UNIVERSIDADE FEDERAL DE PERNAMBUCO
CCEN-CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

ROBSON CARLOS DA SILVA REIS

CORPOS NÃO-EUCLIDEANOS COM POSTO UM

Recife
2017

Robson Carlos da Silva Reis

CORPOS NÃO-EUCLIDEANOS COM POSTO UM

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestrado em Matemática.

Orientador: Prof. Dr. EDUARDO SHIRLIPPE GOES LEANDRO

Recife

2017

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

R375c Reis, Robson Carlos da Silva
Corpos não-euclideanos com posto um / Robson Carlos da Silva Reis. – 2017.
99 f.

Orientador: Eduardo Shirlippe Goes Leandro.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CCEN, Matemática, Recife, 2017.
Inclui referências.

1. Matemática. 2. Ramificação. I. Leandro, Eduardo Shirlippe Goes (orientador). II. Título.

510 CDD (23. ed.) UFPE- MEI 2017-145

ROBSON CARLOS DA SILVA REIS

CORPOS NÃO-EUCLIDEANOS COM POSTO UM

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovada em: 22/02/2017.

BANCA EXAMINADORA

_____

Profº. Dr. Eduardo Shirlippe Goes Leandro (Orientador)
Universidade Federal de Pernambuco

_____

Profº. Dr. Manoel José Machado Soares Lemos (Examinador Interno)
Universidade Federal de Pernambuco

_____

Profº. Dr. Roberto Callejas Bedregal (Examinador Externo)
Universidade Federal da Paraíba

Dedico ao Criador do Universo Jeová Deus.

Agradecimentos

Primeiramente, gostaria de agradecer a Jeová Deus pela vida, por ter me dado uma mente e energias que me proporcionaram realizar esse trabalho.

À minha família, à minha esposa pela paciência que teve durante todas as horas vagas que passei digitando esse trabalho.

Ao professor Antonio Carlos Rodrigues Monteiro, pela atenção e por todo auxílio técnico que ele forneceu, bem como por me receber em sua casa para trabalharmos na produção dessa dissertação.

Ao professor Eduardo Leandro por ter se empenhado em ministar um curso de Teoria dos Números Algébricos, por aceitar ser meu orientador e por todo auxílio.

Aos meus colegas que também deram atenção ao meu trabalho e me ajudaram com comentários úteis.

(Bíblia Sagrada, Jó 26: 7) *"Ele estende os céus do norte sobre o vazio, Suspende a terra sobre o nada".*

(Bíblia Sagrada, Jó 26: 7)

Resumo

Dizemos que um corpo de números $\mathbb{K}$ é Euclidiano em relação à norma algébrica usual N, se, para quaisquer inteiros algébricos α e β de $\mathbb{K}$, com β não nulo, existe um inteiro algébrico γ em $\mathbb{K}$ tal que $|N(\alpha - \beta\gamma)| < |N(\beta)|$, o "algoritmo de Euclides" de K. Se $\mathbb{K}$ é Euclidiano, então o seu anel de inteiros algébricos, A, é um domínio de ideais principais e, portanto, um domínio de fatoração única, o que é um resultado muito útil na resolução de equações diofantinas. Em 1952, E.S. Barnes e H.P.F. Swinnerton-Dyer mostraram que, no caso em que $\mathbb{K}/\mathbb{Q}$ é uma extensão quadrática, existem, exatamente, vinte e um corpos Euclidianos em relação à norma usual. Para corpos cúbicos e de grau quatro, H. Davenport e, mais tarde, J.W.S. Cassels, mostraram que existe apenas um número finito de corpos Euclidianos, se o grupo das unidades A^* tem posto um. Por exemplo, Cassels mostrou que corpos cúbicos complexos $\mathbb{K}$ não podem ser Euclidianos se $-\Delta_{\mathbb{K}} > 420^2$, com $\Delta_{\mathbb{K}}$ sendo o discriminante de $\mathbb{K}$; há, portanto, apenas um número finito deles. Cioffari usou a cota de Cassels para determinar todos os corpos Euclidianos da forma $\mathbb{Q}(\sqrt[3]{d})$, mostrando que os únicos tais corpos euclidianos são: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{3})$ e $\mathbb{Q}(\sqrt[3]{10})$. Nesta dissertação, apresentamos um estudo detalhado das técnicas que ele usou para obter o resultado.

Palavras-chaves: Ramificação. Unidades. Euclidiano.

Abstract

We say that a number field $\mathbb{K}$ is Euclidean if, for any algebraic integers $\alpha \in \mathbb{K}$ and $\beta \in \mathbb{K}$, with $\beta \neq 0$, there is an algebraic integer $\gamma \in \mathbb{K}$ such that $|N(\alpha - \beta\gamma)| < |N(\beta)|$, the "Euclidean algorithm", where N is the algebraic norm in $\mathbb{K}/\mathbb{Q}$. If $\mathbb{K}$ is Euclidean, then its ring of algebraic integers, A, is a principal ideal domain and, therefore, a unique factorization domain, which is a very useful fact in solving Diophantine equations. In 1952, E.S. Barnes and H.P.F. Swinnerton-Dyer showed that, in the case where $\mathbb{K}/\mathbb{Q}$ is a quadratic extension, there are exactly twenty one Euclidean number fields, with N being the usual norm. For cubic and quartic fields, H. Davenport, and later J.W.S. Cassels, have shown that there is only a finite number of Euclidean number fields, when the rank of the group of units of A is one (that includes cubic fields with two complex embeddings and quartic fields with four complex embeddings). For example, Cassels has shown that a complex cubic number fields $\mathbb{K}$ cannot be Euclidean if $-\Delta_{\mathbb{K}} > 420^2$, with $\Delta_{\mathbb{K}}$ being the discriminant of $\mathbb{K}$, so there is only a finite number of them. Cioffari used Cassels' bound to determine all Euclidean number fields of the form $\mathbb{Q}\left(\sqrt[3]{d}\right)$, the pure cubic fields, showing that the only Euclidean number fields in this case are $\mathbb{Q}\left(\sqrt[3]{2}\right)$, $\mathbb{Q}\left(\sqrt[3]{3}\right)$ and $\mathbb{Q}\left(\sqrt[3]{10}\right)$. We give a detailed account of the techniques they used to get this result.

Key-words: Ramification. Units. Euclidean.

Sumário

1 Um Pouco da História

1.1 Introdução

Desde a época escolar, temos contato com o algoritmo de Euclides, que garante que dados inteiros a e b com $b \neq 0$, então, podemos dividir a por b de forma que a norma(valor absoluto) do resto seja menor que a norma de b. Os inteiros possuem muitas outras propriedades interessantes como: ser domínio de ideais principais o que resulta em ser um domínio de fatoração única. Essas propriedades, na verdade, são apenas consequências de $\mathbb{Z}$ ser Euclidiano. Todo conjunto que possui um algoritmo de divisão é de fatoração única.

No século XIX, Carl F. Gauss considerou outro domínio de integridade que possuía um algoritmo de Euclides, portanto, com um comportamento semelhante dos inteiros: os inteiros de Gauss

$$\mathbb{Z}[i] = \{x \in \mathbb{C} \mid x = a + bi \;\; a,\; b \in \mathbb{Z}\}.$$

Uma norma (N) que torna os inteiros de Gauss Euclidiano é $N(x) = |x|^2$, onde $|\ |$ é o módulo complexo. Outro domínio Euclidiano em relação a mesma norma, relevante na Teoria dos Números, é formado pelos inteiros de Eisenstein :p

$$\mathbb{Z}[\omega] = \{x \in \mathbb{C} \mid x = a + b\omega \;\; a,\; b \in \mathbb{Z} \;\; , \omega = e^{2\pi i/3}\}.$$

Uma extensão finita $\mathbb{K}/\mathbb{Q}$ é dita Euclidiana se o seu anel de inteiros algébricos for Euclidiano. Nessa dissertação, nos concentramos nos corpos Euclidianos em relação à norma algébrica:

$$N(x) = \sigma_1(x)\,\sigma_2(x)\ldots\sigma_m(x),$$

onde $\sigma_1, \sigma_1, \ldots, \sigma_m$ são as imersões de $\mathbb{K}/\mathbb{Q}$ em $\mathbb{C}$. Dessa maneira, $\mathbb{Q}(i)$ e $\mathbb{Q}(\omega)$ são Euclidianos. É natural, então, a seguinte pergunta: Quais são os corpos Euclidianos em relação à norma usual, N? Nessa dissertação sempre estaremos nos referindo à norma algébrica, usual mencionada acima.

