Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

A Equação Diofantina $v(v+1) = u(u+a)(u+2a)$: uma generalização da equação de Mordell

por

Thiago Porto de Almeida Freitas

Brasília
2013

Agradecimentos

- À Deus, que por meio de sua escrita em linhas tortuosas, me permitiu mais essa conquista;

- À minha mãe, Izabel, e ao meu irmão, Herculano, pelo apoio e por sempre me receberem de braços e corações abertos quando voltava para casa;

- Ao meu pai, Iran, e ao meu irmão, Ian, pela torcida;

- Aos meus familiares por sempre acreditarem na minha capacidade;

- Ao Prof. Hemar Godinho pela orientação, generosidade, ensinamentos, palavras de incentivo e confiança;

- Aos professores Cícero, Daniela, Noraí e Trajano por aceitarem a participar da banca e pelas correções e sugestões que enriqueceram o trabalho;

- Aos professores do Departamento de Matemática da UnB por terem contribuído na minha formação acadêmica, especialmente: ao Prof. Helder Matos, que no curso de verão de Álgebra Linear em 2003, me fez acreditar que estudar na UnB era algo possível e à Profa. Cátia pelos ensinamentos e exemplo de profissional;

- Aos técnicos-administrativos do Departamento de Matemática da UnB pela qualidade de seus serviços, especialmente: à Bruna, por toda paciência e qualidade nas informações dadas na reta final;

- Aos professores do Departamento de Matemática do Campus Catalão / UFG, que

somaram esforços e possibilitaram o meu afastamento das atividades docentes, para que pudesse dedicar integralmente ao doutorado;

- Ao Walter pela acolhida na Kit e pelos momentos de risadas e palavras de motivação;

- Aos amigos - Ricardo, Marcelo, Luciana Borges, Élida, Fabrício, Lucas, Ana Paula Stoppa, Ana Paula Purcina, Elcimar, Michele e Lady - que apesar da distância nesse período, se mantiveram presentes em minha vida, com palavras de incentivo e carinho;

- Aos amigos - Fagner, Evander, Fabiana, Anyelle, Bianka, Jander, Aline, Daniel, Jhone e Raquel - pela torcida;

- Aos amigos da trupe da Teoria dos Números, em especial: à Ana Paula Chaves e à Luciana Ventura pelos grandes e divertidos momentos que passamos juntos;

- Aos amigos - Vagner, Thaynara, Joaby, Cris, Kalyana, Elon, Tarcísio, Wembesom, Raimundo, Vinícius, Daiane, Reinaldo, Adriana, Simone, Mariana, Andréia, Kelem, Paulo Ângelo, Daniele, João Paulo, Sunamita, Luciene, Miguel, Júnior e Ricardo - que com sorriso e palavras tornavam alegres os dias desse período;

- Aos amigos que fiz neste período em Brasília - academia, voluntários da Copa das Confederações e UnB - pelos momentos de diversão e descontração;

- Ao CNPq e a Capes pelo apoio financeiro.

Resumo

Seja a um número natural. Nesta tese, discutimos a Equação Diofantina $v(v+1) = u(u+a)(u+2a)$ e algumas propriedades aritméticas importantes do corpo cúbico associado. E ainda, apresentamos os detalhes dos casos $a = 2$ e $a = 5$.

Palavras-chaves : Equação Diofantina, Bases Integrais, Unidades Fundamentais.

Abstract

Let $a \in \mathbb{N}$. In this thesis, we discuss the Diophantine Equation $v(v+1) = u(u+a)(u+2a)$ and some important arithmetic properties of the associated cubic field. We also present a detailed account of the cases $a = 2$ and $a = 5$.

Keywords : Diophantine Equation, Integral Bases, Fundamental Units.

Sumário

Introdução

As equações matemáticas aparecem em vários contextos da ciência, como por exemplo, Engenharia, Biologia, Medicina, etc. Em muitos casos, tais equações representam um modelo matemático dentro do universo que está inserido e, em geral, a resolução destas consiste no grande desafio a ser enfrentado. Tal desafio para ser solucionado pode requerer desde apenas operações aritméticas elementares até um instrumental não trivial de conceitos e resultados. No primeiro extremo temos por exemplo, explicitar as raízes de uma equação do segundo grau, $ax^2 + bx + c = 0$, com a, b e c números reais, e no outro, o Último Teorema de Fermat [1], cuja demonstração foi apresentada à comunidade matemática em 1994 pelo matemático britânico Andrew Wiles, após mais de 300 anos de estudos desenvolvidos por diversos matemáticos.

Paralelamente à busca de solucionar as equações matemáticas que surgiram ao longo da história, houve a necessidade do desenvolvimento do raciocínio matemático, pois à medida que um problema é resolvido, de forma natural, generalizações são propostas e estas passam a requerer ferramentas sofisticadas, proporcionando grandes avanços na evolução das ciências, em especial, na Teoria dos Números.

No que tange o estudo da resolução de equações algébricas diofantinas, isto é, determinar soluções inteiras racionais para uma equação do tipo $f(x_1, x_2, \cdots, x_n) = 0$, onde f é uma função de n variáveis com coeficentes inteiros racionais e $n > 2$, houve um grande desenvolvimento comparado aos primeiros estudos formais, apresentados por Diofanto de Alexandria, por meio da sua série de livros conhecida como *Arithmetica*.

[1] O Último Teorema de Fermat assegura que não existem x, y e z inteiros racionais tais que a equação $x^n + y^n = z^n$, para $n > 2$, possua solução, salvo os casos triviais: $(0, 0, 0); (1, 0, 1); (0, 1, 1)$.

Um dos problemas célebres apresentados na referida coleção consiste na determinação da idade de uma pessoa por meio do enigma: *a infância dele foi de um sexto de vida; um doze avos foi com a juventude enquanto bigodes cresciam; ele casou-se um sétimo depois; e seu filho nasceu cinco anos depois; o filho viveu metade da idade do pai, e o pai morreu quatro anos depois do filho.* No caso, sendo x a idade da pessoa do problema descrito, a equação associada a tal enigma consiste em:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4,$$

cuja solução é $x = 84$ anos.

Desde a época de Diofanto de Alexandria, grandes matemáticos contribuíram para ampliar o entendimento do universo das equações algébricas diofantinas. Muitas dessas contribuições surgiram nas tentativas frustradas de demonstrar resultados que se encontravam em aberto, como por exemplo, a Lei da Reciprocidade Quadrática e o Último Teorema de Fermat. No primeiro caso, em 1796, Gauss apresenta a demonstração, treze anos após as primeiras observações empíricas feitas por Euler. No segundo caso, vários matemáticos dedicaram parte de sua vida para demonstrá-lo, movidos pelo intrigante comentário de Fermat em suas notas sobre o mesmo, a saber: *encontrei uma demonstração verdadeiramente maravilhosa disto, mas esta margem é estreita demais para contê-la.* Entre as provas frustradas do resultado, se encontra a anunciada pelo matemático francês Lamé, em 1874, a qual utilizava a condição de fatoração única em irredutíveis sobre um dos conjuntos definidos na demonstração, conforme apontamento de Liouville, e que Kummer, por meio de uma carta, mostrara que tal condição não era válida em alguns casos.

A resolução de uma equação diofantina consiste em responder,na ordem em que se apresenta, os seguintes questionamentos:

- A equação possui solução?
- Se a equação possui solução, o número de soluções é finito ou infinito?
- Se a equação possui solução, é possível explicitar as soluções? Em caso afirmativo, explicite.

Cada uma das questões supracitadas apresenta em contextos diferentes dificuldades diferentes para a obtenção de sua resposta, e de acordo com as respostas obtidas, podemos nos encontrar diante da resolução de problemas interessantes. Em matemática, o

termo *interessante* não está necessariamente associado a problemas de difícil enunciado e/ou compreensão. Por exemplo, em 1939, Paul Erdös, ver [6], demonstrou que o produto de k números inteiros positivos consecutivos jamais consistiria em um quadrado perfeito, isto é, a equação diofantina $n(n+1)\cdots(n+k-1) = l^2$ não possui solução.

Em 1963, Mordell, ver [16], determinou quais inteiros racionais podiam ser escritos simultaneamente como produto de dois inteiros consecutivos e três inteiros consecutivos, isto é, estudou a equação diofantina dada por $y(y+1) = x(x+1)(x+2)$. Na ocasião, Mordell mostrou que 0, 6 e 210 eram os únicos inteiros que satisfaziam a equação dada.

Em 1972, os matemáticos Boyd e Kisilevsky, ver [3], deduziram quais eram os inteiros racionais escritos simultaneamente como produto de três inteiros consecutivos e quatro inteiros consecutivos, e concluíram que $0, 24, 120$ e 175560 eram os únicos números com esta propriedade.

É um fato que vários trabalhos ao longo dos tempos inspiraram outros trabalhos e aqui não é diferente. Esta tese foi motivada pelo trabalho de Mordell e tem como objetivo investigar a equação diofantina associada a seguinte questão: quais são os inteiros racionais que podem ser escritos simultaneamente como um produto de dois inteiros racionais consecutivos e um produto de três termos consecutivos em uma progressão aritmética de razão a, com $a \in \mathbb{N}$, ou seja, estudar a equação

$$v(v+1) = u(u+a)(u+2a). \tag{1}$$

Para promover o estudo, por meio de uma determinada mudança de variáveis, concluímos que resolver (1) é equivalente a resolver a equação

$$2y^2 = x^3 - 4a^2x + 2. \tag{2}$$

A equivalência entre (1) e (2) se mostra importante, pois *a priori* não conseguimos responder nenhum dos questionamentos anteriormente apresentado. Contudo, em [15], Mordell mostrou que a equação $ey^2 = ax^3 + bx^2 + cx + d$ possui um número finito de soluções, caso o lado direito da equação não possua o fator x^2, ou seja, (2) possui um número finito de soluções. Diante disto, motivado pela terceira questão, buscamos construir um cenário onde pudéssemos explicitar as soluções. Neste contexto, surgiu a necessidade de compreender mais profundamente alguns aspectos do corpo cúbico de números algébricos $\mathbb{K} = \mathbb{Q}(\theta)$, onde θ é a menor raíz do polinômio $f(t) = t^3 - 4a^2t + 2$.

Na perspectiva de atingir o objetivo proposto, este trabalho foi organizado em dois capítulos, os quais apresentamos na sequência:

- no primeiro capítulo caracterizamos o discriminante de $\mathbb{K}$ e apresentamos uma base integral e um conjunto de unidades fundamentais para $\mathbb{K}$. Ademais, fazemos uma análise do número de classes de $\mathbb{K}$ e fornecemos um algoritmo que nos possibilita calcular este número, visando investigar os casos onde o conjunto de inteiros algébricos de $\mathbb{K}$ é munido da propriedade de fatoração única;
- no segundo capítulo discutimos, por meio das ferramentas construídas no primeiro capítulo, a equação diofantina $v(v+1) = u(u+a)(u+2a)$, em especial, os casos $a = 2$ e $a = 5$, pois nestes o anel de inteiros associado possui a propriedade de fatoração única.

Capítulo 1

O Corpo Cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, com $\theta^3 - 4a^2\theta + 2 = 0$

Neste capítulo discutimos os seguintes aspectos algébricos acerca do corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, com $\theta^3 - 4a^2\theta + 2 = 0$ e $a \in \mathbb{N}$: discriminante, base integral, sistema de unidades fundamentais, regulador e número de classes. Para o desenvolvimento do capítulo abordamos, no início de cada seção, os conceitos supracitados sob um ponto de vista macro, isto é, quando $\mathbb{K}$ consiste de um corpo de números de grau n, e na sequência levamos estes para o nosso contexto. Denotaremos por $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Os aspectos elementares da teoria de números algébricos, que fornecem o suporte para este capítulo, podem ser consultados em [1] e [20].

1.1 Discriminante e Base Integral

Dado $\mathbb{K}$ um corpo de números de grau n, sabemos que este pode ser visto como um espaço vetorial sobre $\mathbb{Q}$. Nesta direção, faz sentido o conceito de base e nesta seção iremos explorá-lo e relacioná-lo com o conceito de discriminante, a ser definido, que consiste numa importante quantidade relacionada aos elementos do corpo dado e seus conjugados.

Definição 1.1. Sejam $\mathbb{K}$ um corpo de números de grau n, $\alpha_1, \alpha_2, \cdots, \alpha_n$ elementos de $\mathbb{K}$ e $\sigma_1, \sigma_2, \cdots, \sigma_n$ os monomorfismos de $\mathbb{K}$ sobre $\mathbb{C}$ que fixam $\mathbb{Q}$. O discriminante de

$\alpha_1, \alpha_2, \cdots, \alpha_n$, denotado por $\Delta[\alpha_1, \alpha_2, \cdots, \alpha_n]$, é dado por

$$\Delta[\alpha_1, \alpha_2, \cdots, \alpha_n] = (det(\sigma_i(\alpha_j)))^2,$$

com $i = 1, \cdots, n$ e $j = 1, \cdots, n$.

Lema 1.1. *Seja $\mathbb{K}$ um corpo de números de grau n. Se $\alpha_1, \alpha_2, \cdots, \alpha_n$ e $\beta_1, \beta_2, \cdots, \beta_n$ são bases de $\mathbb{K}$ sobre $\mathbb{Q}$, então $\dfrac{\Delta[\beta_1, \beta_2, \cdots, \beta_n]}{\Delta[\alpha_1, \alpha_2, \cdots, \alpha_n]} = l^2$, para algum número racional l não-nulo.*

Demonstração: Por hipótese $\alpha_1, \alpha_2, \cdots, \alpha_n$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, então qualquer elemento de $\mathbb{K}$ pode ser escrito como combinação linear destes elementos. Como $\beta_1, \beta_2, \cdots, \beta_n$ são elementos de $\mathbb{K}$, temos que existem números racionais c_{ij}, com $i = 1, \cdots, n$ e $j = 1, \cdots, n$, tais que $\beta_j = \sum_{i=1}^{n} c_{ij}\alpha_i$.

Agora, por meio da Definição 1.1, obtemos que

$$\Delta[\beta_1, \beta_2, \cdots, \beta_n] = (det(c_{ij}))^2 \Delta[\alpha_1, \alpha_2, \cdots, \alpha_n],$$

de onde segue o resultado, visto que $0 \neq (det(c_{ij}))^2 \in \mathbb{Q}$, pois $c_{ij} \in \mathbb{Q}$, com $i = 1, \cdots, n$ e $j = 1, \cdots, n$.

■

Teorema 1.1. *Seja $\mathbb{K}$ um corpo de números de grau n. O discriminante de qualquer base de $\mathbb{K}$ sobre $\mathbb{Q}$ é sempre um número racional não-nulo.*

Demonstração: Pelo Lema 1.1 temos que se para uma determinada base de $\mathbb{K}$ sobre $\mathbb{Q}$ o discriminante desta é racional, as demais bases possuirão a mesma propriedade.

Como $\mathbb{K}$ é um corpo de números de grau n, temos que existe um número algébrico θ tal que $\mathbb{K} = \mathbb{Q}(\theta)$, onde uma base natural de $\mathbb{K}$ sobre $\mathbb{Q}$ é dada por $1, \theta, \theta^2, \cdots, \theta^{n-1}$.

Sendo $\theta = \theta_1, \theta_2, \cdots, \theta_n$, as raízes do polinômio minimal de θ temos por meio da Definição 1.1 que

$$\Delta[1, \theta, \theta^2, \cdots, \theta^{n-1}] = \left\{ det \begin{bmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{bmatrix} \right\}^2 = \prod_{i<j} (\theta_i - \theta_j)^2, \qquad (1.1)$$

onde a última igualdade acontece, pois tal determinante é do tipo Determinante de Vandermonde.

Como as raízes do polinômio minimal são distintas, segue a partir do lado direito de (1.1) que $\Delta[1, \theta, \theta^2, \cdots, \theta^{n-1}] \neq 0$. E ainda, o desenvolvimento do produto do lado direito de (1.1) resulta em um polinômio simétrico em $\theta_1, \cdots, \theta_n$, e uma vez que todo polinômio simétrico em $\theta_1, \cdots, \theta_n$ é escrito como combinação dos polinômios simétricos elementares, que são os coeficientes do polinômio minimal de θ, obtemos $\Delta[1, \theta, \theta^2, \cdots, \theta^{n-1}]$ racional.

■

Corolário 1.1. *Seja $\mathbb{K}$ um corpo de números de grau n. Se $\alpha_1, \cdots, \alpha_n$ é uma base de inteiros algébricos de $\mathbb{K}$ sobre $\mathbb{Q}$, então $\Delta[\alpha_1, \cdots, \alpha_n]$ é um inteiro racional não-nulo.*

Demonstração: Como $\alpha_1, \cdots, \alpha_n$ são inteiros algébricos, e como o conjunto de inteiros algébricos constitui um anel, segue que $\Delta[\alpha_1, \cdots, \alpha_n]$ é um inteiro algébrico. Por meio do Teorema 1.1, temos que o discriminante é racional. Como todo inteiro algébrico racional é um inteiro racional, segue o resultado desejado.

■

Corolário 1.2. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\omega_1, \cdots, \omega_n$ elementos de $\mathbb{K}$. Temos que $\Delta[\omega_1, \cdots, \omega_n] \neq 0$ se, e somente se, $\omega_1, \cdots, \omega_n$ são linearmente independentes sobre $\mathbb{Q}$.*

Demonstração: Num sentido, suponhamos que $\omega_1, \cdots, \omega_n$ sejam linearmente dependentes sobre $\mathbb{Q}$, então existem números racionais $a_1, \cdots, a_n$, não todos nulos, tais que

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n = 0.$$

Sejam $\sigma_1, \cdots, \sigma_n$ os monomorfismos de $\mathbb{K}$ sobre $\mathbb{C}$ que fixam $\mathbb{Q}$. Aplicando estes monomorfismos na igualdade acima, colocando $\omega_j^{(i)} = \sigma_i(\omega_j)$, obtemos o seguinte sistema homogêneo nas variáveis $a_1, \cdots, a_n$:

$$\begin{cases} a_1\omega_1^{(1)} + a_2\omega_2^{(1)} + \cdots + a_n\omega_n^{(1)} &= 0 \\ a_1\omega_1^{(2)} + a_2\omega_2^{(2)} + \cdots + a_n\omega_n^{(2)} &= 0 \\ \vdots & \vdots \ \vdots \\ a_1\omega_1^{(n)} + a_2\omega_2^{(n)} + \cdots + a_n\omega_n^{(n)} &= 0 \end{cases}.$$

Como este sistema possui uma solução não trivial, temos que $\Delta[\omega_1, \cdots, \omega_n] = 0$, o que contradiz a hipótese. Portanto, $\omega_1, \cdots, \omega_n$ são linearmente independentes sobre $\mathbb{Q}$.

No outro sentido, suponhamos que $\omega_1, \cdots, \omega_n$ são linearmente independentes sobre $\mathbb{Q}$. Como $\mathbb{K}$ é um corpo de grau n, segue que $\omega_1, \cdots, \omega_n$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Assim, pelo Teorema 1.1 obtemos que $\Delta[\omega_1, \cdots, \omega_n] \neq 0$.

■

Definição 1.2. Seja $\mathbb{K}$ um corpo de números e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$. Uma $\mathbb{Z}$-base para $(\mathcal{O}_\mathbb{K}, +)$ é denominada base integral de $\mathbb{K}$.

Definição 1.3. Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$. Seja I um ideal não-nulo de $\mathcal{O}_\mathbb{K}$. Se $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ são elementos de I tais que todo elemento $\alpha \in I$ pode ser expressado unicamente da maneira $\alpha = a_1\epsilon_1 + a_2\epsilon_2 + \cdots + a_n\epsilon_n$, com $a_1, \cdots, a_n \in \mathbb{Z}$, então $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ é uma $\mathbb{Z}$-base do ideal I.

Teorema 1.2. *Sejam $\mathbb{K}$ um corpo de números de grau n e I um ideal não-nulo de $\mathcal{O}_\mathbb{K}$.*

(i) Sejam $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ e $\mu_1, \mu_2, \ldots, \mu_n$ duas bases de I. Então,

$$\Delta[\epsilon_1, \epsilon_2, \cdots, \epsilon_n] = \Delta[\mu_1, \mu_2, \ldots, \mu_n]$$

e

$$\epsilon_i = \sum_{j=1}^{n} c_{ij}\mu_j, i = 1, \cdots, n,$$

onde c_{ij}, para $i = 1, \cdots, n$ e $j = 1, \cdots, n$, são inteiros racionais tais que $|det(c_{ij})| = 1$.

(ii) Sejam $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ uma base de I e $\mu_1, \mu_2, \ldots, \mu_n \in I$ tais que

$$\Delta[\mu_1, \mu_2, \ldots, \mu_n] = \Delta[\epsilon_1, \epsilon_2, \cdots, \epsilon_n].$$

Então $\mu_1, \mu_2, \ldots, \mu_n$ é uma base de I.

