdot 3^6 a b^3 y z^2 - 3^6 b^4 z^3 \\
& \quad + 2^4 3^2 a^4 b y z^2 - 2^3 3^3 a^3 b^2 z^3 - 2^2 3^5 a b^3 y z^2 + 2 \cdot 3^6 b^4 z^3 - 2^2 a^3 z^3 + 3^3 b^2 z^3) \\
&= x^3 + 2a x^2 z - a x y^2 + 3b x y z + a^2 x z^2 - b y^3 + b^2 z^3 + a b y z^2 = Z.
\end{aligned}$$

Portanto,

$$\begin{aligned}
Z &= \frac{1}{2^2 3^3 a^3} (2^2 a^3 X^3 - 3aXU^2 - 3^2 a \Delta X y^2 - 3U^3 - 3^2 \Delta U y^2 + 2a \Delta U z^2 \\
& \quad + 3^3 b V^3 + 2 \cdot 3^2 b \Delta V z^2 + \Delta^2 z^3),
\end{aligned}$$

o que prova o resultado. $\square$

Para finalizar esta seção, enunciamos um resultado que é um caso particular do Teorema 4.25. Ele nos dá uma regra importante para calcular uma base p -integral de um corpo cúbico.

Teorema 5.3. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz de $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$. Sejam $p \in \mathbb{Z}$ um número primo, $\frac{u + \theta}{p^i}$ e $\frac{x + y\theta + \theta^2}{p^j}$ elementos p -integrais do corpo $\mathbb{K}$, com $u, x, y \in \mathbb{Z}$ e $i, j \in \mathbb{N}$ maiores possíveis. Assim,*

$$\left\{ 1, \frac{u + \theta}{p^i}, \frac{x + y\theta + \theta^2}{p^j} \right\}$$

é uma base p -integral do corpo $\mathbb{K}$ e $v_p(\mathbb{K}) = s_p - 2(i + j)$.

Demonstração. Basta notar que é um caso particular do Teorema 4.25. $\square$

Observação 5.4. Como $v_p(D(\mathbb{K})) \geq 0$, para todo $p \in \mathbb{Z}$ primo, segue que $i + j \leq \frac{s_p}{2}$. Dessa forma, se $s_p = 0$ ou $s_p = 1$, então $i = j = 0$. E se $s_p = 2$ ou $s_p = 3$, então $(i, j) = (0, 0)$ ou $(0, 1)$. Note que $(i, j) = (1, 0)$ não ocorre pois $i \leq j$.

5.2 Bases 2-integrais de um corpo cúbico

Note que, dada θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_2(a) < 2$ ou $v_2(b) < 3$, obtemos as seguintes possibilidades:

1. $b \equiv 1 \pmod{2}$
2. $b \equiv 0 \pmod{2}$
 - (a) $b \equiv 2 \pmod{4}$
 - i. $a \equiv 0 \pmod{2}$
 - ii. $a \equiv 1 \pmod{4}$
 - iii. $a \equiv 3 \pmod{4}$
 - A. $s_2 \equiv 1 \pmod{2}$
 - B. $s_2 \equiv 0 \pmod{2}$
 - $\Delta_2 \equiv 3 \pmod{4}$
 - $\Delta_2 \equiv 1 \pmod{4}$
 - (b) $b \equiv 0 \pmod{4}$
 - i. $a \equiv 3 \pmod{4}$
 - ii. $a \equiv 1 \pmod{4}$
 - iii. $a \equiv 0 \pmod{2}$
 - A. $b \equiv 4 \pmod{8}$
 - B. $b \equiv 0 \pmod{8}$

O teorema que provamos nesta seção analisa as 10 possibilidades para encontrar bases 2-integrais para o corpo $\mathbb{K}$.

Teorema 5.5. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_2(a) < 2$ ou $v_2(b) < 3$. Uma base 2-integral para o corpo $\mathbb{K}$ é dada na seguinte tabela:*

Tabela 5.1: Base 2-integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$.

Caso	condição	base 2-integral	s_2	$v_2(D(\mathbb{K}))$
A1	$b \equiv 1 \pmod{2}$	$\{1, \theta, \theta^2\}$	0	0
A2	$a \equiv 0 \pmod{2}$ e $b \equiv 2 \pmod{4}$	$\{1, \theta, \theta^2\}$	2	2
A3	$a \equiv 0 \pmod{2}$ e $b \equiv 4 \pmod{8}$	$\left\{1, \theta, \frac{\theta^2}{2}\right\}$	4	2
A4	$a \equiv 2 \pmod{4}$ e $b \equiv 0 \pmod{8}$	$\left\{1, \theta, \frac{\theta^2}{2}\right\}$	5	3
A5	$a \equiv 1 \pmod{4}$ e $b \equiv 0 \pmod{4}$	$\left\{1, \theta, \frac{\theta + \theta^2}{2}\right\}$	2	0
A6	$a \equiv 3 \pmod{4}$ e $b \equiv 0 \pmod{4}$	$\{1, \theta, \theta^2\}$	2	2
A7	$a \equiv 1 \pmod{4}$ e $b \equiv 2 \pmod{4}$	$\{1, \theta, \theta^2\}$	3	3
A8	$a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{2}$ e $s_2 \equiv 1 \pmod{2}$	$\left\{1, \theta, \frac{x + y\theta + \theta^2}{2^m}\right\}$, com $m = \frac{s_2 - 3}{2}$, $3x \equiv -2a \pmod{2^m}$ e $ay \equiv \frac{3b}{2} \pmod{2^m}$	$s_2 \geq 5$ $s_2 \equiv 1 \pmod{2}$	3
A9	$a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$, $s_2 \equiv 0 \pmod{2}$ e $\Delta_2 \equiv 3 \pmod{4}$	$\left\{1, \theta, \frac{x + y\theta + \theta^2}{2^m}\right\}$, com $m = \frac{s_2 - 2}{2}$, $3x \equiv -2a \pmod{2^m}$ e $ay \equiv \frac{3b}{2} \pmod{2^m}$	$s_2 \geq 4$ $s_2 \equiv 0 \pmod{2}$	2
A10	$a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$, $s_2 \equiv 0 \pmod{2}$ e $\Delta_2 \equiv 1 \pmod{4}$	$\left\{1, \theta, \frac{x + y\theta + \theta^2}{2^{m+1}}\right\}$, com $m = \frac{s_2 - 2}{2}$, $3x \equiv -1 \pmod{2^{m+1}}$ e $ay \equiv \frac{3b}{2} + 2^m \pmod{2^{m+1}}$	$s_2 \geq 4$ $s_2 \equiv 0 \pmod{2}$	0

Fonte: [3], p. 27.

Demonstração. Primeiramente, lembremos que $\Delta = D(\theta) = 4a^3 - 27b^2 = 2^2a^3 - 3^3b^2$, e pela Definição 5.1, segue que

$$\Delta_2 = \frac{\Delta}{2^{s_2}} = \frac{2^2a^3 - 3^3b^2}{2^{s_2}} \equiv 1 \pmod{2},$$

pois $2 \nmid \Delta_2$.

Caso A1: Por hipótese,

$$b \equiv 1 \pmod{2} \Rightarrow b = 2n + 1, \text{ para algum } n \in \mathbb{Z}.$$

Dessa forma, $b^2 = 4n^2 + 4n + 1 \equiv 1 \pmod{4}$. Além disso,

$$\Delta = 2^2 a^3 - 3^3 b^2 \equiv 1 \pmod{2} \Rightarrow s_2 = v_2(\Delta) = 0.$$

Com isso, pela Observação 5.4 e pelo Teorema 5.3, segue que $i = j = 0$ e $v_2(D(\mathbb{K})) = 0$. Como θ e θ^2 são elementos 2-integrais do corpo $\mathbb{K}$, segue que $\{1, \theta, \theta^2\}$ é uma base 2-integral para o corpo $\mathbb{K}$.

Caso A2: Por hipótese,

$$a \equiv 0 \pmod{2} \Rightarrow a = 2k, \quad k \in \mathbb{Z} \Rightarrow a^3 = 2^3 k^3,$$

$$b \equiv 2 \pmod{4} \Rightarrow b = 4q + 2, \quad q \in \mathbb{Z} \Rightarrow b^2 = 2^2(4q^2 + 4q + 1).$$

Dessa forma,

$$\Delta = 2^2 a^3 - 3^3 b^2 = 2^2(2^3 k^3) - 3^3[2^2(4q^2 + 4q + 1)] = 2^2[2^3 k^3 - 3^3(4q^2 + 4q + 1)],$$

e assim,

$$s_2 = v_2(\Delta) = 2.$$

Com isso, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(1, 0)$. Vamos mostrar que para todo $x, y \in \mathbb{Z}$, o elemento $\frac{x + y\theta + \theta^2}{2} \in \mathbb{K}$ não é 2-integral. Vamos supor que este elemento seja 2-integral para algum $x, y \in \mathbb{Z}$. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{2}, \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{4}, \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{8}. \end{cases}$$

Dessa forma, uma vez que $a = 2k$ e $b = 4q + 2$, segue que

- $X = 3x + 2a \equiv 3x \equiv 0 \pmod{2} \Rightarrow x \equiv 0 \pmod{2} \Rightarrow x = 2r, \quad r \in \mathbb{Z}$.
- $Z \equiv -4kry^2 + 24qry + 12ry - 4qy^3 - 2y^3 + 16q^2 + 16q + 4 + 8kqy + 4ky \equiv 0 \pmod{8} \equiv 0 \pmod{4} \Rightarrow -2y^3 \equiv 0 \pmod{4} \Rightarrow y^3 \equiv 0 \pmod{2} \Rightarrow y \equiv 0 \pmod{2}$.
Com isso, $Z \equiv 4 \equiv 0 \pmod{8}$, o que é um absurdo.

Portanto, não existem $x, y \in \mathbb{Z}$ de modo que $\frac{x + y\theta + \theta^2}{2}$ seja 2-integral. Pela Observação 5.4, $\frac{x + \theta}{2}$ também não é 2-integral, para todo $x \in \mathbb{Z}$. Logo, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base 2-integral para o corpo $\mathbb{K}$ e $v_2(D(\mathbb{K})) = s_2 = 2$.

Caso A3: Por hipótese,

$$a \equiv 0 \pmod{2} \Rightarrow a = 2k, \quad k \in \mathbb{Z} \Rightarrow a^3 = 2^3 k^3,$$

$$b \equiv 4 \pmod{8} \Rightarrow b = 8q + 4 = 4(2q + 1), \quad q \in \mathbb{Z} \Rightarrow b^2 = 2^4(4q^2 + 4q + 1).$$

Dessa forma,

$$\Delta = 2^5 k^3 - 3^3 2^4(4q^2 + 4q + 1) = 2^4[2k^3 - 3^3(4q^2 + 4q + 1)] \Rightarrow s_2 = v_2(\Delta) = 4.$$

Agora, considere o elemento $\frac{\theta^2}{2} \in \mathbb{K}$. Note que, com a notação do Teorema 5.1, segue que

- $X = 2a \equiv 0 \pmod{2}$,
- $Y = a^2 \equiv 0 \pmod{4}$,
- $Z = b^2 = 2^4(4q^2 + 4q + 1) \equiv 0 \pmod{8}$.

Portanto, $\frac{\theta^2}{2}$ é um elemento 2-integral do corpo $\mathbb{K}$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{2^2} \in \mathbb{K}$ seja 2-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{2^2}, \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^4}, \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^6}. \end{cases}$$

Dessa forma,

1. $X \equiv 3x \equiv 0 \pmod{4} \Rightarrow x \equiv 0 \pmod{4}$,
2. $Y = -ay^2 + a^2 + 3by \equiv 0 \pmod{16}$,
3. $Z = -axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{64} \equiv 0 \pmod{16}$, e assim,

$$-axy^2 - by^3 + aby \equiv 0 \pmod{16}.$$

Se $y \equiv 1 \pmod{2}$, então $y = 2r + 1$, com $r \in \mathbb{Z}$. Pela Equação 2, segue que

$$-ay^2 + a^2 + 3by \equiv 0 \pmod{16} \equiv 0 \pmod{4},$$

e assim,

$$-ay^2 \equiv -a(4r^2 + 4r + 1) \equiv 0 \pmod{4} \Rightarrow a \equiv 0 \pmod{4}.$$

Dessa forma, pela Equação 3, segue que

$$-axy^2 - by^3 + aby \equiv -by^3 \equiv -b(8r^3 + 12r^2 + 6r + 1) \equiv -b(6r + 1) \equiv b \equiv 0 \pmod{16},$$

o que é um absurdo, uma vez que $b \not\equiv 0 \pmod{8}$. Portanto, $y \equiv 0 \pmod{2}$. Agora, seja $a \equiv 2 \pmod{4}$. Pela Equação 2, segue que

$$-ay^2 + a^2 + 3by \equiv 0 \pmod{16} \equiv 0 \pmod{8} \Rightarrow a^2 \equiv 16q^2 + 16q + 4 \equiv 4 \equiv 0 \pmod{8},$$

o que é um absurdo. Portanto, $a \equiv 0 \pmod{4}$. Com isso, pela Equação 2, segue que

$$3by = 3(16qr + 8r) \equiv 0 \pmod{16} \Rightarrow 8r \equiv r \equiv 0 \pmod{16}.$$

Logo,

$$y \equiv 0 \pmod{16} \equiv 0 \pmod{4} \Rightarrow y = 4r', \quad r' \in \mathbb{Z}.$$

Dessa forma, pela Equação 3, segue que

$$-axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv b^2 + aby \equiv 0 \pmod{64},$$

e assim,

$$16 + a(32qr' + 16r') = 16(2aqr' + r' + 1) \equiv 0 \pmod{64} \Rightarrow 16 \equiv 0 \pmod{64},$$

o que é um absurdo. Portanto, para todo $x, y \in \mathbb{Z}$, segue que $\frac{x + y\theta + \theta^2}{2^2}$ não é 2-integral. Agora, vamos supor que para algum $x \in \mathbb{Z}$, o elemento $\frac{x + \theta}{2} \in \mathbb{K}$ seja 2-integral. Assim, pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x \equiv 0 \pmod{2}, \\ Y = 3x^2 - a \equiv 0 \pmod{2^2}, \\ Z = x^3 - ax - b \equiv 0 \pmod{2^3}. \end{cases}$$

Dessa forma,

- $3x \equiv x \equiv 0 \pmod{2}$,
- $3x^2 - a \equiv a \equiv 0 \pmod{4}$ e
- $x^3 - ax - b \equiv b \equiv 0 \pmod{8}$, o que é um absurdo.

Portanto, para todo $x \in \mathbb{Z}$, o elemento $\frac{x + \theta}{2} \in \mathbb{K}$ não é 2-integral. Logo, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{\theta^2}{2}\right\}$ é uma base 2-integral do corpo $\mathbb{K}$ e $v_2(D(\mathbb{K})) = s_2 - 2 = 2$.

Caso A4: Por hipótese,

$$a \equiv 2 \pmod{4} \Rightarrow a = 4k + 2, \quad k \in \mathbb{Z} \Rightarrow a^3 = 2^6 k^3 + 2^5 3k^2 + 2^4 3k + 2^3,$$

$$b \equiv 0 \pmod{8} \Rightarrow b = 8q, \quad q \in \mathbb{Z} \Rightarrow b^2 = 2^6 q^2.$$

Dessa forma,

$$\Delta = 2^5[(2^3 k^3 + 2^2 3k^2 + 2.3k + 1) - 3^3(2q^2)] \Rightarrow s_2 = v_2(\Delta) = 5.$$

Considere o elemento $\frac{\theta^2}{2} \in \mathbb{K}$. Com a notação do Teorema 5.1, segue que

- $X = 2a \equiv 0 \pmod{2}$,
- $Y = a^2 z^2 \equiv 0 \pmod{4}$,
- $Z = b^2 z^3 \equiv 0 \pmod{8}$.

Portanto, $\frac{\theta^2}{2}$ é um elemento 2-integral do corpo $\mathbb{K}$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{2^2} \in \mathbb{K}$ seja 2-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{2^2}, \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^4}, \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^6}. \end{cases}$$

Dessa forma,

1. $X \equiv 3x \equiv x \equiv 0 \pmod{4}$.

2. $Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv -ay^2 + a^2 + 3by \equiv 0 \pmod{16} \equiv 0 \pmod{8} \Rightarrow -(4k+2)y^2 + (4k+2)^2 \equiv -(4k+2)y^2 + 4 \equiv -2(2ky^2 + y^2 - 2) \equiv 2(ky^2 - 1) + y^2 \equiv 0 \pmod{8}$. Assim,

$$2(ky^2 - 1) + y^2 = 8s, \quad s \in \mathbb{Z} \Rightarrow y^2(2k+1) = 8s+2$$

que é par. Logo,

$$y^2 \equiv y \equiv 0 \pmod{2} \Rightarrow y = 2t, \quad t \in \mathbb{Z}.$$

Portanto, $\underbrace{2t^2(2k+1)}_{\text{par}} = \underbrace{4s+1}_{\text{ímpar}}$, o que é um absurdo.

Logo, para todo $x, y \in \mathbb{Z}$, segue que $\frac{x + y\theta + \theta^2}{2^2}$ não é 2-integral. Agora, vamos supor que $\frac{x + \theta}{2} \in \mathbb{K}$ é 2-integral, para algum $x \in \mathbb{Z}$. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x \equiv 0 \pmod{2}, \\ Y = 3x^2 - a \equiv 0 \pmod{2^2}, \\ Z = x^3 - ax - b \equiv 0 \pmod{2^3}. \end{cases}$$

Assim,

- $X \equiv x \equiv 0 \pmod{2}$,
- $Y \equiv a \equiv 0 \pmod{4}$, o que contradiz a hipótese.