Muitas equações diofantinas podem ser resolvidas usando a fatoração única de certos anéis de inteiros algébricos como os inteiros de Gauss e os inteiros de Eisenstein. Por exemplo, podemos mostrar (pela fatoração única em $\mathbb{Z}[i]$) que, se p é primo e congruente a 1 módulo 4, então

$$x^2 + y^2 = p$$

possui solução inteira não trivial. Já da fatoração única em $\mathbb{Z}[\omega]$, obtemos que

$$x^3 + y^3 = z^3$$

não possui solução em com $xyz \neq 0$ em $\mathbb{Z}$.

1.2 O Último Teorema de Fermat e Corpos Euclidianos

O último Teorema de Fermat afirma que se $n > 2$ então

$$x^n + y^n = z^n$$

não possui solução inteira não trivial. Em 1 de março de 1847, o matemático francês Gabriel Lamé anunciou ter resolvido "O último Teorema de Fermat", mas Joseph Liouville percebeu que o argumento assumia que $\mathbb{Z}[\zeta_n]$ possui fatoração única (ζ_n é raiz n-ésima primitiva da unidade).

A partir daí, tanto Cauchy como Lamé passaram alguns poucos meses tentando mostrar a fatoração única em $\mathbb{Z}[\zeta_n]$, mas sem sucesso. Wantzel observou corretamente que para ser de fatoração única é suficiente que seja Euclidiano. Cauchy mostrou que para

$$n \in \{3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15\}$$

$\mathbb{Z}[\zeta_n]$ é Euclidiano, enquanto $\mathbb{Z}[\zeta_{23}]$ não. Hoje sabemos que $\mathbb{Z}[\zeta_n]$ possui fatoração única apenas para um número finito de valores de n. MASLEY; MONTGOMERY, 1976 determinaram todos os $\mathbb{Q}(\zeta_n)$ que são Euclidianos

$$n \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, \ 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}.$$

A fatoração única, tão desejada por Lamé, pode falhar, em alguns anéis de inteiros algébricos, mas ainda podemos resgatar a ideia de fatoração única em ideais, ou seja, cada ideal não nulo do anel de inteiros de um corpo de números se fatora de maneira única como produto de ideais primos (mais, geralmente, esse resultado vale para domínios de Dedekind). Essa fatoração única em ideais é muito útil e será muito utilizada em toda a dissertação. Os resultados dessa seção podem ser conferidos em LENSTRA; POORTEN, 1979

1.3 Corpos Euclidianos Quadráticos

BARNES; SWINNERTON-DYER, 1952 mostraram que, no caso em que $\mathbb{K}/\mathbb{Q}$ é uma extensão quadrática, existem, exatamente, 21 corpos Euclidianos. Cada extensão quadrática de $\mathbb{Q}$ é da forma $\mathbb{K} = \mathbb{Q}\left(\sqrt{d}\right)$ com d inteiro livre quadrados. Os valores de d para os quais $\mathbb{K}$ é Euclidiano são exatamente:

$$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

O grupo das unidades do anel de inteiros de um corpo de números possui uma estrutura muito especial (RIBENBOIM, 2001 páginas 196, 197): é isormofo a

$$G \times \mathbb{Z}^{r+s-1}$$

onde r e s são respectivamente, os números de imersões reais e de imersões complexas não-conjugadas de $\mathbb{K}$ em $\mathbb{C}$ e G é o subgrupo finito das raízes da unidade contidas em $\mathbb{K}$. Dizemos que o posto de $\mathbb{K}$ é

$$r + s - 1.$$

Se $d > 0$ é livre de quadrados, então $\mathbb{Q}\left(\sqrt{d}\right)$ possui posto 1, pois $r = 2,\ s = 0$ e, neste caso, existe apenas um número finito de tais corpos que são Euclidianos.

1.4 Grupo de Classes

Temos a propriedade de fatoração única de ideais em ideais primos em domínios de Dedekind. Além disso, podemos definir ideais fracionários. Um ideal fracionário de um domínio de integridade R com corpo de frações K é um R-submódulo de K tal que existe $r \in R, r \neq 0$, com rI contido em R. Em particular, os ideais de R também são ideais fracionários. Domínios de Dedekind possuem propriedades muito interessantes: em geral, um domínio de fatoração única R não é um domínio de ideais principais, mas, se um domínio de Dedekind for de fatoração única, então é domínio de ideais principais. Nem sempre um domínio de Dedekind é de fatoração única, mas podemos usar os ideais fracionários para desenvolver uma medida do quanto um domínio de Dedekind se afasta de ser de fatoração única. O conjunto dos ideais fracionários de um domínio Dedekind formam um grupo G multiplicativo abeliano e os ideais fracionários principais P formam um subgrupo e, assim, definimos

$$C_K = G/P,$$

o grupo de classes de K. O grupo de classes é finito e denotamos por h_K a sua cardinalidade. Chamamos h_K de número de classes de K, o que torna C_K interessante é que R é de fatoração única se, e somente se,

$$|h_K| = 1\ .$$

Portanto, se

$$|h_K| > 1\ ,$$

então R não será Euclidiano. Esses resultados sobre o grupo de classes desempenham um papel fundamental nessa dissertação.

Os resultados sobre o grupo de classes podem ser conferidos em RIBENBOIM, 2001 seção 8.2.

1.5 Corpos Euclidianos Cúbicos Com Posto Um

DAVENPORT, 1950 e mais tarde CASSELS, 1952 mostraram que existe apenas um número finito de corpos cúbicos complexos Euclidianos. Cassels mostrou que corpos

cúbicos complexos não podem ser euclianos se $-\Delta_{\mathbb{K}} > 420^2$, com $\Delta_{\mathbb{K}}$ sendo o discriminante de $\mathbb{K}$. Há, portanto, um número finito deles (para cada grau, n, existe apenas um número finito de corpos com um dado discriminante).

Vamos estudar nesta dissertação como CIOFFARI, 1979 usou a cota de Cassels para determinar todos os corpos Euclidianos da forma $\mathbb{Q}\left(\sqrt[3]{d}\right)$, mostrando que os únicos tais corpos Euclidianos são:

$$\mathbb{Q}\left(\sqrt[3]{2}\right), \quad \mathbb{Q}\left(\sqrt[3]{3}\right) \quad e \quad \mathbb{Q}\left(\sqrt[3]{10}\right).$$

Os corpos dessa forma possuem uma imersão real e duas complexas, portanto o posto é 1, quase todos eles não são Euclidianos.

1.6 Unidades Excepcionais

A maioria das técnicas usadas para tratar o problema de corpos Euclidianos aponta para as unidades. LENSTRA, 1976 desenvolveu um método que garante que um corpo é Euclidiano a partir do tamanho de sequências excepcionais de unidades. Dizemos que uma unidade u é uma unidade excepcional, se $1-u$ também for unidade e uma sequência excepcional é uma sequência de unidades excepcionais cuja diferença de dois elementos da sequência também é unidade.

O que destaca esse método é que ele fornece exemplos de corpos Euclidianos com grau grande. LENSTRA, 1976 conseguiu exibir vinte exemplos de grau oito. O corpo

$$\mathbb{Q}\left(\zeta^{13} + \zeta^{-13}\right)$$

é de grau seis, é totalmente real, Euclidiano e tem posto cinco.

O corpo $\mathbb{Q}(\alpha)$, onde α é raiz do polinômio

$$1 - 3x^2 + 5x^4 + x^5 - 3x^6 - x^7 + x^8$$

é Euclidiano de grau oito com exatamente quatro pares de imersões complexas conjugadas, portanto, de posto três. Estes dois exemplos são característicos do método das unidades excepcionais de Lenstra.

1.7 Corpos Euclidianos Quárticos

Nessa dissertação, iremos estudar uma família de corpos quárticos com posto 1, os corpos da forma:

$$\mathbb{Q}\left(\sqrt[4]{-sr^2}\right)$$

com r, s inteiros positivos coprimos e livres de quadrados. Estes corpos têm posto um, pois admitem dois pares de imersões complexas conjugadas. LAKEIN, 1972 provou que

$\mathbb{Q}\left(\sqrt[4]{-3}\right)$ é Euclidiano e CIOFFARI, 1979 mostrou que $\mathbb{Q}\left(\sqrt[4]{-2}\right)$, $\mathbb{Q}\left(\sqrt[4]{-7}\right)$ também são Euclidianos. Além disso, CIOFFARI, 1979 mostrou que para diversos valores de d, $\mathbb{Q}\left(\sqrt[4]{-d}\right)$ não é Euclidiano. Na verdade, CIOFFARI, 1979 quase determinou todos os corpos Euclidianos da forma acima, só faltou $\mathbb{Q}\left(\sqrt[4]{-12}\right)$.