Demonstração:

(i) Por um lado, como $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ é uma base de I, temos que existem inteiros racionais c_{ij}, com $i = 1, \cdots, n$ e $j = 1, \cdots, n$, tais que

$$\mu_i = \sum_{j=1}^{n} c_{ij}\epsilon_j. \tag{1.2}$$

Por outro lado, como $\mu_1, \mu_2, \ldots, \mu_n$ é uma base de I, temos que existem inteiros racionais d_{jk}, com $j = 1, \cdots, n$ e $k = 1, \cdots, n$, tais que

$$\epsilon_j = \sum_{k=1}^{n} d_{jk}\mu_k. \tag{1.3}$$

Das expressões (1.2) e (1.3), obtemos que

$$\mu_i = \sum_{j=1}^{n} c_{ij} \sum_{k=1}^{n} d_{jk}\mu_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} c_{ij}d_{jk} \right) \mu_k.$$

Agora como $\mu_1, \mu_2, \ldots, \mu_n$ é uma base de I, temos que estes elementos são linearmente independentes sobre $\mathbb{Q}$, e dessa maneira, obtemos:

$$\sum_{j=1}^{n} c_{ij}d_{jk} = \begin{cases} 1, & \text{se} \quad i = k \\ 0, & \text{se} \quad i \neq k \end{cases}. \tag{1.4}$$

Definamos as matrizes quadradas de ordem n, $C = [c_{ij}]$ e $D = [d_{ij}]$. Pelas considerações anteriores, temos que C e D são matrizes inteiras, que satisfazem

$$CD = I_n, \tag{1.5}$$

onde I_n é a matriz identidade de ordem n, visto que é válido (1.4).

Por (1.5), temos que $det(CD) = det(C)det(D) = det(I_n) = 1$. Como C e D são matrizes inteiras, obtemos que $|det(C)| = |det(D)| = 1$.

Agora, calculando o discriminante dos elementos $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$, temos por meio de (1.3), que

$$\Delta[\epsilon_1, \epsilon_2, \cdots, \epsilon_n] = (det(d_{ij}))^2\Delta[\mu_1, \mu_2, \ldots, \mu_n] = (det(D))^2\Delta[\mu_1, \mu_2, \ldots, \mu_n],$$

ou seja,

$$\Delta[\epsilon_1, \epsilon_2, \cdots, \epsilon_n] = \Delta[\mu_1, \mu_2, \ldots, \mu_n],$$

pois, $|det(D)| = 1$.

(ii) Por hipótese, sabemos que $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ formam uma base para I. Dessa maneira como $\mu_1, \mu_2, \ldots, \mu_n \in I$, existem inteiros racionais d_{ij}, com $i = 1, \cdots, n$ e $j = 1, \cdots, n$, tais que

$$\mu_i = \sum_{j=1}^{n} d_{ij}\epsilon_j, i = 1, \cdots, n. \tag{1.6}$$

De (1.6), segue que

$$\Delta[\mu_1, \mu_2, \ldots, \mu_n] = (det(d_{ij}))^2 \Delta[\epsilon_1, \epsilon_2, \cdots, \epsilon_n]. \tag{1.7}$$

Notemos que pela hipótese $\Delta[\mu_1, \mu_2, \ldots, \mu_n] = \Delta[\epsilon_1, \epsilon_2, \cdots, \epsilon_n]$, logo na relação (1.7), obtemos que $det(d_{ij})^2 = 1$, ou seja, $det(d_{ij}) = \pm 1$.

Assim, a matriz definida por $D = [d_{ij}]$, possui uma matriz inversa $C = [c_{ij}]$, tal que c_{ij}, com $i = 1, \cdots, n$ e $j = 1, \cdots, n$, são inteiros racionais, e ainda

$$\epsilon_i = \sum_{j=1}^{n} c_{ij}\mu_j, i = 1, \cdots, n. \tag{1.8}$$

Agora, consideremos $\alpha \in I$. Como $\epsilon_1, \cdots, \epsilon_n$ constitui uma base de I, temos que existem inteiros racionais $a_1, \cdots, a_n$ tais que

$$\alpha = \sum_{i=1}^{n} a_i\epsilon_i. \tag{1.9}$$

Substituindo (1.8) em (1.9), obtemos

$$\alpha = \sum_{i=1}^{n} a_i \sum_{j=1}^{n} c_{ij}\mu_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} a_i c_{ij} \right) \mu_j = \sum_{j=1}^{n} b_j \mu_j,$$

onde $b_j = \sum_{i=1}^{n} a_i c_{ij} \in \mathbb{Z}$, para $j = 1, \cdots, n$. Assim, mostramos que todo elemento de I pode ser escrito como combinação dos elementos $\mu_1, \cdots, \mu_2$. Falta provarmos que tal escrita é de maneira única.

Suponhamos que α possa ser escrito de duas maneiras distintas, ou seja,

$$\alpha = a_1\mu_1 + \cdots + a_n\mu_n = b_1\mu_1 + \cdots + b_n\mu_n,$$

onde $a_1, \cdots, a_n, b_1, \cdots, b_n$ são inteiros racionais.

Assim, com $c_i = a_i - b_i$, para $i = 1, \cdots, n$, temos que

$$c_1\mu_1 + \cdots + c_n\mu_n = 0.$$

Se existir i tal que $c_i \neq 0$, temos que $\mu_1, \cdots, \mu_n$ são linearmente dependentes sobre $\mathbb{Q}$. Logo, pelo Corolário 1.2, teremos que $\Delta[\mu_1, \mu_2, \cdots, \mu_n] = 0$.

Dessa maneira, por meio da relação (1.7), teríamos que $\Delta[\epsilon_1, \epsilon_2, \cdots, \epsilon_n] = 0$. E assim, novamente pelo Corolário 1.2, obteremos que $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ são linearmente dependentes sobre $\mathbb{Q}$, e isto contradiz o fato deste conjunto ser, por hipótese, base de I. Dessa maneira, α é expressado de maneira única como combinação dos elementos $\mu_1, \cdots, \mu_n$.

Portanto $\mu_1, \mu_2, \cdots, \mu_n$ constitui uma base para o ideal I.

■

Pelo item i. do Teorema 1.2, temos que se $\alpha_1, \cdots, \alpha_n$ e $\beta_1, \cdots, \beta_n$ são bases integrais de $\mathbb{K}$, então os respectivos discriminantes são iguais. Diante dessa característica, denominamos o discriminante de uma base integral como o **discriminante do corpo** $\mathbb{K}$, o qual denotamos por $d(\mathbb{K})$.

1.1.1 Teorema A

Consideremos $f(x) = x^3 - 4a^2x + 2$, com $a \in \mathbb{N}$. Uma vez que f é contínua para todo $x \in \mathbb{R}$, segue pelo Teorema do Valor Intermediário, f possui três raízes reais distintas não-nulas, a saber: θ, θ_1 e θ_2, tais que

$$-3a < \theta < -2a, \quad 0 < \theta_1 < 1 \quad \text{e} \quad a < \theta_2 < 2a. \tag{1.10}$$

Estas raízes não são racionais, pois caso existisse alguma raíz racional para f esta deveria pertencer ao conjunto $\{-2, -1, 1, 2\}$, e nenhum elemento deste conjunto consiste em uma raíz de f [1].

As raízes e coeficientes de f se relacionam da seguinte maneira:

$$\begin{aligned} \theta + \theta_1 + \theta_2 &= 0, \\ \theta\theta_1 + \theta\theta_2 + \theta_1\theta_2 &= -4a^2, \\ \theta\theta_1\theta_2 &= -2 \end{aligned} \tag{1.11}$$

[1] Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ e $n \geq 1$. Se $\alpha = \frac{p}{q}$, p e q relativamente primos, é uma raíz racional não-nula de $f(x)$, então $p|a_0$ e $q|a_n$.

Seja $\mathbb{K} = \mathbb{Q}(\theta)$, onde θ é a raiz de f conforme a relação (1.10). Agora caracterizaremos o discriminante e a base integral de $\mathbb{K}$.

Pelas relações (1.11), obtemos uma expressão para o discriminante de θ, ou seja, o discriminante dos elementos $1, \theta$ e θ^2, a saber:

$$\Delta = 4(64a^6 - 27) = i(\theta)^2 d(\mathbb{K}), \tag{1.12}$$

onde $i(\theta)$ é o índice de θ e $d(\mathbb{K})$ é o discriminante de $\mathbb{K}$.

Teorema 1.3 (Teorema A)**.** *Seja $a \in \mathbb{N}$, $\theta < 0$ tal que $\theta^3 - 4a^2\theta + 2 = 0$ e $\mathbb{K} = \mathbb{Q}(\theta)$. Coloque $A = i(\theta)$.*

(i) *Seja β igual a 3 se $3 \mid a$, ou igual a 0, caso contrário. Então*

$$d(\mathbb{K}) = \frac{\Delta}{A^2} = 2^2 3^\beta \prod_{\substack{p>3 \\ s_p \equiv 1 \pmod 2}} p, \quad e \quad p \equiv \pm 1 \pmod{12},$$

onde $s_p = v_p(\Delta)$ é a valoração p-ádica de Δ.

(ii) *Seja $b \in \mathbb{Z}$ tal que $8a^3b \equiv 3 \ (mod A^2)$. Então uma base integral de $\mathcal{O}_\mathbb{K}$ é dada por* $\Gamma = \left\{1, \theta, \dfrac{4a^2b^2 - 4a^2 + 2ab\theta + \theta^2}{A}\right\}$.

Demonstração:

(i) Nesse caso, usando [10] (ver também [2]), podemos calcular o valor de $d(\mathbb{K})$ e encontramos

$$d(\mathbb{K}) = \frac{\Delta}{A^2} = 2^2 3^\beta \prod_{\substack{p>3 \\ s_p \equiv 1 (mod 2)}} p,$$

onde β igual a 3 se $3 \mid a$, ou igual a 0, caso contrário.

Agora, seja p primo, $p > 3$, tal que $p \mid d(\mathbb{K})$, logo $p \mid \Delta$. Dessa maneira, como p e 2 são relativamente primos, obtemos

$$64a^6 \equiv 27 \pmod{p} \Longrightarrow (8a^3)^2 \equiv 3^3 \pmod{p}.$$

Daí 3^3 é um quadrado módulo p. Assim, $\left(\dfrac{3^3}{p}\right) = 1$, onde $\left(\dfrac{\cdot}{p}\right)$ é o símbolo de Legendre, donde segue que devemos ter $\left(\dfrac{3}{p}\right) = 1$.

Pela Lei da Reciprocidade Quadrática, ver [9], temos

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

Agora,

$$\left(\frac{p}{3}\right) = \begin{cases} 1, & \text{se} \quad p \equiv 1 \pmod 3 \\ -1, & \text{se} \quad p \equiv 2 \pmod 3 \end{cases},$$

e

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{se} \quad p \equiv 1 \pmod 4 \\ -1, & \text{se} \quad p \equiv -1 \pmod 4 \end{cases}.$$

Segue do Teorema Chinês do Resto que

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{se} \quad p \equiv \pm 1 \pmod{12} \\ -1, & \text{se} \quad p \equiv \pm 5 \pmod{12} \end{cases}.$$

Portanto os primos p, $p > 3$, que aparecem na fatoração de $d(\mathbb{K})$ são do tipo $p \equiv \pm 1 \pmod{12}$.

(ii) Seja $\alpha = \dfrac{4a^2b^2 - 4a^2 + 2ab\theta + \theta^2}{A}$. Como 1 e θ são inteiros algébricos, inicialmente vamos mostrar que α é um inteiro algébrico. De fato, temos que α é raíz do polinômio com coeficientes racionais $x^3 + Px^2 + Qx + R$, onde

$$P = \frac{-12a^2b^2 + 4a^2}{A}, \quad Q = \frac{48a^4b^4 - 48a^4b^2 + 12ab}{A^2}$$

e

$$R = \frac{-((8a^3b)(b^2-1)+2)^2}{A^3}.$$

Para concluir que α é um inteiro algébrico, basta mostrarmos que P, Q e R são inteiros racionais, e para isto é suficiente que

$$4a^2(1 - 3b^2) \equiv 0 \pmod A, \tag{1.13}$$

$$12ab(1 + 4a^3b(b^2 - 1)) \equiv 0 \pmod{A^2} \tag{1.14}$$

e

$$(8a^3b)(b^2 - 1) + 2 \equiv 0 \pmod{A^2}, \tag{1.15}$$

onde a última relação implicaria que $((8a^3b)(b^2-1)+2)^2 \equiv 0 \pmod{A^3}$.

Por hipótese, temos que

$$8a^3b \equiv 3 \pmod{A^2}. \tag{1.16}$$

Visto que $\Delta \equiv 0 \pmod{A^2}$ e $mdc(A^2, 4) = 1$, temos que

$$64a^6 \equiv 27 \pmod{A^2}. \tag{1.17}$$

Agora, das relações (1.16) e (1.17) segue que

$$9 \equiv (8a^3b)^2 \equiv 27b^2 \pmod{A^2}.$$

Visto que $mdc(A^2, 9) = 1$, temos

$$3b^2 \equiv 1 \pmod{A^2}, \tag{1.18}$$

ou, equivalentemente,

$$b^2 - 1 \equiv -2b^2 \pmod{A^2}. \tag{1.19}$$

A partir das expressões (1.16) e (1.18), obtemos que

$$8a^3b^3 \equiv 1 \pmod{A^2}. \tag{1.20}$$

Segue imediatamente de (1.18) que (1.13) vale, ou seja, $P \in \mathbb{Z}$.

De (1.14), (1.19) e (1.20) temos que $Q \in \mathbb{Z}$, uma vez que vale

$$12ab(1 - 8a^3b^3) \equiv 0 \pmod{A^2}.$$

E das relações (1.15), (1.19) and (1.20) obtemos $R \in \mathbb{Z}$, visto que

$$-16a^3b^3 + 2 \equiv 2(1 - 8a^3b^3) \equiv 0 \pmod{A^2}.$$

Portanto $\alpha \in \mathcal{O}_{\mathbb{K}}$.

Agora, vamos calcular $\Delta[\Gamma] = \Delta[1, \theta, \alpha]$. Por definição, obtemos:

$$\begin{aligned}
\Delta[\Gamma] &= \begin{vmatrix} 1 & \theta & \dfrac{4a^2b^2 - 4a^2 + 2ab\theta + \theta^2}{A} \\ 1 & \theta_1 & \dfrac{4a^2b^2 - 4a^2 + 2ab\theta_1 + {\theta_1}^2}{A} \\ 1 & \theta_2 & \dfrac{4a^2b^2 - 4a^2 + 2ab\theta_2 + {\theta_2}^2}{A} \end{vmatrix}^2 \\
&= \frac{1}{A^2}\left\{ \begin{vmatrix} 1 & \theta & 4a^2b^2 - 4a^2 \\ 1 & \theta_1 & 4a^2b^2 - 4a^2 \\ 1 & \theta_2 & 4a^2b^2 - 4a^2 \end{vmatrix} + \begin{vmatrix} 1 & \theta & 2ab\theta \\ 1 & \theta_1 & 2ab\theta_1 \\ 1 & \theta_2 & 2ab\theta_2 \end{vmatrix} + \begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \theta_1 & {\theta_1}^2 \\ 1 & \theta_2 & {\theta_2}^2 \end{vmatrix} \right\}^2 \\
&= \frac{1}{A^2}\begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \theta_1 & {\theta_1}^2 \\ 1 & \theta_2 & {\theta_2}^2 \end{vmatrix}^2 \\
&= \frac{\Delta}{A^2} \\
&= d(K).
\end{aligned}$$

Assim, Γ é um conjunto de três inteiros algébricos e $\Delta[\Gamma] = d(\mathbb{K})$; logo, aplicando o Teorema 1.2, concluímos que Γ é uma base integral de $\mathbb{K}$.

■

1.2 Sobre Unidades: o Teorema de Dirichlet

Nesta seção buscamos caracterizar as unidades contidas em $\mathcal{O}_{\mathbb{K}}$. Para isto, mostraremos que unidades que satisfazem uma propriedade especial são capazes de gerar as demais unidades de $\mathcal{O}_{\mathbb{K}}$, culminando na demonstração do Teorema de Dirichlet. Para isto, sejam $\mathbb{K}$ um corpo de números de grau n sobre $\mathbb{Q}$ e $\sigma_1, \cdots, \sigma_n$ os monomorfismos de $\mathbb{K}$ sobre $\mathbb{C}$ que fixam $\mathbb{Q}$. Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$, chamamos σ_i de monomorfismo real; caso contrário, σ_i é dito ser complexo. Sejam r a quantidade de monomorfismos reais e $2s$ a quantidade de monomorfismos complexos, assim $n = r + 2s$. A partir deste momento, $\sigma_1, \cdots, \sigma_r$ denotarão os monomorfismos reais e $\sigma_{r+1}, \cdots, \sigma_{r+s}$ os complexos, a menos de conjugados.

Definição 1.4. Seja $\mathbb{K}$ um corpo de números de grau n. Para $\alpha \in \mathbb{K}$, definimos $\beta_i(\alpha) = |\sigma_i(\alpha)|$, para $i = 1, 2, \cdots, r+s$. Estas quantidades denominamos as valorações de α.

Lema 1.2. *Seja $\mathbb{K}$ um corpo de números de grau n.*

(i) Se $m \in \mathbb{Z}$, então $\beta_i(m) = |m|$, para $i = 1, 2, \cdots, r+s$.

(ii) Se $u, v \in \mathbb{K}$, então $\beta_i(uv) = \beta_i(u)\beta_i(v)$, para $i = 1, 2, \cdots, r+s$.

Demonstração:

(i) De fato, por definição $\sigma_1, \cdots, \sigma_n$ são monomorfismos de $\mathbb{K}$ sobre $\mathbb{C}$ que fixam $\mathbb{Q}$, logo $\sigma_i(a) = a$, para todo $a \in \mathbb{Q}$ e $i = 1, \cdots, n$. Dessa maneira, dado $m \in \mathbb{Z} \subseteq \mathbb{Q}$, temos que

$$\beta_i(m) = |\sigma_i(m)| = |m|,$$

para $i = 1, 2, \cdots, r+s$.

(ii) Para $i = 1, 2, \cdots, r+s$ e $u, v \in \mathbb{K}$ temos que

$$\beta_i(uv) = |\sigma_i(uv)| = |\sigma_i(u)\sigma_i(v)| = |\sigma_i(u)||\sigma_i(v)| = \beta_i(u)\beta_i(v).$$

■

Lema 1.3. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$. Temos que $u \in \mathcal{O}_\mathbb{K}$ é uma unidade se, e somente se, $|N(u)| = 1$, onde $N(u)$ é a norma [2] de u. Além disso, o produto de duas unidades é também uma unidade.*

Demonstração: Num sentido, como $u \in \mathcal{O}_\mathbb{K}$ é uma unidade, temos que existe $v \in \mathcal{O}_\mathbb{K}$ tal que $uv = 1$. Dessa maneira,

$$N(uv) = N(1) \Longrightarrow N(u)N(v) = 1,$$

visto que a norma é multiplicativa. Mas, $u, v \in \mathcal{O}_\mathbb{K}$, logo $N(u), N(v) \in \mathbb{Z}$. Dessa maneira, $|N(u)| = 1$.

Por outro lado, se $|N(u)| = 1$, então

$$N(u) = \pm 1 \Longrightarrow \sigma_1(u) \cdots \sigma_n(u) = \pm 1,$$

[2] Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \cdots, \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Dado $\alpha \in \mathbb{K}$, o produto $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ é denominado a **norma** de α.

onde $\sigma_1, \cdots, \sigma_n$ são os monomorfismos de $\mathbb{K}$ sobre $\mathbb{C}$ que fixam $\mathbb{Q}$. Sem perda de generalidade, suponhamos que $\sigma_1(u) = u$. Coloquemos $v = \sigma_2(u) \cdots \sigma_n(u)$. Temos que $v \in \mathcal{O}_{\mathbb{K}}$.

Dessa maneira, $uv = 1$, isto é, u é unidade em $\mathcal{O}_{\mathbb{K}}$.

■

Lema 1.4. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Se ϵ é uma unidade de $\mathcal{O}_{\mathbb{K}}$, então $\beta_1(\epsilon)^{d_1} \cdots \beta_{r+s}(\epsilon)^{d_{r+s}} = 1$ com $d_i = \begin{cases} 1, & se \quad \sigma_i \quad é\ real \\ 2, & se \quad \sigma_i \quad é\ complexo \end{cases}$.*

Demonstração: Dado ϵ uma unidade de $\mathcal{O}_{\mathbb{K}}$, temos pelo Lema 1.3 que $|N(\epsilon)| = 1$. Contudo, uma vez que $n = r + 2s$, o lado esquerdo desta igualdade pode ser expandido da seguinte maneira:

$$\begin{aligned} |N(\epsilon)| &= \left|\prod_{i=1}^{n} \sigma_i(\epsilon)\right| = \left|\prod_{i=1}^{r+s} \sigma_i(\epsilon) \prod_{i=r+s+1}^{r+2s} \sigma_i(\epsilon)\right| = \left|\prod_{i=1}^{r+s} \sigma_i(\epsilon) \prod_{i=r+1}^{r+s} \sigma_{i+s}(\epsilon)\right| \\ &= \left|\prod_{i=1}^{r+s} \sigma_i(\epsilon) \prod_{i=r+1}^{r+s} \bar{\sigma_i}(\epsilon)\right| = \left|\prod_{i=1}^{r} \sigma_i(\epsilon) \prod_{i=r+1}^{r+s} \sigma_i(\epsilon)\bar{\sigma_i}(\epsilon)\right| \\ &= \prod_{i=1}^{r} |\sigma_i(\epsilon)| \prod_{i=r+1}^{r+s} |\sigma_i(\epsilon)|^2 = \prod_{i=1}^{r+s} \beta_i(\epsilon)^{d_i}, \end{aligned}$$

onde $d_i = \begin{cases} 1, & \text{se} \quad \sigma_i \quad \text{é real} \\ 2, & \text{se} \quad \sigma_i \quad \text{é complexo} \end{cases}$, e concluímos o resultado.