Portanto, para todo $x \in \mathbb{Z}$, segue que $\frac{x + \theta}{2} \in \mathbb{K}$ não é 2-integral. Pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{\theta^2}{2}\right\}$ é uma base 2-integral para o corpo $\mathbb{K}$ e $v_2(D\mathbb{K}) = s_2 - 2 = 3$.

Caso A5: Por hipótese,

$$a \equiv 1 \pmod{4} \Rightarrow a = 4k + 1, \quad k \in \mathbb{Z} \Rightarrow a^3 = 2^6k^3 + 2^43k^2 + 2^23k + 1$$

$$b \equiv 0 \pmod{4} \Rightarrow b = 4q, \quad q \in \mathbb{Z} \Rightarrow b^2 = 2^4q^2.$$

Dessa forma,

$$\Delta = [2^2(2^6k^3 + 2^43k^2 + 2^23k + 1) - 3^32^4q^2] \Rightarrow s_2 = v_2(\Delta) = 2.$$

Com isso, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Considere o elemento $\frac{\theta + \theta^2}{2} \in \mathbb{K}$. Com a notação do Teorema 5.1, segue que

- $X = 2a \equiv 0 \pmod{2}$,
- $Y = -a + a^2 + 3b \equiv a(a - 1) = 4k(4k + 1) \equiv 0 \pmod{2^2}$,
- $Z = -b + b^2 + ab \equiv -b + ab = 16kq \equiv 0 \pmod{2^3}$.

Portanto, $\frac{\theta + \theta^2}{2}$ é 2-integral. Com isso, $j = 1$ e $i = 0$. Logo, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{\theta + \theta^2}{2}\right\}$ é uma base 2-integral para o corpo $\mathbb{K}$ e $v_2(D(\mathbb{K})) = 2 - 2 = 0$.

Caso A6: Por hipótese,

$$a \equiv 3 \pmod{4} \Rightarrow a = 4k + 3, \quad k \in \mathbb{Z} \Rightarrow a^3 = 2^6 k^3 + 2^4 3^2 k^2 + 2^2 3^3 k + 3^3,$$

$$b \equiv 0 \pmod{4} \Rightarrow b = 4q, \quad q \in \mathbb{Z} \Rightarrow b^2 = 2^4 q^2.$$

Dessa forma,

$$\Delta = 2^2 3^3 (2^6 k^3 + 2^4 3^2 k^2 + 2^2 3^3 k + 1 - 2^2 q^2) \Rightarrow s_2 = v_2(\Delta) = 2.$$

Assim, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{2} \in \mathbb{K}$ seja 2-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{2}, \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^2}, \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^3}. \end{cases}$$

Dessa forma,

$$1. \quad X \equiv 3x \equiv x \equiv 0 \pmod{2}.$$

$$2. \quad Y \equiv -ay^2 + a^2 \equiv 0 \pmod{4}. \text{ Como } -ay^2 + a^2 = -(4k+3)y^2 + 16k^2 + 24k + 9, \text{ segue que } Y \equiv -3y^2 + 1 \equiv 0 \pmod{4}. \text{ Suponha que } y \text{ seja par, ou seja, } y = 2r, \quad r \in \mathbb{Z}. \text{ Assim,}$$

$$-3y^2 + 1 = -3 \cdot 4r^2 + 1 \equiv 1 \pmod{4}.$$

O que contradiz o item 2. Logo, $y = 2r + 1$ e

$$-3y^2 + 1 = -3(4r^2 + 4r + 1) + 1 \equiv 2 \pmod{4},$$

o que também contradiz o item 2.

Portanto, para todo $x, y \in \mathbb{Z}$, segue que o elemento $\frac{x + y\theta + \theta^2}{2}$ não é 2-integral. Logo, $i = j = 0$ e, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base 2-integral para o corpo $\mathbb{K}$ e $v_2(D(\mathbb{K})) = s_2 = 2$.

Caso A7: Por hipótese,

$$a \equiv 1 \pmod{4} \Rightarrow a = 4k + 1, \quad k \in \mathbb{Z} \Rightarrow a^3 = 2^4 k^3 + 2^3 k + 1,$$

$$b \equiv 2 \pmod{4} \Rightarrow b = 4q + 2, \quad q \in \mathbb{Z} \Rightarrow b^2 = 2^4 q^2 + 2^4 q + 2^2.$$

Dessa forma,

$$\begin{aligned} \Delta &= 2^2(2^4 k^3 + 2^3 k + 1) - 3^3(2^4 q^2 + 2^4 q + 2^2) \\ &= 2^2(2^4 k^3 + 2^3 k + 1) - 3^3 2^2(2^2 q^2 + 2^2 q + 1) \\ &= 2^2[2^4 k^3 + 2^3 k + 1 - 3^3(2^2 q^2 + 2^2 q) - 3^3] \\ &= 2^2[2^4 k^3 + 2^3 k - 3^3 2^2(q^2 + q) - 26] \\ &= 2^3[2^3 k^3 + 2^2 k - 3^3 2(q^2 + q) - 13], \end{aligned}$$

e assim, $s_2 = v_2(\Delta) = 3$. Novamente, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{2} \in \mathbb{K}$ seja 2-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{2}, \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^2}, \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^3}. \end{cases}$$

Dessa forma,

1. $X \equiv 3x \equiv x \equiv 0 \pmod{2}$.
2. $Y \equiv -ay^2 + a^2 + 3by \equiv 0 \pmod{4}$. Como $-ay^2 + a^2 + 3by = -y^2(4k+1) + (16k^2 + 8k + 1) + 3y(4q+2)$, segue que $Y \equiv -y^2 + 1 + 6y \equiv -y^2 + 1 + 2y \equiv 0 \pmod{4}$. Suponha $y = 2r$, $r \in \mathbb{Z}$. Assim,

$$-y^2 + 1 + 2y = -4r^2 + 1 + 4r \equiv 1 \pmod{4},$$

o que contradiz o item 2. Logo, $y = 2r + 1$ e

$$-y^2 + 1 + 2y = -4r^2 + 2 \equiv 2 \pmod{4},$$

o que também contradiz o item 2.

Portanto, para todo $x, y \in \mathbb{Z}$, segue que o elemento $\frac{x + y\theta + \theta^2}{2}$ não é 2-integral. Logo, $i = j = 0$ e, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base 2-integral para o corpo $\mathbb{K}$ e $v_2(D(\mathbb{K})) = s_2 = 3$.

Caso A8: Por hipótese, $s_2 \equiv 1 \pmod{2}$,

$$a \equiv 3 \pmod{4} \Rightarrow a = 4k + 3, \quad k \in \mathbb{Z} \Rightarrow a^3 = 2^6k^3 + 2^43^2k^2 + 2^23^3k + 3^3,$$

$$b \equiv 2 \pmod{4} \Rightarrow b = 4q + 2, \quad q \in \mathbb{Z} \Rightarrow b^2 = 2^4q^2 + 2^4q + 2^2.$$

Dessa forma,

$$\begin{aligned} \Delta &= 2^2(2^6k^3 + 2^43^2k^2 + 2^23^3k + 3^3) - 3^32^2(2^2q^2 + 2^2q + 1) \\ &\equiv (\text{mod } 2^23^3 - 2^23^3)16 \equiv 0 \pmod{16} \Rightarrow s_2 = v_2(\Delta) \geq 4. \end{aligned}$$

Agora, uma vez que s_2 é ímpar, segue que $s_2 \geq 5$. Assim, $s_2 - 3$ é um número par e positivo, ou seja, $m = \frac{s_2 - 3}{2} \in \mathbb{N}$. Além disso, $2m + 3 = s_2 = v_2(\Delta)$, ou seja,

$$2^{2m+3} | \Delta \text{ e } 2^{2m+3+1} \nmid \Delta.$$

Vamos definir $x, y, z \in \mathbb{Z}$ de modo que

$$\begin{cases} 3x \equiv -2a \pmod{2^m}, \\ ay \equiv \frac{3b}{2} \pmod{2^m}, \\ z = 1. \end{cases}$$

Com a notação do Teorema 5.2, segue que

- $X = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{2^m}$.
- $3bU = 3b(9by - 2a^2) = 3^3b^2y - 6a^2b = 3^3b^3y - 2^2a^3y + 2^2a^3y - 6a^2b$
 $= 2^2a^3y - \Delta y - 6a^2b = 2^2a^2(ay) - \Delta y - 6a^2b \equiv 2^2a^2\left(\frac{3b}{2}\right) - \Delta y - 6a^2b \pmod{2^{m+2}}$
 $\equiv 2^2a^2\left(\frac{3b}{2}\right) - 6a^2b \equiv a^2b\left(\frac{2^23}{2} - 6\right) \equiv 0 \pmod{2^{m+2}} \Rightarrow 3bU \equiv 0 \pmod{2^{m+2}}.$

Como $2|b$ e $2^2 \nmid b$, segue que $2|3b$ e $2^2 \nmid 3b$. Assim,

$$3bU \equiv 0 \pmod{2^{m+2}} \Rightarrow U \equiv 0 \pmod{2^{m+1}}.$$

- $V = 2ay - 3bz = 2ay - 3b \equiv 2\left(\frac{3b}{2}\right) - 3b \pmod{2^{m+1}} \equiv 0 \pmod{2^{m+1}}$
- $Y = \frac{1}{2^23a^2}(2^2a^2X^2 - U^2 - 3\Delta y^2) \equiv \frac{-3\Delta y^2}{2^23a^2} \pmod{2^{2m}} \equiv \frac{-\Delta y^2}{2^2a^2} \equiv 0 \pmod{2^{2m}}.$
- $Z = \frac{1}{2^23^3a^3}(2^2a^3X^3 - 3aXU^2 - 3^2a\Delta Xy^2 - 3U^3 - 3^2\Delta Uy^2 + 2a\Delta U + 3^3bV^3$
 $+ 2 \cdot 3^2b\Delta V + \Delta^2) \equiv 0 \pmod{2^{3m}}.$

Com isso, pelo Teorema 5.1, segue que $\frac{x + y\theta + \theta^2}{2^m}$ é um elemento 2-integral do corpo $\mathbb{K}$, com x e y da forma que foram dados anteriormente e $m = \frac{s_2 - 3}{2}$. Agora, suponha que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{2^{m+1}}$ seja um elemento 2-integral do corpo $\mathbb{K}$. Pelo Teorema 5.1 e usando a notação do Teorema 5.2, segue que

$$\begin{cases} X &= 3x + 2a \equiv 0 \pmod{2^{m+1}}. \\ Y &= \frac{1}{2^23a^2}(2^2a^2X^2 - U^2 - 3\Delta y^2) \equiv 0 \pmod{2^{2m+2}}. \\ Z &= \frac{1}{2^23^3a^3}(2^2a^3X^3 - 3aXU^2 - 3^2a\Delta Xy^2 - 3U^3 - 3^2\Delta Uy^2 + 2a\Delta U + 3^3bV^3 \\ &\quad + 2 \cdot 3^2b\Delta V + \Delta^2) \equiv 0 \pmod{2^{3m+3}}. \end{cases}$$

Note que $\frac{s_2 - 3}{2} \in \mathbb{Z} \Rightarrow m + 1 = \frac{s_2 - 1}{2} = r \in \mathbb{Z}$ e $r \geq 2$. Com isso,

1. $X = 3x + 2(4k + 3) \equiv 0 \pmod{2^r} \equiv 0 \pmod{4} \equiv 3x + 6 \pmod{4} \equiv 3x + 2 \pmod{4} \Rightarrow 3x \equiv -2 \pmod{4} \Rightarrow -x \equiv -2 \pmod{4} \Rightarrow x \equiv 2 \pmod{4}.$
2. $Y \equiv \frac{1}{2^23a^2}(U^2 + 3\Delta y^2) \equiv 0 \pmod{2^{2m+2}},$ e assim,

$$\frac{1}{2^23a^2}(U^2 + 3\Delta y^2) = 2^{2m+2}l, \quad \text{com } l \in \mathbb{Z},$$

ou seja,

$$\frac{1}{3a^2}(U^2 + 3\Delta y^2) = 2^{2m+4}l \Rightarrow U^2 + 3\Delta y^2 \equiv 0 \pmod{2^{2m+4}}.$$

3. Com a notação do Teorema 5.1, segue que

$$\begin{aligned} Y &= 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^{2m+2}} \equiv 0 \pmod{2} \\ \Rightarrow a(a - y^2) &\equiv a - y^2 \equiv 0 \pmod{2} \Rightarrow y^2 \equiv a \equiv 1 \pmod{2} \Rightarrow y \equiv 1 \pmod{2} \end{aligned}$$

Dessa forma, uma vez que $2^{2m+3}|\Delta$ e $2^{2m+3+1} \nmid \Delta$, segue que $\Delta = 2^{2m+3}d$, com $2 \nmid d$. Pelo item 2, segue que

$$U^2 + 3\Delta y^2 \equiv 0 \pmod{2^{2m+4}} \Rightarrow U^2 + 3\Delta y^2 = 2^{2m+4}e,$$

onde $e \in \mathbb{Z}$. Assim,

$$U^2 + 3(2^{2m+3}d)y^2 = 2^{2m+4}e \Rightarrow U^2 = 2^{2m+3}(2e - 3dy^2).$$

Agora, como $2 \nmid e$ e $2 \nmid y^2$, segue que $2^{2m+3}|U^2$ e $2^{2m+3+1} \nmid U^2$, o que é uma contradição.

Portanto, para todo $x, y \in \mathbb{Z}$, o elemento $\frac{x + y\theta + \theta^2}{2^{m+1}}$ não é 2-integral. Suponhamos, agora, que para algum $x \in \mathbb{Z}$, o elemento $\frac{x + \theta}{2}$ seja 2-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x \equiv 0 \pmod{2}, \\ Y = 3x^2 - a \equiv 0 \pmod{2^2}, \\ Z = x^3 - ax - b \equiv 0 \pmod{2^3}. \end{cases}$$

Assim,

- $X \equiv x \equiv 0 \pmod{2}$.
- $Y \equiv a \equiv 0 \pmod{4}$, o que contradiz a hipótese.

Portanto, para todo $x \in \mathbb{Z}$, segue que $\frac{x + \theta}{2} \in \mathbb{K}$ não é 2-integral. Logo, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{x + y\theta + \theta^2}{2^m}\right\}$ é uma base 2-integral para o corpo $\mathbb{K}$ e $v_2(D\mathbb{K}) = s_2 - 2(m+1) = 3$.

Para os casos **A9** e **A10**, por hipótese, segue que $s_2 \equiv 0 \pmod{2}$,

$$a \equiv 3 \equiv -1 \pmod{4} \Rightarrow a = 4k - 1, \quad k \in \mathbb{Z} \Rightarrow a^3 = 2^6k^3 - 2^43k^2 + 2^23k - 1,$$

$$b \equiv 2 \pmod{4} \Rightarrow b = 4q + 2, \quad q \in \mathbb{Z} \Rightarrow b^2 = 2^4q^2 + 2^4q + 2^2.$$

Dessa forma,

$$\begin{aligned} \Delta &= 2^2(2^6k^3 - 2^43k^2 + 2^23k - 1) - 3^3(2^4q^2 + 2^4q + 2^2) \\ &= 2^2(2^6k^3 - 2^43k^2 + 2^23k - 1) - 3^32^2(2^2q^2 + 2^2q + 1) \\ &\equiv (\text{mod } -4 - 12)16 \equiv 0 \pmod{16} \Rightarrow s_2 = v_2(\Delta) \geq 4. \end{aligned}$$

Como estamos considerando s_2 par, então podemos definir $m = \frac{s_2 - 2}{2} \in \mathbb{N}$. Além disso, $2m + 2 = s_2 = v_2(\Delta)$, ou seja,

$$2^{2m+2}|\Delta \text{ e } 2^{2m+2+1} \nmid \Delta.$$

Caso A9: Por hipótese, segue que $\Delta_2 \equiv 3 \pmod{4}$. Vamos definir $x, y, z \in \mathbb{Z}$ de modo que

$$\begin{cases} 3x \equiv -2a \pmod{2^m}, \\ ay \equiv \frac{3b}{2} \pmod{2^m}, \\ z = 1. \end{cases}$$

Com a notação do Teorema 5.2, segue que

- $X = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{2^m}$.
- $3bU = 3b(9by - 2a^2) = 2^2a^2(ay) - \Delta y - 2.3a^2b \equiv 2^2a^2\left(\frac{3b}{2}\right) - \Delta y - 2.3a^2b$
 $\equiv a^2b\left(\frac{2^23}{2} - 6\right) \equiv 0 \pmod{2^{m+2}} \Rightarrow 3bU \equiv 0 \pmod{2^{m+2}}.$

Como $2|b$ e $2^2 \nmid b$, segue que $2|3b$ e $2^2 \nmid 3b$. Assim,

$$3bU \equiv 0 \pmod{2^{m+2}} \Rightarrow U \equiv 0 \pmod{2^{m+1}}.$$

- $V = 2ay - 3b \equiv 2\left(\frac{3b}{2}\right) - 3b \equiv 0 \pmod{2^{m+1}}.$
- $Y = \frac{1}{2^23a^2}(2^2a^2X^2 - U^2 - 3\Delta y^2) \equiv \frac{-3\Delta y^2}{2^23a^2} \pmod{2^{2m}} \equiv \frac{-\Delta y^2}{2^2a^2} \equiv 0 \pmod{2^{2m}}.$
- $Z = \frac{1}{2^23^3a^3}(2^2a^3X^3 - 3aXU^2 - 3^2a\Delta Xy^2 - 3U^3 - 3^2\Delta Uy^2 + 2a\Delta U + 3^3bV^3$
 $+ 2.3^2b\Delta V + \Delta^2) \equiv 0 \pmod{2^{3m}}.$