Agora vejamos outra família de corpos quárticos, os corpos da forma:

$$\mathbb{Q}\left(\sqrt{-m}, \sqrt{n}\right)$$

com m inteiro não negativo e n inteiro, também possuem posto um, pois admitem dois pares de imersões conjugadas. LEMMERMEYER, 2011 determinou todos os corpos dessa forma que são Euclidianos:

$$\mathbb{Q}\left(\sqrt{-1}, \sqrt{2}\right), \quad \mathbb{Q}\left(\sqrt{-1}, \sqrt{3}\right), \quad \mathbb{Q}\left(\sqrt{-1}, \sqrt{5}\right), \quad \mathbb{Q}\left(\sqrt{-1}, \sqrt{7}\right),$$
$$\mathbb{Q}\left(\sqrt{-2}, \sqrt{-3}\right), \quad \mathbb{Q}\left(\sqrt{-2}, \sqrt{5}\right), \quad \mathbb{Q}\left(\sqrt{-3}, \sqrt{2}\right), \quad \mathbb{Q}\left(\sqrt{-3}, \sqrt{5}\right),$$
$$\mathbb{Q}\left(\sqrt{-3}, \sqrt{-7}\right), \quad \mathbb{Q}\left(\sqrt{-3}, \sqrt{-11}\right), \quad \mathbb{Q}\left(\sqrt{-3}, \sqrt{17}\right), \quad \mathbb{Q}\left(\sqrt{-3}, \sqrt{-19}\right)$$
$$\mathbb{Q}\left(\sqrt{-7}, \sqrt{5}\right).$$

1.8 Corpos Euclidianos de Grau Grande

LENSTRA, 1975 deu um exemplo de corpo Euclidiano bem especial, $\mathbb{Q}(\zeta_{11})$, corpo ciclotômico de grau 10 e posto do grupo das unidades 5.

O método das unidades excepcionais de Lenstra foi explorado por vários pesquisadores e isso resultou na descoberta de muitos exemplos com grau maior que 8. Por exemplo, LEUTBECHER; MARTINET, 1982 encontraram dois exemplos de corpos Euclidianos com grau 10:

$\mathbb{Q}(\alpha)$ com α raiz de

$$p(x) = 1 + 2x + 3x^2 - 4x^3 - 7x^4 + x^5 + 7x^6 + 2x^7 - 4x^8 - x^9 + x^{10}$$

e $\mathbb{Q}(\beta)$ com β raiz de

$$g(x) = 1 + 2x - 2x^2 - 5x^3 + x^4 + 6x^5 + 4x^6 - 4x^7 - 4x^8 + x^9 + x^{10}.$$

MCKENZIE, 1988 mostrou na sua tese que $\mathbb{Q}(\zeta_{13})$ é Euclidiano. Assim, temos um exemplo de grau 12. HOURIET, 2007 encontrou mais um exemplo de corpo Euclidiano com grau 12 e posto 6.

Uma conjectura de H. W. Lenstra, ainda sem muita evidência em seu favor, afirma que, se o posto do grupo das unidades do corpo é pelo menos três (talvez mesmo para pelo menos dois) então quase todos os corpos de um grau fixado são Euclidianos com respeito à norma algébrica, e, assim, têm grupo de classes de ordem um.

2 Base Inteira e Fatoração de Ideais

Neste capítulo, determinamos a base inteira do corpo cúbico puro geral e seu discriminante e, em seguida, tecemos alguns comentários sobre a fatoração em ideais primos de ideais gerados por primos inteiros. Embora os resultados provados neste capítulo sejam fundamentais no que segue, os métodos usados nas demostrações são básicos em Teoria Algébrica dos Números.

2.1 Base Inteira e Discriminante

Sejam $x_1, \ldots, x_n$ em um corpo de números $\mathbb{K}$ de grau n e $\sigma_1, \sigma_2, ..., \sigma_n$ as imersões de $\mathbb{K}$ em $\mathbb{C}$, definimos

$$\Delta(x_1, \ldots, x_n) = det(\sigma_i(x_j))^2,$$

o discriminate da n-upla $(x_1, \ldots, x_n)$ em $\mathbb{K}$.

Vejamos os resultados que serão fundamentais nesta seção:

Proposição 2.1.1. *Seja $y = (y_1, \ldots, y_n)$ e $x = (x_1, \ldots, x_n)$ e C uma matriz tal que $y = Cx$, todos com coordenadas em um corpo de números $\mathbb{K}$, então*

$$\Delta(y_1, \ldots, y_n) = (det\ C)^2 \Delta(x_1, \ldots, x_n).$$

Demonstração. Veja RIBENBOIM, 2001 páginas $20 - 21$. □

A próxima proposição desempenha um papel crucial nos resultados dessa seção, iremos demonstrá-la, mas precisaremos de um resultado elementar sobre módulos.

Teorema 2.1.1. *Seja R um domínio de ideais principais e M um R-módulo livre de posto n. Se M' é um submódulo de M, então*

1. *M' é um submódulo livre de posto $q \leq n$*
2. *Existe uma base $\{\epsilon_1, \ldots, \epsilon_n\}$ de M e elementos $a_1, \ldots, a_q$ de R tais que*

$$a_1 \mid a_2 \mid \cdots \mid a_q$$

de maneira que

$$\{a_1\epsilon_1, \ldots, a_q\epsilon_q\}$$

é base do R-módulo livre M'.

Demonstração. Veja ENDLER, 1986 páginas $48 - 50$. □

Proposição 2.1.2. *Seja G um grupo abeliano livre de posto n com geradores $\{g_1, \ldots, g_n\}$ e H um subgrupo também livre de posto n com geradores $\{h_1, \ldots, h_n\}$. Se C é a matriz tal que*

$$(h_1, \ldots, h_n) = C\,(g_1, \ldots, g_n)\,,$$

então

$$|det\, C| = [G : H]\,.$$

Demonstração. Inicialmente, note que um grupo abeliano livre é um $\mathbb{Z}-$módulo livre. Assim, pelo Teorema 2.1.1, temos que G e H possuem bases especiais, $\{g_1^{'}, \ldots, g_n^{'}\}$, $\{h_1^{'}, \ldots, h_n^{'}\}$, respectivamente, tais que

$$h_i^{'} = a_i g_i^{'}\,, \quad a_i \in \mathbb{Z}.$$

Assim, C é uma matriz diagonal com $c_{ii} = a_i$, portanto $det\ C = a_1 \ldots a_n$.

Agora, iremos mostrar que $[G : H] = a_1 \ldots a_n$. Faremos isso via homomorfismo de módulos. Temos que

$$G = \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_n\ ;$$

$$H = \mathbb{Z}a_1 g_1 \oplus \cdots \oplus \mathbb{Z}a_n g_n.$$

Considerando o homomorfismo de módulos

$$\varphi\colon \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_n \to \frac{\mathbb{Z}g_1}{\mathbb{Z}a_1 g_1} \times \cdots \times \frac{\mathbb{Z}g_1}{\mathbb{Z}a_1 g_n}$$

$$x_1 g_1 + \cdots + g_n x_n \longmapsto (x_1 g_1 + \mathbb{Z}a_1 g_1, \ldots, x_n g_n + \mathbb{Z}a_n g_n).$$

Temos que onúcleo desse homomorfismo é

$$\mathbb{Z}a_1 g_1 \oplus \cdots \oplus \mathbb{Z}a_n g_n = H.$$

Portanto, pelo Teorema do Núcleo e da Imagem para módulos (veja ASH, 2000 seção 4.2)

$$G/H = \frac{\mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_n}{\mathbb{Z}a_1 g_1 \oplus \cdots \oplus \mathbb{Z}a_n g_n} \cong \frac{\mathbb{Z}g_1}{\mathbb{Z}a_1 g_1} \times \cdots \times \frac{\mathbb{Z}g_1}{\mathbb{Z}a_1 g_n}.$$

Mostraremos que

$$\frac{\mathbb{Z}g_i}{\mathbb{Z}a_i g_i} \cong \mathbb{Z}_{a_i}$$

que mostra que G/H possui exatamente $a_1 \ldots a_n$ elementos.
Mas

$$\sigma\colon \mathbb{Z}g_i \to \mathbb{Z}_{a_i}$$

$$x_i g_i \longmapsto x_i \overline{1}$$

é homorfismo com núcleo $\mathbb{Z}a_i g_i$. Para concluir o resultado, basta notar que se

$$(h_1, \ldots, h_n) = C_H(h_1^{'}, \ldots, h_n^{'}),$$

então $det(C_H) = \pm 1$. Analogamente,

$$(g_1, \ldots, g_n) = C_G(g_1^{'}, \ldots, g_n^{'}),$$

então $det(C_G) = \pm 1$. □

Proposição 2.1.3. *Seja $f(x) = irr(\alpha, \mathbb{Q})$ o polinômio mínimo de α em $\mathbb{Q}[x]$, então*

$$\Delta\left(1, \ldots, \alpha^{n-1}\right) = (-1)^{\binom{n}{2}} N\left(f^{'}(\alpha)\right).$$

Demonstração. Veja ASH, 2003 página 10 seção 2.3.6. □

Definição 2.1.1. *Dizemos que um inteiro algébrico α é de Eisenstein para um primo inteiro p, se $irr(\alpha, \mathbb{Q})$ é de Eisenstein em p.*