■

Dado $\mathbb{K}$ um corpo de números, um resultado clássico que caracteriza as unidades de $\mathcal{O}_{\mathbb{K}}$ é o Teorema de Dirichlet, enunciado a seguir.

Teorema 1.4 (Teorema das Unidades de Dirichlet)**.** *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Sejam r e s, respectivamente, as quantidades de monomorfismos reais e complexos não-conjugados de $\mathbb{K}$ tal que $n = r + 2s$. Então $\mathcal{O}_{\mathbb{K}}$ contém $r+s-1$ unidades $\epsilon_1, \cdots, \epsilon_{r+s-1}$ tais que toda unidade de $\mathcal{O}_{\mathbb{K}}$ pode ser expressada de maneira única da forma $\rho\epsilon_1^{n_1} \cdots \epsilon_{r+s-1}^{n_{r+s-1}}$, onde ρ é uma raíz da unidade em $\mathcal{O}_{\mathbb{K}}$ e $n_1, \cdots, n_{r+s-1}$ são inteiros racionais. As unidades $\epsilon_1, \cdots, \epsilon_{r+s-1}$ são denominadas unidades fundamentais.*

A partir deste momento, iremos estabelecer um critério para definir quando um conjunto de unidades $\epsilon_1, \cdots, \epsilon_{r+s-1} \in \mathcal{O}_{\mathbb{K}}$ constituirá um conjunto de unidades fundamentais.

Para a construção do critério mencionado, iremos considerar $\epsilon_1, \cdots, \epsilon_{r+s-1}$ unidades em $\mathcal{O}_{\mathbb{K}}$ que satisfaçam as seguintes relações:

$$\begin{cases} \beta_i(\epsilon_j) < 1 \quad i = 1, 2, \cdots, r+s, i \neq j \\ \beta_j(\epsilon_j) > 1 \end{cases}, \tag{1.21}$$

e apresentaremos, a seguir, por meio de uma sucessão de lemas, a justificativa de que tais unidades constituem um conjunto de unidades fundamentais.

Definição 1.5. Sejam $\mathbb{K}$ um corpo de números de grau n e $\epsilon_1, \cdots, \epsilon_t$, com $t \geq 1$, unidades em $\mathcal{O}_{\mathbb{K}}$. As unidades $\epsilon_1, \cdots, \epsilon_t$ são ditas independentes se, e somente, se $\epsilon_1^{r_1} \cdots \epsilon_t^{r_t} = 1$, com $r_1, \cdots, r_t$ inteiros racionais, implicar $r_1 = \cdots = r_t = 0$.

Lema 1.5. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Temos que unidades $\epsilon_1, \cdots, \epsilon_{r+s-1}$, que satisfazem a condição* (1.21)*, são independentes.*

Demonstração: Suponhamos que $r + s \geq 2$. A conclusão do caso $r + s = 1$ é imediata. Sejam $\epsilon_1, \cdots, \epsilon_{r+s-1}$ as unidades que satisfaçam as condições (1.21). Suponhamos, por absurdo, que tais unidades não sejam independentes, logo existem inteiros racionais, $\mu_1, \cdots, \mu_{r+s-1}$, não todos nulos, tais que

$$\epsilon_1^{\mu_1} \cdots \epsilon_{r+s-1}^{\mu_{r+s-1}} = 1. \tag{1.22}$$

De (1.22), temos que $\epsilon_1^{-\mu_1} \cdots \epsilon_{r+s-1}^{-\mu_{r+s-1}} = 1$, assim podemos assumir sem perda de generalidade que existe $j \in \{1, 2, \cdots, r+s-1\}$ tal que μ_j é positivo. Dessa maneira, reorganizaremos as unidades acima da seguinte maneira: $\epsilon_1, \cdots, \epsilon_k$, com $k \geq 1$, são as unidades tais que $\mu_1, \cdots, \mu_k$ são positivos e as demais possuem expoentes não-positivos.

Sejam $\beta = \beta_1^{d_1} \cdots \beta_k^{d_k}$ e $\beta' = \beta_{k+1}^{d_{k+1}} \cdots \beta_{r+s}^{d_{r+s}}$, com $d_i = \begin{cases} 1, & \text{se } \sigma_i \text{ é real} \\ 2, & \text{se } \sigma_i \text{ é complexo} \end{cases}$.

Pelos Lemas 1.2 e 1.4 temos que β' é multiplicativa,

$$\beta'(1) = 1 \tag{1.23}$$

e

$$\beta^{'}(\epsilon) = \beta(\epsilon)^{-1}, \tag{1.24}$$

onde ϵ é uma unidade de $\mathcal{O}_{\mathbb{K}}$.

Notemos que para $j = 1, \ldots, k$, temos que

$$\beta^{'}(\epsilon_j) = (\beta_{k+1}^{d_{k+1}} \cdots \beta_{r+s}^{d_{r+s}})(\epsilon_j) = \beta_{k+1}^{d_{k+1}}(\epsilon_j) \cdots \beta_{r+s}^{d_{r+s}}(\epsilon_j) < 1, \tag{1.25}$$

visto que $\beta_i^{d_i}(\epsilon_j) < 1$, para $i = k+1, \cdots, r+s$.

Agora para $j = k+1, \cdots, r+s-1$, temos que

$$\beta(\epsilon_j) = (\beta_1^{d_1} \cdots \beta_k^{d_k})(\epsilon_j) = \beta_1^{d_1}(\epsilon_j) \cdots \beta_k^{d_k}(\epsilon_j) < 1, \tag{1.26}$$

pois $\beta_i^{d_i}(\epsilon_j) < 1$, para $i = 1, \cdots, k$.

Das relações (1.22) e (1.23), sabendo que $\beta^{'}$ é multiplicativa, temos que

$$1 = \beta^{'}(1) = \beta^{'}\left(\prod_{j=1}^{r+s-1} \epsilon_j^{\mu_j}\right) = \prod_{j=1}^{k} \beta^{'}(\epsilon_j)^{\mu_j} \prod_{j=k+1}^{r+s-1} \beta^{'}(\epsilon_j)^{\mu_j}.$$

Agora, usando (1.24), no segundo fator do lado direito da última igualdade, segue que

$$1 = \prod_{j=1}^{k} \beta^{'}(\epsilon_j)^{\mu_j} \prod_{j=k+1}^{r+s-1} \beta(\epsilon_j)^{-\mu_j}.$$

Como $\mu_j > 0$, para $j = 1, \cdots, k$ e $\mu_j < 0$, para $j = k+1, \cdots, r+s-1$, segue pelas relações (1.25) e (1.26) que o lado direito da igualdade acima é estritamente menor do que 1, o que contradiz tal igualdade. Portanto, $\mu_1 = \cdots = \mu_{r+s-1} = 0$, e assim, $\epsilon_1, \cdots, \epsilon_{r+s-1}$ são independentes.

■

Lema 1.6. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Seja $\omega_1, \cdots, \omega_n$ uma base integral de $\mathbb{K}$. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$ possui a propriedade $\beta_j(\alpha) \leq L$, para $j = 1, 2, \cdots, r+s$, então as coordenadas c_i, com $i = 1, \cdots, n$, de α na base integral dada, satisfazem $|c_i| \leq \dfrac{n! L M^{n-1}}{|d(\mathbb{K})|^{1/2}}$, onde $d(\mathbb{K})$ é o discriminante de $\mathbb{K}$ e $M = max\{|\sigma_i(\omega_j)|, 1 \leq i, j \leq n\}$.*

Demonstração: Como c_i, para $i = 1, \cdots, n$, são as coordenadas de α na base integral $\omega_1, \cdots, \omega_n$, temos que $\alpha = c_1\omega_1 + \cdots + c_n\omega_n$. Daí, aplicando os n monomorfismos de $\mathbb{K}$ sobre $\mathbb{C}$ que fixam $\mathbb{Q}$, obtemos o sistema:

$$\begin{array}{rcl} \sigma_1(\alpha) & = & c_1\sigma_1(\omega_1) + \cdots + c_n\sigma_1(\omega_n) \\ \sigma_2(\alpha) & = & c_1\sigma_2(\omega_1) + \cdots + c_n\sigma_2(\omega_n) \\ \vdots & \vdots & \vdots \\ \sigma_n(\alpha) & = & c_1\sigma_n(\omega_1) + \cdots + c_n\sigma_n(\omega_n) \end{array}.$$

Dessa maneira, obtemos pela Regra de Cramer, de resolução de sistemas lineares, que

$$c_i = \frac{det(N_i)}{det(D)}, \tag{1.27}$$

onde $D = [\sigma_i(\omega_j)]$, para $1 \leq i, j \leq n$, e N_i é a matriz constituída a partir de D, pela troca da i-ésima coluna pela coluna formada de $\sigma_1(\alpha), \cdots, \sigma_n(\alpha)$.

Como $\omega_1, \cdots, \omega_n$ é uma base integral de $\mathbb{K}$, segue

$$d(\mathbb{K}) = (det(\sigma_i(\omega_j)))^2 = (det(D))^2,$$

ou seja,

$$det(D) = |d(\mathbb{K})|^{1/2}. \tag{1.28}$$

Agora, calculando o determinante de N_i pela i-ésima coluna, temos que

$$det(N_i) = \sum_{k=1}^{n} \sigma_k(\alpha)(-1)^{k+i}\Delta_k, \tag{1.29}$$

onde Δ_k consiste do determinante de uma matriz de ordem $n-1$ e cujas entradas estão no conjunto $\{\sigma_p(\omega_q) | 1 \leq p, q \leq n\}$. Como $|\sigma_p(\omega_q)| \leq M$, para todo p e q, temos que

$$|\Delta_k| \leq (n-1)!M^{n-1}. \tag{1.30}$$

Dessa maneira, para $i = 1, \cdots, n$, temos por meio das relações (1.29) e (1.30), que

$$|det(N_i)| \leq \sum_{k=1}^{n} |\sigma_k(\alpha)||\Delta_k| \leq (n-1)!M^{n-1} \sum_{k=1}^{n} \beta_k(\alpha) \leq (n-1)!M^{n-1} \sum_{k=1}^{n} L,$$

visto que, por hipótese, $\beta_k(\alpha) \leq L$. Dessa maneira,

$$|det(N_i)| \leq Ln!M^{n-1}. \tag{1.31}$$

Das relações (1.27),(1.28) e (1.31), concluímos para $i = 1, 2, \cdots, n$ que

$$|c_i| = \frac{|det(N_i)|}{|det(D)|} \leq \frac{n!LM^{n-1}}{|d(\mathbb{K})|^{1/2}}.$$

■

Lema 1.7. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$. Existe uma quantidade finita de elementos $\alpha \in \mathcal{O}_\mathbb{K}$ tal que todas as valorações de α estão abaixo de um limite dado.*

Demonstração: Seja $\alpha \in \mathcal{O}_\mathbb{K}$ tal que $\beta_i(\alpha) \leq L$, para todo $i = 1, 2, \cdots, r + s$. Seja $\omega_1, \cdots, \omega_n$ uma base integral de $\mathbb{K}$. Dessa maneira, existem inteiros racionais $c_1, \cdots, c_n$, tais que α pode ser expressado da seguinte maneira

$$\alpha = c_1\omega_1 + \cdots + c_n\omega_n.$$

Mas pelo Lema 1.6, temos que $|c_i| = \dfrac{|det(N_i)|}{|det(D)|} \leq \dfrac{n!LM^{n-1}}{|d(\mathbb{K})|^{1/2}}$, ou seja, o número de possíveis escolhas para cada c_i é dado por $2\left[\dfrac{n!LM^{n-1}}{|d(\mathbb{K})|^{1/2}}\right] + 1$, onde $[x]$ é a parte inteira de x.

Portanto a quantidade de elementos de $\mathcal{O}_\mathbb{K}$ que satisfazem a propriedade inicial dada é no máximo $\left(2\left[\dfrac{n!LM^{n-1}}{|d(\mathbb{K})|^{1/2}}\right] + 1\right)^n$, o que conclui o resultado.

■

Lema 1.8. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$. Para toda unidade $\epsilon \in \mathcal{O}_\mathbb{K}$, com $\beta_v(\epsilon) \leq 1$, para $v = 1, 2, \cdots, r+s-1$, existem inteiros racionais $\mu_1, \cdots, \mu_{r+s-1}$ tais que a unidade dada por $\tau = \epsilon\epsilon_1^{\mu_1} \cdots \epsilon_{r+s-1}^{\mu_{r+s-1}}$ satisfaz as condições $1 < \beta_v(\tau) \leq a_v$, onde $a_v = \beta_v(\epsilon_v)$, para $v = 1, \cdots, r + s - 1$ e $\beta_{r+s}(\tau) \leq \beta_{r+s}(\epsilon)$.*

Demonstração: O caso $r + s = 1$, segue imediatamente pelo Lema 1.4.

Assim, vamos considerar $r + s \geq 2$. Por hipótese, seja ϵ uma unidade de $\mathcal{O}_\mathbb{K}$ que satisfaça $\beta_v(\epsilon) \leq 1$, para $v = 1, 2, \cdots, r + s - 1$.

Consideremos as unidades $\tau \in \mathcal{O}_\mathbb{K}$, da forma $\tau = \epsilon\epsilon_1^{k_1} \cdots \epsilon_{r+s-1}^{k_{r+s-1}}$, com $k_v \geq 0$ para $v = 1, 2, \cdots, r + s - 1$.

Temos que existe L tal que $\beta_v(\tau) \leq L$, para $v = 1, \cdots, r+s$. De fato, para $v = 1, \cdots, r+s-1$, temos

$$\beta_v(\tau) = \beta_v(\epsilon\epsilon_1^{k_1} \cdots \epsilon_{r+s-1}^{k_{r+s-1}}) = \beta_v(\epsilon)\beta_v(\epsilon_1)^{k_1} \cdots \beta_v(\epsilon_{r+s-1})^{k_{r+s-1}} < \beta_v(\epsilon_v) = a_v,$$

visto que $\beta_v(\epsilon) \leq 1$, $\beta_v(\epsilon_u) < 1$, para $v \neq u$ e k_v é inteiro positivo.

Agora, $\beta_{r+s}(\tau) = \beta_{r+s}(\epsilon\epsilon_1^{k_1} \cdots \epsilon_{r+s-1}^{k_{r+s-1}}) \leq \beta_{r+s}(\epsilon)$, visto que $\prod_{i=1}^{r+s-1} \beta_{r+s}(\epsilon_i)^{k_i} < 1$.

Dessa maneira, $\beta_v(\tau)$, para $v = 1, \cdots, r+s$, é limitado. Assim, pelo Lema 1.7, existe uma quantidade finita de τ para ser considerada. Neste conjunto, consideraremos τ tal que $\beta_{r+s}(\tau)$ é minimal. Mostraremos que para esta unidade é válido $\beta_v(\tau) > 1$, para todo $v = 1, 2, \cdots, r+s-1$.

Assim, suponhamos por absurdo, que exista $v_0 \in \{1, 2, \cdots, r+s-1\}$ tal que $\beta_{v_0}(\tau) \leq 1$.

Para $v = 1, 2, \cdots, r+s-1$ e $v \neq v_0$, temos

$$\beta(\epsilon_{v_0}\tau) = \beta_v(\epsilon_{v_0})\beta_v(\tau) < \beta_v(\tau) \leq a_v. \tag{1.32}$$

Para $v = v_0$, temos que

$$\beta_{v_0}(\epsilon_{v_0}\tau) = \beta_{v_0}(\epsilon_{v_0})\beta_{v_0}(\tau) \leq \beta_{v_0}(\epsilon_{v_0}) = a_{v_0}. \tag{1.33}$$

E ainda, para $v = r+s$, temos que

$$\beta_{r+s}(\epsilon_{v_0}\tau) = \beta_{r+s}(\epsilon_{v_0})\beta_{r+s}(\tau) < \beta_{r+s}(\tau) \tag{1.34}$$

Pelas desigualdades (1.32), (1.33) e (1.34) temos que $\epsilon_{v_0}\tau$ é uma unidade que está no conjunto finito de unidades considerado, contudo contradiz a hipótese de τ ser o elemento do conjunto que possui o menor valor de $\beta_{r+s}(\tau)$. Portanto, $\beta_v(\tau) > 1$, para $v = 1, 2, \cdots, r+s-1$.

■

Lema 1.9. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$. Existe uma unidade $\epsilon_0 = \epsilon_1^{\mu_1} \cdots \epsilon_{r+s-1}^{\mu_{r+s-1}} \in \mathcal{O}_\mathbb{K}$ tal que $\beta_v(\epsilon_0) > 1$, para $v = 1, 2, \cdots, r+s-1$.*

Demonstração: Basta tomarmos $\epsilon = 1$ no Lema 1.8 .

■

Lema 1.10. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Para cada unidade $\epsilon \in \mathcal{O}_{\mathbb{K}}$, existem inteiros $\gamma_1, \cdots, \gamma_{r+s-1}$ tais que a unidade $\tau = \epsilon\epsilon_1^{\gamma_1} \cdots \epsilon_{r+s-1}^{\gamma_{r+s-1}}$ satisfaz $1 < \beta_v(\tau) \leq a_v$, onde $a_v = \beta_v(\epsilon_v)$, com $v = 1, 2, \cdots, r+s-1$ e $\beta_{r+s}(\tau) \leq 1$.*

Demonstração: O caso $r+s = 1$, segue imediatamente do Lema 1.4. Suponhamos $r+s \geq 2$. Seja ϵ uma unidade de $\mathcal{O}_{\mathbb{K}}$. Coloquemos $X = max\{\beta_v(\epsilon) | 1 \leq v \leq r+s-1\}$.

Pelo Lema 1.9, temos que existe uma unidade $\epsilon_0 = \epsilon_1^{\mu_1} \cdots \epsilon_{r+s-1}^{\mu_{r+s-1}} \in \mathcal{O}_{\mathbb{K}}$ que satisfaz $\beta_v(\epsilon_0) > 1$, para $v = 1, 2, \cdots, r+s-1$. Definamos $Y = min\{\beta_v(\epsilon_0) | 1 \leq v \leq r+s-1\}$. Segue que $Y > 1$. Dessa maneira, iremos escolher $k \in \mathbb{N}$ tal que $Y^k \leq X$. Logo

$$\beta_v(\epsilon_0)^k \geq Y^k \geq X \geq \beta_v(\epsilon), \tag{1.35}$$

para $v = 1, 2, \cdots, r+s-1$.

Seja $\lambda = \epsilon\epsilon_0^{-k}$. Observemos que λ é uma unidade de $\mathcal{O}_{\mathbb{K}}$, e assim por (1.35), temos para $v = 1, 2, \cdots, r+s-1$ que

$$\beta_v(\lambda) = \beta_v(\epsilon\epsilon_0^{-k}) = \frac{\beta_v(\epsilon)}{\beta_v(\epsilon_0)^k} \leq 1. \tag{1.36}$$

A condição (1.36), nos permite aplicar o Lema 1.8 para λ, e assim existem inteiros racionais $\delta_1, \cdots, \delta_{r+s-1}$ tal que a unidade $\tau = \lambda\epsilon_1^{\delta_1} \cdots \epsilon_{r+s-1}^{\delta_{r+s-1}}$ satisfaz $1 < \beta_v(\tau) \leq a_v$, para $v = 1, \cdots, r+s-1$.

Notemos que

$$\begin{array}{rcrcl} \tau & = & \lambda\epsilon_1^{\delta_1} \cdots \epsilon_{r+s-1}^{\delta_{r+s-1}} & = & \epsilon\epsilon^{-k}\epsilon_1^{\delta_1} \cdots \epsilon_{r+s-1}^{\delta_{r+s-1}} \\ & = & \epsilon\left(\epsilon_1^{\mu_1} \cdots \epsilon_{r+s-1}^{\mu_{r+s-1}}\right)^{-k} \epsilon_1^{\delta_1} \cdots \epsilon_{r+s-1}^{\delta_{r+s-1}} & = & \epsilon\epsilon_1^{\delta_1 - k\mu_1} \cdots \epsilon_{r+s-1}^{\delta_{r+s-1} - k\mu_{r+s-1}} \\ & & & = & \epsilon\epsilon_1^{\gamma_1} \cdots \epsilon_{r+s-1}^{\gamma_{r+s-1}}, \end{array}$$

onde $\gamma_i = \delta_i - k\mu_i$, para $i = 1, 2, \cdots, r+s-1$.

Como $\beta_v(\tau) > 1$, para $v = 1, \cdots, r+s-1$, segue pelo Lema 1.4 que $\beta_{r+s}(\tau) \leq 1$.

■

Lema 1.11. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$. Existe uma quantidade finita de unidades $\eta_1, \cdots, \eta_h \in \mathcal{O}_\mathbb{K}$ tais que toda unidade $\epsilon \in \mathcal{O}_\mathbb{K}$ é escrita como $\epsilon = \eta_j \epsilon_1^{\rho_1} \cdots \epsilon_{r+s-1}^{\rho_{r+s-1}}$ para algum $j \in \{1, 2, \cdots, h\}$ e alguns inteiros racionais $\rho_1, \cdots, \rho_{r+s-1}$.*

Demonstração: Dado ϵ um unidade de $\mathcal{O}_\mathbb{K}$, temos pelo Lema 1.10, que esta pode ser expressada da seguinte maneira

$$\epsilon = \eta \epsilon_1^{-\mu_1} \cdots \epsilon_{r+s-1}^{-\mu_{r+s-1}},$$

com $\mu_1, \cdots, \mu_{r+s-1}$ inteiros racionais e para alguma unidade η com as seguintes propriedades: $\beta_v(\eta) \leq a_v$, onde $a_v = \beta_v(\epsilon_v)$, para $v = 1, 2, \cdots, r+s-1$, e $\beta_{r+s}(\eta) \leq 1$.