Com isso, pelo Teorema 5.1, segue que $\frac{x + y\theta + \theta^2}{2^m}$ é um elemento 2-integral do corpo $\mathbb{K}$, com x e y da forma que foram dados anteriormente e $m = \frac{s_2 - 2}{2}$. Agora, suponha que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{2^{m+1}}$ seja um elemento 2-integral do corpo $\mathbb{K}$. Pelo Teorema 5.1 e usando a notação do Teorema 5.2, segue que

$$\begin{cases} X &= 3x + 2a \equiv 0 \pmod{2^{m+1}}, \\ Y &= \frac{1}{2^23a^2}(2^2a^2X^2 - U^2 - 3\Delta y^2) \equiv 0 \pmod{2^{2m+2}}, \\ Z &= \frac{1}{2^23^3a^3}(2^2a^3X^3 - 3aXU^2 - 3^2a\Delta Xy^2 - 3U^3 - 3^2\Delta Uy^2 + 2a\Delta U + 3^3bV^3 \\ &\quad + 2.3^2b\Delta V + \Delta^2) \equiv 0 \pmod{2^{3m+3}}. \end{cases}$$

Note que $m + 1 = \frac{s_2}{2} \geq 2$. Dessa forma,

1. $X \equiv 0 \pmod{2^{m+1}} \equiv 0 \pmod{4} \Rightarrow 3x + 2a \equiv 3x - 2 \equiv 0 \pmod{4}$
 $\Rightarrow 3x \equiv 2 \pmod{4} \Rightarrow x \equiv -2 \pmod{4}.$
2. $Y \equiv \frac{1}{2^23a^2}(-U^2 - 3\Delta y^2) \equiv 0 \pmod{2^{2m+2}} \Rightarrow \frac{1}{2^23a^2}(-U^2 - 3\Delta y^2) = 2^{2m+2}B, B \in \mathbb{Z}$
 $\Rightarrow -\frac{1}{3a^2}(U^2 + 3\Delta y^2) = 2^{2m+4} \Rightarrow U^2 + 3\Delta y^2 \equiv 0 \pmod{2^{2m+4}}.$

3. Com a notação do Teorema 5.1, segue que

$$\begin{aligned} Y = 3x^2 + 4ax - ay^2 + a^2 + 3by &\equiv 0 \pmod{2^{2m+2}} \equiv 0 \pmod{16} \equiv 0 \pmod{2} \\ \Rightarrow a(a - y^2)a - y^2 &\equiv 0 \pmod{2} \Rightarrow y^2 \equiv a \equiv 1 \pmod{2} \Rightarrow y \equiv 1 \pmod{2}. \end{aligned}$$

Agora, uma vez que $2^{2m+2}|\Delta$ e $2^{2m+2+1} \nmid \Delta$, segue que $\Delta = 2^{2m+2}d$, com $2 \nmid d$. Pela Equação 2, segue que

$$U^2 + 3\Delta y^2 \equiv 0 \pmod{2^{2m+4}} \Rightarrow U^2 + 3\Delta y^2 = 2^{2m+4}A,$$

onde $A \in \mathbb{Z}$. Assim,

$$U^2 + 3(2^{2m+2}d)y^2 = 2^{2m+4}A \Rightarrow U^2 = 2^{2m+2}(2A - 3dy^2).$$

Agora, como $2 \nmid e$ e $2 \nmid y^2$, segue que $2^{2m+2}|U^2$ e $2^{2m+2+1} \nmid U^2$, ou seja, $U^2 = 2^{2m+2}E$, com $2 \nmid E$. Uma vez que $2m+2 = s_2 = v_2(\Delta)$, segue que

$$U^2 + 3\Delta y^2 = 2^{2m+2}E + 3 \cdot 2^{2m+2}\Delta_2 y^2 = 2^{2m+2}(E + 3\Delta_2 y^2) \equiv 0 \pmod{2^{2m+4}},$$

e assim,

$$E + 3\Delta_2 y^2 \equiv 0 \pmod{2^2}.$$

Note que

$$U^2 = 2^{2m+2}E \Rightarrow U = 2^{m+1}F,$$

onde $F^2 = E$. Com isso, uma vez que E é ímpar, segue que

$$F = 2l + 1, l \in \mathbb{Z} \text{ e } E = F^2 = 4l^2 + 4l + 1 \equiv 1 \pmod{4}.$$

Assim,

$$E + 3\Delta_2 y^2 \equiv 1 + 3\Delta_2 \equiv 0 \pmod{2^2} \Rightarrow 3\Delta_2 \equiv -1 \pmod{4} \Rightarrow \Delta_2 \equiv 1 \pmod{4},$$

o que contradiz a hipótese. Portanto, para todo $x, y \in \mathbb{Z}$, segue que o elemento $\frac{x + y\theta + \theta^2}{2^{m+1}}$ não é 2-integral. Da mesma maneira que foi feita no caso **A8**, mostra-se que para todo $x \in \mathbb{Z}$, o elemento $\frac{x + \theta}{2} \in \mathbb{K}$ não é 2-integral. Logo, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{x + y\theta + \theta^2}{2^m}\right\}$ é uma base 2-integral para o corpo $\mathbb{K}$ e $v_2(D(\mathbb{K})) = s_2 - 2m = 2$.

Caso A10: Por hipótese, segue que $\Delta_2 \equiv 1 \pmod{4}$. Vamos definir $x, y, z \in \mathbb{Z}$ de modo que

$$\begin{cases} 3x \equiv -2a \pmod{2^{m+1}} & ay \equiv \frac{3b}{2} + 2^m \pmod{2^{m+1}}, \\ z = 1. \end{cases}$$

Com a notação do Teorema 5.2, segue que

- $X = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{2^{m+1}}.$
- $3bU = 3b(9by - 2a^2) = 2^2a^2(ay) - \Delta y - 2.3a^2b$
 $\equiv 2^2a^2\left(\frac{3b}{2} + 2^m\right) - \Delta y - 2.3a^2b \pmod{2^{m+3}} \equiv 2.3a^2b + 2^{m+2}a^2 - 2.3a^2b$
 $\equiv (16k^2 - 8k + 1)2^{m+2} \equiv 2^{m+2} \pmod{2^{m+3}}.$

Como $2|b$ e $2^2 \nmid b$, segue que $2|3b$ e $2^2 \nmid 3b$. Assim,

$$3bU2^{m+2} \equiv 2^{m+3} \pmod{\Rightarrow} U \equiv 2^{m+1} \pmod{2^{m+2}}.$$

- $V = 2ay - 3b \equiv 2\left(\frac{3b}{2} + 2^m\right) - 3b \equiv 2^{m+1} \pmod{2^{m+2}}.$
- $Y = \frac{1}{2^2 3 a^2} (2^2 a^2 X^2 - U^2 - 3\Delta y^2) \equiv 0 \pmod{2^{2m+2}}.$
- $Z = \frac{1}{2^2 3^3 a^3} (2^2 a^3 X^3 - 3aXU^2 - 3^2 a\Delta Xy^2 - 3U^3 - 3^2 \Delta Uy^2 + 2a\Delta U + 3^3 bV^3 + 2 \cdot 3^2 b\Delta V + \Delta^2) \equiv 0 \pmod{2^{3m+3}}.$

Com isso, pelo Teorema 5.1, segue que $\frac{x + y\theta + \theta^2}{2^m}$ é um elemento 2-integral do corpo $\mathbb{K}$, com x e y da forma que foram dados anteriormente e $m = \frac{s_2 - 2}{2}$. Note que $m + 1 = \frac{s_2}{2}$. Pela Observação 5.4, sabemos que $i + j \leq \frac{s_2}{2}$. Logo, devemos ter $j = m + 1$ e $i = 0$, ou seja, $\left\{1, \theta, \frac{x + y\theta + \theta^2}{2^{m+1}}\right\}$ é uma base 2-integral para o corpo $\mathbb{K}$ e $v_2(D(\mathbb{K})) = s_2 - 2(m + 1) = 0$, o que completa a demonstração. $\square$

Corolário 5.6. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irredutível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_2(a) < 2$ ou $v_2(b) < 3$. Vamos definir os inteiros*

- R_2 dado por:
 1. $3R_2 \equiv -2 \pmod{2^{\lceil \frac{s_2}{2} \rceil}}$, se $a \equiv 3 \pmod{4}$ e $b \equiv 2 \pmod{4}$;
 2. $R_2 = 0$, caso contrário.
- S_2 dado por:
 1. $aS_2 \equiv \frac{3b}{2} + 2^{\lceil \frac{s_2}{2} \rceil - 1} \pmod{2^{\lceil \frac{s_2}{2} \rceil}}$, se $a \equiv 3 \pmod{4}$ e $b \equiv 2 \pmod{4}$;
 2. $S_2 = 1$, se $a \equiv 1 \pmod{4}$ e $b \equiv 0 \pmod{4}$;
 3. $S_2 = 0$, caso contrário.
- $e T_2$ é igual a
 1. $\frac{s_2}{2}$, se $a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, s_2 \equiv 0 \pmod{2}$ e $\Delta_2 \equiv 1 \pmod{4}$;
 2. $\frac{s_2 - 2}{2}$, se $a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, s_2 \equiv 0 \pmod{2}$ e $\Delta_2 \equiv 3 \pmod{4}$;
 3. $\frac{s_2 - 3}{2}$, se $a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}$ e $s_2 \equiv 1 \pmod{2}$;
 4. 1, se
 - (a) $a \equiv 0 \pmod{2}$ e $b \equiv 4 \pmod{8}$, ou
 - (b) $a \equiv 2 \pmod{4}$ e $b \equiv 0 \pmod{8}$, ou
 - (c) $a \equiv 1 \pmod{4}$ e $b \equiv 0 \pmod{4}$
 5. 0, caso contrário.

Assim, $\left\{1, \theta, \frac{R_2 + S_2\theta + \theta^2}{2^{T_2}}\right\}$ é uma base 2-integral para o corpo $\mathbb{K}$.

Demonstração. Segue diretamente do Teorema 5.5. $\square$

5.3 Bases 3-integrais de um corpo cúbico

Note que, dada θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_3(a) < 2$ ou $v_3(b) < 3$, obtemos as seguintes possibilidades:

1. $v_3(a) = 0$.
2. $v_3(a) \geq 1$
 - (a) $v_3(b) = 0$.
 - i. $a \not\equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{9}$.
 - ii. $a \not\equiv 3 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{9}$.
 - iii. $a \equiv 3 \pmod{9}$, $b^2 \equiv 4 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{27}$.
 - iv. $a \equiv 3 \pmod{9}$ e $b^2 \not\equiv 4 \pmod{9}$.
 - v. $a \equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{27}$.
 - (b) $v_3(b) = 1$.
 - i. $v_3(a) > 1$.
 - ii. $v_3(a) = 1$.
 - (c) $v_3(b) \geq 2$.
 - i. $v_3(a) \geq 2$.
 - A. $v_3(b) = 2$ e $v_3(a) \geq 3$.
 - B. $v_3(b) = 2$ e $v_3(a) = 2$.
 - ii. $v_3(a) = 1$.

O teorema que provamos nesta seção analisa as 11 possibilidades para encontrar bases 3-integrais para o corpo $\mathbb{K}$.

Teorema 5.7. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_3(a) < 2$ ou $v_3(b) < 3$. Uma base 3-integral para o corpo $\mathbb{K}$ é dada na seguinte tabela:*

Tabela 5.2: Base 3-integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$.

Caso	condição	base 3-integral	s_3	$v_3(D(\mathbb{K}))$
B1	$v_3(a) = 0$	$\{1, \theta, \theta^2\}$	0	0
B2	$v_3(a) = v_3(b) = 1$	$\{1, \theta, \theta^2\}$	3	3
B3	$1 = v_3(b) < v_3(a)$	$\{1, \theta, \theta^2\}$	5	5
B4	$2 = v_3(a) = v_3(b)$	$\left\{1, \theta, \frac{\theta^2}{3}\right\}$	6	4
B5	$2 = v_3(b) < v_3(a)$	$\left\{1, \theta, \frac{\theta^2}{3}\right\}$	7	5
B6	$1 = v_3(a) < v_3(b)$	$\left\{1, \theta, \frac{\theta^2}{3}\right\}$	3	1
B7	$v_3(b) = 0, v_3(a) \geq 1,$ $a \not\equiv 3 \pmod{9}$ e $b \equiv a + 1 \pmod{9}$	$\left\{1, \theta, \frac{1 - b\theta + \theta^2}{3}\right\}$	3	1
B8	$v_3(b) = 0, v_3(a) \geq 1,$ $a \not\equiv 3 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{9}$	$\{1, \theta, \theta^2\}$	3	3
B9	$v_3(b) = 0,$ $a \equiv 3 \pmod{9},$ $b^2 \equiv 4 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{27}$	$\left\{1, \theta, \frac{1 - b\theta + \theta^2}{3}\right\}$	5	3
B10	$v_3(b) = 0,$ $a \equiv 3 \pmod{9}$ e $b^2 \not\equiv 4 \pmod{9}$	$\{1, \theta, \theta^2\},$	4	4
B11	$v_3(b) = 0,$ $a \equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{27}$	$\left\{1, \frac{b + \theta}{3}, \frac{x + y\theta + \theta^2}{3^m}\right\},$ com $m = \left\lfloor \frac{s_3 - 2}{2} \right\rfloor,$ $x \equiv -\frac{2a}{3} \pmod{3^m}$ e $2ay \equiv 3b \pmod{3^{m+2}}$	$s_3 \geq 6$	$s_3 - 2 \left\lfloor \frac{s_3}{2} \right\rfloor$

Fonte: [3], p. 40.

Demonstração. Vamos lembrar que $\Delta = 2^2a^3 - 3^3b^2$ e $s_3 = v_3(\Delta)$.

Caso B1: Por hipótese, segue que $v_3(a) = 0$, ou seja, $3 \nmid a$. Assim, $3 \nmid \Delta$ e $s_3 = v_3(\Delta) = 0$. Com isso, pela Observação 5.4, segue que $i = j = 0$. Logo, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 = 0$.

Caso B2: Por hipótese, segue que $v_3(a) = v_3(b) = 1$. Assim, $a = 3k$, $k \in \mathbb{Z}$, $3 \nmid k$ e $b = 3q$, $q \in \mathbb{Z}$, $3 \nmid q$. Dessa forma,

$$\Delta = 2^2 3^3 k^3 - 3^6 q^2 = 3^3 (2^2 k^3 - 3^3 q^2), \text{ com } 3 \nmid k^3 \text{ e } 3 \nmid q^2 \Rightarrow s_3 = v_3(\Delta) = 3.$$

Com isso, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{3} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue

que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^2}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3}. \end{cases}$$

Assim,

- $Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3} \equiv 0 \pmod{3}$
 $\Rightarrow x^3 \equiv 0 \pmod{3} \Rightarrow x \equiv 0 \pmod{3}.$
- $Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv ay^2 \equiv 0 \pmod{3^2} \Rightarrow y^2 \equiv 0 \pmod{3}$
 $\Rightarrow y \equiv 0 \pmod{3}.$

Com esses dois fatos, segue que

$$Z \equiv b^2 \equiv 0 \pmod{3^3} \Rightarrow b \equiv 0 \pmod{3^2},$$

o que contradiz o fato de $v_3(b) = 1$. Portanto, para todo $x, y \in \mathbb{Z}$, segue que o elemento $\frac{x + y\theta + \theta^2}{3}$ não é 3-integral. Logo, segue que $i = j = 0$ e, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 = 3$.

Caso B3: Por hipótese, segue que $v_3(a) > 1 \Rightarrow v_3(a) \geq 2 \Rightarrow a = 3^2k$, $k \in \mathbb{Z}$ e $v_3(b) = 1 \Rightarrow b = 3q$, $q \in \mathbb{Z}$, $3 \nmid q$. Dessa forma,

$$\Delta = 2^2 3^6 k^3 - 3^5 q^2 = 3^3(2^2 3^3 k^3 - 3^2 q^2), \text{ com } 3 \nmid q^2 \Rightarrow s_3 = v_3(\Delta) = 3.$$

Novamente, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{3} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^2}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3}. \end{cases}$$

Assim,

- $Y \equiv 3x^2 \equiv 0 \pmod{3^2} \Rightarrow x^2 \equiv 0 \pmod{3} \Rightarrow x \equiv 0 \pmod{3}.$
- $Z \equiv 0 \pmod{3^3} \equiv 0 \pmod{3^2} \Rightarrow by^3 \equiv 0 \pmod{3^2} \Rightarrow y^3 \equiv 0 \pmod{3}$
 $\Rightarrow y \equiv 0 \pmod{3}.$

Com isso, $Z \equiv b^2 \equiv 0 \pmod{3^3}$, o que é um absurdo, pois $b^2 = 3^2 q^2$, com $3 \nmid q^2$. Portanto, para todo $x, y \in \mathbb{Z}$, segue que o elemento $\frac{x + y\theta + \theta^2}{3}$ não é 3-integral. Assim, $i = j = 0$ e, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 = 5$.

Caso B4: Por hipótese,

$$\begin{aligned} v_3(a) = v_3(b) = 2 &\Rightarrow a = 3^2k \text{ e} \\ b = 3^2q, \text{ com } 3 \nmid k \text{ e } 3 \nmid q. \end{aligned}$$

Dessa forma,

$$\Delta = 2^2 3^6 k^3 - 3^7 q^2 = 3^6 (2^2 k^3 - 2 q^2), \text{ com } 3 \nmid q^2 \Rightarrow s_3 = v_3(D(\mathbb{K})) = 6.$$

Considere o elemento $\frac{\theta^2}{3} \in \mathbb{K}$. Com a notação do Teorema 5.1, segue que

- $X = 2a \equiv 0 \pmod{3}$.
- $Y = a^2 \equiv 0 \pmod{3^2}$.
- $Z = b^2 \equiv 0 \pmod{3^3}$.