Lema 2.1.1. *Sejam α um inteiro algébrico, $\mathbb{K} = \mathbb{Q}(\alpha)$ e $B_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathbb{K}$. Se α for de Eisenstein em p, então*

$$p \nmid [B_{\mathbb{K}} : \mathbb{Z}[\alpha]].$$

Demonstração. Suponha que α seja de Eisenstein em p com $irr(\alpha, \mathbb{Q})$

$$b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n.$$

Temos que p divide cada b_i. Daí,

$$p \mid \alpha^n = -b_0 - b_1\alpha - \cdots - b_{n-1}\alpha^{n-1}.$$

Agora suponha, por absurdo, que

$$p \mid [B_{\mathbb{K}} : \mathbb{Z}[\alpha]].$$

Então, pelo Teorema de Cauchy, $\frac{B_{\mathbb{K}}}{\mathbb{Z}[\alpha]}$ possui um subgrupo H de ordem p. Logo, existe $\gamma \in B_{\mathbb{K}}$, tal que

$$\gamma \notin \mathbb{Z}[\alpha],\ p\gamma \in \mathbb{Z}[\alpha].$$

Assim, podemos escrever γ como

$$\gamma = \frac{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}}{p} + \beta,$$

com $\beta \in \mathbb{Z}[\alpha]$, $\quad 0 < a_i \leqslant p-1$ para $\quad 0 \leqslant i \leqslant n-1$.

Suponha que exista j com

$$p \nmid a_j,\ \ p \mid a_i\ \ (0 \leqslant i < j).$$

Como p divide α^n e

$$\gamma\alpha^{n-1-j} = \frac{a_j\alpha^{n-1}}{p} + \frac{a_{j+1}\alpha^n + \cdots + a_{n-1}\alpha^{2n-2-j}}{p} + \beta\alpha^{n-1-j}.$$

Concluimos que

$$\frac{a_j\alpha^{n-1}}{p},$$

é um inteiro algébrico e assim possui norma inteira.

Daí, como

$$N\left(\frac{a_j\alpha^{n-1}}{p}\right) = \frac{a_j^n N\left(\alpha\right)^{n-1}}{p^n}$$

e $p^2 \nmid N\left(\alpha\right)$, pois α é de Eisenstein em p. Temos que $p \mid a_j$, uma contradição. Portanto,

$$p \nmid \left[B_{\mathbb{K}} : \mathbb{Z}\left[\alpha\right]\right].$$

□

Lema 2.1.2. *Se* $ab^2 \not\equiv \pm 1 \ (mod\ 9) \Rightarrow ba^2 \not\equiv \pm 1 \ (mod\ 9)$.

Demonstração. De fato, se

$$ab^2 \equiv \pm 1 (\text{mod } 9) \Rightarrow 1 \equiv \left(ab^2\right)^2 \equiv b^3\left(ba^2\right) \ (\text{mod } 9),$$

mas os únicos cubos módulo 9 são ± 1 e 0. □

Teorema 2.1.2. *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt[3]{d})$, $d \in \mathbb{Z}$ *livre de cubos* $(d = ab^2)$ *com* a, b *livres de quadrados,* $d \not\equiv \pm 1 \ (mod\ 9)$. *Se* $\alpha = \sqrt[3]{d}$, *então*

$$\mathcal{A} = \{1, \alpha, \frac{\alpha^2}{b}\}$$

é base inteira e

$$\Delta_{\mathbb{K}} = -27a^2b^2$$

$$\left[B_{\mathbb{K}} : \mathbb{Z}\left[\alpha\right]\right] = b.$$

Demonstração. Pela Proposição 2.2.3,

$$\Delta\left(1, \alpha, \alpha^2\right) = (-1)\, N(3\alpha^2) = -27\left(ab^2\right)^2.$$

Por outro lado, escrevendo $\{1,\ \alpha,\ \alpha^2\}$, em termos de uma base inteira de $[B_{\mathbb{K}} : \mathbb{Z}]$, pelas Proposições 2.1.1 e 2.1.2, obtemos

$$\Delta\left(1, \alpha, \alpha^2\right) = \left[B_{\mathbb{K}} : \mathbb{Z}\left[\alpha\right]\right]^2 \Delta_{\mathbb{K}}.$$

Assim,

$$-27\left(ab^2\right)^2 = \left[B_{\mathbb{K}} : \mathbb{Z}\left[\alpha\right]\right]^2 \Delta_{\mathbb{K}}.$$

Além disso,

$$irr\left(\alpha, \mathbb{Q}\right) = x^3 - ab^2,$$

portanto, α é de Eisenstein em p para qualquer primo p que divida a. Então, se p divide a, pelo Lema 2.2.1

$$p \nmid \left[B_{\mathbb{K}} : \mathbb{Z}\left[\alpha\right]\right].$$

Portanto,

$$a^2 \mid \Delta_{\mathbb{K}}.$$

Mas,

$$\mathbb{Q}\left(\sqrt[3]{ab^2}\right) = \mathbb{Q}\left(\sqrt[3]{ba^2}\right).$$

Analogamente, obtemos que

$$b^2 \mid \Delta_{\mathbb{K}}.$$

Daí,

$$a^2b^2 \mid \Delta_{\mathbb{K}}.$$

Vamos mostrar que

$$3 \nmid \left[B_{\mathbb{K}} : \mathbb{Z}\left[\alpha\right]\right].$$

Assim,

$$27a^2b^2 \mid \Delta_{\mathbb{K}}.$$

Podemos supor que $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$, com $9 \nmid d$, pois podemos trocar o gerador $\sqrt[3]{ab^2}$ por $\sqrt[3]{ba^2}$. Temos que $irr\left(\sqrt[3]{d} - d, \mathbb{Q}\right)$ é

$$\left(x + d\right)^3 - d = x^3 + 3dx^2 + 3d^2x + \left(d^3 - d\right),$$

que é de Eisenstein em 3, pois

$$9 \nmid \left(d^3 - d\right) = \left(d - 1\right) d \left(d + 1\right),$$

o produto de três números consecutivos, exatamente um deles é divisível por 3.
Se

$$3 \mid d \pm 1, \quad 9 \text{ não divide } d^3 - d, \text{ pois } 9 \nmid d \pm 1.$$

Caso contrário, se

$$3 \mid d, \quad 9 \text{ não divide } d^3 - d, \text{ pois } 9 \nmid d.$$

Temos,

$$\mathbb{Q}\left(\alpha - d\right) = \mathbb{Q}\left(\alpha\right), \qquad \mathbb{Z}[\alpha - d] = \mathbb{Z}[\alpha].$$

Daí, pelo Lema 2.1.1

$$3 \nmid \left[B_{\mathbb{Q}(\alpha - d)} : \mathbb{Z}\left[\alpha - d\right]\right] = \left[B_{\mathbb{K}} : \mathbb{Z}\left[\alpha\right]\right].$$

Portanto,

$$27a^2b^2 \mid \Delta_{\mathbb{K}}.$$

Também concluímos que

$$[B_{\mathbb{K}} : \mathbb{Z}[\alpha]] \mid b.$$

Nesse momento, a Proposição 2.1.2 é fundamental. Temos que

$$[B_{\mathbb{K}} : \mathbb{Z}[\alpha]] = \left[B_{\mathbb{K}} : \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\frac{\alpha^2}{b}\right]\left[\mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\frac{\alpha^2}{b} : \mathbb{Z}[\alpha]\right].$$

$$1 = 1 + 0\alpha + 0\frac{\alpha^2}{b};$$

$$\alpha = 01 + 1\alpha + 0\frac{\alpha^2}{b};$$

$$\alpha^2 = 01 + 0\alpha + b\frac{\alpha^2}{b};$$

$$\begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{bmatrix} \begin{bmatrix} 1 \\ \alpha \\ \frac{\alpha^2}{b} \end{bmatrix}$$

.