Coloque $A = max\{1, a_1, \cdots, a_{r+s-1}\}$, logo $\beta_v(\eta) \leq A$. Segue pelo Lema 1.7, que é finita a quantidade de unidades η com tal propriedade, que vamos por denotar por $\eta_1, \cdots, \eta_h$. Portanto $\epsilon = \eta_j \epsilon_1^{\rho_1} \cdots \epsilon_{r+s-1}^{\rho_{r+s-1}}$, para algum $j \in \{1, 2, \cdots, h\}$ e alguns inteiros racionais $\rho_1, \cdots, \rho_{r+s-1}$.

■

Teorema 1.5 (Critério)**.** *As unidades $\epsilon_1, \cdots, \epsilon_{r+s-1}$ definidas em* (1.21) *constituem um conjunto de unidades fundamentais, ou seja, satisfazem o Teorema de Dirichlet.*

Demonstração: Seja $U(\mathcal{O}_\mathbb{K})$ o grupo das unidades de $\mathcal{O}_\mathbb{K}$. Pelo Lema 1.11, temos que

$$U(\mathcal{O}_\mathbb{K}) =< \epsilon_1, \cdots, \epsilon_{r+s-1}, \eta_1, \cdots, \eta_h > .$$

Consideremos $H =< \epsilon_1, \cdots, \epsilon_{r+s-1} >$. Temos que H é subgrupo de $U(\mathcal{O}_\mathbb{K})$.

Pelo Lema 1.11, existem h classes laterais de H em $U(\mathcal{O}_\mathbb{K})$, e assim o grupo quociente $U(\mathcal{O}_\mathbb{K})/H$ tem ordem h.

Assim, dado $\epsilon \in U(\mathcal{O}_\mathbb{K})$ temos que $(\epsilon H)^h = H$. Logo $\epsilon^h \in H$. Dessa maneira, para toda unidade $\epsilon \in \mathcal{O}_\mathbb{K}$, existem inteiros racionais $a_1, \cdots, a_{r+s-1}$ tais que

$$\epsilon^h = \epsilon_1^{a_1} \cdots \epsilon_{r+s-1}^{a_{r+s-1}}.$$

Sejam $\lambda_1, \cdots, \lambda_m$, com $m \geq r+s$, unidades de $\mathcal{O}_\mathbb{K}$. Logo, pelo raciocínio anterior, temos que existem inteiros racionais a_{ij}, com $i = 1, \cdots, m$ e $j = 1, \cdots, r+s-1$, tais

que

$$\begin{cases} \lambda_1^h &= \epsilon_1^{a_{11}} \cdots \epsilon_{r+s-1}^{a_{1r+s-1}} \\ \vdots & \vdots \quad\quad \vdots \\ \lambda_m^h &= \epsilon_1^{a_{m1}} \cdots \epsilon_{r+s-1}^{a_{mr+s-1}} \end{cases} . \tag{1.37}$$

Agora, consideremos o sistema homogêneo de $r+s-1$ equações lineares em m variáveis $x_1, \cdots, x_m$:

$$\begin{cases} a_{11}x_1 + \cdots + a_{m1}x_m &= 0 \\ \vdots & \vdots \quad \vdots \\ a_{1r+s-1}x_1 + \cdots + a_{mr+s-1}x_m &= 0 \end{cases} .$$

Como $m \geq r+s > r+s-1$, o sistema acima possui uma solução não-trivial $(x_1, \cdots, x_m) \in \mathbb{Q}^m$. Multiplicando cada x_i pelo mínimo múltiplo comum dos denominadores de $x_1, \cdots, x_m$, uma vez que o sistema acima é homogêneo, podemos supor sem perda de generalidade que $(x_1, \cdots, x_m) \in \mathbb{Z}^m$.

Dessa maneira, usando (1.37), temos

$$\begin{aligned} \lambda_1^{hx_1} \cdots \lambda_m^{hx_m} &= (\epsilon_1^{a_{11}} \cdots \epsilon_{r+s-1}^{a_{1r+s-1}})^{hx_1} \cdots (\epsilon_1^{a_{m1}} \cdots \epsilon_{r+s-1}^{a_{mr+s-1}})^{hx_m} \\ &= \epsilon_1^{h(a_{11}x_1 + \cdots + a_{m1}x_m)} \cdots \epsilon_{r+s-1}^{h(a_{1r+s-1}x_1 + \cdots + a_{mr+s-1}x_m)} \\ &= 1. \end{aligned}$$

Logo, concluímos que quaisquer m unidades de $\mathcal{O}_\mathbb{K}$ com $m \geq r+s$ são não independentes. Portanto não existem mais do que $r+s-1$ unidades independentes em $\mathcal{O}_\mathbb{K}$.

Agora, pelo Lema 1.5, as unidades $\epsilon_1, \cdots, \epsilon_{r+s-1}$ são independentes. Logo, usando o *Teorema de Caracterização de Grupos Abelianos Finitamente Gerados* , ver [19], segue que $U(\mathcal{O}_\mathbb{K})$ é o produto direto de grupo cíclicos, sendo $r+s-1$ de ordem infinita e o restante de ordem finita. Contudo, os elementos de um grupo cíclico de ordem finita são raízes da unidade. Dessa forma, toda unidade de $\mathcal{O}_\mathbb{K}$ pode ser escrita na forma $\eta\epsilon_1^{x_1} \cdots \epsilon_{r+s-1}^{x_{r+s-1}}$, onde η é uma raiz da unidade e $x_1, \cdots, x_{r+s-1}$ são inteiros racionais.

Falta mostrar que tal representação é única. Para isto, suponhamos que

$$\epsilon = \eta\epsilon_1^{x_1} \cdots \epsilon_{r+s-1}^{x_{r+s-1}} = \theta\epsilon_1^{y_1} \cdots \epsilon_{r+s-1}^{x_{r+s-1}},$$

onde η e θ são raízes da unidade e $x_1, \cdots, x_{r+s-1}, y_1, \cdots, y_{r+s-1}$ são inteiros racionais.

Logo,

$$\eta\theta^{-1} = \epsilon_1^{y_1 - x_1} \cdots \epsilon_{r+s-1}^{y_{r+s-1} - x_{r+s-1}}. \tag{1.38}$$

Como η e θ são raízes da unidades, segue que $\eta\theta^{-1}$ também é, e assim, existe $k \in \mathbb{N}$, $k \neq 0$, tal que

$$(\eta\theta^{-1})^k = 1. \tag{1.39}$$

De (1.38) e (1.39), obtemos que

$$\epsilon_1^{k(y_1 - x_1)} \cdots \epsilon_{r+s-1}^{k(y_{r+s-1} - x_{r+s-1})} = 1. \tag{1.40}$$

Como $\epsilon_1, \cdots, \epsilon_{r+s-1}$ são independentes, segue de (1.40) que

$$k(x_1 - y_1) = \cdots = k(x_{r+s-1} - y_{r+s-1}) = 0 \Longrightarrow x_1 = y_1, \cdots, x_{r+s-1} = y_{r+s-1},$$

visto que $k \neq 0$. Dessa maneira, segue $\eta = \theta$, o que conclui a unicidade.

■

A partir do Teorema de Dirichlet, temos que todo corpo de números possui um conjunto de unidades de $\mathcal{O}_\mathbb{K}$ que gera as demais unidades de $\mathcal{O}_\mathbb{K}$. Estas unidades são denominadas unidades fundamentais. Agora, consideramos dois conjuntos de unidades fundamentais para $\mathcal{O}_\mathbb{K}$: $\epsilon_1, \cdots, \epsilon_{r+s-1}$ e $\varepsilon_1, \cdots, \varepsilon_{r+s-1}$.

Por um lado, como $\epsilon_1, \cdots, \epsilon_{r+s-1}$ é um conjunto de unidades fundamentais, segue que toda unidade pode ser gerada por elas, logo para $j = 1, 2, \cdots, r+s-1$, temos

$$\varepsilon_j = \xi^{b_j} \epsilon_1^{a_{1j}} \cdots \epsilon_{r+s-1}^{a_{r+s-1j}}, \tag{1.41}$$

onde ξ é uma raiz da unidade em $\mathcal{O}_\mathbb{K}$ e a_{ij}, b_j são inteiros racionais.

Por outro lado, $\varepsilon_1, \cdots, \varepsilon_{r+s-1}$ também é um conjunto de unidades fundamentais e por raciocínio semelhante, obtemos, para $j = 1, 2, \cdots, r+s-1$, que

$$\epsilon_j = \rho^{b_j'} \varepsilon_1^{a_{1j}'} \cdots \varepsilon_{r+s-1}^{a_{r+s-1j}'}, \tag{1.42}$$

onde ρ é uma raíz da unidade em $\mathcal{O}_\mathbb{K}$ e a_{ij}', b_j' são inteiros racionais.

Substituindo (1.42) em (1.41), obtemos que

$$\begin{aligned}
\varepsilon_j &= \xi^{b_j}\epsilon_1^{a_{1j}}\cdots\epsilon_{r+s-1}^{a_{r+s-1j}} &&= \xi^{b_j}\prod_{k=1}^{r+s-1}\epsilon_k^{a_{kj}} \\
&= \xi^{b_j}\prod_{k=1}^{r+s-1}\left(\rho^{b_k^{'}}\prod_{l=1}^{r+s-1}\varepsilon_l^{a_{lk}^{'}}\right)^{a_{kj}} &&= \xi^{b_j}\prod_{k=1}^{r+s-1}\left(\rho^{b_k^{'}a_{kj}}\prod_{l=1}^{r+s-1}\varepsilon_l^{a_{lk}^{'}a_{kj}}\right) \\
&= \xi^{b_j}\rho^{\sum_{k=1}^{r+s-1}b_k^{'}a_{kj}}\cdot\prod_{l=1}^{r+s-1}\varepsilon_l^{\sum_{k=1}^{r+s-1}a_{lk}^{'}a_{kj}}.
\end{aligned}$$

Como a representação das unidades é única, concluímos que

$$\sum_{k=1}^{r+s-1}a_{lk}^{'}a_{kj} = \begin{cases} 1, & \text{se } l = j \\ 0, & \text{se } l \neq j \end{cases} \tag{1.43}$$

Definindo as matrizes $A = [a_{ij}]$ e $A^{'} = [a_{ij}^{'}]$, de ordem $r+s-1$, segue pela relação (1.43), que $AA^{'} = I_{r+s-1}$, onde I_{r+s-1} é a matriz identidade de ordem $r+s-1$. Daí,

$$det(AA^{'}) = det(I_{r+s-1}) \Longrightarrow det(A)det(A^{'}) = 1.$$

Como as entradas das matrizes A e $A^{'}$ são inteiros racionais segue que $|det(A)| = |det(A^{'}| = 1$.

Agora, consideremos $\sigma_1, \cdots, \sigma_{r+s}$ os monomorfismos de $\mathbb{K}$ sobre $\mathbb{C}$ que fixam $\mathbb{Q}$, a menos de conjugados.

Para $k = 1, \cdots, r+s-1$, usando a relação (1.41), obtemos que

$$\sigma_k(\varepsilon_j) = \sigma_k\left(\xi^{b_j}\prod_{l=1}^{r+s-1}\epsilon_l^{a_{lj}}\right) = \sigma_k(\xi^{b_j})\prod_{l=1}^{r+s-1}\sigma_k(\epsilon_l)^{a_{lj}},$$

logo

$$log(|\sigma_k(\varepsilon_j)|) = log\left(\prod_{l=1}^{r+s-1}|\sigma_k(\epsilon_l)|^{a_{lj}}\right) = \sum_{l=1}^{r+s-1}a_{lj}log|\sigma_k(\epsilon_l)|. \tag{1.44}$$

Agora, sejam as matrizes $L = [log|\sigma_i(\epsilon_j)|]$ e $L^{'} = [log|\sigma_i(\varepsilon_j)|]$, de ordem $r+s-1$.

Usando (1.44), obtemos que $L^{'} = LA$, ou seja, $|det(L^{'})| = |det(L)|$, visto que $|det(A)| = 1$.

Daí, obtemos que o número real não-negativo $|det(log|\sigma_i(\epsilon_j)|)|$ independente da escolha do conjunto de unidades fundamentais $\epsilon_1, \cdots, \epsilon_{r+s-1} \in \mathcal{O}_{\mathbb{K}}$. Este número denominamos o **regulador de** $\mathbb{K}$, e o denotamos por $Reg_{\mathbb{K}}$.

1.2.1 Teorema B

Agora, apresentaremos um conjunto de unidades fundamentais para o corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, com $\theta^3 - 4a^2\theta + 2 = 0$. Uma vez que $\mathbb{K}$ é um corpo real, segue que o conjunto de unidades fundamentais é constituído por dois elementos.

Lema 1.12. *Para todo $\alpha = u + v\theta + t\theta^2 \in \mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta^3 - 4a^2\theta + 2 = 0$, temos*

$$N(\alpha) = u^3 - 2v^3 + 4t^3 + 8a^2u^2t - 4a^2uv^2 + 16a^4ut^2 + 8a^2vt^2 + 6uvt.$$

Demonstração: De fato, temos

$$\begin{aligned} N(\alpha) = \; & (u + v\theta + t\theta^2)(u + v\theta_1 + t{\theta_1}^2)(u + v\theta_2 + t{\theta_2}^2) \\ = \; & u^3 + u^2v(\theta + \theta_1 + \theta_2) + u^2t(\theta^2 + {\theta_1}^2 + {\theta_2}^2) + t^3(\theta\theta_1\theta_2)^2 \\ & + uvt(\theta({\theta_1}^2 + {\theta_2}^2) + \theta_1(\theta^2 + {\theta_2}^2) + \theta_2(\theta^2 + {\theta_1}^2)) + v^3\theta\theta_1\theta_2 \\ & + ut^2((\theta\theta_1)^2 + (\theta\theta_2)^2 + (\theta_1\theta_2)^2) + v^2t(\theta{\theta_1}^2\theta_2 + \theta\theta_1{\theta_2}^2 + \theta^2\theta_1\theta_2) \\ & + vt^2(\theta{\theta_1}^2{\theta_2}^2 + \theta^2\theta_1{\theta_2}^2 + \theta^2{\theta_1}^2\theta_2) + uv^2(\theta\theta_1 + \theta\theta_2 + \theta_1\theta_2). \end{aligned}$$

Agora, usando as relações (1.11), obtemos o resultado desejado.

■

Teorema 1.6 (Teorema B)**.** *Seja $a \in \mathbb{N}$, $\theta < 0$ tal que $\theta^3 - 4a^2\theta + 2 = 0$ e $\mathbb{K} = \mathbb{Q}(\theta)$. Para $a \geq 2$, sejam $\epsilon_1 = a\theta^2 - 2a^2\theta + 1$ e $\epsilon_2 = 4a^4\theta^2 + 2a^2\theta - 16a^6 + 1$. Então o conjunto $\{\epsilon_1, \epsilon_2\}$ é um conjunto de unidades fundamentais de $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Aplicando o Lema 1.12 para os elementos $\epsilon_1 = a\theta^2 - 2a^2\theta + 1$ e $\epsilon_2 = 4a^4\theta^2 + 2a^2\theta - 16a^6 + 1$ obtemos que

$$N(\epsilon_1) = N(\epsilon_2) = 1.$$

ou seja, ϵ_1 e ϵ_2 são unidades em $\mathcal{O}_{\mathbb{K}}$.

Sejam $\sigma_1 : \theta \mapsto \theta$, $\sigma_2 : \theta \mapsto \theta_1$ e $\sigma_3 : \theta \mapsto \theta_2$, os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$.

Para $\alpha \in \mathbb{K}$, consideremos $\beta_i(\alpha)$, com $i = 1, 2$ ou 3, as valorações de α, conforme a Definição 1.4.

Nesse momento, iremos mostrar que ϵ_1 é um elemento de $\mathcal{O}_{\mathbb{K}}$ que satisfaz as condições

$$\beta_1(\epsilon_1) > 1, \quad \beta_2(\epsilon_1) < 1 \quad \text{e} \quad \beta_3(\epsilon_1) < 1. \tag{1.45}$$

De fato, consideremos a função $g(x) = ax^2 - 2a^2x + 1$. Esta função é contínua em $\mathbb{R}$. Analisemos para quais valores de x temos que $|g(x)| < 1$, isto é equivalente a resolver a seguinte desigualdade:

$$-1 < ax^2 - 2a^2x + 1 < 1. \tag{1.46}$$

Analisando a segunda desigualdade de (1.46), obtemos que x deve pertencer ao seguinte intervalo:

$$I_1 = \{x \in \mathbb{R} | 0 < x < 2a\}. \tag{1.47}$$

De modo análogo, analisando a primeira desigualdade de (1.46), obtemos que

$$I_2 = \left\{ x \in \mathbb{R} \,|\, x < a - \frac{\sqrt{a^4 - 2a}}{a} \;\text{ ou }\; x > a + \frac{\sqrt{a^4 - 2a}}{a} \right\}. \tag{1.48}$$

Uma vez que $a - \dfrac{\sqrt{a^4 - 2a}}{a} > 0$ e $a + \dfrac{\sqrt{a^4 - 2a}}{a} < 2a$, visto que $a \geq 2$, obtemos pela interseção de (1.47) e (1.48), que o conjunto de valores de x tais que $|g(x)| < 1$ é dado por

$$I_3 = I_1 \cap I_2 = \left\{ x \in \mathbb{R} \,|\, 0 < x < a - \frac{\sqrt{a^4 - 2a}}{a} \;\text{ ou }\; a + \frac{\sqrt{a^4 - 2a}}{a} < x < 2a \right\}. \tag{1.49}$$

Seja $f(x) = x^3 - 4a^2x + 2$ o polinômio minimal de θ. Sendo θ, θ_1 e θ_2 as raízes de f, temos por meio de (1.10) que

$$-3a < \theta < -2a, \quad 0 < \theta_1 < 1 \quad \text{e} \quad a < \theta_2 < 2a. \tag{1.50}$$

Como θ não pertence ao conjunto dado em (1.49), pois θ é negativo, temos que $|g(\theta)| \geq 1$. Contudo, a igualdade não ocorre, pois caso contrarío obteríamos que θ é um número racional, o que é um absurdo. Portanto,

$$|g(\theta)| > 1 \Longrightarrow |a\theta^2 - 2a^2\theta + 1| > 1,$$

ou seja,

$$\beta_1(\epsilon_1) > 1. \tag{1.51}$$

Agora, analisando $f(x)$ nos extremos das condições do intervalo definido em (1.49), segue pelo Teorema do Valor Intermediário, que f possui uma raíz em cada uma das condições.

Para $a \geq 2$, temos que $a + \dfrac{\sqrt{a^4 - 2a}}{a} > 1$, daí θ_2 é a raiz de f que está entre $a + \dfrac{\sqrt{a^4 - 2a}}{a}$ e $2a$. Dessa maneira, obtemos

$$|g(\theta_2)| < 1 \Longrightarrow |a\theta_2^2 - 2a^2\theta_2 + 1| < 1,$$

donde segue

$$\beta_3(\epsilon_1) < 1. \tag{1.52}$$

Por eliminação, concluímos que θ_1 é a raiz de f que está entre 0 e $a - \dfrac{\sqrt{a^4 - 2a}}{a}$, e assim,

$$|g(\theta_1)| < 1 \Longrightarrow |a\theta_1^2 - 2a^2\theta_1 + 1| < 1,$$

ou seja,

$$\beta_2(\epsilon_1) < 1. \tag{1.53}$$

Das relações (1.51), (1.52) e (1.53), obtemos que ϵ_1 satisfaz (1.45).

Agora iremos demonstrar que ϵ_2 é um elemento de $\mathcal{O}_{\mathbb{K}}$ que satisfaz as condições

$$\beta_1(\epsilon_2) < 1, \quad \beta_2(\epsilon_2) > 1 \quad \text{e} \quad \beta_3(\epsilon_2) < 1. \tag{1.54}$$

Para isto, considereremos a função $h(x) = 4a^4x^2 + 2a^2x - 16a^6 + 1$. Esta função é contínua para todo $x \in \mathbb{R}$. Iremos analisar para quais valores de x, temos que $|h(x)| < 1$, ou seja,

$$-1 < 4a^4x^2 + 2a^2x - 16a^6 + 1 < 1. \tag{1.55}$$

Pelo lado direito da desigualdade (1.55), obtemos que x satisfaz a seguinte desigualdade:

$$I_4 = \left\{ x \in \mathbb{R} | \frac{-1 - \sqrt{1 + 64a^6}}{4a^2} < x < \frac{-1 + \sqrt{1 + 64a^6}}{4a^2} \right\}. \tag{1.56}$$

De modo semelhante, realizando da primeira desigualdade de (1.55) obtemos que:

$$I_5 = \left\{ x \in \mathbb{R} | x < \frac{-1 - \sqrt{64a^6 - 7}}{4a^2} \text{ ou } x > \frac{-1 + \sqrt{64a^6 - 7}}{4a^2} \right\}. \tag{1.57}$$

Fazendo interseção dos conjuntos apontados em (1.56) e (1.57), obtemos que o conjunto solução de (1.55) é dado por

$$I_6 = C_1 \cup C_2, \tag{1.58}$$

onde

$$C_1 = \left\{ x \in \mathbb{R} | \frac{-1 - \sqrt{1 + 64a^6}}{4a^2} < x < \frac{-1 - \sqrt{64a^6 - 7}}{4a^2} \right\}$$

e

$$C_2 = \left\{ x \in \mathbb{R} | \frac{-1 + \sqrt{64a^6 - 7}}{4a^2} < x < \frac{-1 + \sqrt{1 + 64a^6}}{4a^2} \right\}.$$

Observemos que o primeiro intervalo de (1.58) é um intervalo de números negativos e o segundo intervalo é de números maiores do que 1, visto que $\frac{-1 + \sqrt{64a^6 - 7}}{4a^2} > 1$.