Assim, pelo Teorema 5.1, segue que $\frac{\theta^2}{3}$ é um elemento 3-integral do corpo $\mathbb{K}$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{3^2} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3^2}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^4}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^6}. \end{cases}$$

Assim,

- $X \equiv 3x \equiv 0 \pmod{3^2} \Rightarrow x \equiv 0 \pmod{3}$.
- $Y \equiv 0 \pmod{3^4} \equiv 0 \pmod{3^2} \Rightarrow ay^2 \equiv 0 \pmod{3^3} \Rightarrow y^2 \equiv 0 \pmod{3} \Rightarrow y \equiv 0 \pmod{3}$.
- $Z \equiv 0 \pmod{3^6} \equiv 0 \pmod{3^4} \Rightarrow x^3 \equiv 0 \pmod{3^4} \Rightarrow x \equiv 0 \pmod{3^2}$.

Com isso,

$$Z \equiv 0 \pmod{3^6} \equiv 0 \pmod{3^5} \Rightarrow b^2 \equiv 0 \pmod{3^5} \Rightarrow b \equiv 0 \pmod{3^3},$$

o que é um absurdo. Portanto, para todo $x, y \in \mathbb{Z}$, segue que o elemento $\frac{x + y\theta + \theta^2}{3^2}$ não é 3-integral. Agora, suponhamos que exista $x \in \mathbb{Z}$ tal que o elemento $\frac{x + \theta}{3} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3}. \\ Y = 3x^2 - a \equiv 0 \pmod{3^2}. \\ Z = x^3 - ax - b \equiv 0 \pmod{3^3}. \end{cases}$$

Assim,

- $Y \equiv 3x^2 \equiv 0 \pmod{3^2} \Rightarrow x^2 \equiv 0 \pmod{3} \Rightarrow x \equiv 0 \pmod{3}$.
- $Z \equiv b \equiv 0 \pmod{3^3}$, o que é um absurdo.

Portanto, para todo $x \in \mathbb{Z}$, segue que $\frac{x + \theta}{3}$ não é um elemento integral do corpo $\mathbb{K}$. Pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{\theta^2}{3}\right\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 - 2 = 4$.

Caso B5: Por hipótese,

$$\begin{aligned} v_3(a) > 2 &\Rightarrow v_3(a) \geq 3 \Rightarrow a = 3^3k, \ k \in \mathbb{Z}, \\ v_3(b) = 2 &\Rightarrow b = 3^2q, \ q \in \mathbb{Z}, \ 3 \nmid q. \end{aligned}$$

Dessa forma,

$$\Delta = 2^2 3^9 k^3 - 3^7 q^2 = 3^7 (2^2 3^2 k^3 - q^2), \text{ com } 3 \nmid q^2 \Rightarrow s_3 = v_3(D(\mathbb{K})) = 7.$$

Considere o elemento $\frac{\theta}{3} \in \mathbb{K}$. Com a notação do Teorema 5.1, segue que

- $X = 2a \equiv 0 \pmod{3}$.
- $Y = a^2 \equiv 0 \pmod{3^2}$.
- $Z = b^2 \equiv 0 \pmod{3^3}$.

o que nos dá que $\frac{\theta^2}{3}$ é um elemento 3-integral do corpo $\mathbb{K}$. Suponha que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{3^2} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3^2}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^4}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^6}. \end{cases}$$

Assim,

- $X \equiv 3x \equiv 0 \pmod{3^2} \Rightarrow x \equiv 0 \pmod{3}$.
- $Z \equiv 0 \pmod{3^6} \equiv 0 \pmod{3^3} \Rightarrow by^3 \equiv 0 \pmod{3^3} \Rightarrow y^3 \equiv y \equiv 0 \pmod{3}$.
- $Y \equiv 3x^2 + 4ax \equiv 0 \pmod{3^4} \Rightarrow 3x + 4a \equiv 0 \pmod{3^3} \Rightarrow 3x \equiv 0 \pmod{3^3} \Rightarrow x \equiv 0 \pmod{3}$.

Com isso,

$$Z \equiv b^2 \equiv 0 \pmod{3^5} \Rightarrow b \equiv 0 \pmod{3^3},$$

o que não ocorre. Portanto, para todo $x, y \in \mathbb{Z}$, segue que o elemento $\frac{x + y\theta + \theta^2}{3^2}$ não é 3-integral. Além disso, da mesma forma que foi feita no caso **B4**, mostra-se que para todo $x \in \mathbb{Z}$, o elemento $\frac{x + \theta}{3} \in \mathbb{K}$ não é 3-integral. Portanto, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{\theta^2}{3}\right\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 - 3 = 5$.

Caso B6: Por hipótese,

$$\begin{aligned} v_3(a) = 1 &\Rightarrow a = 3k, \quad k \in \mathbb{Z}, \quad 3 \nmid k, \\ v_3(b) > 1 &\Rightarrow v_3(b) \geq 2 \Rightarrow b = 3^2q, \quad q \in \mathbb{Z}. \end{aligned}$$

Dessa forma

$$\Delta = 2^2 3^3 k^3 - 3^7 q^2 = 3^3(2^2 k^3 - 3^4 q^4), \text{ com } 3 \nmid k \Rightarrow s_3 = v_3(\Delta) = 3.$$

Com isso, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Considere o elemento $\frac{\theta^2}{3} \in \mathbb{K}$. Com a notação do Teorema 5.1, segue que

- $X = 2a \equiv 0 \pmod{3}$.
- $Y = a^2 \equiv 0 \pmod{3^2}$.
- $Z = b^2 \equiv 0 \pmod{3^3}$.

e concluímos que este elemento é 3-integral do corpo $\mathbb{K}$. Logo, $(i, j) = (0, 1)$. Portanto, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{\theta^2}{3}\right\}$ é uma base 3-integral do corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 - 2 = 1$.

Caso B7: Por hipótese, segue que

$$\begin{aligned} v_3(a) \geq 1 &\Rightarrow a = 3k, \quad k \in \mathbb{Z} \Rightarrow 3^3 | a^3, \\ v_3(b) = 0 &\Rightarrow 3 \nmid b. \end{aligned}$$

Também por hipótese,

$$\begin{aligned} a \not\equiv 3 \pmod{9} &\Rightarrow \frac{a}{3} \not\equiv 1 \pmod{3} \Rightarrow \left(\frac{a}{3}\right)^3 \not\equiv 1 \pmod{3}, \\ b^2 \equiv a + 1 \pmod{9} &\Rightarrow b^2 \equiv 3k + 1 \pmod{9} \equiv 1 \pmod{3}. \end{aligned}$$

Dessa forma,

$$\Delta = 2^2 a^3 - 3^3 b^2 \Rightarrow 3^3 | \Delta.$$

Além disso,

$$\frac{\Delta}{3^3} = \frac{2^2 a^3}{3^3} - b^2 \equiv \left(\frac{a^3}{3}\right) - 1 \pmod{3} \not\equiv 0 \pmod{3} \Rightarrow 3 \nmid \frac{\Delta}{3},$$

ou seja, $s_3 = v_3(\Delta) = 3$. Assim, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Considere o elemento $\frac{1 - b\theta + \theta^2}{3} \in \mathbb{K}$. Com a notação do Teorema 5.1, segue que

- $X = 3 - 2a \equiv 0 \pmod{3}$.
- $Y = 3 + 4a - ab^2 + a^2 - 3b^2 \equiv 3 + 4a - ab^2 - 3b^3 \pmod{3^2}$
 $\equiv 3 + 4a - a(a+1) - 3(a+1) \pmod{3^2} \equiv 3a \equiv 0 \pmod{3^2}$.
- $Z = 1 + 2a - ab^2 - 3b^2 + a^2 + b^4 + b^2 - ab^2$
 $\equiv 1 + 2a - a(a+1) - 3(a+1) + a^2 + (a+1)^2 + a + 1 \equiv -a(a+1) \pmod{3^3} \equiv 0 \pmod{3^3}$.

e concluímos que $\frac{1 - b\theta + \theta^2}{3}$ é um elemento 3-integral do corpo $\mathbb{K}$. Portanto, $(i, j) = (0, 1)$. Logo, pelo Teorema 5.3, segue que $\left\{1, \theta \frac{1 - b\theta + \theta^2}{3}\right\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 - 2 = 1$.

Caso A8: Por hipótese,

$$\begin{aligned} v_3(a) &\geq 1 \Rightarrow 3|a \Rightarrow 3^3|a^3 \\ v_3(b) &= 0 \Rightarrow 3 \nmid b. \end{aligned}$$

Também por hipótese, segue que $a \not\equiv 3 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{9}$. Dessa forma

$$\begin{aligned} \Delta &= 2^2a^3 - 3^3b^2 = 2^2a^3 - 3^3(b^2 - (a + 1) + (a + 1)) \\ &= 4a^3 - 3^3(a + 1) - 3^3(b^2 - (a + 1)). \end{aligned}$$

Note que

$$3 \nmid a + 1 \Rightarrow 3^3|3^3(a + 1) \text{ e } 3^4 \nmid 3^2(a + 1).$$

Assim,

$$3^3|4a^3 - 3^3(a + 1) \text{ e } 3^4 \nmid 4a^3 - 3^3(a + 1),$$

ou seja,

$$v_3(4a^3 - 3^3(a + 1)) = 3.$$

Além disso,

$$\begin{aligned} 3 \nmid b &\Rightarrow b \equiv 1 \text{ ou } 2 \pmod{3} \\ &\Rightarrow b = 3k + 1 \text{ ou } b = 3k + 2, \text{ com } k \in \mathbb{Z} \\ &\Rightarrow b^2 = 3^2k^2 + 2 \cdot 3k + 1 \text{ ou } b^2 = 3^2k^2 + 2^2 \cdot 3k + 2^2. \end{aligned}$$

Agora, se $a = 3q$, $q \in \mathbb{Z}$, então $a + 1 = 3q + 1$. Assim,

$$b^2 - (a + 1) = 3^2k^2 + 2 \cdot 3k - 3q \equiv 0 \pmod{3},$$

ou seja,

$$b^2 - (a + 1) = 3^2k^2 + 2^2 \cdot 3k - 3q + 3 \equiv 0 \pmod{3},$$

e assim, $3^4|3^3(b^2 - (a + 1))$. Logo,

$$s_3 = v_3(\Delta) = v_3(4a^3 - 3^3(a + 1) - 3^3(b^2 - (a + 1))) = 3.$$

Com isso, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{3} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^2}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3}. \end{cases}$$

Note que, como $a \equiv 0 \pmod{3}$ e $a \not\equiv 3 \pmod{9}$, segue que $a \equiv 0$ ou $6 \pmod{9}$. Se $a \equiv 0 \pmod{9}$, então

$$Y \equiv 3x^2 + 3by \equiv 0 \pmod{9} \Rightarrow x^2 + by \equiv 0 \pmod{3}.$$

E, uma vez que $3 \nmid b$, para que isso ocorra, obtemos as seguintes possibilidades:

1. $x \equiv y \equiv 0 \pmod{3}$.
2. $x \equiv y \equiv 1 \pmod{3}$ e $b \equiv 2 \pmod{3}$.
3. $x \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{3}$ e $b \equiv 1 \pmod{3}$.
4. $x \equiv 2 \pmod{3}$, $y \equiv 1 \pmod{3}$ e $b \equiv 2 \pmod{3}$.
5. $x \equiv y \equiv 2 \pmod{3}$ e $b \equiv 1 \pmod{3}$.

Vamos analisar cada caso:

1. Se $x \equiv y \equiv 0 \pmod{3}$, então $Z \equiv b^2 \equiv 0 \pmod{3^3}$, o que não ocorre.
2. Se $x \equiv y \equiv 1 \pmod{3}$ e $b \equiv 2 \pmod{3}$, então $x = 3r + 1$ e $y = 3s + 1$, com $r, s \in \mathbb{Z}$. Assim,

$$\begin{aligned} Z &\equiv 1 + 3b(3r + 3s + 1) - b + b^2 \equiv 0 \pmod{9} \Rightarrow (b + 1)^2 \equiv 0 \pmod{9} \\ &\Rightarrow b - 1 \equiv 0 \pmod{9} \Rightarrow b^2 \equiv 1 \pmod{9}. \end{aligned}$$

Mas, por hipótese,

$$a \equiv 0 \pmod{9} \Rightarrow a + 1 \equiv 1 \pmod{9}.$$

Assim, $b^2 \equiv 1 \equiv a + 1 \pmod{9}$, o que é um absurdo.

3. Se $x \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{3}$ e $b \equiv 1 \pmod{3}$, então $x = 3r + 1$ e $y = 3s + 2$, com $r, s \in \mathbb{Z}$ e, dessa forma,

$$\begin{aligned} Z &\equiv 1 + 3b(6r + 3s + 2) + b + b^2 \equiv 1 + 7b + b^2 \equiv b^2 - 2b + 1 \equiv (b - 1)^2 \\ &\equiv 0 \pmod{9} \Rightarrow b - 1 \equiv 0 \pmod{9} \Rightarrow b^2 \equiv 1 \pmod{9} \equiv a + 1 \pmod{9}, \end{aligned}$$

o que é um absurdo.

4. Se $x \equiv 2 \pmod{3}$, $y \equiv 1 \pmod{3}$ e $b \equiv 2 \pmod{3}$, então $x = 3r + 2$, $y = 3s + 1$ e $b = 3t + 2$ com $r, s, t \in \mathbb{Z}$. Com isso,

$$\begin{aligned} x^2 &\equiv 12r + 4 \pmod{9}, \quad x^3 \equiv 8 \equiv -1 \pmod{9}, \\ y^2 &\equiv 6s + 1 \pmod{9}, \quad y^3 \equiv 1 \pmod{9}, \\ b^2 &\equiv 12t + 4 \pmod{9} \quad \text{e} \quad bxy \equiv 6r + 12s + 6t + 4 \pmod{9}. \end{aligned}$$

Dessa forma,

$$Z \equiv -1 - 3 + 2 + 12r + 4 \equiv 0 \pmod{9} \Rightarrow 2(6r + 1) \equiv 0 \pmod{9} \Rightarrow 6r + 1 \equiv 0 \pmod{9}.$$

Se $r = 3r'$, $r' \in \mathbb{Z}$, então $1 \equiv 0 \pmod{9}$, que é um absurdo. Se $r = 3r' + 1$, $r' \in \mathbb{Z}$, então $9 \equiv 0 \pmod{9}$, que é um absurdo. Se $r = 3r' + 2$, $r' \in \mathbb{Z}$, então $13 \equiv 0 \pmod{9}$, que também é um absurdo. Portanto, este caso não ocorre.

5. Se $x \equiv y \equiv 2 \pmod{3}$ e $b \equiv 1 \pmod{3}$, então $x = 3r + 2$, $y = 3s + 2$ e $b = 3t + 1$ com $r, s, t \in \mathbb{Z}$. Com isso,

$$\begin{aligned} x^2 &\equiv 12r + 4 \pmod{9}, \quad x^3 \equiv -1 \pmod{9}, \\ y^2 &\equiv 12s + 4 \pmod{9}, \quad y^3 \equiv -1 \pmod{9}, \\ b^2 &\equiv 6t + 1 \pmod{9}, \quad by^3 \equiv 24t - 1 \pmod{9} \quad \text{e} \\ bxy &\equiv 6r + 6s + 12t + 4 \pmod{9}. \end{aligned}$$

Assim, $Z \equiv 0 \pmod{3^3} \equiv 0 \pmod{9} \Rightarrow 13 - 18t \equiv 13 \equiv 0 \pmod{9}$, o que é um absurdo.

Portanto, $a \equiv 6 \pmod{9}$. Assim,

$$\begin{aligned} Y &\equiv 3x^2 + 24x - 6y^2 + 3by \equiv 0 \pmod{9} \\ &\Rightarrow x^2 + 8x - 2y^2 + by \equiv 0 \pmod{3} \\ &\Rightarrow x(x + 2) + y(y + b) \equiv 0 \pmod{3} \end{aligned}$$

que, por sua vez, ocorre nas possibilidades:

1. $x \equiv y \equiv 0 \pmod{3}$.
2. $x \equiv 0 \pmod{3}$ e $y \equiv -b \pmod{3}$.
3. $y \equiv 0 \pmod{3}$ e $x \equiv -2 \equiv 1 \pmod{3}$.
4. $x \equiv -2 \equiv 1 \pmod{3}$ e $y \equiv -b \pmod{3}$.

Novamente, analisamos cada caso.

1. Se $x \equiv y \equiv 0 \pmod{3}$, então

$$Z \equiv 0 \pmod{3^3} \equiv 0 \pmod{3} \Rightarrow b^2 \equiv 0 \pmod{3},$$

o que é um absurdo.

2. Se $x \equiv 0 \pmod{3}$ e $y \equiv -b \pmod{3}$, então

$$Z \equiv b^2 - by^3 \equiv 0 \pmod{3} \Rightarrow b^2(b^2 + 1) \equiv 0 \pmod{3} \Rightarrow b^2 \equiv -1 \equiv 2 \pmod{3},$$

que não tem solução.

3. Se $y \equiv 0 \pmod{3}$ e $x \equiv -2 \equiv 1 \pmod{3}$, então

$$Z \equiv 1 + b^2 \equiv 0 \pmod{3} \Rightarrow b^2 \equiv -1 \equiv 2 \pmod{3},$$

que não tem solução.