Por isso, pela Proposição 2.1.2

$$\left[\mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\frac{\alpha^2}{b} : \mathbb{Z}[\alpha]\right] = det\left|\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{bmatrix}\right| = b.$$

Assim, temos

$$\left[B_{\mathbb{K}} : \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\frac{\alpha^2}{b}\right] = 1.$$

Daí,

$$B_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\frac{\alpha^2}{b}$$

que também resulta em

$$[B_{\mathbb{K}} : \mathbb{Z}[\alpha]] = b.$$

Disso, também obtemos o discriminante

$$\Delta_{\mathbb{K}} = -27a^2b^2,$$

pois

$$-27a^2b^4 = [B_{\mathbb{K}} : \mathbb{Z}[\alpha]]^2\Delta_{\mathbb{K}}.$$

□

Teorema 2.1.3. *Seja* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$, $d \in \mathbb{Z}$ *livre de cubos* $d = ab^2$ *com* a, b *livre de quadrados,* $d \equiv \pm 1 \ (mod\ 9)$. *Sejam* $\alpha = \sqrt[3]{d}$, $\beta = \frac{\alpha^2}{b}$ *e* $\gamma = \frac{1 \pm \alpha + \alpha^2}{3}$, *então*

$$\mathcal{B} = \{\alpha, \beta, \gamma\}$$

é base inteira e

$$\Delta_{\mathbb{K}} = -3a^2b^2$$

$$[B_{\mathbb{K}} : \mathbb{Z}[\alpha]] = 3b.$$

Demonstração. Já vimos que α e β são inteiros algébricos, agora vamos mostrar que γ também é. De fato,

$$(3\gamma - 1)^3 = [\alpha(\pm 1 + \alpha)]^3$$

$$27\gamma^3 - 27\gamma^2 + 9\gamma - 1 = \alpha^3[(\pm 1)^3 + \alpha^3 \pm 3\alpha(\pm + \alpha)]$$

$$= d[\pm 1 + d \pm 3(3\gamma - 1)].$$

Assim, obtemos que $irr(\gamma, \mathbb{Q})$ é

$$x^3 - x^2 + x[\frac{9(1 \mp d)}{27}] - \frac{1 + d(\mp 2 + d)}{27} = 0$$

$$x^3 - x^2 + x[\frac{(1 \mp d)}{3}] - \frac{(d \mp 1)^2}{27} = 0.$$

Ou seja, se $d \equiv 1 \pmod 9$, então $irr(\gamma, \mathbb{Q})$ é

$$x^3 - x^2 + x[\frac{(1 - d)}{3}] - \frac{(d - 1)^2}{27} = 0,$$

que possui coeficientes inteiros, pois 9 divide $(1 - d)$. Se $d \equiv -1 \pmod 9$, então $irr(\gamma, \mathbb{Q})$ é

$$x^3 - x^2 + x[\frac{(1 + d)}{3}] - \frac{(d + 1)^2}{27} = 0,$$

que também possui coeficientes inteiros, pois 9 divide $(1 + d)$.

Agora, mostraremos que α, β, γ é base inteira. Temos que $G_1 = B_{\mathbb{K}}$, $G = \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma$ bem como $\mathbb{Z}[\alpha]$ são grupos abelianos (com a operação soma). É suficiente mostrarmos que

$$[G_1 : G] = 1.$$

Vimos, no caso anterior, que

$$-27\left(ab^2\right)^2 = \Delta\left(1, \alpha, \alpha^2\right) = [B_{\mathbb{K}} : \mathbb{Z}[\alpha]]^2 \Delta_{\mathbb{K}};$$

$$a^2b^2 \mid \Delta_{\mathbb{K}}.$$

Então

$$[B_{\mathbb{K}} : \mathbb{Z}[\alpha]]^2 \mid 9b^2.$$

O que nos dá

$$[B_{\mathbb{K}} : \mathbb{Z}[\alpha]] \mid 3b.$$

$$\begin{array}{c} B_{\mathbb{K}} \\ | \\ 1 \\ | \\ \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma \\ | \\ 3b \\ | \\ \mathbb{Z}[\alpha] \end{array}$$

Vamos mostrar que

$$[\mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma : \mathbb{Z}[\alpha]] = 3b$$

e pela multiplicidade do índice

$$[B_{\mathbb{K}} : \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma] = 1.$$

$$1 = c_0\alpha + c_1\frac{\alpha^2}{b} + c_2\frac{1 \pm \alpha + \alpha^2}{3}$$

Como $1, \alpha, \alpha^2$ é base de $\mathbb{K}$ sobre $\mathbb{Q}$. Temos que $c_2 = 3$. O coeficiente de α é $c_0 = \mp 1$. O coeficiente de α^2 é

$$\frac{c_1}{b} + 1 = 0 \quad \text{, o que nos dá} \quad c_1 = -b.$$

Assim,

$$1 = \mp 1\alpha - b\beta + 3\gamma;$$

$$\alpha = 1\alpha + 0\beta + 0\gamma;$$

$$\beta = 0\alpha + b\beta + 0\gamma.$$

$$\begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \end{bmatrix} = \begin{bmatrix} \mp 1 & -b & 3 \\ 1 & 0 & 0 \\ 0 & b & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$$

Portanto, pela Proposição 2.1.2

$$[\mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma : \mathbb{Z}[\alpha]] = |\det \begin{bmatrix} \mp 1 & -b & 3 \\ 1 & 0 & 0 \\ 0 & b & 0 \end{bmatrix}| = 3b.$$

Assim,

$$B_{\mathbb{K}} = \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma,$$

pois

$$[B_{\mathbb{K}} : \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma] = 1.$$

Concluímos também que

$$[B_{\mathbb{K}} : \mathbb{Z}[\alpha]] = 3b.$$

O que nos dá

$$\Delta_{\mathbb{K}} = -3a^2b^2,$$

pois

$$-27a^2b^4 = [B_{\mathbb{K}} : \mathbb{Z}[\alpha]]^2 \Delta_{\mathbb{K}}.$$

□

Teorema 2.1.4. *Seja* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$, $d \in \mathbb{Z}$ *livre de cubos* $d = ab^2$ *com* a *e* b *livres de quadrados,* $d \equiv \pm 1 \ (mod\ 9)$. *Seja* $\alpha = \sqrt[3]{d}$, *então*

$$A = \{1, \alpha, \frac{1 \pm \alpha \pm \frac{\alpha^2}{b}}{3}\}$$

é base inteira e

$$\Delta_{\mathbb{K}} = -3a^2b^2;$$

$$[B_{\mathbb{K}} : \mathbb{Z}\,[\alpha]] = 3b.$$

Demonstração. Vamos usar a base inteira que encontramos no Teorema anterior (2.1.3)

$$\{\alpha, \beta, \gamma\}.$$

Mostraremos que o índice

$$m = [\mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma : \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\frac{1 \pm \alpha \pm \frac{\alpha^2}{b}}{3}] = 1.$$

Isso garante que A seja base inteira. Já temos as coordenadas de 1 e de α na base A. Vejamos agora as coordenadas de $\frac{1 \pm \alpha \pm \frac{\alpha^2}{b}}{3}$. Sabemos que $1, \alpha, \alpha^2$ é base de $\mathbb{K}$ sobre $\mathbb{Q}$. Por isso, se

$$\frac{1 \pm \alpha \pm \frac{\alpha^2}{b}}{3} = c_0\alpha + c_1\beta + c_2\gamma$$

O coeficiente do 1

$$\frac{c_2}{3} = \frac{1}{3}, \qquad c_2 = 1;$$

O coeficiente de α é

$$c_0 \pm \frac{c_2}{3} = c_0 \pm \frac{1}{3} = \pm\frac{1}{3}, \qquad c_0 = 0;$$

O coeficiente de α^2

$$\frac{c_1}{b} + \frac{c_2}{3} = \pm\frac{1}{3b}, \qquad c_1 = \frac{\pm 1 - b}{3};$$

$$\begin{bmatrix} 1 \\ \alpha \\ \frac{1\pm\alpha\pm\frac{\alpha^2}{b}}{3} \end{bmatrix} = \begin{bmatrix} \mp 1 & -b & 3 \\ -1 & 0 & 0 \\ 0 & \frac{\pm 1-b}{3} & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$$

.

Assim, temos que o índice m pela Proposição 2.1.2 vale

$$|\det \begin{bmatrix} \mp 1 & -b & 3 \\ -1 & 0 & 0 \\ 0 & \frac{\pm 1-b}{3} & 1 \end{bmatrix}| = 1.$$

□

2.2 Fatorando o Ideal Gerado por Primo Inteiro

A demonstração de que certos corpos não são Euclidianos depende da fatoração em $B_{\mathbb{K}}$ (anel de inteiros de $\mathbb{K}$) de ideais principais de $B_{\mathbb{K}}$ gerados por primos inteiros. Trataremos da fatoração destes ideais nesta seção.

Nesta seção, para um inteiro algébrico $\alpha \in \mathbb{K}$, denotaremos por $g(x) = irr(\alpha, \mathbb{Q})$, o polinômio mínimo de α em $\mathbb{Q}[x]$ e por $\overline{g(x)}$ a redução de $g(x)$ módulo um primo inteiro p. Seja

$\overline{g(x)} = \prod \overline{g_i(x)}$ a fatoração de $g(x)$ em irredutíveis mônicos de $\mathbb{Z}_p[x]$.