Por (1.10), temos que θ_1 é um número positivo menor do que 1, dessa maneira, confrontando com (1.58) obtemos que $|h(\theta_1)| \geq 1$. Notemos que a igualdade não ocorre, pois caso contrário, obteríamos que θ_1 ou seria racional ou não estaria entre 0 e 1, o que é um absurdo. Portanto,

$$|h(\theta_1)| > 1 \Longrightarrow |4a^4\theta_1^2 + 2a^2\theta_1 - 16a^6 + 1| > 1,$$

ou seja,

$$\beta_2(\epsilon_2) > 1. \tag{1.59}$$

Agora, avaliando $f(x)$ nos extremos dos intervalos definidos em (1.58), segue pelo Teorema do Valor Intermediário, que f possui uma raiz em cada um dos intervalos considerados.

Diante das características das raízes θ e θ_2 de f, apresentadas em (1.10), obtemos que θ e θ_2 pertencem, respectivamente, ao primeiro e ao segundo intervalos de (1.58). Dessa maneira, temos que

$$|h(\theta)| < 1 \Longrightarrow |4a^4\theta^2 + 2a^2\theta - 16a^6 + 1| < 1$$

e

$$|h(\theta_2)| < 1 \Longrightarrow |4a^4\theta_2^2 + 2a^2\theta_2 - 16a^6 + 1| < 1,$$

ou seja,

$$\beta_1(\epsilon_2) < 1 \tag{1.60}$$

e

$$\beta_3(\epsilon_2) < 1. \tag{1.61}$$

De (1.59), (1.60) e (1.61), temos que (1.54) é satisfeita.

Agora, como as relações (1.45) e (1.54) são válidas, segue pelo critério estabelecido no início desta seção, ver Teorema 1.5, que ϵ_1 e ϵ_2 constituem um conjunto de unidades fundamentais.

■

Observamos que para a fixado, o conjunto de unidades fundamentais descrito no teorema anterior, consistirá do mesmo obtido pelo Método de Voronoi, ver [5].

1.3 Número de Classes

Seja $\mathbb{K}$ um corpo de números. Seja $I(\mathbb{K})$ o grupo de ideais fracionários de $\mathcal{O}_{\mathbb{K}}$. Seja $P(\mathbb{K})$ o subgrupo de ideais principais de $I(\mathbb{K})$. Então o grupo quociente $I(\mathbb{K})/P(\mathbb{K})$ é chamado de grupo de classes de $\mathbb{K}$ e é denotado por $H(\mathbb{K})$. A cardinalidade deste grupo quociente denomina-se o número de classes de $\mathbb{K}$, e é denotado por $h(\mathbb{K})$. O matemático Minkowski demonstrou que $h(\mathbb{K})$ é sempre finito. Nesta seção exploraremos o conceito de número de classes de um corpo real de grau 3.

O conceito de número de classes de um corpo de números $\mathbb{K}$ possui uma relação especial com fatoração em irredutíveis dos elementos de $\mathcal{O}_{\mathbb{K}}$, uma vez que $\mathcal{O}_{\mathbb{K}}$ *constitui um domínio de fatoração única se, e somente se,* $h(\mathbb{K}) = 1$, ver [20].

Sejam $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ e $\zeta_{\mathbb{K}}(s) = \sum_{I \subseteq \mathcal{O}_{\mathbb{K}}} \frac{1}{N(I)^s}$, respectivamente, a função zeta de Riemann e a função zeta-Dedekind. Sobre a primeira função, é conhecido que a série que a define é convergente, 1 é pólo simples de resíduo 1, ver [17]. A soma que define a

segunda função é sobre todos os ideais não-nulos I contidos em $\mathcal{O}_\mathbb{K}$ e $N(I)$ é a norma do ideal I [3]. E ainda, algo semelhante a função zeta podemos obter para a função zeta-Dedekind. Dessa maneira, recorreremos ao Teorema 55 de [8].

Lema 1.13. *Seja $\mathbb{K}$ um corpo de números de grau n. Se V é a quantidade de ideais de $\mathbb{K}$ com norma menor do que v e $h(\mathbb{K})$ é o número de classes de $\mathbb{K}$, então*

$$\lim_{v\to\infty} \frac{V}{v} = h(\mathbb{K})\kappa,$$

tal que $\kappa = \dfrac{2^{r+s}\pi^s Reg_\mathbb{K}}{w\sqrt{|d(\mathbb{K})|}}$, onde $d(\mathbb{K})$ é o discriminante de $\mathbb{K}$, $Reg_\mathbb{K}$ é o regulador de $\mathbb{K}$, w é a quantidade de raízes da unidade, r a quantidade de monomorfismos reais e s a quantidade de monomorfismos complexos, a menos de conjugação.

Lema 1.14. *A série $\zeta_\mathbb{K}(s) = \displaystyle\sum_{I\subseteq\mathcal{O}_\mathbb{K}} \frac{1}{N(I)^s}$, onde I percorre todos os ideais de $\mathcal{O}_\mathbb{K}$, converge para todo $s > 1$ e $\lim\limits_{s\to1}(s-1)\zeta_\mathbb{K}(s) = h(\mathbb{K})\kappa$, tal que $\kappa = \dfrac{2^{r+s}\pi^s Reg_\mathbb{K}}{w\sqrt{|d(\mathbb{K})|}}$, onde $d(\mathbb{K})$ é o discriminante de $\mathbb{K}$, $Reg_\mathbb{K}$ é o regulador de $\mathbb{K}$, w é a quantidade de raízes da unidade, r a quantidade de monomorfismos reais e s a quantidade de monomorfismos complexos, a menos de conjugação.*

Demonstração: Seja $F(n)$ a quantidade de ideais com norma igual a n. Dessa maneira, considerando T como descrito no Lema 1.13, temos a seguinte igualdade de limites:

$$h(\mathbb{K})\kappa = \lim_{t\to\infty}\frac{T}{t} = \lim_{n\to\infty}\frac{F(1)+F(2)+\cdots+F(n)}{n}. \tag{1.62}$$

Sejam $I_1, I_2, \cdots, I_t, \cdots$ os ideais de $\mathcal{O}_\mathbb{K}$, organizados conforme o crescimento do valor da norma n_t, ou seja, $n_1 \le n_2 \le \cdots \le n_t \le \cdots$. Dessa maneira, temos que

$$F(1)+F(2)+\cdots+F(n_t-1) < t \le F(1)+F(2)+\cdots+F(n_t),$$

ou seja,

$$\frac{F(1)+F(2)+\cdots+F(n_t-1)}{n_t-1}\left(1-\frac{1}{n_t}\right) < \frac{t}{n_t} \le \frac{F(1)+F(2)+\cdots+F(n_t)}{n_t}. \tag{1.63}$$

[3] Seja $\mathbb{K}$ um corpo de números de graun n. Seja I um ideal não nulo de $\mathcal{O}_\mathbb{K}$. A **norma do ideal** I, denotada por $N(I)$, é o inteiro positivo definido por $N(I) = \sqrt{\dfrac{D(I)}{d(\mathbb{K})}}$, onde $D(I)$ é o discriminante do ideal I.

Tomando o limite da expressão (1.63), quando t vai para infinito, obtemos por meio de (1.62), que:

$$\lim_{t\to\infty} \frac{t}{n_t} = h(\mathbb{K})\kappa,$$

mais ainda, para todo $\delta > 0$, existe t suficientemente grande, tal que para todo $t^{'} \geq t$ temos que $|\frac{t^{'}}{n_{t^{'}}} - h(\mathbb{K})\kappa| < \delta$, ou seja,

$$\frac{h(\mathbb{K})\kappa - \delta}{t'} < \frac{1}{n_{t'}} < \frac{h(\mathbb{K})\kappa + \delta}{t'}. \tag{1.64}$$

Das propriedades da função Zeta, ver [17], é conhecido que a série $\sum_{t=1}^{\infty} \frac{1}{t^s}$ é convergente para $s > 1$ e que 1 é pólo simples de resíduo 1, ou seja, $\lim_{s\to 1}(s-1)\sum_{t=1}^{\infty} \frac{1}{t^s} = 1$.

Dessa maneira, obtemos que

$$\sum_{t'>t}^{\infty} \frac{1}{(t')^s} \text{ é convergente} \tag{1.65}$$

e

$$\lim_{s\to 1}(s-1)\sum_{t'>t} \frac{1}{(t')^s} = 1. \tag{1.66}$$

Notemos que usando (1.64) e (1.65), por meio do critério da comparação, para $s > 1$ temos que

$$\zeta_{\mathbb{K}}(s) := \sum_{I\in\mathcal{O}_{\mathbb{K}}} \frac{1}{N(I)^s} = \sum_{t=1}^{\infty} \frac{1}{n_t^s}$$

é convergente.

Ainda da relação (1.64), obtemos que

$$\frac{(h(\mathbb{K})\kappa - \delta)^s}{(t')^s} < \frac{1}{n_{t'}^s} < \frac{(h(\mathbb{K})\kappa + \delta)^s}{(t')^s},$$

ou ainda,

$$(s-1)(h(\mathbb{K})\kappa - \delta)^s \sum_{t'>t} \frac{1}{(t')^s} < (s-1)\sum_{t'>t} \frac{1}{n_{t'}^s} < (s-1)(h(\mathbb{K})\kappa + \delta)^s \sum_{t'>t} \frac{1}{(t')^s}. \tag{1.67}$$

Tomando o limite quando s tende a 1, usando (1.66) na desigualdade (1.67), obtemos:

$$h(\mathbb{K})\kappa - \delta \leq \lim_{s\to 1}(s-1)\sum_{t'>t}\frac{1}{n_{t'}^s} \leq h(\mathbb{K})\kappa + \delta. \tag{1.68}$$

Observemos que

$$\lim_{s\to 1}(s-1)\zeta_{\mathbb{K}}(s) = \lim_{s\to 1}(s-1)\sum_{I\in\mathcal{O}_{\mathbb{K}}}\frac{1}{N(I)^s} = \lim_{s\to 1}(s-1)\sum_{t=1}^{\infty}\frac{1}{n_t^s} = \lim_{s\to 1}(s-1)\sum_{t'>t}\frac{1}{n_{t'}^s},$$

logo por (1.68), obtemos

$$h(\mathbb{K})\kappa - \delta \leq \lim_{s\to 1}(s-1)\zeta_{\mathbb{K}}(s) \leq h(\mathbb{K})\kappa + \delta,$$

donde segue

$$\lim_{s\to 1}(s-1)\zeta_{\mathbb{K}}(s) = h(\mathbb{K})\kappa,$$

visto que δ é arbitrário e pequeno.

■

Com este resultado, Dedekind obteve uma relação para o número de classes $h(\mathbb{K})$ por meio da seguinte expressão:

$$Reg_{\mathbb{K}}h_{\mathbb{K}} = \frac{w\kappa_{\mathbb{K}}\sqrt{|d(\mathbb{K})|}}{2^{r+s}\pi^s}.$$

Em nosso contexto, a expressão anterior torna-se

$$Reg_{\mathbb{K}}h_{\mathbb{K}} = \frac{\kappa_{\mathbb{K}}\sqrt{|d(\mathbb{K})|}}{4}, \tag{1.69}$$

uma vez que 1 e -1 são as únicas raízes da unidade em um corpo de números de grau 3, ver [1], $r = 3$ e $s = 0$.

A partir deste momento, buscaremos estabelecer uma estimativa para $\kappa_{\mathbb{K}}$, que nos possibilite efetivamente calcular $h(\mathbb{K})$. Tal discussão será norteada pelos trabalhos de Loubotin, ver [11], [12] e [13].

Lema 1.15. *Seja $\mathbb{K}$ um corpo de números. Se ζ e $\zeta_{\mathbb{K}}$ são, respectivamente, as funções zeta de Riemann e zeta-Dedekind, então $\frac{\zeta_{\mathbb{K}}}{\zeta}(s) = \sum_{n=1}^{\infty}\frac{\phi_n}{n^s}$, onde $\phi_n = \sum_{j|n}\mu(j)F(\frac{n}{j})$, μ é a função de Mobius e $F(n)$ é a quantidade de ideais de $\mathcal{O}_{\mathbb{K}}$ cuja norma é n.*

Demonstração: Temos que

$$\zeta_{\mathbb{K}}(s) = \sum_{I \in \mathcal{O}_{\mathbb{K}}} \frac{1}{N(I)^s} = \sum_{n=1}^{\infty} \frac{F(n)}{n^s}. \tag{1.70}$$

Como $\phi_n = \sum_{j|n} \mu(j) F(\frac{n}{j})$, segue pela Fórmula de Inversão de Mobius que

$$F(n) = \sum_{d|n} \phi(\frac{n}{d}). \tag{1.71}$$

Das expressões (1.70) e (1.71) obtemos

$$\zeta_{\mathbb{K}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|n} \phi(\frac{n}{d}) = \sum_{n=1}^{\infty} \sum_{d|n} \frac{1}{n^s} \phi(\frac{n}{d}) = \sum_{n=1}^{\infty} \frac{\phi_n}{n^s} \sum_{m=1}^{\infty} \frac{1}{m^s} = \sum_{n=1}^{\infty} \frac{\phi_n}{n^s} \zeta(s),$$

ou seja,

$$\frac{\zeta_{\mathbb{K}}}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\phi_n}{n^s}.$$

■

Definamos para $x > 0$ e $\alpha > 0$, a seguinte integral

$$H_{(a,b,c)}(x) = \frac{1}{2i\pi} \int_{\alpha - i\infty}^{\alpha + i\infty} \Gamma\left(\frac{s}{2}\right)^a \Gamma\left(\frac{s+1}{2}\right)^b \Gamma(s)^c x^{-s} ds, \tag{1.72}$$

onde $\Gamma(s) = \displaystyle\int_0^{\infty} t^{s-1} e^{-t} dt$ é a Função Gama.

Definamos para $A > 0$,

$$K_{(a,b,c)}(A) = I_{(a,b,c)}(A) + A J_{(a,b,c)}(A), \tag{1.73}$$

onde $I_{(a,b,c)}(A) = \displaystyle\int_A^{\infty} H_{(a,b,c)}(x) dx$ e $J_{(a,b,c)}(A) = \displaystyle\int_A^{\infty} \frac{H_{(a,b,c)}(x)}{x} dx$.

Considerando $(a, b, c) = (2, 0, 0)$ e usando as relações (2) e (5) de [11], obtemos o resultado a seguir.

Lema 1.16. *Seja $\mathbb{K}$ um corpo de números de grau 3. Então*

$$\kappa_{\mathbb{K}} = \frac{1}{\pi} \sum_{n=1}^{\infty} \frac{\phi_n}{n} K_{(2,0,0)}\left(\frac{n}{A_{\mathbb{K}}}\right),$$

onde ϕ_n é tomado como no Lema 1.15 e $A_{\mathbb{K}} = \dfrac{\sqrt{d_{\mathbb{K}}}}{\pi^{3/2}}$.

O Lema 1.16 nos apresenta uma fórmula para $\kappa_{\mathbb{K}}$. Contudo esta fórmula é dada em função de $K_{(2,0,0)}(X)$. Assim, a partir deste momento, temos por objetivo obter uma expressão para $K_{(2,0,0)}(X)$.

Lema 1.17. *Temos que* $K_{(2,0,0)}(X) = \pi + a_0(X)X + \sum_{n=1}^{\infty} a_n(X)\frac{X^{2n+1}}{(n!)^2}$, *onde*

$$a_0(X) = 2log^2(X) + 4(\gamma+1)log(X) + \frac{\pi^2}{6} + 2\gamma^2 + 4\gamma - 4$$

e

$$a_n(X) = \left(\frac{2}{n} + \frac{2}{n+\frac{1}{2}}\right)\left(log(X) + \gamma - \sum_{k=1}^{n}\frac{1}{k}\right) - \left(\frac{1}{n^2} + \frac{1}{\left(n+\frac{1}{2}\right)^2}\right),$$

com $\gamma = 0,577215$ *a constante de Euler.*

Demonstração: De (1.72) e (1.73), temos que

$$\begin{aligned}
K_{(2,0,0)}(X) = &\ I_{(2,0,0)}(X) + XJ_{(2,0,0)}(X)\\
= &\ \int_X^{\infty} H_{(2,0,0)}(x)dx + X\int_X^{\infty}\frac{H_{(2,0,0)}(x)}{x}dx\\
= &\ \int_X^{\infty}\left[\frac{1}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma\left(\frac{s}{2}\right)^2 x^{-s}ds\right]dx + X\int_X^{\infty}\frac{1}{x}\left[\frac{1}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma\left(\frac{s}{2}\right)^2 x^{-s}ds\right]dx\\
= &\ \frac{1}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma\left(\frac{s}{2}\right)^2\frac{X^{-s+1}}{-1+s}ds + \frac{X}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma\left(\frac{s}{2}\right)^2\frac{X^{-s}}{s}ds\\
= &\ \frac{X}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma\left(\frac{s}{2}\right)^2 X^{-s}\left[\frac{1}{-1+s}+\frac{1}{s}\right]ds,
\end{aligned}$$

ou seja,

$$K_{(2,0,0)}(X) = \frac{X}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma(u)^2X^{-2u}\left[\frac{1}{u}+\frac{1}{u-\frac{1}{2}}\right]du. \tag{1.74}$$

Agora, precisamos resolver a integral do lado direito da igualdade anterior. Para isto recorreremos a teoria de várias complexas, em especial, a resolução de integrais via o Teorema dos Resíduos, ver [17]. Para isto, definamos

$$f(u) = \Gamma(u)^2X^{1-2u}\left[\frac{1}{u}+\frac{1}{u-\frac{1}{2}}\right]. \tag{1.75}$$

Notemos que $\frac{1}{2}$ é um pólo simples de f, $-1, -2, \cdots$, são pólos duplos de f e 0 é um pólo de ordem 3.

Calculando os resíduos de f:

- em $u = \frac{1}{2}$;

  Temos que

$$\lim_{s\to\frac{1}{2}}(u-\frac{1}{2})f(u) = \lim_{s\to\frac{1}{2}}\Gamma(u)^2X^0\left(\frac{u-\frac{1}{2}}{u}+\frac{u-\frac{1}{2}}{u-\frac{1}{2}}\right) = \Gamma\left(\frac{1}{2}\right)^2 = \pi.$$

  Portanto

$$Res(f)\Big|_{u=\frac{1}{2}} = \pi. \tag{1.76}$$

- em $u = 0$;

  nesse caso, consideremos a expansão em série de Laurent de cada um dos termos que compõe a expressão de $f(u)$. Como 0 é um pólo de ordem 3 de f, temos que

$$f(u) = \frac{b_{-3}}{u^3} + \frac{b_{-2}}{s^2} + \frac{b_{-1}}{s} + b_0 + b_1u + \cdots. \tag{1.77}$$

  As expansões em série de Laurent de cada um dos fatores do lado direito de (1.75), são:

$$\Gamma(u)^2 = \frac{a_{-2}}{u^2} + \frac{a_{-1}}{u} + a_0 + a_1u + \cdots, \tag{1.78}$$

$$X^{1-2u} = X - 2Xlog(X)u + 2Xlog^2(X)u^2 - \frac{4}{3}Xlog^3(X)u^3 + \frac{2}{3}Xlog^4(X)u^4 + \cdots \tag{1.79}$$

  e

$$\frac{1}{u-\frac{1}{2}} = -2 - 4u - 8u^2 - 16u^3 - 32u^4 - 64u^5 - 128u^6 + \cdots \tag{1.80}$$

  Efetuando as operações necessárias com as relações (1.78), (1.79) e (1.80), temos por meio de (1.77) que

$$Res(f)\,|_{u=0} = X(2a_{-2}log^2(X) + (2a_{-1} + 4a_{-2})log(X) + a_0 - 4a_{-2} - 2a_{-1}). \tag{1.81}$$

Assim, precisamos determinar os coeficientes a_{-2}, a_{-1} e a_0 da expansão em série de Laurent da função Γ.