4. Se $x \equiv -2 \equiv 1 \pmod{3}$ e $y \equiv -b \pmod{3}$, então $x = 3r + 1$ e $y = 3s - b$, com $r, s \in \mathbb{Z}$. Além disso, estamos considerando $a = 9k + 6$, $k \in \mathbb{Z}$. Assim,

$$\begin{aligned} Z &\equiv b^4 - 9b^3s - 18b^2k - 14b^2 + 63bs + 126k + 49 \equiv 0 \pmod{27} \equiv 0 \pmod{9} \\ &\Rightarrow (b^2 - 7)^2 - 9(b^3s + 2b^2k - 7bs - 14k) \equiv (b^2 - 7)^2 \equiv 0 \pmod{9} \Rightarrow b^2 \equiv 7 \pmod{9}, \end{aligned}$$

o que é um absurdo, pois $a + 1 \equiv 7 \pmod{9}$.

Logo, para todo $x, y \in \mathbb{Z}$, segue que $\frac{x + y\theta + \theta^2}{3}$ não é um elemento 3-integral do corpo $\mathbb{K}$. Portanto, $(i, j) = (0, 0)$ e, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 = 3$.

Caso B9: Por hipótese,

$$\begin{cases} a \equiv 3 \pmod{9} \Rightarrow a = 9k + 3, \ k \in \mathbb{Z}, \\ v_3(b) = 0 \Rightarrow 3 \nmid b, \\ b^2 \equiv 4 \pmod{9} \Rightarrow b^2 = 9q + 4, \ q \in \mathbb{Z} \\ b^2 \not\equiv a + 1 \pmod{27}. \end{cases}$$

Dessa forma,

$$\Delta = 4a^3 - 27[b^2 - (a + 1) + (a + 1)] = 4a^3 - 27(a + 1) - 27[b^2 - (a + 1)].$$

Note que,

$$\begin{aligned} 4a^3 - 27(a + 1) &= 4[3(3k + 1)]^3 - 3^3(9k + 4) = 3^6(4k^3 + 4k^4 + k) \\ &\Rightarrow v_3(4a^3 - 27(a + 1)) \geq 6 \quad \text{e} \\ 27[b^2 - (a + 1)] &= 3^3(9q + 4 - 9k - 3 - 1) = 3^5(q - k) \\ &\Rightarrow v_3(27[b^2 - (a + 1)]) = 5. \end{aligned}$$

Portanto, $s_3 = v_3(\Delta) = 5$. Vamos supor que exista $x \in \mathbb{Z}$ tal que o elemento $\frac{x + \theta}{3} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3}. \\ Y = 3x^2 - a \equiv 0 \pmod{3^2}. \\ Z = x^3 - ax - b \equiv 0 \pmod{3^3}. \end{cases}$$

Desse modo,

1. $Y = 3x^2 - a \equiv 0 \pmod{3^2} \Rightarrow 3x^2 \equiv a \equiv 3 \pmod{9} \Rightarrow x^2 \equiv 1 \pmod{3} \Rightarrow x \equiv \pm 1 \pmod{3}$.
2. $Z = x^3 - ax - b \equiv 0 \pmod{3^3} \Rightarrow b \equiv x^3 - ax \pmod{27}$.

(a) se $x \equiv 1 \pmod{3}$, então $x = 3r + 1$, $r \in \mathbb{Z}$ e

$$b \equiv 9r + 1 - 3ar - a \equiv (1 - a) - 3r(a - 3) \equiv 1 - a \pmod{27}.$$

(b) se $x \equiv -1 \pmod{3}$, então $x = 3r - 1$, $r \in \mathbb{Z}$ e

$$b \equiv 9r - 1 - 3ar + a \equiv -(1 - a) - 3r(a - 3) \equiv -(1 - a) \pmod{27}.$$

Logo, $b \equiv \pm(1 - a) \pmod{27}$. Assim,

$$b^2 \equiv (1 - a)^2 \equiv 1 - 2a + a^2 \pmod{27}.$$

Note que

$$a^2 + 1 = 81k^2 + 2.27k + 9 + 1 \equiv 10 \pmod{27}.$$

Assim, $b^2 \equiv 10 - 2a \pmod{27}$. Além disso,

$$10 - 2a = 4 - 18k = 1 + 3 - 18k \equiv 1 + 3 + 9k \pmod{27} \Rightarrow b^2 \equiv 10 - 2a \equiv 1 + a \pmod{27},$$

o que é um absurdo.

Portanto, para todo $x \in \mathbb{Z}$, segue que $\frac{x + \theta}{3}$ não é um elemento 3-integral do corpo $\mathbb{K}$.

Agora, considere o elemento $\frac{1 - b\theta + \theta^2}{3} \in \mathbb{K}$. Neste caso, com a notação do Teorema 5.1, segue que

- $X = 3 - 2a$.
- $Y = 3 + 4a - ab^2 + a^2 - 3b^2$.
- $Z = 1 + 2a - ab^2 - 3b^2 + a^2 + b^4 + b^2 - ab^2$.

Com isso,

- $a \equiv 0 \pmod{3} \Rightarrow X \equiv 0 \pmod{3}$.
- $a = 3k + 3$ e $b^2 = 9q + 4 \Rightarrow Y \equiv -9 \equiv 0 \pmod{3^2}$.
- $Z = 1 + 2a - ab^2 - 3b^2 + a^2 + b^4 + b^2 - ab^2 = (b^2 - (a + 1))^2$.

Note que

$$\begin{aligned} a + 1 &\equiv 4 \pmod{9} \equiv b^2 \pmod{9} \Rightarrow b^2 - (a + 1) \equiv 0 \pmod{9} \\ &\Rightarrow (b^2 - (a + 1))^2 \equiv 0 \pmod{9^2} \equiv 0 \pmod{27} \Rightarrow Z \equiv 0 \pmod{3^3}. \end{aligned}$$

Portanto, $\frac{1 - b\theta + \theta^2}{3}$ é um elemento 3-integral de $\mathbb{K}$. Agora, vamos supor que existam

$x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{3^2} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3^2}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^4}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^6}. \end{cases}$$

Assim,

- $X \equiv 3x + 6 \equiv 0 \pmod{9} \Rightarrow x + 2 \equiv 0 \pmod{3} \Rightarrow x \equiv -2 \equiv 1 \pmod{3}$
 $\Rightarrow x = 3B + 1$, com $B \in \mathbb{Z}$.
- $Y \equiv 0 \pmod{3^4} \equiv 0 \pmod{3^2} \Rightarrow 3 + 12 - 3y^2 + 3by \equiv 0 \pmod{9}$
 $\Rightarrow 3(5 - y^2 + by) \equiv 0 \pmod{9} \Rightarrow 5 - y^2 + by \equiv 0 \pmod{3}$
 $\Rightarrow y(b - y) \equiv -5 \equiv 1 \pmod{3}$.

Isto ocorre quando

$$y \equiv b - y \equiv 1 \pmod{3} \quad \text{ou} \quad y \equiv b - y \equiv -1 \pmod{3}$$

e, em ambos os casos, obtemos

$$y \equiv -b \pmod{3} \Rightarrow y = 3C - b, \text{ com } C \in \mathbb{Z}.$$

Dessa forma, uma vez que $a \equiv 3 \pmod{9}$, obtemos as seguintes possibilidades:

1. $a \equiv 3 \pmod{27}$, $x \equiv 1 \pmod{3}$ e $y \equiv -b \pmod{3}$.
2. $a \equiv 12 \pmod{27}$, $x \equiv 1 \pmod{3}$ e $y \equiv -b \pmod{3}$.
3. $a \equiv 21 \pmod{27}$, $x \equiv 1 \pmod{3}$ e $y \equiv -b \pmod{3}$.

Vamos analisar essas possibilidades.

1. Se $a \equiv 3 \pmod{27}$, então $a = 27A + 3$, com $A \in \mathbb{Z}$. Neste caso, $b^2 \not\equiv 4 \pmod{27}$, pois $b^2 \not\equiv a + 1 \equiv 4 \pmod{27}$. Além disso,

$$\begin{aligned} Y &\equiv -27Ab^2 + 270A - 6b^2 + 27bC + 27bC + 27B^2 + 54B - 27C^2 + 24 \equiv 0 \pmod{3^4} \\ &\Rightarrow 9B^2 - 9C^2 + 18B + 9bC + 2(4 - b^2) \equiv 0 \pmod{3^3}, \end{aligned}$$

e, uma vez que $b^2 \not\equiv 4 \pmod{27}$, segue que

$$B^2 - C^2 + 2B + bC \not\equiv 0 \pmod{3} \Rightarrow B(B + 2) + C(b - C) \not\equiv 0 \pmod{3},$$

que ocorre nos casos

- (a) $B \equiv 0 \pmod{3}$ e $C \equiv -b \pmod{3}$.
- (b) $B \equiv 1 \pmod{3}$ e $C \equiv -b \pmod{3}$.
- (c) $B \equiv 2 \pmod{3}$ e $C \equiv 0 \pmod{3}$.
- (d) $B \equiv 2 \pmod{3}$ e $C \equiv b \pmod{3}$.

Assim,

- (a) Se $B \equiv 0 \pmod{3}$ e $C \equiv -b \pmod{3}$, então $B = 3J$ e $C = 3K - b$, com $J, K \in \mathbb{Z}$. Assim, $x = 9J + 1$ e $y = 9K - 4b$. Com isso, segue que

$$\begin{aligned} Z &\equiv 0 \pmod{3^6} \equiv 0 \pmod{3^4} \Rightarrow \\ Z &\equiv (286 - 540b^2)A + (270 - 432b^2)bK + (216 - 540b^2)J + 64b^4 - 71b^2 + 16 \\ &\equiv 0 \pmod{3^4} \end{aligned}$$

Agora, uma vez que $b^2 = 9q + 4$, segue que

$$(286 - 540b^2)A \equiv (270 - 432b^2)bK \equiv (216 - 540b^2)J \equiv 0 \pmod{3^4}.$$

E ainda,

$$Z \equiv 64b^4 - 71b^2 + 16 \equiv 72q + 9q + 108 \equiv 27 \equiv 0 \pmod{3^3},$$

o que é um absurdo.

- (b) Para $B \equiv 1 \pmod{3}$ e $C \equiv -b \pmod{3}$, segue que $x = 3J + 4$ e $y = 9K - 4b$, com $J, K \in \mathbb{Z}$. Com isso, de maneira análoga ao caso (a), obtemos que $Z \equiv 54 \equiv 0 \pmod{3^4}$, que é uma contradição.
- (c) Para $B \equiv 2 \pmod{3}$ e $C \equiv 0 \pmod{3}$, segue que $x = 9J + 7$ e $y = 9K - b$, com $J, K \in \mathbb{Z}$. Com isso, $Z \equiv 54 \equiv 0 \pmod{3^4}$, que é uma contradição.

- (d) Para $B \equiv 2 \pmod{3}$ e $C \equiv b \pmod{3}$, segue que $x = 9J + 7$ e $y = 9K + 2b$, com $J, K \in \mathbb{Z}$. Com isso, $Z \equiv 27 \equiv 0 \pmod{3^4}$, que é um absurdo.

2. Se $a \equiv 12 \pmod{27}$, então $a = 27A + 12$, com $A \in \mathbb{Z}$. Neste caso,

$$\begin{aligned} Y &\equiv -27Ab^2 + 756A - 15b^2 + 27B^2 - 108C^2 + 195 \equiv 0 \pmod{3^4} \\ &\Rightarrow 9B^2 - 36C^2 - 5b^2 + 11 \equiv 3 \pmod{3^3}. \end{aligned}$$

Uma vez que $b^2 \equiv 4 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{27}$, segue que

$$B^2 - C^2 \not\equiv 0 \pmod{3},$$

que acontece nos casos

- (a) $B \equiv 0 \pmod{3}$ e $C \equiv b \pmod{3}$.
- (b) $B \equiv 1 \pmod{3}$ e $C \equiv 0 \pmod{3}$.
- (c) $B \equiv 2 \pmod{3}$ e $C \equiv 0 \pmod{3}$.
- (d) $B \equiv 0 \pmod{3}$ e $C \equiv -b \pmod{3}$.

Assim,

- (a) Se $B \equiv 0 \pmod{3}$ e $C \equiv b \pmod{3}$, então $B = 3J$ e $C = 3K + b$, com $J, K \in \mathbb{Z}$. Assim, $x = 9J + 1$ e $y = 9K + 2b$. Com isso, segue que

$$\begin{aligned} Z &\equiv 0 \pmod{3^6} \equiv 0 \pmod{3^4} \Rightarrow \\ Z &\equiv (702 - 54b^2)A - (297 + 108b^2)bK + (1755 - 378b^2)J - 8b^4 - 17b^2 + 169 \\ &\equiv 0 \pmod{3^4}. \end{aligned}$$

Agora, uma vez que $b^2 = 9q + 4$, segue que

$$Z \equiv -8b^4 - 17b^2 + 169 \equiv 27 \equiv 0 \pmod{3^4},$$

o que é um absurdo.

- (b) Se $B \equiv 1 \pmod{3}$ e $C \equiv 0 \pmod{3}$, então $x = 9J + 4$ e $y = 9K - b$, com $J, K \in \mathbb{Z}$. Com isso, $Z \equiv 27 \equiv 0 \pmod{3^4}$, que é um absurdo.
- (c) Se $B \equiv 2 \pmod{3}$ e $C \equiv 0 \pmod{3}$, então $x = 9J + 7$ e $y = 9K - b$, com $J, K \in \mathbb{Z}$. Com isso, chegamos que $Z \equiv 54 \equiv 0 \pmod{3^4}$, que é um absurdo.
- (d) Se $B \equiv 0 \pmod{3}$ e $C \equiv -b \pmod{3}$, então $x = 9J + 1$ e $y = 9K - 4b$, com $J, K \in \mathbb{Z}$. Com isso, $Z \equiv 27 \equiv 0 \pmod{3^4}$, que não ocorre.

3. Se $a \equiv 21 \equiv -6 \pmod{27}$, então $a = 27A - 6$, com $A \in \mathbb{Z}$. Neste caso,

$$\begin{aligned} Y &\equiv -17Ab^2 - 216A + 3b^2 - 27bC + 27b^2 - 54B + 54C^2 + 15 \equiv 0 \pmod{3^4} \\ &\Rightarrow -9Ab^2 - 72A + b^2 - 9bC + 9B^2 - 18B + 18C^2 + 5 \\ &\equiv 9B(B - 2) + 9C(2C - b) + b^2 + 5 \equiv 0 \pmod{3^3}. \end{aligned}$$

Como $b^2 \equiv 4 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{27}$, segue que

$$B(B - 2) + C(2C - b) \not\equiv 0 \pmod{3},$$

o que ocorre nos casos

- (a) $B \equiv 0 \pmod{3}$ e $C \equiv b \pmod{3}$.
- (b) $B \equiv 1 \pmod{3}$ e $C \equiv 0 \pmod{3}$.
- (c) $B \equiv 1 \pmod{3}$ e $C \equiv -b \pmod{3}$.
- (d) $B \equiv 2 \pmod{3}$ e $C \equiv b \pmod{3}$.

Desse modo,

- (a) Se $B \equiv 0 \pmod{3}$ e $C \equiv b \pmod{3}$, então $B = 3J$ e $C = 3K + b$, com $J, K \in \mathbb{Z}$. Assim, $x = 9J + 1$ e $y = 9K + 2b$. Com isso, segue que

$$\begin{aligned} Z &\equiv 0 \pmod{3^6} \equiv 0 \pmod{3^4} \Rightarrow \\ Z &\equiv -(270 + 54b^2)A + (189 + 108b^2)bK + (135 + 270b^2)J - 8b^4 + 19b^2 + 25 \\ &\equiv 0 \pmod{3^4} \end{aligned}$$

Como $b^2 = 9q + 4$, segue que

$$Z \equiv -8b^4 + 19b^2 + 2527 \equiv 0 \pmod{3^4},$$

o que é um absurdo.

- (b) Se $B \equiv 1 \pmod{3}$ e $C \equiv 0 \pmod{3}$, então $x = 9J + 4$ e $y = 9K - b$, com $J, K \in \mathbb{Z}$. Com isso, $Z \equiv 27 \equiv 0 \pmod{3^4}$, que é um absurdo.
- (c) Se $B \equiv 1 \pmod{3}$ e $C \equiv -b \pmod{3}$, então $x = 9J + 4$ e $y = 9K - 4b$, com $J, K \in \mathbb{Z}$. Com isso, segue que $Z \equiv 54 \equiv 0 \pmod{3^4}$, que é uma contradição.
- (d) Se $B \equiv 2 \pmod{3}$ e $C \equiv b \pmod{3}$, então $x = 9J + 7$ e $y = 9K + 2b$, com $J, K \in \mathbb{Z}$. Com isso, $Z \equiv 27 \equiv 0 \pmod{3^4}$, o que não ocorre.

Portanto, para todo $x, y \in \mathbb{Z}$, segue que $\frac{x + y\theta + \theta^2}{3^2}$ não é um elemento 3-integral do corpo $\mathbb{K}$. Logo, $(i, j) = (0, 1)$ e, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{1 - b\theta + \theta^2}{3}\right\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 - 2 = 3$.