Os teoremas que temos para fatorar $pB_{\mathbb{K}}$ são os seguintes:

Teorema 2.2.1. *Sejam $\mathbb{K} = \mathbb{Q}(\alpha)$ um corpo de números e p um primo inteiro. Se $B_{\mathbb{K}} = \mathbb{Z}[\alpha]$, então*

$$pB_{\mathbb{K}} = \prod \left(p, \overline{g_i(\alpha)}\right).$$

Demonstração. Veja RIBENBOIM, 2001 páginas $196 - 197$. □

Teorema 2.2.2 (Dedekind)**.** *Sejam $\mathbb{K} = \mathbb{Q}(\alpha)$ um corpo de números e p um primo inteiro que não divide $[B_{\mathbb{K}} : \mathbb{Z}[\alpha]]$. Então*

$$pB_{\mathbb{K}} = \prod \left(p, \overline{g_i(\alpha)}\right).$$

Demonstração. Veja MARCUS, 1977 Teorema 27, página 79.

□

Corolário 2.2.1. *Se* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$*, com* d *um inteiro livre de cubos,* $d = ab^2$*, e* p *um primo que divide* d*, então*

$$pB_{\mathbb{K}} = \mathfrak{P}^3 \quad (\mathfrak{P} \textit{ ideal primo}).$$

Demonstração. Podemos supor que p^2 não divide ab^2. Se $ab^2 = ps$, então p e s são coprimos. Temos que

$$(\sqrt[3]{ab^2}B_{\mathbb{K}})^3 = (pB_{\mathbb{K}})(sB_{\mathbb{K}})$$

Assim, como $pB_{\mathbb{K}}$ e $sB_{\mathbb{K}}$ são coprimos (se algum ideal primo dividisse ambos, conteria $p,\ s$), então $pB_{\mathbb{K}}$ é um cubo, pela fatoração única em ideais primos. □

Se p não divide $d = ab^2$ e $p \neq 3$, então p não divide $[B_{\mathbb{K}} : \mathbb{Z}[\sqrt[3]{d}]]$. De fato, pelos Teoremas 2.1.2 e 2.1.3

$$[B_{\mathbb{K}} : \mathbb{Z}[\sqrt[3]{d}]] = b, \quad \text{se} \quad \not\equiv \pm 1 \pmod 9;$$

$$[B_{\mathbb{K}} : \mathbb{Z}[\sqrt[3]{d}]] = 3b, \quad \text{se} \quad \equiv \pm 1 \pmod 9.$$

Lema 2.2.1. *Sejam* p *e* q *primos tais que* $p \not\equiv 1$ *(mod* q*). Então*

$$\varphi \colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*$$

$$x \longmapsto x^q$$

é uma bijeção de grupos multiplicativos.

Demonstração. Dado x em $\mathbb{Z}_p^*$, temos que

$$x^{p-1} = 1.$$

Se x está no núcleo de φ, então $x^q = 1$, por isso a ordem de x divide

$$mdc(p-1, q) = 1.$$

Daí, $x^1 = x = 1$. Assim, o núcleo de φ é trivial e temos uma bijeção. □

Corolário 2.2.2. *Se* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$ *e* p *não divide* d*,* $p \equiv 2$ *(mod* 3*), então*

$$pB_{\mathbb{K}} = \mathfrak{P}_1\mathfrak{P}_2 \quad (\textit{fatoração em primos}).$$

Demonstração. Desde que $p \not\equiv 1 \pmod 3$, então, pelo Lema 2.2.1, existe um único $b \in \mathbb{Z}_p^*$ tal que

$$\bar{d} = b^3.$$

Assim, podemos fatorar o polinômio $x^3 - d$ em $\mathbb{Z}_p^*$. De fato,

$$\overline{g\,(x)} = x^3 - b^3 = (x-b)\left(x^2 + bx + b^2\right) \quad \text{(fatoração em irredutíveis)},$$

pois x^2+bx+b^2 irredutível, já que b é a única raiz de $g\,(x)$ em $\mathbb{Z}_p$ e $g(x)$ não possui raízes múltiplas, pois

$$\overline{g}'(x) = 3x^2, \quad \overline{g}(x) \quad \text{são coprimos.}$$

Portanto,

$$pB_{\mathbb{K}} = \left(p, \sqrt[3]{d} - b\right)\left(p, \sqrt[3]{d}^2 + \sqrt[3]{d}b + b^2\right) = \mathfrak{P}_1\mathfrak{P}_2.$$

Pelo Teorema 6. □

Corolário 2.2.3. *Se* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$*,* p *não divide* d *e* $p \equiv 1\ (mod\ 3)$*, então*

$$pB_{\mathbb{K}} = \mathfrak{P} \quad \textit{se } d \textit{ não for cubo em } \mathbb{Z}_p^*;$$

$$pB_{\mathbb{K}} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3 \quad \textit{se } d \textit{ for cubo em } \mathbb{Z}_p^*.$$

Demonstração. Como $\mathbb{Z}_p^*$ é cíclico, então

$$\mathbb{Z}_p^* = \langle h \rangle, \quad \text{para algum} \quad h \in \mathbb{Z}_p^*.$$

Por isso, a ordem de h é $p-1$, pois h é um gerador de $\mathbb{Z}_p^*$. Assim, dado $x \in \mathbb{Z}_p^*$, temos que

$$x^3 = \left(h^u\right)^3 = 1 \Longleftrightarrow (p-1) \mid 3u.$$

Há, portanto, exatamente, três possibilidades para u

$$\frac{p-1}{3}; \frac{2\,(p-1)}{3} \quad \text{e} \quad (p-1).$$

Portanto, $x^3 = \bar{d}$ não possui solução em $\mathbb{Z}_p$ ou possui três soluções distintas, ou seja, há duas possibilidades para fatoração de $x^3 = \bar{d}$, ou ele se fatora como produto de três fatores lineares distintos ou é irredutível, portanto

$$pB_{\mathbb{K}} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3 \ \text{ fatoração em primos distintos,}$$

se d for um cubo módulo p. Caso contrário,

$$pB_{\mathbb{K}} = \mathfrak{P} \ \text{ é um ideal primo,}$$

se d não for um cubo módulo p. □

Por fim, vejamos a fatoração do ideal gerado por 3.

Proposição 2.2.1. *Suponha que* 3 *não divide* $d = ab^2$*. Se* $ab \not\equiv \pm 1\ (mod\ 9)$

$$3B_{\mathbb{K}} = \mathfrak{P}^3.$$

Caso contrário,

$$3B_{\mathbb{K}} = \mathfrak{P}_1^2\mathfrak{P}_2.$$

Demonstração. Se 3 não divide $d = ab^2$ e $d \not\equiv \pm 1 \pmod 9$, então 3 não divide $[B_{\mathbb{K}} : \mathbb{Z}[\alpha]] = b$, assim, pelo Teorema 2.2.2, podemos usar a fatoração do polinômio mínimo de α em $\mathbb{Z}_3$

$$irr(\alpha, \mathbb{Q}) = x^3 - d = (x - m)^3,$$

pois todos os elementos de $\mathbb{Z}_3$ são cubos. Por isso,

$$3B_{\mathbb{K}} = \mathfrak{P}^3.$$

Para o caso $d \equiv \pm 1 \pmod 9$, veja COHEN, 1993 página 344.

□

3 A Cota de Cassels

Cassels mostrou que existe apenas um número finito de corpos cúbicos com grupo das unidades de posto um. Neste capítulo, iremos dar uma visão mais efetiva deste resultado, exibiremos explicitamente um conjunto finito que contém todos os corpos cúbicos puros Euclidianos. Conceitos de Teoria dos Números Algébricos como: ramificação de primos, unidades, bases inteiras, normas, discriminantes, fatoração de ideais, grupo de classes são ferramentas indespensáveis.

3.1 Definição e Equivalência

Definição 3.1.1. *Dizemos que um corpo de números* $\mathbb{K}$ *é Euclidiano, se, para quaisquer inteiros algébricos* α *e* β *de* $\mathbb{K}$*, com* β *não nulo, existe um inteiro algébrico* γ *em* $\mathbb{K}$ *tal que*

$$|N(\alpha - \beta\gamma)| < |N(\beta)|,$$

com N *sendo a norma algébrica de* $\mathbb{K}$*.*

Para um corpo de números $\mathbb{K}$, denotaremos por $B_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathbb{K}$.