Desse modo multiplicando ambos os membros de (1.78) por u^2 e sabendo que 0 é pólo de resíduo 1 da função $\Gamma(u)$, temos que

$$s^2\Gamma(u)^2 = a_{-2} + a_{-1}u + a_0u^2 + a_1u^3 + \cdots \Longrightarrow \lim_{u\to 0} u^2\Gamma(u)^2 = a_{-2} \Longrightarrow a_{-2} = 1.$$

Logo, a expressão (1.78) torna-se

$$\Gamma(u)^2 = \frac{1}{u^2} + \frac{a_{-1}}{u} + a_0 + a_1u + \cdots \tag{1.82}$$

Agora, multiplicando ambos os membros de (1.82) por u^2 e efetuando a primeira derivada em relação a u da expressão obtida, teremos:

$$2u^2\Gamma(u)^2\left[\frac{\Gamma^{'}(u)}{\Gamma(u)} + \frac{1}{u}\right] = a_{-1} + 2ua_0 + 3u^2a_1 + \cdots$$

Tomando o limite, quando u tende a 0, na expressão anterior, obtemos:

$$\lim_{u\to 0} 2u^2\Gamma(u)^2\left[\frac{\Gamma^{'}(u)}{\Gamma(u)} + \frac{1}{u}\right] = a_{-1} \Longrightarrow a_{-1} = -2\gamma,$$

visto que $\lim_{u\to 0}\left(\frac{\Gamma^{'}(u)}{\Gamma(u)} + \frac{1}{u}\right) = -\gamma$, onde γ é a constante de Euler.
Logo, a expressão (1.82) pode ser reescrita da seguinte maneira:

$$\Gamma(u)^2 = \frac{1}{u^2} - \frac{2\gamma}{u} + a_0 + a_1u + \cdots \tag{1.83}$$

Agora, multiplicando ambos os membros de (1.83) por u^2 e em seguida tomando a derivada de segunda ordem da expressão obtida temos:

$$u^2\Gamma(u)^2\left[2\left(\frac{\Gamma^{'}(u)}{\Gamma(u)} + \frac{1}{u}\right)^2 + \Psi^{'}(u+1)\right] = a_0,$$

onde $\Psi(u) = \dfrac{\Gamma^{'}(u)}{\Gamma(u)}$.
Tomando o limite na expressão acima, quando u tende a 0, temos que

$$a_0 = 2\gamma^2 + \frac{\pi^2}{6},$$

visto que $\Psi^{'}(1) = \dfrac{\pi^2}{6}$.

Substituindo os valores obtidos para a_{-2}, a_{-1} e a_0 na expressão (1.81), obtemos que

$$Res(f)\,|_{u=0} = X(2log^2(X) + 4(\gamma - 1)log(X) + \frac{\pi^2}{6} + 2\gamma^2 + 4\gamma - 4). \qquad (1.84)$$

- em $u = -1, -2, -3, \cdots$.

  Nesse caso, sabendo que tais valores são polos de ordem 2 de f e procedendo de maneira análoga ao caso anterior, obteremos que o resíduo de f em $-n$ será dado por:

$$\frac{X^{2n+1}}{(n!)^2}\left[\left(\frac{2}{n} + \frac{2}{n+\frac{1}{2}}\right)\left(log(X) + \gamma - \sum_{k=1}^{n}\frac{1}{k}\right) - \left(\frac{1}{n^2} + \frac{1}{\left(n+\frac{1}{2}\right)^2}\right)\right] \qquad (1.85)$$

Agora, aplicando o Teorema dos Resíduos para a resolução da integral dada em (1.74), obtemos por meio de (1.76), (1.84) e (1.85), o resultado desejado.

■

Do item (a), da Proposição 1, de [11], temos uma estimativa para $H_{(0,0,N)}(x)$.

Lema 1.18. *Para $x > 0$ e $N > 1$ temos que $0 \leq H_{(0,0,N)}(x) \leq \dfrac{2^{N-1}e^{-x^{1/N}}}{x^{1-1/N}}$.*

Lema 1.19. *Para $X > 0$, temos que $0 < K_{(2,0,0)}(X) \leq \dfrac{8e^{-X}}{X}$.*

Demonstração: Por definição, temos que

$$\begin{aligned} K_{(2,0,0)}(X) = &\ I_{(2,0,0)}(X) + XJ_{(2,0,0)}(X) \\ = &\ \frac{X}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma\left(\frac{s}{2}\right)^2\frac{X^{-s}}{s-1}ds + \frac{X}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma\left(\frac{s}{2}\right)^2\frac{X^{-s}}{s}ds. \end{aligned}$$

Como $\dfrac{X^{-s}}{s} \leq \dfrac{X^{-s}}{s-1}$, segue na expressão anterior que,

$$K_{(2,0,0)}(X) \leq 2I_{(2,0,0)}(X) = 2\int_X^\infty\left[\frac{1}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty}\Gamma\left(\frac{s}{2}\right)^2 x^{-s}ds\right]dx. \qquad (1.86)$$

Fazendo a mudança de variável $s = 2u$ em (1.86), obtemos que

$$K_{(2,0,0)}(X) \leq 2\int_X^\infty \left[\frac{1}{2i\pi}\int_{\alpha-i\infty}^{\alpha+i\infty} \Gamma(u)^2(x^2)^{-u}2du\right]dx = 4\int_X^\infty H_{(0,0,2)}(x^2)dx. \quad (1.87)$$

Aplicando o Lema 1.18 no lado direito da desigualdade (1.87), obtemos

$$K_{(2,0,0)} \leq 8\int_X^\infty \frac{e^{-x}}{x}dx \leq 8\int_X^\infty \frac{e^{-x}}{X}dx = \frac{8}{X}\int_X^\infty e^{-x}dx = \frac{8e^{-X}}{X},$$

de onde segue a estimativa desejada.

■

Como a função ϕ_n é multiplicativa, segue que precisamos entender como calcular ϕ_{p^k}, onde p é um número primo. Por meio do trabalho de Barrucand-Loxton-William, ver [4], temos a tabela a seguir, que consta de informações relativas ao comportamento dos valores ϕ_{p^k} e $F(p^k)$ conforme a fatoração em ideais primos do ideal $< p > \subseteq \mathcal{O}_{\mathbb{K}}$. Nela f é inteiro maior ou igual a 1 tal que $d_{\mathbb{K}} = f^2 d_L$, onde L é o subcorpo quadrático real do fecho normal de $\mathbb{K}$ e $\left(\frac{a}{b}\right)$ denota o Símbolo de Kronecker [4].

[4]Sejam $m > 0$, $d \equiv 0$ ou $1 \pmod 4$ com d não quadrado perfeito. O Símbolo de Kronecker $\left(\frac{d}{m}\right)$ é definido por:

- $\left(\frac{d}{p}\right) = 0$, se $p|d$;
- $\left(\frac{d}{2}\right) = \begin{cases} 1, & \text{se } d \equiv 1 \pmod 8 \\ -1, & \text{se } d \equiv 5 \pmod 8 \end{cases}$;
- $\left(\frac{d}{p}\right)$ = Símbolo de Legendre, para p primo ímpar e $p \nmid d$;
- Se $m = \prod_{r=1}^{v} p_r$, onde p_r são primos, então $\left(\frac{d}{m}\right) = \prod_{r=1}^{v}\left(\frac{d}{p_r}\right)$.

Para propriedades, ver [9].

Caso	$< p >$	Observação	k	F_{p^k}	ϕ_{p^k}
p **não divide** $d_{\mathbb{K}}$					
I	$\mathcal{P}$	$\left(\frac{d_{\mathbb{K}}}{p}\right) = 1$	$k \equiv 0 \pmod 3$	1	1
			$k \equiv 1 \pmod 3$	0	-1
			$k \equiv 2 \pmod 3$	0	0
II	$\mathcal{P}_1\mathcal{P}_2$	$\left(\frac{d_{\mathbb{K}}}{p}\right) = -1$	$k \equiv 0 \pmod 2$	$\frac{k+2}{2}$	1
			$k \equiv 1 \pmod 2$	$\frac{k+1}{2}$	0
III	$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$	$\left(\frac{d_{\mathbb{K}}}{p}\right) = 1$	qualquer	$\frac{(k+1)(k+2)}{2}$	$k+1$
p **divide** $d_{\mathbb{K}}$					
IV	$\mathcal{P}_1^2\mathcal{P}_2$	p não divide f	qualquer	$k+1$	1
V	$\mathcal{P}^3$	p divide f	qualquer	1	0

Notamos pela tabela anterior que $|\phi_{p^k}| \leq k+1 = d(p^k)$, onde $d(n)$ denota o número de divisores positivos de $n \geq 1$. A função $d(n)$ é multiplicativa, ver [9]. Dessa maneira, escrevendo $n = p_1^{k_1} \cdots p_r^{k_r}$ temos que

$$|\phi_n| = |\phi_{p_1^{k_1} \cdots p_r^{k_r}}| = |\phi_{p_1^{k_1}} \cdots \phi_{p_r^{k_r}}| = |\phi_{p_1^{k_1}}| \cdots |\phi_{p_r^{k_r}}| \leq (k_1+1) \cdots (k_r+1),$$

ou seja,

$$|\phi_n| \leq d(p_1^{k_1}) \cdots d(p_r^{k_r}) = d(p_1^{k_1} \cdots p_r^{k_r}) = d(n). \tag{1.88}$$

Dado $N \in \mathbb{N}$, definimos as seguintes somas:

$$S_N(n) = \sum_{k=N+1}^{n} \frac{d(k)}{k^2}, \tag{1.89}$$

para $n > N$ e convencione $S_N(N) = 0$;

$$S_N(\infty) = \sum_{k=N+1}^{\infty} \frac{d(k)}{k^2} \tag{1.90}$$

e

$$S(x) = \sum_{1 \leq k \leq x} \frac{d(k)}{k}. \tag{1.91}$$

Lema 1.20. *Dado $N \in \mathbb{N}$, temos que $S_N(\infty) \leq \dfrac{(log(eN)+2)^2}{N}$.*

Demonstração: Observamos que, usando a expressão (1.91), temos

$$S(n) - S(n-1) = \sum_{1\leq k\leq n} \frac{d(k)}{k} - \sum_{1\leq k\leq n-1} \frac{d(k)}{k} = \frac{d(n)}{n}.$$

Assim,

$$\begin{aligned} S_N(\infty) &= \sum_{n>N} \frac{d(n)}{n^2} = \sum_{n>N} \frac{\frac{d(n)}{n}}{n} \\ &= \sum_{n>N} \frac{S(n)-S(n-1)}{n} = \sum_{n>N} \frac{S(n)}{n(n+1)} - \frac{S(N)}{N+1}. \end{aligned}$$

Logo

$$S_N(\infty) \leq \sum_{n>N} \frac{S(n)}{n(n+1)}. \tag{1.92}$$

Temos que

$$S(x) = \sum_{1\leq k\leq x} \frac{d(k)}{k} \leq \left(\sum_{1\leq k\leq x} \frac{1}{k}\right)^2 \leq \left(\int_1^x \frac{1}{k}dk\right)^2 = log^2(x) \leq log^2(ex).$$

Dessa maneira, na expressão (1.92), obtemos:

$$S_N(\infty) \leq \sum_{n>N} \frac{S(n)}{n(n+1)} \leq \sum_{n>N} \frac{log^2(en)}{n(n+1)} \leq \int_N^\infty \frac{log^2(et)}{t^2}dt. \tag{1.93}$$

Fazendo $u = log(et)$, a integral do lado direito de (1.93) torna-se $\displaystyle\int_{log(eN)}^\infty u^2 e^{1-u}du$. Aplicando integração por partes nesta e realizando as operações necessárias, obteremos

$$\int_N^\infty \frac{log^2(et)}{t^2}dt = \frac{log^2(eN) + 2log(eN) + 2}{N}. \tag{1.94}$$

Substituindo (1.94) em (1.93), obtemos

$$S_N(\infty) \leq \frac{log^2(eN) + 2log(eN) + 2}{N} = \frac{(log(eN)+2)^2 - 2log(eN) - 2}{N},$$

e assim

$$S_N(\infty) \leq \frac{(log(eN)+2)^2}{N},$$

o que conclui o resultado.

■

Lema 1.21. *Para $N \in \mathbb{N}$, seja $R_{\mathbb{K}}(N) = \left| \sum_{n>N} \frac{\phi_n}{n} K_{(2,0,0)}\left(\frac{n}{A_{\mathbb{K}}}\right) \right|$. Então*

$$R_{\mathbb{K}}(N) \leq \frac{8A_{\mathbb{K}}(log(eN)+2)^2 e^{-N/A_{\mathbb{K}}}}{N}.$$

Demonstração: Pela Desigualdade Triangular, obtemos que

$$R_{\mathbb{K}}(N) = \left| \sum_{n>N} \frac{\phi_n}{n} K_{(2,0,0)}\left(\frac{n}{A_{\mathbb{K}}}\right) \right| \leq \sum_{n>N} \left|\frac{\phi_n}{n}\right| \left| K_{(2,0,0)}\left(\frac{n}{A_{\mathbb{K}}}\right) \right|.$$

Usando a expressão (1.88) e aplicando o Lema 1.19 no lado direito da desigualdade anterior, obtemos

$$R_{\mathbb{K}}(N) \leq \sum_{n>N} \frac{d(n)}{n} \frac{8e^{-n/A_{\mathbb{K}}}}{n/A_{\mathbb{K}}},$$

ou seja,

$$R_{\mathbb{K}}(N) \leq 8A_{\mathbb{K}} \sum_{n>N} \frac{d(n)}{n^2} e^{-n/A_{\mathbb{K}}}. \tag{1.95}$$

Notemos que

$$S_N(n) - S_N(n-1) = \sum_{k=N+1}^{n} \frac{d(k)}{k^2} - \sum_{k=N+1}^{n-1} \frac{d(k)}{k^2} = \frac{d(n)}{n^2}.$$

Dessa maneira, substituindo na expressão (1.95), obtemos

$$\begin{aligned} R_{\mathbb{K}}(N) &\leq 8A_{\mathbb{K}} \sum_{n>N} (S_N(n) - S_N(n-1)) e^{-n/A_{\mathbb{K}}} \\ &= 8A_{\mathbb{K}} \sum_{n>N} S_N(n)(e^{-n/A_{\mathbb{K}}} - e^{-(n+1)/A_{\mathbb{K}}}) \\ &\leq 8A_{\mathbb{K}} S_N(\infty) \sum_{n>N} (e^{-n/A_{\mathbb{K}}} - e^{-(n+1)/A_{\mathbb{K}}}), \end{aligned}$$

onde a última desigualdade é válida pois $S_N(n) \leq S_N(\infty)$.

Logo,

$$R_{\mathbb{K}}(N) \leq 8A_{\mathbb{K}}S_N(\infty)e^{-(N+1)/A_{\mathbb{K}}}, \tag{1.96}$$

pois $\sum_{n>N}(e^{-n/A_{\mathbb{K}}} - e^{-(n+1)/A_{\mathbb{K}}}) = e^{-(N+1)/A_{\mathbb{K}}}$.

Agora, usando a estimativa dada pelo Lema 1.20 na expressão (1.96) temos que

$$R_{\mathbb{K}}(N) \leq \frac{8A_{\mathbb{K}}(log(eN)+2)^2e^{-(N+1)/A_{\mathbb{K}}}}{N} \leq \frac{8A_{\mathbb{K}}(log(eN)+2)^2e^{-N/A_{\mathbb{K}}}}{N}.$$

■

O Lema 1.21 nos diz que à medida que N é suficientemente grande, temos que $R_{\mathbb{K}}(N)$ se aproxima de zero.

Da expressão (1.69) e do Lema 1.16, temos que

$$h_{\mathbb{K}} = \frac{\sqrt{d_{\mathbb{K}}}}{4Reg_{\mathbb{K}}}\frac{1}{\pi}\sum_{n\geq 1}\frac{\phi_n}{n}K_{(2,0,0)}\left(\frac{n}{A_{\mathbb{K}}}\right).$$

Notemos que podemos separar a soma anterior da seguinte maneira:

$$h_{\mathbb{K}} = \underbrace{\frac{\sqrt{d_{\mathbb{K}}}}{4Reg_{\mathbb{K}}}\frac{1}{\pi}\sum_{n\geq 1}^{N}\frac{\phi_n}{n}K_{(2,0,0)}\left(\frac{n}{A_{\mathbb{K}}}\right)}_{I} + \underbrace{\frac{\sqrt{d_{\mathbb{K}}}}{4Reg_{\mathbb{K}}}\frac{1}{\pi}\sum_{n=N+1}^{\infty}\frac{\phi_n}{n}K_{(2,0,0)}\left(\frac{n}{A_{\mathbb{K}}}\right)}_{II} \tag{1.97}$$

Dessa maneira, temos um algoritmo para obter o número de classes $h(\mathbb{K})$. Este consiste da seguinte dinâmica: conhecendo $d_{\mathbb{K}}$ e $Reg_{\mathbb{K}}$, usamos o Lema 1.21, e determinamos N tal que a parte II da soma (1.97) tenha módulo menor do que $\frac{1}{2}$. Logo, visto que $h(\mathbb{K})$ é um inteiro positivo, segue que $h_{\mathbb{K}}$ será o inteiro mais próximo da parcela I de (1.97). Para efetivamente calcularmos a parcela I, necessitaremos explicitar os valores de ϕ_n, com $1 \leq n \leq N$. Para isto, recorreremos a tabela anteriormente apresentada e ao Teorema de Kummer, ver [20], que caracteriza a fatoração em ideais primos dos ideias $< p >$, onde p é um número primo.

Teorema 1.7 (Teorema de Kummer)**.** *Seja $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$ seu anel de inteiros. Dado um primo racional p, suponhamos que o polinômio minimal f de θ sobre $\mathbb{Q}$ possua a seguinte fatoração em irredutíveis sobre $\mathbb{Z}_p$:*

$$\bar{f} = \bar{g_1}^{e_1}\cdots\bar{g_l}^{e_l},$$

onde a barra denota a aplicação natural $\mathbb{Z}[t] \to \mathbb{Z}_p[t]$. *Então se* f_i *é qualquer polinômio tal que* $\bar{f}_i = \bar{g}_i$, *o ideal* $\mathcal{P}_i =< p, f_i(\theta) >$, *para* $i = 1, \cdots, l$, *é um ideal primo e a fatoração em ideais primos de* $< p >$ *em* $\mathcal{O}_\mathbb{K}$ *é dada por*

$$< p >= \mathcal{P}_1^{e_1} \cdots \mathcal{P}_l^{e_l}.$$

Observação 1.1. Seja $n \in \mathbb{N}$, tal que $\left(\frac{d_\mathbb{K}}{n}\right) = -1$, então $\phi_n = 0$.

De fato, escrevendo n como produto de primos, $n = p_1^{a_1} \cdots p_r^{a_r}$, temos que

$$\left(\frac{d_\mathbb{K}}{n}\right) = \left(\frac{d_\mathbb{K}}{p_1}\right)^{a_1} \cdots \left(\frac{d_\mathbb{K}}{p_r}\right)^{a_r} = -1.$$

Logo existe algum $j \in \{1, \cdots, r\}$, tal que $\left(\frac{d_\mathbb{K}}{p_j}\right) = -1$ e a_j é ímpar. Dessa maneira, pela Tabela anterior, temos que $\phi_{p_j^{a_j}} = 0$, donde segue $\phi_n = 0$, visto que ϕ_n é multiplicativa.

1.3.1 Teorema C

Para obtermos o resultado desta subseção, usaremos o seguinte resultado de Louboutin, ver Teorema 1 de [12].

Lema 1.22. *Seja* $\mathbb{K}$ *um corpo cúbico não normal e* $d_\mathbb{K}$ *seu discriminante. Temos*

$$h_\mathbb{K} Reg_\mathbb{K} \geq \frac{1}{55} \frac{\sqrt{d_\mathbb{K}}}{\log d_\mathbb{K}}, \quad \textit{desde que } d_\mathbb{K} \geq 4 \cdot 10^5,$$

onde $h_\mathbb{K}$ *é o número de classes de* $\mathbb{K}$ *e* $Reg_\mathbb{K}$ *seu regulador.*

Teorema 1.8 (Teorema C)**.** *Seja* $\mathbb{K} = \mathbb{Q}(\theta)$ *um corpo de números, onde* θ *é raiz do polinômio dado por* $f(x) = x^3 - 4a^2x + 2$. *Suponha que* $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$. *Então*

$$h_\mathbb{K} = 1 \ \textit{ se, e somente se, } \ a = 1, 2.$$

Mais ainda, para $a = 5$, *temos* $h_\mathbb{K} = 1$, *embora neste caso* $\mathcal{O}_\mathbb{K} \neq \mathbb{Z}[\theta]$.

Demonstração: Seja θ a raíz de $f(x)$ tal que

$$-3a < \theta < -2a.$$

Consideremos $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$ e tomamos

$$\epsilon_1 = a\theta^2 - 2a^2\theta + 1 \text{ and } \epsilon_2 = 4a^4\theta^2 + 2a^2\theta - 16a^6 + 1.$$

Pelo Teorema 1.6, sabemos que $\{\epsilon_1, \epsilon_2\}$ é um conjunto de unidades fundamentais de $\mathbb{K}$. Iremos calcular o regulador $Reg_{\mathbb{K}}$ de $\mathbb{K}$.

$$Reg_{\mathbb{K}} = \left\| \begin{vmatrix} \log|\epsilon_1| & \log|\epsilon_2| \\ \log|\overline{\epsilon_1}| & \log|\overline{\epsilon_2}| \end{vmatrix} \right\| = |\log|\epsilon_1| \cdot \log|\overline{\epsilon_2}| - \log|\epsilon_2| \cdot \log|\overline{\epsilon_1}||.$$

O polinômio característico de ϵ_1 é dado por $F_a(x) = x^3 - (8a^3+3)x^2 + (4a^3+3)x - 1$ e as raízes são

$$\gamma_3 = \epsilon_1 < \gamma_2 < \gamma_1 = \overline{\epsilon_1}.$$

Usando o Maple, ver [14], temos que ϵ_1 e $\overline{\epsilon_1}$ satisfazem

$$\epsilon_1 = 8a^3 + 2.5 - \frac{7}{32a^3} + O\left(\frac{1}{a^9}\right),$$
$$\overline{\epsilon_1} = \frac{1}{4a^3} - \frac{1}{16a^6} + O\left(\frac{1}{32a^9}\right),$$

onde O é o Símbolo de Landau.