Caso B10: Por hipótese,

$$\begin{cases} v_3(b) = 0 \Rightarrow 3 \nmid b, \\ a \equiv 3 \pmod{9} \Rightarrow a = 9k + 3, \ k \in \mathbb{Z}, \\ b^2 \not\equiv 4 \pmod{9}, \end{cases}$$

ou seja, $b^2 \not\equiv a + 1 \pmod{9}$. Assim,

$$\Delta = 4a^3 - 27(a + 1) - 27[b^2 - (a + 1)].$$

Note que

$$4a^3 - 27(a + 1) = 4 \cdot 3^6 k^3 + 4 \cdot 3^6 k^2 + 3^6 k \Rightarrow v_3(4a^3 - 27(a + 1)) \geq 6 \text{ e}$$

$$27[b^2 - (a + 1)] = 3^3(b^2 - 4) - 3^5 k \Rightarrow v_3(27[b^2 - (a + 1)]) = 4.$$

Portanto, $s_3 = v_3(\Delta) = 4$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{3} \in \mathbb{K}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{3}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^2}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3}. \end{cases}$$

Com isso,

$$\begin{aligned} Y &\equiv 3x^2 + 4(9k + 3)x - (9k + 3)y^2 + 3by \equiv 0 \pmod{9} \\ &\Rightarrow 3x^2 + 12x - 3y^2 + 3by \equiv 0 \pmod{9} \\ &\Rightarrow x^2 + 4x - y^2 + by \equiv 0 \pmod{3} \\ &\Rightarrow x(x + 1) - y(y - b) \equiv 0 \pmod{3}. \end{aligned}$$

e, para que isso ocorra, obtemos as seguintes possibilidades:

1. $x \equiv y \equiv 0 \pmod{3}$.
2. $x \equiv 0 \pmod{3}$ e $y \equiv b \pmod{3}$.
3. $x \equiv 1 \pmod{3}$ e $y \equiv -b \pmod{3}$.
4. $x \equiv 2 \pmod{3}$ e $y \equiv 0 \pmod{3}$.
5. $x \equiv 2 \pmod{3}$ e $y \equiv b \pmod{3}$.

Vamos analisar as possibilidades:

1. Se $x \equiv y \equiv 0 \pmod{3}$, então

$$\begin{aligned} Z &\equiv b^2 + ay \equiv 0 \pmod{27} \Rightarrow b(b + ay) \equiv 0 \pmod{27} \\ &\Rightarrow b + ay \equiv 0 \pmod{27} \equiv 0 \pmod{9} \Rightarrow b \equiv 0 \pmod{9}, \end{aligned}$$

o que é um absurdo.

2. Se $x \equiv 0 \pmod{3}$ e $y \equiv b \pmod{3}$, seja $y = 3B + b$, $B \in \mathbb{Z}$. Logo,

$$\begin{aligned} Z &\equiv 0 \pmod{27} \equiv 0 \pmod{9} \\ &\Rightarrow -by^3 + b^2 + aby \equiv -b(3B + b)^3 + b^2 + ab(3B + b) \equiv b^2[(a + 1) - b^2] \equiv 0 \pmod{9}. \end{aligned}$$

Assim, uma vez que $b^2 \not\equiv a + 1 \pmod{9}$, segue que $b^2 \equiv 0 \pmod{9}$. Assim, $b \equiv 0 \pmod{3}$, o que é um absurdo.

3. Se $x \equiv 1 \pmod{3}$ e $y \equiv -b \pmod{3}$, então $x = 3A + a$, $A \in \mathbb{Z}$ e

$$\begin{aligned} Z &\equiv x^3 + 2ax^2 + b^2 \equiv (3^3A^3 + 3^32A^2 + 3^34A + 8) + 2.3(3^2A^2 + 4.3A + 4) + b^2 \\ &\equiv 32 + b^2 \equiv 0 \pmod{9} \Rightarrow b^2 \equiv 4 \pmod{9}, \end{aligned}$$

o que é um absurdo.

4. Se $x \equiv 2 \pmod{3}$ e $y \equiv 0 \pmod{3}$, então $x = 3A + 2$, $A \in \mathbb{Z}$ e $y = 3B + b$, $B \in \mathbb{Z}$. Assim,

$$\begin{aligned} Z &\equiv x^3 - by^3 + b^2 \equiv 0 \pmod{3} \Rightarrow (3A + 2)^3 - b(3B + b)^3 + b^2 \\ &\equiv -1 + b^2(1 - b^2) \equiv 0 \pmod{3} \Rightarrow b^2(1 - b^2) \equiv 1 \pmod{3} \Rightarrow b^2 \equiv 1 \pmod{3} \end{aligned}$$

Mas $1 - b^2 \equiv 1 \pmod{3} \Rightarrow b^2 \equiv 0 \pmod{3}$, o que é um absurdo.

5. Se $x \equiv 2 \pmod{3}$ e $y \equiv b \pmod{3}$, então $x = 3A + 1$, $A \in \mathbb{Z}$ e $y = 3B - b$, $B \in \mathbb{Z}$. Assim,

$$\begin{aligned} Z &\equiv 0 \pmod{27} \equiv 0 \pmod{9} \\ &\Rightarrow 7 - 6b^2 + b^4 - 2b^2 \equiv (b^2 - 4)^2 \equiv 0 \pmod{9} \\ &\Rightarrow b^2 \equiv 4 \pmod{0}, \end{aligned}$$

o que é um absurdo.

Portanto, para todo $x, y \in \mathbb{Z}$, segue que $\frac{x + y\theta + \theta^2}{3}$ não é um elemento 3-integral do corpo $\mathbb{K}$. Com isso, pela Observação 5.4, para todo $x \in \mathbb{Z}$, segue que o elemento $\frac{x + \theta}{3}$ também não é um elemento 3-integral do corpo $\mathbb{K}$. Logo, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 = 4$.

Caso B11: Por hipótese,

$$\begin{cases} v_3(b) = 0 \Rightarrow 3 \nmid b, \\ a \equiv 3 \pmod{9} \Rightarrow a = 9k + 3, \quad k \in \mathbb{Z}, \\ b^2 \equiv a + 1 \pmod{27} \Rightarrow b^2 = 3^3q + 3^2k + 2^2, \quad q \in \mathbb{Z}. \end{cases}$$

Dessa forma,

$$\begin{aligned} \Delta &= 2^2(9k + 3)^3 - 3^3(3^3q + 3^2k + 2^2) = 2^23^6k^3 + 2^23^6k^2 + 3^6k - 3^6q \\ &\Rightarrow s_3 = v_3(\Delta) \geq 6. \end{aligned}$$

Considere o elemento $\frac{b + \theta}{3} \in \mathbb{K}$. Com a notação do Teorema 5.1, segue que

- $X = 3b \equiv 0 \pmod{3}$.
- $Y = 3b^2 - a = 3(3^3q + 3^2k + 2^2) - 9k - 3 = 3^4q + 3^3k - 3^2k + 3^2 \equiv 0 \pmod{3^2}$.
- $Z = b^3 - ab - b = b(3^3q + 3^2k + 2^2) - b(a + 1) = 27bq \equiv 0 \pmod{3^3}$.

e concluímos que $\frac{b + \theta}{3}$ é um elemento 3-integral do corpo $\mathbb{K}$. Vamos supor que exista $x \in \mathbb{Z}$ tal que o elemento $\frac{x + \theta}{3^2}$ seja 3-integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x \equiv 0 \pmod{3^2}. \\ Y = 3x^2 - a \equiv 0 \pmod{3^4}. \\ Z = x^3 - ax - b \equiv 0 \pmod{3^6}. \end{cases}$$

Com isso,

- $3x \equiv 0 \pmod{3^2} \Rightarrow x \equiv 0 \pmod{3}$,
- $3x^2 - a \equiv 0 \pmod{3^4} \equiv 0 \pmod{3^3} \Rightarrow a \equiv 0 \pmod{3^3}$, o que não ocorre.

Portanto, para todo $x \in \mathbb{Z}$, segue que $\frac{x+\theta}{3^2}$ não é um elemento 3-integral do corpo $\mathbb{K}$. Com isso, concluímos que $i = 1$. Agora, como $s_3 \geq 6$, podemos definir $m = \left\lfloor \frac{s_3 - 2}{2} \right\rfloor \in \mathbb{Z}$ como a parte inteira da fração e $m \geq 2$. Note que $2m + 2 = s_3 \Rightarrow 3^{2m+2} \mid \Delta$. Vamos definir $x, y, z \in \mathbb{Z}$ de modo que

$$\begin{cases} x \equiv \frac{-2a}{3} \pmod{3^m}. \\ 2ay \equiv 3b \pmod{3^{m+2}}. \\ z = 1. \end{cases}$$

Assim, com a notação do Teorema 5.2, segue que

- $X = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{3^{m+1}}$.
- $3bU = 3b(9by - 2a^2) = (2^2a^3 - \Delta)y - 6a^2b = 4a^3y - 6a^2b - \Delta y$
 $\equiv 4a^3y - 6a^2b \pmod{3^{2m+2}} \equiv (2ay)(2a^2) - 6a^2b \pmod{3^{m+4}} \equiv 3b(2a^2) - 6a^2b$
 $\equiv 0 \pmod{3^{m+4}}$

Assim,

$$3bU \equiv 0 \pmod{3^{m+4}} \Rightarrow U \equiv 0 \pmod{3^{m+3}}.$$

- $V = 2ay - 3b \equiv 3b - 3b \equiv 0 \pmod{3^{m+2}}$.
- $Y = \frac{1}{2^2 3 a^2} (2^2 a^2 X^2 - U^2 - 3 \Delta y^2) \equiv 0 \pmod{3^{2m}}$.
- $Z = \frac{1}{2^2 3^3 a^3} (2^2 a^3 X^3 - 3aXU^2 - 3^2 a \Delta X y^2 - 3U^3 - 3^2 \Delta U y^2 + 2a \Delta U + 3^3 b V^3$
 $+ 2 \cdot 3^2 b \Delta V + \Delta^2) \equiv 0 \pmod{3^{3m}}$.

Portanto, pelo Teorema 5.1, segue que $\frac{x+y\theta+\theta^2}{3^m}$ é um elemento 3-integral do corpo $\mathbb{K}$, com $m = \left\lfloor \frac{s_3 - 2}{2} \right\rfloor$ e x e y como definidos anteriormente. Note que, como $i = 1$ e, pela Observação 5.4, $i + j \leq \frac{s_3}{2}$, segue que $j \leq \frac{s_3 - 2}{2} = m$ e concluímos que $j = m$. Portanto, pelo Teorema 5.3, segue que $\left\{ 1, \frac{b+\theta}{3}, \frac{x+y\theta+\theta^2}{3^m} \right\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e $v_3(D(\mathbb{K})) = s_3 - 2(m+1) = s_3 - 2 \left\lfloor \frac{s_3}{2} \right\rfloor$, onde $\left\lfloor \frac{s_3}{2} \right\rfloor$ representa a parte inteira da fração. O que completa a demonstração. $\square$

Corolário 5.8. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_3(a) < 2$ ou $v_3(b) < 3$. Vamos definir os inteiros*

- R_3 dado por:

1. $R_3 \equiv \frac{-2a}{3} \pmod{3^{\lceil \frac{s_3}{2} \rceil - 1}}$, se $a \equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{27}$.
 2. $R_3 = 1$, se
 - (a) $v_3(a) \geq 1$, $a \not\equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{9}$, ou
 - (b) $a \equiv 3 \pmod{9}$, $b^2 \equiv 4 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{27}$.
 3. $R_3 = 0$, caso contrário.
- S_3 dado por:
 1. $\frac{2a}{3}S_3 \equiv b \pmod{3^{\lceil \frac{s_3}{2} \rceil}}$, se $a \equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{27}$;
 2. $S_3 = -b$, se
 - (a) $v_3(a) \geq 1$, $a \not\equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{9}$, ou
 - (b) $a \equiv 3 \pmod{9}$, $b^2 \equiv 4 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{27}$;
 3. $S_3 = 0$, caso contrário.
 - e T_3 é igual a
 1. $\left\lceil \frac{s_3}{2} \right\rceil - 1$, se $a \equiv 3 \pmod{9}$, $v_3(b) = 0$ e $b^2 \equiv a + 1 \pmod{27}$;
 2. 1, se
 - (a) $v_3(b) = v_3(a) = 2$, ou
 - (b) $v_3(a) > v_3(b) = 2$, ou
 - (c) $v_3(a) = 1$ e $v_3(b) = 0$, ou
 - (d) $v_3(b) = 0$, $v_3(a) \geq 1$, $a \not\equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{9}$, ou
 - (e) $v_3(b) = 0$, $a \equiv 3 \pmod{9}$, $b^2 \equiv 4 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{27}$;
 3. 0, caso contrário.

Com isso, $\left\{1, \theta, \frac{R_3 + S_3\theta + \theta^2}{3^{T_3}}\right\}$ é uma base 3-integral para o corpo $\mathbb{K}$, exceto no caso em que $a \equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{27}$. Neste caso, $\left\{1, \frac{b + \theta}{3}, \frac{R_3 + S_3\theta + \theta^2}{3^{T_3}}\right\}$ é uma base 3-integral para o corpo $\mathbb{K}$.

Demonstração. Segue diretamente do Teorema 5.7. □

5.4 Bases p -integrais de um corpo cúbico

Note que, dada θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$, com $p \in \mathbb{Z}$ primo, $p > 3$, obtemos as seguintes possibilidades:

1. $v_p(a) = v_p(b) = 0$.
2. $v_p(a) = 0$ e $v_p(b) \geq 1$ ou $v_p(b) = 0$ e $v_p(a) \geq 1$.
3. $v_p(a) \geq 1$ e $v_p(b) \geq 1$.

- (a) $v_p(b) = 1$.
- (b) $v_p(b) \geq 2$.
 - i. $v_p(a) = 1$.
 - ii. $v_p(a) \geq 2$.

O teorema que provamos nesta seção analisa as 5 possibilidades para encontrar bases p -integrais para o corpo $\mathbb{K}$.

Teorema 5.9. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irredutível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$, para $p \in \mathbb{Z}$ um número primo maior que 3. Uma base p -integral para o corpo $\mathbb{K}$ é dada na seguinte tabela:*

Tabela 5.3: Base p -integral para o corpo $\mathbb{K} = \mathbb{Q}(\theta)$, com $p > 3$.

Caso	condição	base p -integral	s_p	$v_p(D(\mathbb{K}))$
C1	$v_p(a) = 0$ e $v_p(b) \geq 1$ ou $v_p(a) \geq 1$ e $v_p(b) = 0$	$\{1, \theta, \theta^2\}$	0	0
C2	$1 = v_p(b) \leq v_p(a)$	$\{1, \theta, \theta^2\}$	2	2
C3	$2 = v_p(b) \leq v_p(a)$	$\left\{1, \theta, \frac{\theta^2}{p}\right\}$	4	2
C4	$1 = v_p(a) < v_p(b)$	$\left\{1, \theta, \frac{\theta^2}{p}\right\}$	3	1
C5	$v_p(a) = v_p(b) = 0$	$\left\{1, \theta, \frac{x + y\theta + \theta^2}{p^m}\right\}$, com $m = \left\lfloor \frac{s_p}{2} \right\rfloor$, $3x \equiv -2a \pmod{p^m}$ e $2ay \equiv 3b \pmod{p^m}$	$s_p \geq 0$	$s_p - 2 \left\lfloor \frac{s_p}{2} \right\rfloor$

Fonte: [3], p. 56.

Demonstração. Lembremos que $\Delta = 2^2a^3 - 3^3b^2$, $s_p = v_p(\Delta)$ e $\Delta_p = \frac{\Delta}{p^{s_p}}$.

Caso C1: Por hipótese,

$$\begin{cases} v_p(a) = 0 \text{ e } v_p(b) \geq 1 \text{ ou} \\ v_p(a) \geq 1 \text{ e } v_p(b) = 0. \end{cases}$$

Se $v_p(a) = 0$ e $v_p(b) \geq 1$, então $p \nmid a \Rightarrow p \nmid a^3$. Por outro lado, se $v_p(a) \geq 1$ e $v_p(b) = 0$, então $p \nmid b \Rightarrow p \nmid b^2$. Em ambos os casos, segue que $p \nmid \Delta$. Assim,

$$s_p = v_p(\Delta) = 0.$$

Pela Observação 5.4, segue que $(i, j) = (0, 0)$. Logo, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base p -integral para o corpo $\mathbb{K}$ e $v_p(D(\mathbb{K})) = s_p = 0$.

Caso C2: Por hipótese,

$$\begin{cases} v_p(a) \geq 1 \Rightarrow a = pq, \quad q \in \mathbb{Z} \text{ e} \\ v_p(b) = 1 \Rightarrow b = pk, \quad k \in \mathbb{Z}, \quad p \nmid k. \end{cases}$$

Dessa forma,

$$\Delta = 2^2 p^3 q^3 - 3^3 p^2 k^2 = p^2(2^2 p q^3 - 3^3 k^2), \quad p \nmid k^2 \Rightarrow s_p = v_p(\Delta) = 2.$$

Com isso, pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Vamos supor que existam $x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{p} \in \mathbb{K}$ seja p -integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{p}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{p^2}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{p^3}. \end{cases}$$

Assim,

- $X \equiv 3x \equiv 0 \pmod{p} \Rightarrow x \equiv 0 \pmod{p}.$
- $Z \equiv 0 \pmod{p^3} \equiv 0 \pmod{p^2} \Rightarrow -by^3 \equiv 0 \pmod{p^2} \Rightarrow y^3 \equiv 0 \pmod{p} \Rightarrow y \equiv 0 \pmod{p}.$

Com estes dois fatos, segue que

$$Z \equiv b^2 \equiv 0 \pmod{p^3} \Rightarrow b \equiv 0 \pmod{p^2},$$

o que é um absurdo. Portanto, para todo $x, y \in \mathbb{Z}$, segue que $\frac{x + y\theta + \theta^2}{p}$ não é um elemento p -integral do corpo $\mathbb{K}$. Logo, pelo Teorema 5.3, segue que $\{1, \theta, \theta^2\}$ é uma base p -integral para o corpo $\mathbb{K}$ e $v_p(D(\mathbb{K})) = s_p = 2$.