Para cada α em $\mathbb{K}$ seja

$$M(\mathbb{K}, \alpha) = min\{|N(\alpha - \gamma)| : \gamma \in B_{\mathbb{K}}\}.$$

O Mínimo Euclidiano de $\mathbb{K}$ é

$$M(\mathbb{K}) = max\{M(\mathbb{K}, \alpha) : \alpha \in \mathbb{K}\}.$$

Proposição 3.1.1. $\mathbb{K}$ *é Euclidiano se, e somente se, para cada* x *em* $\mathbb{K}$ *existe* α *em* $B_{\mathbb{K}}$ *tal que*

$$|N(x - \alpha)| < 1.$$

Demonstração. De fato, $\mathbb{K}$ é o corpo de frações de $B_{\mathbb{K}}$. Assim, se $x \in \mathbb{K}$, então

$$x = \frac{\alpha}{\beta} \text{ com } \alpha,\ \beta \in B_{\mathbb{K}}.$$

Agora suponha que $\mathbb{K}$ é Euclidiano. Assim, existem $q,\ r$ em $B_{\mathbb{K}}$ tais que

$$\alpha = q\beta + r \qquad |N(\beta)| > |N(r)|.$$

De forma que

$$\frac{\alpha}{\beta} - q = \frac{r}{\beta}.$$

Tomando normas, obtemos

$$\left|N\left(\frac{\alpha}{\beta} - q\right)\right| = \left|N\left(\frac{r}{\beta}\right)\right| = \frac{|N(r)|}{|N(\beta)|} < 1.$$

Portanto, para qualquer x em $\mathbb{K}$, temos

$$M(\mathbb{K}, x) < 1.$$

Vejamos a recíproca. Sejam α, β inteiros algébricos de $\mathbb{K}$, com $\beta \neq 0$. Então, tomando $x = \frac{\alpha}{\beta}$, existe $\gamma \in B_{\mathbb{K}}$ tal que

$$|N(x - \gamma)| < 1.$$

O que garante

$$|N(\alpha - \beta\gamma)| < |N(\beta)|.$$

Assim, $\mathbb{K}$ é Euclidiano. □

Essa equivalência é a base do algoritmo que Ciofari usa para verificar que um corpo é Euclidiano.

Se $M(\mathbb{K}) < 1$, então $\mathbb{K}$ é Euclidiano. Por isso muitos trabalhos foram públicados a respeito do mínimo Euclidiano, $M(\mathbb{K})$. Veja por exemplo, CAVALLAR; LEMMERMEYER, 2012

3.2 Ramificação Total e Unidades Fundamentais

Nesta seção apresentaremos alguns resultados que apontam uma forte relação entre ramificação e não ser Euclidiano. Vejamos antes alguns resultados clássicos que serão necessários. Inicialmente, vamos caracterizar o grupo $\mathbb{E}$ das unidades de $B_{\mathbb{K}}$.

Teorema 3.2.1. *(Dirichlet) Seja* $\mathbb{K}$ *um corpo de números de grau* n*. Se* $\mathbb{K}$ *possui* r *imersões reais e* $2s$ *imersões complexas conjugadas, então*

$$\mathbb{E} \cong \mathbb{Z}^{r+s-1} \times G,$$

onde G *é um grupo finito, consistindo das raízes da unidade em* $\mathbb{K}$*.*

Demonstração. Veja RIBENBOIM, 2001 páginas 196 e 197.

□

Esse teorema é muito útil, pois mostra a existência de uma base para $\mathbb{E}$.

Corolário 3.2.1. *Existem $r+s-1$ unidades $u_1, u_2 \ldots, u_{r+s-1}$ tais que qualquer unidade u se escreve de maneira única como*

$$u = \zeta u_1^{e_1} \ldots u_{r+s-1}^{e_{r+s-1}}, \quad \text{onde } \zeta \text{ é uma raiz da unidade em } \mathbb{K}.$$

Definição 3.2.1. *Chamamos os geradores, de ordem infinita, u_i, de unidades fundamentais.*

Teorema 3.2.2. *(Dedekind) Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos de números. Os ideais primos de $B_{\mathbb{K}}$ que se ramificam em $B_{\mathbb{L}}$ são exatamente os que dividem o discriminante de $\mathbb{L}/\mathbb{K}$, denotado por $\Delta(\mathbb{L}/\mathbb{K})$, ou simplemente $\Delta_{\mathbb{L}}$ quando $\mathbb{K} = \mathbb{Q}$.*

Demonstração. Veja RIBENBOIM, 2001 páginas 238,239. □

Corolário 3.2.2. *Se $\mathbb{K} = \mathbb{Q}(\sqrt[n]{m})$ com m e n inteiros $(n > 0)$ e m livre de n-ésimas potências. Se p não divide n nem m, então p não se ramifica.*

Demonstração. Pela Proposição 2.13 ,

$$|\Delta\left(1, \sqrt[n]{m}, \ldots \sqrt[n]{m}^{n-1}\right)| = |N\left(n\sqrt[n]{m}^{n-1}\right)| = n^n m^{n-1}.$$

Pelas Proposições 2.1.1 e 2.1.3, $\Delta(\mathbb{K}/\mathbb{Q})$ divide $n^n m^{n-1}$. Portanto, o resultado segui do Teorema 3.2.2. □

O Teorema que segui mostra o quanto o grupo das unidades e a ramifição total de primos, estão relacionados com a propriedade de ser Euclidiano.

Teorema 3.2.3. *Seja $\mathbb{K}$ um corpo de números de grau primo q, com l unidades fundamentais. Suponha que existam pelo menos $l+2$ primos distintos que se ramificam totalmente em $B_{\mathbb{K}}$, então $\mathbb{K}$ não é Euclidiano.*

Demonstração. Sejam $\{\epsilon_1, \ldots, \epsilon_l\}$ as unidades fundamentais e $\{p_1, \ldots, p_{l+2}\}$ os $l+2$ primos que se ramificam totalmente em $\mathbb{K}$. Então

$$p_i B_{\mathbb{K}} = \mathfrak{P}_i^q \quad \text{(fatoração em primos)}.$$

Se q se ramifica totalmente, então façamos $p_1 = q$. Suponha que $h_{\mathbb{K}} = 1$, então

$$\mathfrak{P}_i = b_i B_{\mathbb{K}}.$$

Portanto, b_i^q e p_i são associados em $B_{\mathbb{K}}$, por isso, pelo Corolário 3.2.1

$$b_i^q \zeta \epsilon_1^{t_{i1}} \ldots \epsilon_l^{t_{il}} = p_i.$$

Com ζ raiz primitiva da unidade, mas como $\mathbb{K} \subset \mathbb{R}$, então $\zeta = \pm 1$. Se $\zeta = -1$, como $(-1)^q = 1$ (q é primo), podemos substituir b_i, por $-b_i$. Assim,

$$b_i^q \epsilon_1^{t_{i1}} \dots \epsilon_l^{t_{il}} = p_i.$$

Vamos mostrar que podemos encontrar $x_1, \dots, x_{l+1}$ de maneira que

$$\left(b_1^{qx_1} \epsilon_1^{x_1 t_{11}} \dots \epsilon_l^{x_1 t_{1l}}\right) \dots \left(b_{l+1}^{qx_{l+1}} \epsilon_1^{x_{l+1} t_{(l+1)1}} \dots \epsilon_l^{x_{l+1} t_{(l+1)l}}\right) = p_1^{x_1} \dots p_{l+1}^{x_{l+1}},$$

seja uma q-ésima potência em $B_{\mathbb{K}}$. O expoente de ϵ_i é

$$t_{1i}x_1 + \dots + t_{(l+1)i}x_{l+1}.$$

Se consideramos

$$t_{1i}x_1 + \dots + t_{(l+1)i}x_{l+1} = 0 \ \text{ em } \ \mathbb{Z}_q,$$

para $i = 1, \dots, l$. Obtemos um sistema linear homogêneo com l equações e $l+1$ incógnitas, logo, possui solução não trivial em $\mathbb{Z}_q$ e, dessa maneira, existe y em $B_{\mathbb{K}}$ tal que

$$y^q = p_1^{x_1} \dots p_{l+1}^{x_{l+1}}.$$

Dessa maneira,

$$y = \sqrt[q]{p_1^{x_1} \dots p_{l+1}^{x_{l+1}}} \in B_{\mathbb{K}}.$$

Como $(x_1, \dots, x_{l+1}) \neq (0, \dots, 0)$ em $\mathbb{Z}_q$, para pelo menos um x_i, temos que q não divide x_i e portanto, $y \notin Q$. Por isso,

$$\mathbb{K} = \mathbb{Q}\left(\sqrt[q]{p_1^{x_1} \dots p_{l+1}^{x_{l+1}}}\right).$$

Mas, pelo Corolário 3.2.2, p_{l+2} não se ramifica, pois não divide $qp_1^{x_1} \dots p_{l+1}^{x_{l+1}}$, temos um absurdo. □

O Teorema anterior nos possibilita limitar e muito os corpos Euclidianos que satisfazem a condição de Cassels.

Teorema 3.2.4 (Cassels, Davenport)**.** *Seja* $\mathbb{K}$ *é um corpo cúbico complexo. Se*

$$|\Delta_{\mathbb{K}}| > 176400,$$

então $\mathbb{K}$ *não é Euclidiano.*

Demonstração. Veja CASSELS, 1952. □

CIOFFARI, 1979 é fundamentado no Teorema 3.24. Cassels limitou a um número finito de corpos e Cioffari explicitou-os. A maioria dos artigos sobre corpos Euclidianos trata de casos particulares, de exemplos. Veremos uma versão do Teorema de Cassels para corpos quárticos complexos. Porém, em geral, ainda não temos um resultado dessa magnitude.