No mesmo sentido, o polinômio característico de ϵ_2 é $G_a(x) = x^3 + (16a^6 - 3)x^2 + 3x - 1$ e suas respectivas raízes são

$$\delta_3 = \overline{\epsilon_2} < \delta_2 < \delta_1 = \epsilon_2$$

que satisfazem

$$\epsilon_2 = \frac{1}{4a^3} - \frac{3}{32a^6} + O\left(\frac{1}{a^9}\right)$$
$$\overline{\epsilon_2} = -16a^6 + 3 + \frac{3}{16a^6} + O\left(\frac{1}{a^9}\right).$$

Portanto, obtemos que

$$\begin{aligned} |\log|\epsilon_2| \cdot \log|\overline{\epsilon_1}| - \log|\epsilon_1| \cdot \log|\overline{\epsilon_2}|| \cong\ & \log|8a^3 + 2.5 - \frac{7}{32a^3}| \cdot \log|16a^6 - 3 - \frac{3}{16a^6}| \\ & - \log|\frac{1}{4a^3} - \frac{1}{16a^6}| \cdot \log|\frac{1}{4a^3} - \frac{3}{32a^6}| \\ & =: R_1. \end{aligned}$$

Visto que $d_{\mathbb{K}} = 4(64a^6 - 27) \geq 4 \cdot 10^5$, para $a \geq 4$, aplicamos o Lema 1.22 e obtemos

$$h_{\mathbb{K}} \geq \frac{1}{55}\ \frac{1}{R_1}\ \frac{\sqrt{4(64a^6 - 27)}}{\log(4(64a^6 - 27))}\ > 1$$

para $a \geq 22$.

Para $a < 22$, vamos encontrar todos os corpos cúbicos definidos por meio $f(x)$ cujo números de classes é igual a 1.

Neste momento, aplicaremos o algoritmo, que é descrito a partir da relação (1.97), para $a = 2$. Nesse caso, temos que $N = 110$. Tendo o valor de N, uma vez que neste caso, $d(\mathbb{K}) = 16276$, $Reg_{\mathbb{K}} = 16,80408264$ e $A_{\mathbb{K}} = 22,91126305$, os valores de ϕ_n, com $n = 1, \cdots, 110$, são obtidos com o auxílio da tabela dada anteriormente, que associa os valores de ϕ_{p^k} com a fatoração do ideal $< p >$ em ideais primos em $\mathcal{O}_{\mathbb{K}}$ e do Teorema 1.7. Dessa maneira, obtemos para $a = 2$, o número de classes é igual a 1.

Para $a = 3$, temos que $N = 438$, $d(\mathbb{K}) = 186516$, $Reg_{\mathbb{K}} = 28,41187934$ e $A_{\mathbb{K}} = 77,55918512$. Daí usando o algoritmo, a tabela anterior e o Teorema 1.7 obtemos, nesse caso, que o número de classes é igual a 3.

Procedemos, por meio do mesmo raciocínio, para os demais valores de a, com $a < 22$. Daí obtemos que os únicos corpos cúbicos definidos por meio de $f(x)$ e que o número de classes é igual a 1 são para os casos $a = 1, 2$ e 5.

Observamos que para o caso $a = 1$ não foi necessário aplicar o algoritmo, pois pelo trabalho de Mordell, ver [16], $\mathcal{O}_{\mathbb{K}}$ é domínio de fatoração única.

■

Observação 1.2. Observamos que o valor de $h_{\mathbb{K}}$ cresce rapidamente, de modo que seu valor fique maior do que 10^6, como nos casos $a = 474$, 489 and 492. Para os valores $a \leq 24$, apresentamos a tabela abaixo com os valores de $h_{\mathbb{K}}$.

a	1, 2 e 5	3	4	6	7	8	9	10	11	12	13
$h_{\mathbb{K}}$	1	3	4	18	10	14	36	28	48	42	38
a	14	15	16	17	18	19	20	21	22	23	24
$h_{\mathbb{K}}$	80	135	88	72	126	164	132	216	168	396	280

Capítulo 2

A Equação Diofantina $v(v+1) = u(u+a)(u+2a)$

Neste capítulo estamos interessados em determinar os inteiros positivos que podem simultaneamente ser escritos como um produto de dois inteiros consecutivos e como o produto de três termos consecutivos em uma progressão aritmética de razão a. Em outras palavras, estamos interessados nas soluções inteiras da Equação Diofantina

$$v(v+1) = u(u+a)(u+2a), u, v, a \in \mathbb{N}. \tag{2.1}$$

É fácil ver que 0 tem a propriedade mencionada e os pares (u, v) que resultam 0 como resposta denominaremos de *soluções triviais*. O caso $a = 1$ foi discutido por Mordell, ver [16], e ele provou que as únicas soluções não triviais de (2.1) são $(1, 2)$, $(1, -3)$, $(5, 14)$ e $(5, -15)$, ou seja, 6 e 210 são os únicos inteiros racionais não nulos que podem ser escritos simultanemanete como um produto de dois inteiros consecutivos e como o produto de três inteiros consecutivos.

Não consiste um problema fácil resolver a equação (2.1) para um valor arbitrário de a, visto que as soluções dependem de algumas características de determinados corpos cúbicos. Diante disso, neste trabalho, explicitamos as soluções para os casos $a = 2$ e $a = 5$, conforme enunciado no próximo teorema, pois nestes casos, temos que os anéis de inteiros do corpo associado constituem um domínio de fatoração única.

Teorema 2.1. *Seja $a \in \{2, 5\}$. Os únicos inteiros racionais não nulos que são simultaneamente um produto de dois inteiros racionais consecutivos e um produto de três*

termos consecutivos de uma progressão aritmética de razão a são:

$$\begin{aligned} &4032,\ 215760,\ \ e\ \ 314160 && \text{para } a = 2,\\ &42,\ 1056,\ 244125000,\ 15438186750\ \ e\ \ 15813188250 && \text{para } a = 5. \end{aligned}$$

A demonstração do teorema consiste em resolver a equação diofantina dada em (2.1). Inicialmente, façamos a seguinte mudança de variáveis:

$$x \leftrightarrow 2u + 2a \ \text{ e } \ y \leftrightarrow 2v + 1, \tag{2.2}$$

dessa maneira a equação (2.1) torna-se

$$2y^2 = x^3 - 4a^2x + 2. \tag{2.3}$$

Diante das equações de mudança de variáveis, temos de modo imediato, que x é par. Se $x < 0$, seja $t = -x > 0$, como $y \neq 0$, obtemos de (2.3) que $-t^3 + 4a^2t + 2 = 2y^2 \geq 2$. Logo $4a^2t \geq t^3$, o que acarreta $t \leq 2a$, ou seja, $x \geq -2a$. Assim, segue o seguinte lema:

Lema 2.1. *Se (x, y) é uma solução inteira de (2.3) então x é par e $y \neq 0$. Se $x < 0$ então $0 > x \geq -2a$. E ainda, as soluções $(0, \pm 1)$ e $(\pm 2a, \pm 1)$ de (2.3) correspondem as soluções triviais da equação (2.1).*

Para darmos continuidade à demonstração, seja θ a raiz negativa de $x^3 - 4a^2x + 2$ e consideremos $\mathbb{K} = \mathbb{Q}(\theta)$ o corpo estudado no capítulo anterior, em especial, é válido (1.10).

Seja $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Nos casos onde $\mathcal{O}_{\mathbb{K}}$ constitui um domínio de fatoração única, segue da equação (2.3) que $N(\theta) = -2$, logo θ é um primo em $\mathcal{O}_{\mathbb{K}}$. Mais ainda, $N(\theta^3/2) = -1$, mostrando que $2 = \rho\theta^3$, onde ρ é uma unidade em $\mathcal{O}_{\mathbb{K}}$. Seja (x, y) uma solução de (2.3). Visto que $\theta^3 \mid 2$ e x é par (ver Lemma 2.1), então $\theta \mid (x - \theta)$ mas $\theta^2 \nmid (x - \theta)$. Isto prova o seguinte resultado.

Lema 2.2. *Seja $\mathcal{O}_{\mathbb{K}}$ um domínio de fatoração única, então θ é um primo, $2 = \rho\theta^3$ onde ρ é uma unidade e $\theta \mid (x - \theta)$ mas $\theta^2 \nmid (x - \theta)$.*

Reescrevamos a equação (2.3) como

$$\rho\theta^3 y^2 = (x - \theta)(x^2 + \theta x + (\theta^2 - 4a^2)), \tag{2.4}$$

e seja π um primo em $\mathcal{O}_{\mathbb{K}}$ que divida ambos $x-\theta$ e $x^2+\theta x+(\theta^2-4a^2)$. Em particular π divide

$$\theta(x^2+\theta x+(\theta^2-4a^2))-\theta(x-\theta)(x+2\theta) = 3\theta^3-4a^2\theta. \tag{2.5}$$

Como $\theta^3-4a^2\theta+2=0$, segue $4a^2\theta=\theta^3+2$. Daí a partir da equação (2.5) obtemos

$$3\theta^3-4a^2\theta = 2(\theta^3-1) = \rho\theta^3(\theta-1)(\theta^2+\theta+1).$$

Logo $\pi=\theta$ ou π é um divisor de $\theta-1$ ou $1+\theta+\theta^2$.

Lema 2.3. *Temos que* $N(\theta-1)=4a^2-3$ *e* $N(\theta^2+\theta+1)=16a^4+12a^2+9$.

Demonstração: No caso de $\theta-1$, aplicamos o Lema 1.12, usando $u=-1$, $v=1$ e $t=0$. E no caso de $\theta^2+\theta+1$, usamos o mesmo Lema, contudo considerando $u=v=t=1$.

■

Lema 2.4. *Seja* $\delta = mdc(\theta-1, \theta^2+\theta+1)$ *em* $\mathcal{O}_{\mathbb{K}}$. *Então* $N(\delta)$ *divide* 27. *Se* $mdc(a,3)=1$ *então* $\theta-1$ *e* $\theta^2+\theta+1$ *são coprimos.*

Demonstração: Da definição de δ, e por meio do Lema 2.3, temos que $N(\delta)$ divide $N(\theta-1)=4a^2-3$ e $N(\theta^2+\theta+1)=16a^4+12a^2+9$. Em particular, $N(\delta)$ divide

$$16a^4+12a^2+9-(4a^2-3)(4a^2+6)=27.$$

Finalmente, observamos que se $|N(\delta)|=3^t>1$ então $N(\theta-1)=4a^2-3\equiv 0 \pmod 3$, e isto é possível se, e somente se $a\equiv 0 \pmod 3$, o que conclui o resultado.

■

A equação (2.4) nos mostra que todos os primos $\pi\neq\theta$ que aparecem na fatoração de $x-\theta$ devem ter expoentes pares, salvo os primos que dividem simultaneamente $\theta-1$ e $\theta^2+\theta+1$.

A estratégia que adotaremos é determinar a fatoração em primos de $\theta-1$ e $\theta^2+\theta+1$ em $\mathcal{O}_{\mathbb{K}}$, digamos

$$\theta-1=\pi_1^{\ell_1}\cdots\pi_m^{\ell_m} \quad \text{and} \quad \theta^2+\theta+1=\omega_1^{i_1}\cdots\omega_n^{i_n}$$

e escrevemos

$$x - \theta = \pm\theta\, \epsilon_1^r\, \epsilon_2^s\, \pi_1^{\ell_1^*} \cdots \pi_m^{\ell_m^*}\, \omega_1^{i_1^*} \cdots \omega_n^{i_n^*}\, (A + B\theta + C\theta^2)^2, \tag{2.6}$$

onde ϵ_1, ϵ_2 são as unidades fundamentais dadas pelo Teorema 1.6, o elemento $A + B\theta + C\theta^2$ de $\mathcal{O}_{\mathbb{K}}$ expressado em termos da base integral dada pelo Teorema 1.3, e $r, s, \ell_1^*, \ldots, \ell_m^*, i_1^*, \ldots, i_n^* \in \{0, 1\}$.

Na sequência expandimos o lado direito de (2.6), e usando a relação $\theta^3 = 4a^2\theta - 2$, obteremos

$$x - \theta = \pm F(A, B, C) + (\pm 1)G(A, B, C)\theta + (\pm 1)H(A, B, C)\theta^2 \tag{2.7}$$

onde F, G e H são polinômios quadráticos em A, B and C. Os valores possíveis de x são obtidos pela resolução do sistema

$$\begin{array}{rcl} \pm x & = & F(A, B, C) \\ \mp 1 & = & G(A, B, C) \\ 0 & = & H(A, B, C). \end{array} \tag{2.8}$$

Observamos que

$$N(x - \theta) = x^3 - 4a^2 + 2 = 2y^2.$$

Portanto, segue de (2.6) que

$$2y^2 = \pm 2N(\pi_1)^{\ell_1^*} \cdots N(\pi_m)^{\ell_m^*}\, N(\omega_1)^{i_1^*} \cdots N(\omega_n)^{i_n^*}\, N(A + B\theta + c\theta^2)^2,$$

e assim,

$$N(\pi_1)^{\ell_1^*} \cdots N(\pi_m)^{\ell_m^*}\, N(\omega_1)^{i_1^*} \cdots N(\omega_n)^{i_n^*} = D^2 \in \mathbb{N}, \tag{2.9}$$

com $\ell_1^*, \ldots, \ell_m^*, i_1^*, \ldots, i_n^* \in \{0, 1\}$.

2.1 O caso $a = 2$

Quando $a = 2$, a equação a ser considerada é dada por

$$2y^2 = x^3 - 16x + 2. \tag{2.10}$$

Temos também que $\Delta = 2^2 \times 13 \times 313$, e segue pelos teoremas 1.3 e 1.6 que $d(\mathbb{K}) = \Delta$, as unidades fundamentais são

$$\epsilon_1 = 2\theta^2 - 8\theta + 1 \quad \text{e} \quad \epsilon_2 = 64\theta^2 + 8\theta - 1023,$$

e a base integral $\{1, \theta, \theta^2\}$.

Observamos que se (x, y) é uma solução da equação (2.10) então pelo Lema 2.1 temos que x é par, $x \geq -4$ e as soluções $(\pm 4, \pm 1)$ correspondem as soluções triviais de (2.1). Uma vez que não existem soluções com $x < 4$, a partir deste momento, assumiremos que

$$x \text{ é par}, \quad x \geq 6. \tag{2.11}$$

Como $N(\theta - 1) = 13$ e $N(1 + \theta + \theta^2) = 313$ (ver Lema 2.3), então eles são ambos primos em $\mathcal{O}_{\mathbb{K}}$. De (2.6) temos que

$$x - \theta = \pm\theta(2\theta^2 - 8\theta + 1)^r(64\theta^2 + 8\theta - 1023)^s(\theta - 1)^{\ell^*}(1 + \theta + \theta^2)^{i^*}(A + B\theta + C\theta^2)^2,$$

com $r, s, \ell^*, i^* \in \{0, 1\}$. De acordo com (2.9), $N(\theta - 1)^{\ell^*} N(1 + \theta + \theta^2)^{i^*}$ deve ser um quadrado em $\mathbb{N}$, logo $\ell^* = i^* = 0$. Dessa maneira, temos

$$x - \theta = \pm\theta(2\theta^2 - 8\theta + 1)^r(64\theta^2 + 8\theta - 1023)^s(A + B\theta + C\theta^2)^2, \tag{2.12}$$

com $r, s \in \{0, 1\}$.

CASO 1: $(r, s) = (1, 1)$**.**

Nesse caso, a equação (2.12) torna-se

$$x - \theta = \pm\theta(2\theta^2 - 8\theta + 1)(64\theta^2 + 8\theta - 1023)(A + B\theta + C\theta^2)^2,$$

donde obtemos o seguinte sistema (ver (2.8) e os respectivos comentários)

$$\begin{aligned} -33C^2 - 2B^2 + AB + 16BC - 4AC &= 0, && (2.13)\\ 264C^2 + 16B^2 + A^2 - 8AB - 132BC + 32AC &= 1, && (2.14)\\ -32C^2 - 2B^2 - 4A^2 + 16BC - 4AC &= -x. && (2.15) \end{aligned}$$

Observe que $8\times$ (2.13) + (2.14) resulta em

$$A^2 - 4BC = 1, \tag{2.16}$$

e podemos reescrever (2.13) como

$$C^2 = (B - 4C)(A - 2(B - 4C)). \tag{2.17}$$

Se $B - 4C = 0$ ou $A - 2(B - 4C) = 0$, então $C = 0$ e $A = \pm 1$ (ver (2.16)). Assim $B = 0$ ou $B \notin \mathbb{Z}$ (um impossibilidade). Se $B = 0$ então $x = 4$ (ver (2.11) e (2.15)). Dessa maneira, segue de (2.16) que $mdc(B - 4C,\ A - 2(B - 4C)) = 1$, visto que A é ímpar. Assim, existem inteiros m e n tais que

$$B - 4C = m^2,\ A - 2(B - 4C) = n^2 \text{ and } C = mn.$$

Logo

$$A = 2m^2 + n^2 \text{ and } B = m^2 + 4mn.$$

Substituindo estas relações em (2.16), obtemos a equação de Thue

$$4m^4 - 4m^3n - 12m^2n^2 + n^4 = 1. \tag{2.18}$$

Por meio do software PARI/GP [18], determinamos que as únicas soluções inteiras de (2.18) são dadas por $(m, n) \in \{(0, 1), (0, -1)\}$, o que nos leva a obter $A^2 = 1$, $B = C = 0$ e $x = 4$ (ver (2.11) e (2.15)). Portanto, não existe solução neste caso.

CASO 2: $(r, s) = (1, 0)$**.**

Neste caso, a equação (2.12) torna-se

$$x - \theta = \pm\theta(2\theta^2 - 8\theta + 1)(A + B\theta + C\theta^2)^2,$$

e assim iremos considerar o seguinte sistema para determinar possíveis valores para x:

$$\begin{aligned} -1089C^2 - 66B^2 - 4A^2 + 33AB + 544BC - 132AC &= 0, && (2.19)\\ 8968C^2 + 544B^2 + 33A^2 - 264AB - 4356BC + 1088AC &= 1, && (2.20)\\ -1088C^2 - 66B^2 - 4A^2 + 32AB + 528BC - 132AC &= -x. && (2.21) \end{aligned}$$

Notemos que $8\times$ (2.19) + (2.20) resulta em

$$(A + 16C)^2 + 16B^2 - 4BC = 1. \tag{2.22}$$

De (2.19), segue que B e C possuem a mesma paridade e a partir de (2.22) concluímos que B e C são pares.

Das relações (2.19) e (2.21), obtemos

$$B(A + 16C) = x + C^2. \tag{2.23}$$

Observamos que segue de (2.11) e (2.23) que $B \neq 0$, dessa maneira substituindo

$$A + 16C = \frac{x + C^2}{B}$$

em (2.22) temos

$$\frac{x^2}{B^2} + \frac{2xC^2}{B^2} + \frac{C^4}{B^2} + 16B^2 - 4BC = 1. \tag{2.24}$$

Notemos que

$$0 \ \leq \ (B-C)^2((B+C)^2 + 2B^2) + 12B^4 \ = \ C^4 + 15B^4 - 4BC^3,$$

logo

$$\frac{C^4}{B^2} + 16B^2 - 4BC \geq B^2. \tag{2.25}$$

Com esta informação e (2.11), a equação (2.24) mostra que não existem soluções com $x \geq 6$.

CASO 3: $(r, s) = (0, 1)$**.**

Neste caso, a equação (2.12) torna-se

$$x - \theta = \pm\theta(64\theta^2 + 8\theta - 1023)(A + B\theta + C\theta^2)^2,$$

de onde obtemos o seguinte sistema:

$$\begin{aligned} -C^2 + 4A^2 + AB &= 0, && (2.26)\\ A^2 - 4BC &= 1, && (2.27)\\ -32AB - 2B^2 - 128A^2 - 4AC &= -x. && (2.28) \end{aligned}$$

Multiplicando ambos os membros de (2.27) por C, obtemos que $A \mid C$, visto que $A \mid C^2$ da relação (2.26). Dessa maneira, $A \mid 1$, ou seja, $A = \pm 1$.

Quando $A = 1$, segue de (2.27), que $B = 0$ ou $C = 0$. Se $B = 0$, em (2.26), obtemos $C = \pm 2$. Então $(1, 0, 2)$ e $(1, 0, -2)$ satisfazem as relações (2.26)-(2.28), de onde obtemos,

$$x = 136 \ \text{ ou } \ x = 120. \tag{2.29}$$

Se $C = 0$, em (2.26), temos $B = -4$. Logo, por meio de (2.28), obtemos

$$x = 32. \tag{2.30}$$

Agora, quando $A = -1$, pela relação (2.27), temos $B = 0$ ou $C = 0$. Se $B = 0$, em (2.26), obtemos $C = \pm 2$, de onde segue que

$$x = 120 \quad \text{ou} \quad x = 136. \tag{2.31}$$

Se $C = 0$, em (2.26), temos $B = 4$. Logo,

$$x = 32. \tag{2.32}$$

CASO 4: $(r, s) = (0, 0)$**.**

Neste caso, a equação (2.12) torna-se

$$x - \theta = \pm\theta(A + B\theta + C\theta^2)^2.$$

Por raciocínio semelhante aos casos anteriores, obtemos o sistema:

$$\begin{aligned} -C^2 + AB + 16BC &= 0, && (2.33)\\ A^2 + 16B^2 + 256C^2 + 32AC - 4BC &= 1, && (2.34)\\ -2B^2 - 32C^2 - 4AC &= -x. && (2.35) \end{aligned}$$

De (2.33) temos

$$C^2 = B(A + 16C). \tag{2.36}$$

Quando $B = 0$, temos $C = 0$. Assim, de (2.35) obtemos

$$x = 0. \tag{2.37}$$

Se $B \neq 0$, das relações (2.34) e (2.36) temos

$$\frac{C^4}{B^2} + 16B^2 - 4BC = 1. \tag{2.38}$$

De (2.25), obtemos $0 < B^2 \leq 1$, ou seja, $B = \pm 1$. Para $B = 1$, a equação (2.38) torna $C^4 - 4C + 15 = 0$, que não possui solução inteira. O mesmo ocorre para $B = -1$.