Caso C3: Por hipótese,

$$\begin{cases} v_p(a) \geq 2 \Rightarrow a = p^2 q, \quad q \in \mathbb{Z}, \\ v_p(b) = 2 \Rightarrow b = p^2 k, \quad k \in \mathbb{Z}, \quad p \nmid k. \end{cases}$$

Dessa forma,

$$\Delta = 2^2 p^6 q^3 - 3^3 p^4 k^2 = p^4(2^2 p^2 q^3 - 3^3 k^3), \quad p \nmid k^2 \Rightarrow s_p = v_p(\Delta) = 4.$$

Considere o elemento $\frac{\theta^2}{p} \in \mathbb{K}$. Com as notações do Teorema 5.1, segue que

- $X = 2a \equiv 0 \pmod{p}.$
- $Y = a^2 \equiv 0 \pmod{p^2}.$
- $Z = b^2 \equiv 0 \pmod{p^3}.$

e concluímos que $\frac{\theta^2}{p}$ é um elemento p -integral do corpo $\mathbb{K}$. Vamos supor que existam

$x, y \in \mathbb{Z}$ tais que o elemento $\frac{x + y\theta + \theta^2}{p^2} \in \mathbb{K}$ seja p -integral. Assim, pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{p^2}. \\ Y = 3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{p^4}. \\ Z = x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{p^6}. \end{cases}$$

Assim,

1. $X \equiv 3x \pmod{p^2} \Rightarrow x \equiv 0 \pmod{p^2}$.
2. $Y \equiv -ay^2 + 3by \equiv 0 \pmod{p^4}$.
3. $Z \equiv -axy^2 + 3bxy - by^3 + b^2 + aby \equiv 0 \pmod{p^6}$.

Agora, seja $y \equiv 0 \pmod{p}$. Pelo item 2, segue que

$$3by \equiv 0 \pmod{p^4} \Rightarrow 3b \equiv 0 \pmod{p^3} \Rightarrow b \equiv 0 \pmod{p^3},$$

o que não ocorre. Dessa forma, devemos ter $y \not\equiv 0 \pmod{p}$, e pelo item 2, segue que

$$\begin{aligned} 3by &\equiv ay^2 \pmod{p^4} \Rightarrow 3b \equiv ay \pmod{p^4} \Rightarrow 3b = p^4A + ay, \text{ com } A \in \mathbb{Z} \\ &\Rightarrow 3bxy = p^2xyA \equiv axy^2 \pmod{p^6} \Rightarrow axy^2 \equiv 3bxy \pmod{p^6}. \end{aligned}$$

Com isso, pelo item 3, segue que

$$\begin{aligned} -axy^2 + 3bxy - by^3 + b^2 + aby &\equiv -by^3 + b^2 + aby \pmod{p^6} \\ &\Rightarrow b(b + ay - y^3) \equiv 0 \pmod{p^6} \Rightarrow b + ay - y^3 \equiv 0 \pmod{p^4} \equiv 0 \pmod{p^2} \\ &\Rightarrow y^3 \equiv 0 \pmod{p^2} \Rightarrow y \equiv 0 \pmod{p}, \end{aligned}$$

o que é uma contradição. Portanto, para todo $x, y \in \mathbb{Z}$, segue que $\frac{x + y\theta + \theta^2}{p^2}$ não é um elemento p -integral do corpo $\mathbb{K}$. Agora, vamos supor que exista $x \in \mathbb{Z}$ tal que o elemento $\frac{x + \theta}{p} \in \mathbb{K}$ seja p -integral. Pelo Teorema 5.1, segue que

$$\begin{cases} X = 3x + 2a \equiv 0 \pmod{p}. \\ Y = 3x^2 - a \equiv 0 \pmod{p^2}. \\ Z = x^3 - ax - b \equiv 0 \pmod{p^3}. \end{cases}$$

Assim,

- $X \equiv 3x \equiv 0 \pmod{p} \Rightarrow x \equiv 0 \pmod{p}$.
- $Z \equiv b \equiv 0 \pmod{p^3}$, o que é um absurdo.

Portanto, para todo $x \in \mathbb{Z}$, segue que $\frac{x + \theta}{p}$ não é um elemento p -integral do corpo $\mathbb{K}$.

Dessa forma, concluímos que $(i, j) = (0, 1)$ e, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{\theta^2}{p}\right\}$ é uma base p -integral para o corpo $\mathbb{K}$ e $v_p(D(\mathbb{K})) = s_p - 2 = 2$.

Caso C4: Por hipótese,

$$\begin{cases} v_p(a) = 1 \Rightarrow a = pk, \ k \in \mathbb{Z}, \ p \nmid k, \\ v_p(b) > 1 \Rightarrow v_p(b) \geq 2 \Rightarrow b = b^2q, \ q \in \mathbb{Z}. \end{cases}$$

Dessa forma,

$$\Delta = 2^2p^3k^3 - 3^3p^4q^2 = p^3(2^2k^3 - 3^3pq^2), \ p \nmid k^3 \Rightarrow s_p = v_p(\Delta) = 3.$$

Pela Observação 5.4, segue que $(i, j) = (0, 0)$ ou $(0, 1)$. Agora, considere o elemento $\frac{\theta^2}{p} \in \mathbb{K}$. Com a notação do Teorema 5.1, segue que

- $X = 2a \equiv 0 \pmod{p}$,
- $Y = a^2 \equiv 0 \pmod{p^2}$,
- $Z = b^2 \equiv 0 \pmod{p^3}$,

e concluímos que $\frac{\theta^2}{p}$ é um elemento p -integral do corpo $\mathbb{K}$, ou seja, $(i, j) = (1, 0)$. Portanto, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{\theta^2}{p}\right\}$ é uma base p -integral para o corpo $\mathbb{K}$ e $v_p(D(\mathbb{K})) = s_p - 2 = 1$.

Caso C5: Por hipótese,

$$v_p(a) = v_p(b) = 0 \Rightarrow p \nmid a \text{ e } p \nmid b.$$

Dessa forma,

$$s_p = v_p(\Delta) \geq 0.$$

Vamos definir $m = \left\lceil \frac{s_p}{2} \right\rceil \in \mathbb{N}$ como a parte inteira da fração. Assim,

$$p^{2m} | \Delta \Rightarrow \Delta = p^{2m} D, \quad D \in \mathbb{Z}.$$

Com isso, vamos definir os inteiros x, y, z de modo que

$$\begin{cases} 3x \equiv -2a \pmod{p^m}. \\ 2ay \equiv 3b \pmod{p^m}. \\ z = 1. \end{cases}$$

Com a notação do Teorema 5.2, segue que

- $X = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{p^m} \Rightarrow X = p^m A, \quad \text{com } A \in \mathbb{Z}.$
- $3bU = 3b(9by - 2a^2) = 2^2 a^3 y - \Delta y - 2 \cdot 3a^2 b = (2ay)(2a^2) - 2 \cdot 3a^2 b$
 $\equiv (3b)(2a^2) - 2 \cdot 3a^2 b \equiv 0 \pmod{p^m} \Rightarrow 3bU \equiv 0 \pmod{p^m}.$

Note que $p \nmid 3$ e $p \nmid b$. Portanto, $p \nmid 3b$ e segue que

$$U \equiv 0 \pmod{p^m} \Rightarrow U = p^m B, \quad \text{com } B \in \mathbb{Z}.$$

- $V = 2ay - 3b \equiv 0 \pmod{p^m} \Rightarrow V = p^m C, \quad \text{com } C \in \mathbb{Z}.$
- $Y = \frac{1}{2^2 3 a^2} (2^2 a^2 X^2 - U^2 - 3 \Delta y^2) = \frac{1}{2^2 3 a^2} (2^2 a^2 p^{2m} A^2 - p^{2m} B^2 - 3 p^{2m} D y^2)$
 $\equiv 0 \pmod{p^{2m}}.$
- $Z = \frac{1}{2^2 3^3 a^3} (2^2 a^3 X^3 - 3aXU^2 - 3^2 a \Delta X y^2 - 3U^3 - 3^2 \Delta U y^2 + 2a \Delta U + 3^3 b V^3$
 $+ 2 \cdot 3^2 b \Delta V + \Delta^2)$
 $= \frac{1}{2^2 3^3 a^3} (2^2 a^3 p^{3m} A^3 - 3a p^m A p^{2m} B^2 - 3^2 a p^{2m} D p^m A y^2 - 3 p^{3m} B^3 - 3^2 p^{2m} D p^m B y^2$

$$\begin{aligned}
& + 2ap^{2m}Dp^mB + 3^3bp^{3m}C^3 + 2 \cdot 3^2bp^{2m}Dp^mC + p^{4m}D^2) \\
& = \frac{1}{2^23^3a^3}(2^2a^3p^{3m}A^3 - 3aAp^{3m}B^2 - 3^2ap^{3m}DAy^2 - 3p^{3m}B^3 - 3^2p^{3m}DBy^2 \\
& \quad + 2ap^{3m}DB + 3^3bp^{3m}C^3 + 2 \cdot 3^2bp^{3m}DC + p^{4m}D^2) \\
& \equiv 0 \pmod{p^{3m}}.
\end{aligned}$$

Portanto, pelo Teorema 5.1, segue que $\frac{x + y\theta + \theta^2}{p^m}$ é um elemento p -integral do corpo $\mathbb{K}$. Agora, pela Observação 5.4, segue que $i + j \leq \frac{s_p}{2}$. Assim, uma vez que $m = \left\lfloor \frac{s_p}{2} \right\rfloor$, segue que $(i, j) = (0, m)$. Logo, pelo Teorema 5.3, segue que $\left\{1, \theta, \frac{x + y\theta + \theta^2}{p^m}\right\}$ é uma base p -integral para o corpo $\mathbb{K}$ e $v_p(D(\mathbb{K})) = s_p - 2\left\lfloor \frac{s_p}{2} \right\rfloor$, o que completa a demonstração. $\square$

Corolário 5.10. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$. Vamos definir os inteiros*

- R_p dado por:
 1. $3R_p \equiv -2a \pmod{p^{\left\lfloor \frac{s_p}{2} \right\rfloor}}$, se $v_p(a) = v_p(b) = 0$.
 2. $R_p = 0$, caso contrário.
- S_p dado por:
 1. $2aS_p \equiv 3b \pmod{p^{\left\lfloor \frac{s_p}{2} \right\rfloor}}$, se $v_p(a) = v_p(b) = 0$.
 2. $S_p = 0$, caso contrário.
- e T_p é igual a
 1. $\left\lfloor \frac{s_p}{2} \right\rfloor$, se $v_p(a) = v_p(b) = 0$;
 2. 1, se $v_p(a) \geq 1$ e $v_p(b) \geq 2$.
 3. 0, caso contrário.

Logo, $\left\{1, \theta, \frac{R_p + S_p\theta + \theta^2}{3^{T_p}}\right\}$ é uma base p -integral para o corpo $\mathbb{K}$.

Demonstração. Segue diretamente do Teorema 5.9. $\square$

5.5 Discriminante de um corpo cúbico

Nesta seção, iremos determinar uma fórmula explícita para o discriminante de um corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$. Para isso, usamos os resultados dos Teoremas 5.5, 5.7 e 5.9. A partir desta fórmula, também determinamos uma fórmula explícita para o índice de θ em termos de a e b .

Teorema 5.11. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$, com $p \in \mathbb{Z}$ um número primo. O discriminante do corpo $\mathbb{K}$ é*

$$D(\mathbb{K}) = \text{sgn}(4a^3 - 27b^2) 2^\alpha 3^\beta \prod_{\substack{p > 3 \\ s_p \text{ ímpar}}} p \prod_{\substack{p > 3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2,$$

onde

- α é igual a

1. 0, se

(a) $b \equiv 1 \pmod{2}$, ou

(b) $a \equiv 1 \pmod{4}$ e $b \equiv 0 \pmod{4}$, ou

(c) $a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$, $s_2 \equiv 0 \pmod{2}$ e $\Delta_2 \equiv 1 \pmod{4}$.

2. 2, se

(a) $a \equiv 0 \pmod{2}$ e $b \equiv 2 \pmod{4}$, ou

(b) $a \equiv 0 \pmod{2}$ e $b \equiv 0 \pmod{8}$, ou

(c) $a \equiv 3 \pmod{4}$ e $b \equiv 0 \pmod{4}$, ou

(d) $a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$, $s_2 \equiv 0 \pmod{2}$ e $\Delta_2 \equiv 3 \pmod{4}$;

3. 3, se $s_2 \equiv 1 \pmod{2}$.

- e β é igual a

1. 0, se

(a) $v_3(a) = 0$, ou

(b) $v_3(b) = 0$, $a \equiv 3 \pmod{9}$, $b^2 \equiv a + 1 \pmod{27}$ e $s_3 \equiv 0 \pmod{2}$.

2. 1, se

(a) $1 = v_3(a) < v_3(b)$, ou

(b) $v_3(b) = 0$, $v_3(a) \geq 1$, $a \not\equiv 3 \pmod{9}$ e $b \equiv a + 1 \pmod{9}$, ou

(c) $v_3(b) = 0$, $a \equiv 3 \pmod{9}$, $b^2 \equiv a + 1 \pmod{27}$ e $s_3 \equiv 1 \pmod{2}$.

3. 3, se

(a) $1 = v_3(a) = v_3(b)$, ou

(b) $v_3(b) = 0$, $v_3(a) \geq 1$, $a \not\equiv 3 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{9}$, ou

(c) $v_3(b) = 0$, $a \equiv 3 \pmod{9}$, $b^2 \equiv 4 \pmod{9}$ e $b^2 \not\equiv a + 1 \pmod{27}$.

4. 4, se

(a) $2 = v_3(a) = v_3(b)$, ou

(b) $v_3(b) = 0$, $a \equiv 3 \pmod{9}$ e $b^2 \not\equiv 4 \pmod{9}$.

5. 5, se $1 \leq v_3(b) < v_3(a)$.

Demonstração. Sabemos que $\Delta = \text{ind}(\theta)^2 D(\mathbb{K})$. Com isso,

$$4a^3 - 27b^2 = \text{ind}(\theta)^2 D(\mathbb{K}) \Rightarrow \text{sgn}(4a^3 - 27b^2) = \text{sgn}(D(\mathbb{K})),$$

uma vez que $\text{ind}(\theta)^2 \geq 0$. Por fim, os expoentes de cada número primo, no discriminante, seguem dos Teoremas 5.5, 5.7 e 5.9, o que completa a demonstração. $\square$

Teorema 5.12. *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$, com $p \in \mathbb{Z}$ um número primo. O índice de θ é dado por*

$$\text{ind}(\theta) = 2^r 3^s \prod_{\substack{2=v_p(b) \leq v_p(a) \\ \text{ou} \\ 1=v_p(a) < v_p(b)}} p,$$

$$\text{com } r = \frac{s_2 - \alpha}{2} \text{ e } s = \frac{s_3 - \beta}{2}.$$

Demonstração. Sabemos que $\Delta = 2^{s_2} 3^{s_3} \prod_{p>3} p^{s_p}$ e $\text{ind}(\theta) = \sqrt{\frac{\Delta}{D(\mathbb{K})}}$. Com isso, pelo Teorema 5.11, segue que

$$\text{ind}(\theta) = \sqrt{\frac{2^{s_2} 3^{s_3} \prod_{p>3} p^{s_p}}{2^\alpha 3^\beta \prod_{\substack{p>3 \\ s_p \text{ ímpar}}} p \prod_{\substack{p>3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2}} = \sqrt{2^{s_2 - \alpha} 3^{s_3 - \beta} \prod_{\substack{p>3 \\ s_p \text{ ímpar}}} p^{s_p - 1} \prod_{\substack{p>3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^{s_p - 2}}.$$

Note que, para cada $p \in \mathbb{Z}$ primo, com $p > 3$, pelo Teorema 5.9, segue que

- se ocorrer o caso **C1**, então $s_p = 0$ e p não aparece como fator de $\text{ind}(\theta)$;
- se ocorrer o caso **C2**, então $s_p = 2$, que é par. Assim, $p^{s_p - 2} = 1$ e p não aparece como fator de $\text{ind}(\theta)$;
- se ocorrer o caso **C3**, então $s_p = 4$, que é par. Logo, $p^{s_p - 2} = p^2$;
- se ocorrer o caso **C4**, então $s_p = 3$, que é ímpar. Logo, $p^{s_p - 1} = p^2$;
- se ocorrer o caso **C5**, então

$$s_p - v_p(D(\mathbb{K})) = s_p - \left(s_p - 2 \left\lfloor \frac{s_p}{2} \right\rfloor \right) = 2 \left\lfloor \frac{s_p}{2} \right\rfloor = 0 \text{ ou } 1$$

e p não aparece como fator de $\text{ind}(\theta)$.

Portanto,

$$\text{ind}(\theta) = \sqrt{2^{s_2 - \alpha} 3^{s_3 - \beta}} \prod_{\substack{2=v_p(b) \leq v_p(a) \\ \text{ou} \\ 1=v_p(a) < v_p(b)}} p = 2^{\frac{s_2 - \alpha}{2}} 3^{\frac{s_3 - \beta}{2}} \prod_{\substack{2=v_p(b) \leq v_p(a) \\ \text{ou} \\ 1=v_p(a) < v_p(b)}} p,$$

o que prova o teorema □

Finalizamos esta seção apresentando uma condição necessária, e suficiente, para que $\mathbb{K} = \mathbb{Q}(\theta)$ seja um corpo monogênico.