Agora, de acordo com (2.11), somente as soluções (x, y) de (2.10) com $x \geq 6$ devem ser consideradas, e assim obtemos as soluções $(32, \pm 127)$, $(120, \pm 929)$ e $(136, \pm 1121)$.

As soluções não triviais correspondentes da equação (2.1) são obtidas usando a mudança linear de variáveis descritas em (2.2), a saber:

$$(14, 63), (14, -64), (58, 464), (58, -465), (66, 560), (66, -561).$$

Portanto, os números

$$0,\ 4032,\ 215760 \text{ e } 314160$$

são os únicos inteiros que podem simultaneamente ser escritos como um produto de dois inteiros consecutivos e como produto de três termos consecutivos de um progressão aritmética de razão igual a 2.

2.2 O caso $a = 5$

Agora, estamos interessados nas soluções inteiras de

$$2y^2 = x^3 - 100x + 2. \tag{2.39}$$

Como $\Delta = 4\times 13^2 \times 61 \times 97$, temos que $d(\mathbb{K}) = 4\times 61\times 97$, as unidades fundamentais são

$$\epsilon_1 = 5\theta^2 - 50\theta + 1 \quad \text{e} \quad \epsilon_2 = 2500\theta^2 + 50\theta - 249999,$$

e a base integral é dada por $\{1, \theta, (\theta^2 + 360\theta + 129500)/13\}$ (ver Teoremas 1.3 e 1.6).

Se (x, y) é uma solução de (2.39), então x deve ser par e $x \geq -10$ (ver Lema 2.1). As soluções $(\pm 10, \pm 1)$ consistem das soluções triviais de (2.1). Mais ainda, é fácil verificar que $(-4, \pm 13)$, $(22, \pm 65)$ são soluções e não existe nenhuma outra solução com $x < 23$. Dessa maneira, a partir deste momento, iremos supor que

$$x \text{ é par} \quad \text{e} \quad x \geq 24. \tag{2.40}$$

O valor da norma $N(\theta - 1) = 97$, que mostra que $\theta - 1$ é um primo em $\mathcal{O}_{\mathbb{K}}$. Todavia $N(\theta^2 + \theta + 1) = 13^2 \times 61$ (ver Lema 2.3) e uma análise mais profunda é necessária ser realizada. Temos

$$\theta^2 + \theta + 1 = (-5\theta^2 - 50\theta + 1)(\theta - 9)(-8\theta^2 + 6\theta + 737)/13$$

onde $-5\theta^2 - 50\theta + 1$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$, $\pi_1 = (-8\theta^2 + 6\theta + 737)/13$ and $\pi_2 = \theta - 9$ são primos em $\mathcal{O}_{\mathbb{K}}$ com $N(\pi_1) = 61$ e $N(\pi_2) = 169$, onde a primalidade de $\theta - 9$ foi verificada com o auxílio do PARI/GP. De (2.6) obtemos que

$$x - \theta = \pm\theta\epsilon_1^r\epsilon_2^s(\theta-1)^{\ell^*}\pi_1^{i_1^*}\pi_2^{i_2^*}(a + b + c((\theta^2 + 360\theta + 129500)/13)^2$$

com $r, s, \ell^*, i_1^*, i_2^* \in \{0, 1\}$.

De acordo com o raciocínio apontado em (2.9), obtemos

$$D^2 = N(\theta-1)^{\ell^*}N(\pi_1)^{i_1^*}N(\pi_2)^{i_2^*} = 97^{\ell^*}61^{i_1^*}13^{2i_2^*},$$

logo $\ell^* = i_1^* = 0$. Portanto, temos os seguintes casos para serem considerados:

$$x - \theta = \pm\theta\epsilon_1^r\epsilon_2^s(\theta-9)^i((A + B\theta + C\theta^2)/13)^2, \tag{2.41}$$

com $r, s, i \in \{0, 1\}$.

Como no caso anterior, para determinarmos os valores possíveis de x, teremos que considerar oito sistemas (ver (2.8)) dependendo dos valores de r, s and i. Tais sistemas são obtidos depois da expansão do lado direito de (2.41) (ver (2.7)). Uma simples análise desses sistemas módulo 4 revela que, como no caso $a = 2$, a situação $x = F(A, B, C)$ e $-1 = G(A, B, C)$ pode ser descartada (ver (2.8)).

CASO 1: $(r, s, i) = (0, 0, 0)$**.**

Neste caso, a equação (2.41) torna-se

$$x - \theta = \pm\theta\frac{(A + B\theta + C\theta^2)^2}{169},$$

e daí consideraremos o seguinte sistema:

$$\begin{aligned} -C^2 + AB + 100BC &= 0, & (2.42)\\ (A + 100C)^2 + 100B^2 - 4BC &= 169, & (2.43)\\ -2B^2 - 200C^2 - 4AC &= -169x. & (2.44) \end{aligned}$$

De (2.42), temos

$$C^2 = B(A + 100C). \tag{2.45}$$

Quando $B = 0$, então $C = 0$ e consequentemente via (2.44) obtemos

$$x = 0. \tag{2.46}$$

Se $B \neq 0$, das expressões (2.43) e (2.45), temos que

$$\frac{C^4}{B^2} + 100B^2 - 4BC = 169. \tag{2.47}$$

Como

$$0 \leq (B-C)^2((B+C)^2 + 2B^2) + 96B^4 = 99B^4 + C^4 - 4B^3C$$

temos que (ver (2.47))

$$169 = \frac{C^4}{B^2} + 100B^2 - 4BC \geq B^2, \tag{2.48}$$

isto é, $B = \pm 1, \pm 2, \ldots, \pm 13$. Substituindo estes valores em (2.47), observamos que somente para $B = \pm 1$ a equação (2.47) possui soluções inteiras, e todas as soluções fornecem $x = -10$ (ver 2.40). Nestes casos, os valores para C são $C = -3$ e $C = 3$, respectivamente.

CASO 2: $(r, s, i) = (1, 0, 0)$.

Neste caso, a equação (2.41) torna-se

$$x - \theta = \pm\theta(5\theta^2 - 50\theta + 1)\frac{(A + B\theta + C\theta^2)^2}{169},$$

e teremos o seguinte sistema a ser considerado:

$$-251001C^2 - 2505B^2 - 25A^2 + 501AB + 50200BC - 5010AC = 0, \tag{2.49}$$

$$5030020C^2 + 50200B^2 + 501A^2 - 10020AB - 1004004BC + 100400AC = 169, \tag{2.50}$$

$$-100400C^2 - 1002B^2 - 10A^2 + 200AB + 20040BC - 2004AC = -169x. \tag{2.51}$$

Observe que $20\times$ (2.49) + (2.50) resulta em

$$(A + 100C)^2 + 100B^2 - 4BC = 169. \tag{2.52}$$

Notemos que $5\times$ (2.51) $-2\times$ (2.49) resulta em

$$845x = 2B(A + 100C) - 2C^2. \tag{2.53}$$

Se $B = 0$, segue de (2.53) que $x < 0$, um contradição com a condição (2.40). Logo, podemos assumir o contrário e reescrever (2.53) como

$$A + 100C = \frac{845x + 2C^2}{2B} \tag{2.54}$$

Substituindo (2.54) em (2.52) temos que

$$\frac{714025x^2}{4B^2} + \frac{845xC^2}{B^2} + \frac{C^4}{B^2} + 100B^2 - 4BC = 169. \tag{2.55}$$

Novamente a condição (2.40) e a desigualdade (2.48) nos leva a obter que $B^2 \leq 169$, logo $B = \pm 1, \pm 2, \ldots, \pm 13$. Por um lado, como $x \geq 24$ e $|B| \leq 13$, não existe valor inteiro de C satisfazendo (2.55). Logo, não existe solução com $x \geq 24$.

CASO 3: $(r, s, i) = (0, 1, 0)$.

Neste caso, a equação (2.41) torna-se

$$x - \theta = \pm\theta(2500\theta^2 + 50\theta - 249999)\frac{(A + B\theta + C\theta^2)^2}{169},$$

e passamos a considerar o seguinte sistema:

$$\begin{aligned} -2C^2 + 50A^2 + 2AB &= 0, & (2.56)\\ A^2 - 4BC &= 169, & (2.57)\\ -200AB - 2B^2 - 5000A^2 - 4AC &= -169x. & (2.58) \end{aligned}$$

Uma consequência direta de (2.56) é que $A \mid C^2$, logo todos os primos divisores de A são também divisores de C. Contudo (2.57) nos diz que qualquer primo divisor de A divide 169 (pois ele divide C). Logo $A = \pm 13^v$ e $C = 13^u C_0$. Olhando para a equação (2.57), se $v \leq u$, então $13^v \mid 13^2$. Se $v > u$, então $u < v \leq 2u$ (pois $A \mid C^2$), e $13^u \mid 13^2$. Em todo caso, temos $A = \pm 13^v$, para algum $0 \leq v \leq 4$.

Para $A = \pm 1$, voltamos para (2.56) e (2.57) para encontrar os valores correspondentes de B and C. Mas os valores obtidos para x, com estes valores A, B, C, são negativos o que contraria (2.40). Assim, vamos considerar que $13 \mid A$. Logo, as equações (2.56) e (2.58) nos garantem que $13 \mid B$ e $13 \mid C$ e, dessa maneira, obtemos o seguinte sistema:

$$\begin{aligned} -2C_0^2 + 50A_0^2 + 2A_0B_0 &= 0, & (2.59)\\ A_0^2 - 4B_0C_0 &= 1, & (2.60)\\ -200A_0B_0 - 2B_0^2 - 5000A_0^2 - 4A_0C_0 &= -x, & (2.61) \end{aligned}$$

onde $A = 13A_0$, $B = 13B_0$ e $C = 13C_0$.

Por análise semelhante ao sistema anterior, a equação (2.59) mostra que $A_0 \mid C_0^2$, mas a equação (2.60) mostra que as únicas possibilidades são $A_0 = \pm 1$ e $B_0 = 0$ ou $C_0 = 0$. Se $B_0 = 0$, então $C_0 = \pm 5$. Logo, temos as soluções (substituindo em (2.61))

$$x = 4980 \quad \text{e} \quad x = 5020. \tag{2.62}$$

Se $C_0 = 0$, então $B_0 = \pm 25$ e obtemos a solução

$$x = 1250. \tag{2.63}$$

CASO 4: $(r, s, i) = (1, 1, 0)$.

Neste caso, a equação (2.41) torna-se

$$x - \theta = \pm\theta(5\theta^2 - 50\theta + 1)(2500\theta^2 + 50\theta - 249999)\frac{(A + B\theta + C\theta^2)^2}{169},$$

e daí segue o seguinte sistema:

$$\begin{aligned} -501C^2 - 5B^2 + AB + 100BC - 10AC &= 0, && (2.64)\\ 10020C^2 + 100B^2 + A^2 - 20AB - 2004BC + 200AC &= 169, && (2.65)\\ -200C^2 - 2B^2 - 10A^2 + 40BC - 4AC &= -169x. && (2.66) \end{aligned}$$

Notemos que $20\times$ (2.64) + (2.65) resulta

$$A^2 - 4BC = 169. \tag{2.67}$$

E ainda podemos reescrever (2.64) da seguinte maneira

$$C^2 = (B - 10C)(A - 5(B - 10C)). \tag{2.68}$$

Se $B - 10C = 0$ ou $A - 5(B - 10C) = 0$, então $C = 0$ e $A = \pm 13$ (veja (2.67)). Logo $B = 0$ ou $B \notin \mathbb{Z}$ (que é impossível). Da equação (2.66), segue que $x = 10$ (veja condição (2.40)).

Caso contrário, seja

$$d = mdc(B - 10C,\ A - 5(B - 10C)).$$

Então $d \mid A$, $d \mid C$ (ver (2.68)), e $d \mid B$. Logo $d \mid 13$ (ver (2.67)), ou seja, $d = 1$ ou 13. Logo, existem inteiros m e n tais que

$$B - 10C = dm^2, \;\; A - 5(B - 10C) = dn^2, \;\; \text{and} \;\; C = dmn.$$

Logo

$$A = d(n^2 + 5m^2) \;\; \text{and} \;\; B = d(m^2 + 10mn).$$

Substituindo estas relações em (2.67) obtemos a equação

$$25m^4 - 4m^3n - 30m^2n^2 + n^4 = \frac{169}{d^2}. \tag{2.69}$$

Usando PARI/GP [18], visto que temos uma Equação de Thue, buscaremos as soluções inteiras (m, n) para cada valor de d, e assim temos

$$\begin{aligned} d = 13 \;\; &: \;\; (m, n) = (0, \pm 1) \\ d = 1 \;\; &: \;\; (m, n) \in \{(-7, -6), (-3, 16), (-2, -11), (2, 11), (3, -16), (7, 6)\}, \end{aligned}$$

de onde segue que

$$\begin{aligned} d = 13 \;\; &: \;\; x = 10 \\ d = 1 \;\; &: \;\; x \in \{1250, 4980, 5020\}. \end{aligned}$$

E concluí a análise deste caso.

CASO 5: $(r, s, i) = (0, 0, 1)$.

Neste caso, a equação (2.41) torna-se

$$x - \theta = \pm\theta(\theta - 9)\frac{(A + B\theta + C\theta^2)^2}{169},$$

e daí segue o seguinte sistema:

$$\begin{aligned} 18B^2 + 1804C^2 - 4AB + 36AC - 400BC &= -169x, \\ -9A^2 - 902B^2 - 90400C^2 + 200AB - 1804AC + 20036BC &= 169, \qquad (2.70) \\ A^2 + 100B^2 + 10018C^2 - 18AB + 200AC - 1804BC &= 0. \qquad (2.71) \end{aligned}$$

Analisando módulo 2, as relações (2.70) e (2.71), obtemos A ímpar e A par, o que é uma contradição. Portanto, o sistema não possui solução inteira.

CASO 6: $(r, s, i) = (0, 1, 1)$.

Neste caso, a equação (2.41) torna-se

$$x - \theta = \pm\theta(\theta - 9)(2500\theta^2 + 50\theta - 249999)\frac{(A + B\theta + C\theta^2)^2}{169},$$

e segue o sistema:

$$\begin{aligned} 44900A^2 + 18B^2 + 4C^2 + 1796AB + 36AC &= -169x, \\ -9A^2 - 2B^2 - 200C^2 - 4AC + 36BC &= 169, \qquad (2.72) \\ -449A^2 + 18C^2 - 18AB - 4BC &= 0. \qquad (2.73) \end{aligned}$$

Analisando módulo 2, as relações (2.72) e (2.73), obtemos A ímpar e A par, o que é uma contradição. Portanto, o sistema não possui solução inteira.

CASO 7: $(r, s, i) = (1, 0, 1)$.

Neste caso, a equação (2.41) torna-se

$$x - \theta = \pm\theta(\theta - 9)(5\theta^2 - 50\theta + 1)\frac{(A + B\theta + C\theta^2)^2}{169},$$

e segue o sistema:

$$\begin{aligned} 190A^2 + 19038B^2 + 1907604C^2 - 3804AB + 38076AC - 381160BC &= -169x, \\ -9519A^2 - 953802B^2 - 95570780C^2 + 190580AB - 1907604AC + 19096076BC &= 169, \\ 951A^2 + 95290B^2 + 9548038C^2 - 19038AB + 190580AC - 1907604BC &= 0. \end{aligned}$$

Analisando módulo 2, a segunda e a terceira equações do sistema acima, obtemos A ímpar e A par, o que é uma contradição. Portanto, o sistema não possui solução inteira.

CASO 8: $(r, s, i) = (1, 1, 1)$.

Neste caso, a equação (2.41) torna-se

$$x - \theta = \pm\theta(\theta - 9)(5\theta^2 - 50\theta + 1)(2500\theta^2 + 50\theta - 249999)\frac{(A + B\theta + C\theta^2)^2}{169},$$

e segue o sistema:

$$\begin{aligned} 90A^2 + 38B^2 + 3804C^2 - 4AB + 76AC - 760BC &= -169x, \\ -19A^2 - 1902B^2 - 190580C^2 + 380AB - 3804AC + 38076BC &= 169, \qquad (2.74) \\ A^2 + 190B^2 + 19038C^2 - 38AB + 380AC - 3804BC &= 0. \qquad (2.75) \end{aligned}$$

Analisando módulo 2, as equações (2.74) e (2.75), obtemos A ímpar e A par, o que é uma contradição. Portanto, o sistema não possui solução inteira.

Dessa maneira, os valores possíveis de x, encontrados após a análise de cada caso, são

$$x \in \{-10, -4, 0, 10, 22, 1250, 4980, 5020\},$$

que nos fornecem as seguintes soluções para a equação (2.39): $(\pm 10, \pm 1), (0, \pm 1)$, $(-4, \pm 13), (22, \pm 65), (1250, \pm 31249), (4980, \pm 248501)$ e $(5020, \pm 251501)$.

Usando a transformação linear (2.2), obtemos as seguintes soluções (u, v) para a equação (2.1): $(-10, 0), (-10, -1), (-7, 6), (-7, -7), (-5, 0), (-5, -1), (0, 0), (0, -1)$, $(6, -33)$, $(6, 32)$, $(620, 15624)$, $(620, -15625)$, $(2485, 124250)$, $(2485, -124251)$, $(2505, 125750)$, e $(2505, -125751)$.

Portanto,

$$0,\ 42,\ 1056,\ 244125000,\ 15438186750 \text{ e } 15813188250$$

são os únicos inteiros que podem ser simultaneamente escritos como um produto de dois inteiros consecutivos e como um produto de três termos consecutivos em uma progressão aritmética de razão 5. Isto completa a demonstração do Teorema 2.1.

Referências Bibliográficas

[1] Alaca, S. e Williams, K. S., *Introductory Algebraic Number Theory*, Cambridge University Press, New York, 2004.

[2] Alaca, S. e Williams, K. S., *On Voronoi's Method for Finding an Integral Basis of a Cubic Field*, Util. Math., Vol. 65, pg. 01 - 04, 2004.

[3] Boyd, D. W. e Kisilevsky, H. H. *The Diophantine Equation* $u(u+1)(u+2)(u+3) = v(v+1)(v+2)$, Pacific Journal of Mathematics, Vol. 40, pg. 23 - 32, 1972.

[4] Barrucand, P., Loxton, J. e Williams, H.C., *Some Explicit Upper Bounds on the Class Number and Regulator of a Cubic Field With Negative Discriminant*, Pacific Journal of Mathematics, Vol. 128, pg. 209 - 222, 1987.

[5] Delone, B. N. e Fadeev, D. K. *The Theory of Irrationalities of the Third Degree*, Vol. 10, American Mathematical Society, 1964.

[6] Erdös, P. *Note on Products of Consecutive Integers*, J. London Math. Soc., Vol. 14, 1939.

[7] Herstein, I. N., *Topics in Algebra*, John Wiley & Sons, New York, 2nd edition, New York, 1975.

[8] Hilbert, D., *The Theory of Algebraic Numbers*, Spring-Verlag, New York, 1991.

[9] Keng, H. L., *Introduction to Number Theory*, Spring-Verlag, New York, 1982.

[10] Llorente, P. e Nart, E., *Effective Determination of the Decomposition of the Rational Primes in a Cubic Field*, Proc. Amer. Math Soc., Vol. 87, pg. 579 - 585, 1983.

[11] Louboutin, S., *Calcul du Nombre de Classes des Corps de Nombres*, Pacific Journal of Mathematics, Vol. 171, pg. 455 - 467, 1992.

[12] Louboutin, S., *Class Number Problems for Cubic Number Fields*, Nagoya Math. J., Vol. 138, pg. 199 - 208, 1995.

[13] Louboutin, S., *Class Number and Class Group Problems for Some Non-Normal Totally Real Cubics Number Fields*, Manuscripta Math, Vol. 106, pg. 411 - 427, 2001.

[14] Maple 16. Waterloo Maple Inc. 2012.

[15] Mordell, L. J., *A statement by Fermat*, Proc. London Math. Soc., 1919.

[16] Mordell, L. J., *On the Integer Solution of* $y(y+1) = x(x+1)(x+2)$, Pacific Journal of Mathematics, Vol. 13, pg. 1347 - 1351, 1963.

[17] Neto, A. L., *Funções de uma Variável Complexa*, Associação Instituto Nacional de Matemática Pura e Aplicada, 1996 [Projeto Euclides].

[18] PARI/GP, version 2.5.1, Bourdeaux, 2012, http://pari.math.u-bordeaux.fr/.

[19] Robinson, D. J. S., *A Course in the Theory of Groups*,Spring-Verlag, New York, 1995 [Graduate Texts in Mathematics].

[20] Stewart, I. N. e Tall, D. O., *Algebraic Number Theory*, John Wiley & Sons, New York, 1978 [Chapman and Hall Mathematics Series].