Teorema 5.13. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$, com $p \in \mathbb{Z}$ um número primo. O conjunto $\{1, \theta, \theta^2\}$ é uma base integral para o corpo $\mathbb{K}$ se, e somente se, $s_2 = \alpha$, $s_3 = \beta$ e, para todo primo $p > 3$, não ocorre $2 = v_p(b) \leq v_p(a)$ e $1 = v_p(a) < v_p(b)$.*

Demonstração. Pela Proposição 3.15, segue que $\{1, \theta, \theta^2\}$ é uma base integral para o corpo $\mathbb{K}$ se, e somente se, $\text{ind}(\theta) = 1$. Pelo Teorema 5.12, segue que

$$\text{ind}(\theta) = 2^r 3^s \prod_{\substack{2=v_p(b) \leq v_p(a) \\ \text{ou} \\ 1=v_p(a) < v_p(b)}} p,$$

com $r = \frac{s_2 - \alpha}{2}$ e $s = \frac{s_3 - \beta}{2}$. Portanto, $\{1, \theta, \theta^2\}$ é uma base integral para o corpo $\mathbb{K}$ se, e somente se,

$$2^r 3^s \prod_{\substack{2=v_p(b) \leq v_p(a) \\ \text{ou} \\ 1=v_p(a) < v_p(b)}} p = 1 \Leftrightarrow r = 0, s = 0.$$

E note que não ocorre $2 = v_p(b) \leq v_p(a)$ ou $1 = v_p(a) < v_p(b)$, ou seja, $s_2 = \alpha$, $s_3 = \beta$ e não ocorre $2 = v_p(b) \leq v_p(a)$ ou $1 = v_p(a) < v_p(b)$. $\square$

5.6 Base integral de um corpo cúbico

Nesta seção, faremos uso dos resultados anteriores para determinar uma base integral para um corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$, com $p \in \mathbb{Z}$ um número primo e para um corpo cúbico puro $\mathbb{K} = \mathbb{Q}(\theta)$, com $\theta = \sqrt[3]{d}$, d livre de cubos e não livre de quadrados.

Teorema 5.14. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$ ou $v_p(b) < 3$, com $p \in \mathbb{Z}$ um número primo. Considere os inteiros $R_2, S_2, T_2, R_3, S_3, T_3, R_p, S_p$ e T_p , com $p > 3$, como nos Corolários 5.6, 5.8 e 5.10, respectivamente. Sejam $R, S \in \mathbb{Z}$ tais que para todo número primo p , implica que*

$$R \equiv R_p \pmod{p^{T_p}} \text{ e } S \equiv S_p \pmod{p^{T_p}}$$

e seja $T = \prod_{p \text{ primo}} p^{T_p}$. Uma base integral para o corpo $\mathbb{K}$ é dada por

1. $\left\{1, \frac{b + \theta}{3}, \frac{R + S\theta + \theta^2}{T}\right\}$, se $v_3(b) = 0$, $a \equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{27}$ e
2. $\left\{1, \theta, \frac{R + S\theta + \theta^2}{T}\right\}$, caso contrário.

Demonstração. Basta aplicar o Teorema 4.28 utilizando as bases p -integrais dadas pelos Corolários 5.6, 5.8 e 5.10. $\square$

Exemplo 5.15. Considere o corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - t + 4$. Neste caso, $a = 1$ e $b = 4$. Assim,

$$\Delta = 2^2 a^3 - 3^3 b^2 = 2^2 - 3^3 2^4 = -2^2(-1 + 3^3 2^2) = -2^2 107.$$

Com isso,

$$s_2 = v_2(\Delta) = 2, \quad s_{107} = v_{107}(\Delta) = 1$$

e

$$s_p = v_p(\Delta) = 0, \text{ para todo primo } p \neq 2 \text{ e } p \neq 107.$$

Uma vez que $a \equiv 1 \pmod{4}$ e $b \equiv 0 \pmod{4}$, pelo Corolário 5.6, segue que $R_2 = 0$, $S_2 = 1$ e $T_2 = 1$. Com isso, pelo Teorema 5.14, segue que $R = 0$, $S = 1$ e $T = 2$ e concluímos que $\left\{1, \theta, \frac{\theta + \theta^2}{2}\right\}$ é uma base integral para o corpo $\mathbb{K}$. Além disso, pelo Teorema 5.11, segue que $D(\mathbb{K}) = -107$.

Exemplo 5.16. Considere o corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - 255t + 3850$. Neste caso, $a = 255 = 3 \cdot 5 \cdot 17$ e $b = 3850 = 2 \cdot 5^2 \cdot 7 \cdot 11$. Assim,

$$\Delta = 2^2 a^3 - 3^3 b^2 = -2^4 3^6 5^3 229$$

Com isso,

$$s_2 = 4, s_3 = 6, s_5 = 3 \text{ e } s_{229} = 1.$$

Além disso,

$$\Delta_2 = \frac{\Delta}{s^2} = 3^6 5^3 229 \equiv 1 \pmod{4}.$$

Agora, uma vez que $a \equiv 3 \pmod{4}$ e $b \equiv 2 \pmod{4}$, pelo Corolário 5.6, segue que $R_2 = 2$, $S_2 = -1$ e $T_2 = 1$. Como $v_3(a) \geq 1$, $a \equiv 3 \pmod{9}$ e $b^2 \equiv a + 1 \pmod{9}$, pelo Corolário 5.8, segue que $R_3 = 1$, $S_3 = 2$ e $T_3 = 2$. Também, como $v_5(a) = 1$ e $v_5(b) = 2$, pelo Corolário 5.10, segue que $R_5 = 0$, $S_5 = 0$ e $T_5 = 1$. Com isso, pelo Teorema 5.14, segue que $R = 10$, $S = -25$ e $T = 90$ e concluímos que $\left\{1, \frac{3850 + \theta}{3}, \frac{10 - 25\theta + \theta^2}{90}\right\}$ é uma base integral para o corpo $\mathbb{K}$. Além disso, pelo Teorema 5.11, segue que $D(\mathbb{K}) = -2^2 \cdot 5 \cdot 229$.

Seja $d \in \mathbb{Z}$ livre de cubos. Assim, podemos escrever d da forma hk^2 , com h livre de quadrados. Neste caso, k também é livre de quadrados e $\text{mdc}(h, k) = 1$. Com isso, sejam $\theta = \sqrt[3]{d}$ e $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico puro, iremos utilizar os resultados anteriores para determinar uma base integral para o corpo $\mathbb{K}$ e seu discriminante.

Teorema 5.17. *Seja $\theta = \sqrt[3]{d}$, com $d \in \mathbb{Z}$ livre de cubos, $d = hk^2$, h livre de quadrados. Considere o corpo cúbico puro $\mathbb{K} = \mathbb{Q}(\theta)$. Uma base integral para o corpo $\mathbb{K}$ é dada por*

1. $\left\{1, \theta, \frac{\theta^2}{k}\right\}$, se $d^2 \not\equiv 1 \pmod{9}$;
2. $\left\{1, \theta, \frac{k^2 \pm k^2\theta + \theta^2}{3k}\right\}$, se $d \equiv \pm 1 \pmod{9}$.

Demonstração. O elemento $\theta = \sqrt[3]{d}$ é uma raiz do polinômio irreduzível $f(t) = t^3 - d \in \mathbb{Z}[t]$. Neste caso, $a = 0$, $b = -d$ e $\Delta = 4a^3 - 27b^2 = -3^3 d^2$. Para encontrar uma base integral para o corpo $\mathbb{K}$, primeiro encontramos bases 2, 3 e p -integral, com $p > 3$. Base 2-integral: como $a = 0$, podem ocorrer os casos **A1**, **A2** e **A3** do Teorema 5.5, ou seja, uma base 2-integral para o corpo $\mathbb{K}$ é

$$\begin{cases} \{1, \theta, \theta^2\}, & \text{se } d \not\equiv 0 \pmod{4}. \\ \left\{1, \theta, \frac{\theta^2}{2}\right\}, & \text{se } d \equiv 0 \pmod{4}. \end{cases} \implies \begin{cases} \{1, \theta, \theta^2\}, & \text{se } 2 \nmid k. \\ \left\{1, \theta, \frac{\theta^2}{2}\right\}, & \text{se } 2 \mid k. \end{cases}$$

Portanto, $\left\{1, \theta, \frac{\theta^2}{k}\right\}$ é uma base 2-integral para o corpo $\mathbb{K}$. Base 3-integral: como $a = 0$,

podem ocorrer os casos **B3**, **B5**, **B7** e **B8** do Teorema 5.7, ou seja, uma base 3-integral para o corpo $\mathbb{K}$ é

$$\begin{cases} \{1, \theta, \theta^2\}, & \text{se } d \not\equiv 0 \pmod{9} \text{ e } d^2 \not\equiv 1 \pmod{9}. \\ \left\{1, \theta, \frac{\theta^2}{3}\right\}, & \text{se } 3^2 \mid d \Leftrightarrow 3 \mid k. \\ \left\{1, \theta, \frac{1+t\theta+\theta^2}{3}\right\}, & \text{se } d^2 \equiv 1 \pmod{9}. \end{cases}$$

Base p -integral, com $p > 3$: como $a = 0$, podem ocorrer os casos **C1**, **C2** e **C3** do Teorema 5.9, ou seja, uma base p -integral para o corpo $\mathbb{K}$ é

$$\begin{cases} \{1, \theta, \theta^2\}, & \text{se } d \not\equiv 0 \pmod{p^2}. \\ \left\{1, \theta, \frac{\theta^2}{p}\right\}, & \text{se } d \equiv 0 \pmod{p^2}. \end{cases} \implies \begin{cases} \{1, \theta, \theta^2\}, & \text{se } p \nmid k. \\ \left\{1, \theta, \frac{\theta^2}{p}\right\}, & \text{se } p \mid k. \end{cases}$$

Portanto, $\left\{1, \theta, \frac{\theta^2}{k}\right\}$ é uma base p -integral para o corpo $\mathbb{K}$, com $p > 3$ primo. Com isso, se $3 \mid k$, então para todo primo p , $\left\{1, \theta, \frac{\theta^2}{k}\right\}$ é uma base p -integral para o corpo $\mathbb{K}$. Logo, é uma base integral. Por outro lado, se $3 \nmid k$, então:

- quando $d^2 \not\equiv 1 \pmod{9}$, segue que $\{1, \theta, \theta^2\}$ é uma base 3-integral para o corpo $\mathbb{K}$ e, assim, $\left\{1, \theta, \frac{\theta^2}{k}\right\}$ é uma base integral para o corpo $\mathbb{K}$.
- quando $d^2 \equiv 1 \pmod{9}$, segue que $\left\{1, \theta, \frac{1+d\theta+\theta^2}{3}\right\}$ é uma base 3-integral para o corpo $\mathbb{K}$. Com isso,

$$\begin{aligned} d \equiv \pm 1 \pmod{9} &\Rightarrow hk^2 \equiv \pm 1 \pmod{9} \\ &\Rightarrow k \equiv k^2 \equiv 1 \pmod{9} \Rightarrow k^2 \equiv 1 \pmod{3}. \end{aligned}$$

Portanto, $R = k^2$. Assim,

$$\pm k^2 \equiv \pm 1 \pmod{3} \equiv t \pmod{3} \Rightarrow S = \pm k^2 \text{ e } T = 3k.$$

Logo, pelo Teorema 4.28, segue que $\left\{1, \theta, \frac{k^2 \pm k^2\theta + \theta}{3k}\right\}$ é uma base integral para o corpo $\mathbb{K}$, o que completa a demonstração. $\square$

Teorema 5.18. *Seja $\theta = \sqrt[3]{d}$, com $d \in \mathbb{Z}$ livre de cubos, $d = hk^2$, h livre de quadrados. Considere o corpo cúbico puro $\mathbb{K} = \mathbb{Q}(\theta)$. O discriminante do corpo $\mathbb{K}$ é*

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

Demonstração. Pelo Teorema 5.17, segue que se $d^2 \not\equiv 1 \pmod{9}$, então $\left\{1, \theta, \frac{\theta^2}{k}\right\}$ é uma base integral para o corpo $\mathbb{K}$. Note que os elementos desta base são inteiros mínimos do

corpo $\mathbb{K}$. Portanto, pelo Teorema 3.40, segue que $\text{ind}(\theta) = k$. Além disso, pela Definição 3.14, segue que

$$D(\mathbb{K}) = \frac{\Delta}{\text{ind}(\theta)^2} = \frac{-3^3 d^2}{k^2} = \frac{-3^3 h^2 k^4}{k^2} \Rightarrow D(\mathbb{K}) = -27h^2 k^2.$$

Por outro lado, se $d \equiv \pm 1 \pmod{9}$, então uma base integral para o corpo $\mathbb{K}$ é $\left\{1, \theta, \frac{k^2 \pm k^2 \theta + \theta}{3k}\right\}$, e assim, $\text{ind}(\theta) = 3^2 k^2$. Portanto,

$$D(\mathbb{K}) = \frac{\Delta}{\text{ind}(\theta)^2} = \frac{-3^3 d^2}{3^2 k^2} = \frac{-3h^2 k^4}{k^2} \Rightarrow D(\mathbb{K}) = -3h^2 k^2,$$

o que completa a demonstração. $\square$

Exemplo 5.19. Considere o corpo cúbico puro $\mathbb{K} = \mathbb{Q}(\sqrt[3]{175})$. Como $175 = 5^2 \cdot 7$ e $175^2 \not\equiv 1 \pmod{9}$, pelos Teoremas 5.17 e 5.18, segue que $\{1, \sqrt[3]{175}, \sqrt[3]{245}\}$ é uma base integral para o corpo $\mathbb{K}$ e $D(\mathbb{K}) = -3^3 5^2 7^2$.

6 Conclusão

Ao longo deste trabalho, pudemos dar uma breve apresentação de conceitos básicos da Teoria Algébrica dos Números (Capítulo 2) destacando, em especial, o fato de que o anel de inteiros $\mathcal{O}_{\mathbb{K}}$, de um corpo de números, é um anel de Dedekind (Observação 2.79). Tal fato é muito importante para que possamos utilizar a fatoração de ideais de $\mathcal{O}_{\mathbb{K}}$ em ideais primos no Capítulo 4.

No Capítulo 3, apresentamos uma base integral para um corpo quadrático (Teorema 3.2) e seu discriminante (Teorema 3.4). Na Seção 3.2, apresentamos os inteiros mínimos e mostramos a existência de uma base integral para um corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$ formada por inteiros mínimos de grau $k = 0, 1, \dots, n - 1$ em θ (Teorema 3.39).

Na Seção 4.1, apresentamos o conceito de elementos p -integrais, onde p representa um número primo. Com isso, na Seção 4.2, mostramos a existência de uma base p -integral para um corpo de números (Teorema 4.15). Além disso, provamos que uma base é integral se, e somente se, é uma base p -integral, para todo primo p (Teorema 4.20). Ainda nesta seção, utilizamos a base integral formada por inteiros mínimos para dar uma representação mais clara dos elementos p -integrais que compõe uma base p -integral (Lema 4.24 e Teorema 4.25). Assim, unindo as bases p -integrais, para cada primo p , conseguimos obter uma base integral (Teorema 4.28).

No Capítulo 5, usamos os resultados de bases p -integrais para encontrá-las em corpos cúbicos $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz do polinômio irreduzível $f(t) = t^3 - at + b \in \mathbb{Z}[t]$, $v_p(a) < 2$, $v_p(b) < 3$. Nas Seções 5.2, 5.3 e 5.4, encontramos bases 2, 3 e p -integrais, com $p > 3$, para tal corpo cúbico (Corolários 5.6, 5.8 e 5.10). Utilizando essas bases, finalizamos encontrando uma base integral para o corpo $\mathbb{K}$ (Teorema 5.14) e para um corpo cúbico puro (Teorema 5.17).

Na referência [3], o autor também utiliza o processo feito no Capítulo 5 para encontrar uma base integral para um corpo quártico $\mathbb{K} = \mathbb{Q}(\theta)$, com θ uma raiz do polinômio irreduzível $f(t) = t^4 + at + b \in \mathbb{Z}[t]$. Neste trabalho, o corpo quártico não foi estudado, mas esses corpos são nossa motivação para usar as bases p -integrais para investigar corpos de números em que θ seja raiz de um polinômio mais geral ou de graus maiores.

Referências

- [1] EMICIDA. *Princípios*. 2019. Disponível em: <<https://open.spotify.com/track/0pfNk7XtQWNNx6Otu34lXl?si=927609713d274086>>.
- [2] ALACA, S. p -integral bases of a cubic field. *Proceedings of the American Mathematical Society*, v. 126, p. 1949–1953, 1998.
- [3] ALACA, S. *p -Integral Bases of Algebraic Number Fields*. Tese (Doutorado) — Carleton University, 1994.
- [4] ALACA, S.; WILLIAMS, K. S. *Introductory Algebraic Number Theory*. 1. ed. New York: Cambridge University Press, 2004.
- [5] ANDRADE, A. A. *Uma Introdução à Teoria dos Números Algébricos*. 1. ed. São José do Rio Preto: Amazon.com, 2021.
- [6] SAMUEL, P. *Algebraic Theory of Numbers*. Paris: HERMANN, 1970.
- [7] RIBENBOIM, P. *Classical Theory of Algebraic Number*. 1. ed. New York: Universitext, Springer, 2001.

Índice Remissivo

Anel (ou domínio) de Dedekind, 23

Anel de inteiros, 16

Anel integralmente fechado, 16

Base p -integral, 57

Base de um ideal, 23

Base integral, 24

Base potente, 32

Corpo cúbico puro, 44

Corpo de números, 20

Corpo de números monogênico, 32

Corpo quadrático, 17

Discriminante de um conjunto, 22

Discriminante de um corpo de números, 24

Discriminante de um elemento, 22

Discriminante de um ideal, 23

Discriminante de um polinômio, 22

Divisor discriminante não essencial, 49

Elemento P -integral, 51

Elemento p -integral, 51

Elemento algébrico, 16

Elemento inteiro, 15

Elemento primitivo, 21

Elemento transcendente, 16

Elementos $\mathbb{K}$ -conjugados, 21

Elementos conjugados, 17

Extensão múltipla, 20

Grau da extensão, 20

Ideal fracionário, 50

Inteiro algébrico, 15

Inteiro mínimo de grau k em θ , 36

Norma de um ideal, 25

Número algébrico, 15

Polinômio característico, 21

Polinômio minimal, 16

Valorização, 50

Índice de um corpo de números, 45

Índice de um elemento, 28

Índice minimal de um corpo de números, 45