Vamos agora mostrar como o Teorema 3.2.3 nos ajuda a encontrar os corpos Euclidianos que satisfazem a cota de Cassels.

Corolário 3.2.3. *Se* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$ *é um corpo cúbico puro Euclidiano, então*

$$d \in \{2,\ 3,\ 5,\ 47,\ 11,\ 13, 23,\ 29,\ 31,\ 41,\ 43,\ 47,\ 59,\ 61,\ 67,\ 79,\ 6,\ 15,$$

$$21,\ 33,\ 39,\ 51,\ 69,\ 12,\ 45,\ 63,\ 99,\ 117,\ 153,\ 207,\ 19,\ 37,\ 73,\ 109,\ 127,\ 163,$$

$$181,\ 199,\ 17,\ 53,\ 71,\ 89,\ 107,\ 179,\ 197,\ 233,\ 10,\ 26,\ 46,\ 62,\ 82,\ 118,\ 134, 206,$$

$$226,\ 35,\ 55,\ 145,\ 215,\ 235,\ 91,\ 161,\ 217,\ 143,\ 28,\ 44,\ 116,\ 172,\ 188,\ 244,\ 316,$$

$$372,\ 388,\ 404,\ 325,\ 575,\ 775,\ 1025,\ 539,\ 1421\}.$$

Demonstração. Suponha que $\mathbb{K}$ seja Euclidiano. Como vimos no capítulo 2, o discriminante de $\mathbb{Q}\left(\sqrt[3]{d}\right)$ depende do resíduo de d módulo 9. Por isso, como a cota de Casssels está em termos do discriminante, iremos analisar cada caso separadamente.

Caso 1: $d \not\equiv \pm 1\ (mod\ 9)$

Nesse caso, temos que 3 se ramifica totalmente em $\mathbb{K}$. Além disso, os primos que dividem o discriminante também se ramificam totalmente. Mas o posto do grupo das unidades de $\mathbb{K}$ é $1 + 1 - 1 = 1$, então o grupo das unidades é gerado por apenas uma unidade fundamental. Dessa maneira, pelo Teorema 3.2.3, d possui no máximo um divisor, um divisor primo diferente 3. Vamos analisar todas as fatorações possíveis de d.

CASO A1: d primo.

Temos que

$$|\Delta_{\mathbb{K}}| = 27d^2 < 176400.$$

Portanto,

$$d < \frac{\sqrt{\frac{176400}{3}}}{3} < 81.$$

Logo,

$$d \in \{2,\ 3,\ 5,\ 47,\ 11,\ 13, 23,\ 29,\ 31,\ 41,\ 43,\ 47,\ 59,\ 61,\ 67,\ 79\}.$$

CASO B1: d é produto de dois primos distintos, $d = p_1p_2 \quad$ com $\quad p_1 < p_2$.

Temos que

$$|\Delta_{\mathbb{K}}| = 27p_1^2p_2^2 < 176400,$$

$$p_1p_2 < \frac{\sqrt{\frac{176400}{3}}}{3} < 81.$$

Se d, possui dois divisores primos, então um deles é o 3, $d = 3p_2$ com

$$d \in \{6,\ 15,\ 21,\ 33,\ 39,\ 51,\ 69\}.$$

CASO C1: $d = 9p_2, \qquad p_2 \quad$ primo.
Analisando o discriminante

$$3p_2 < \frac{\sqrt{\frac{176400}{3}}}{3} < 81.$$

Então,

$$d \in \{12,\ 45,\ 63,\ 99,\ 117,\ 153,\ 207\}.$$

CASO 2: $d \equiv \pm 1\ (mod\ 9)$

Nesse caso, se 3 não divide d, então d pode ter no máximo dois divisores primos distintos primos distintos de 3.

CASO A2: $d = p$ primo

O limite do Cassels é 176400. Assim,

$$|\Delta_{\mathbb{K}}| = 3p^2 < 176400.$$

Portanto,

$$p < \sqrt{\frac{176400}{3}} < 243.$$

Logo, como $p \equiv \pm 1\ (mod\ 9)$

$$p \in \{19,\ 37,\ 73,\ 109,\ 127,\ 163,\ 181,\ 199,\ 17,\ 53,\ 71,\ 89,\ 107,\ 179,\ 197,\ 233\}.$$

CASO B2: d é o produto de dois primos $p_1,\ p_2 \quad$ com $\quad p_1 < p_2$

Temos então

$$|\Delta_{\mathbb{K}}| = 3p_1^2p_2^2 < 176400.$$

Portanto,

$$p_1p_2 < \sqrt{\frac{176400}{3}} < 243.$$

CASO $p_1 = 2$:

Se

$$2p_2 < 243, \quad 2p_2 \equiv \pm 1\ (mod\ 9).$$

Então

$$p_2 < 122 \quad p_2 \equiv \pm 5 \ (mod\ 9).$$

Portanto,

$$p_2 \in \{5,\ 13,\ 23,\ 31,\ 41,\ 59,\ 67,\ 103,\ 113\},$$

$$d \in \{10,\ 26,\ 46,\ 62,\ 82,\ 118,\ 134,\ 206,\ 226\}.$$

CASO $p_1 = 5$:

Se $p_1 = 5$, então

$$p_2 < 243/5 < 49 \quad p_2 \equiv \pm\ 2(mod\ 9),$$

$$p_2 \in \{7,\ 11,\ 29,\ 43,\ 47\},$$

$$d \in \{35,\ 55,\ 145,\ 215,\ 235\}.$$

CASO $p_1 = 7$:

Se $p_1 = 7$, então

$$p_2 < 243/7 < 35 \quad p_2 \equiv \pm\ 5(mod\ 9),$$

$$p_2 \in \{13,\ 23,\ 31\}$$

Portanto,

$$d \in \{91,\ 161,\ 217\}.$$

CASO $p_1 = 11$:

Se $p_1 = 11$, então

$$p_2 < 243/11 < 23 \quad p_2 \equiv \pm\ 5(mod\ 9).$$

Logo $p_2 \in \{13\}$ e $d \in \{143\}$.

CASO $p_1 = 13$:

Não podemos ter $p_1 = 13$. Se $p_1 > 13$, então $p_1 < 17$ e $p_1 p_2 < 17^2 = 289 > 243$. Assim , listamos todos os valores possiveis de $p_1,\ p_2$.

Finalmente, vamos analisar

CASO $d = p_1^2 p_2$ com $p_1 < p_2$:

Novamente,analisando o discriminante e a cota de Cassels, obtemos

$$|d_{\mathbb{K}}| = 3p_1^2 p_2^2 < 176400.$$

Portanto,

$$p_1 p_2 < \sqrt{\frac{176400}{3}} < 243$$

$p_1 = 2$

$$p_2 < 243/2 < 122 \quad p_2 \equiv \pm\, 2 (mod\ 9).$$
$$p_2 \in \{7,\ 11,\ 29,\ 43,\ 47,\ 61,\ 79,\ 83,\ 97,\ 101\},$$
$$d \in \{28,\ 44,\ 116,\ 172,\ 188,\ 244,\ 316,\ 372,\ 388,\ 404\}.$$

$p_1 = 5$

$$p_2 < 243/5 < 49 \quad p_2 \equiv \pm\, 5 (mod\ 9).$$
$$p_2 \in \{13,\ 23,\ 31,\ 41\},$$
$$d \in \{325,\ 575,\ 775,\ 1025\}.$$

$p_1 = 7$

$$p_2 < 243/7 < 35 \quad p_2 \equiv \pm\, 2 (mod\ 9).$$
$$p_2 \in \{11,\ 29\},$$
$$d \in \{539,\ 1421\}.$$

$p_1 = 11$

$$p_2 < 243/11 < 23 \quad p_2 \equiv \pm\, 2 (mod\ 9).$$

p_1 não pode ser 11.

$p_1 = 13$

$$p_2 < 243/11 < 18 \quad p_2 \equiv \pm\, 5 (mod\ 9).$$

p_1 não pode ser 13

Isso encerra nossa lista, pois não podemos ter $p_1 > 13$. □

A partir de agora, os corpos cúbicos puros que podem ser Euclidianos pertencem a um conjunto finito, explícito. Nos próximos capítulos, mostraremos os métodos que Cioffari desenvolveu para descartar a possibilidade de certos corpos cúbicos puros serem Euclidianos.

4 O Corpo de Hilbert e Corpos não Euclidianos

Corpos Euclidianos possuem número de classes 1, logo, se o número de classes não é 1, então o corpo não é Euclidiano. Geralmente, não é fácil determinar o número de classes diretamente, mas enunciaremos um resultado surpreendente (o Teorema de Existência do Corpo de Hilbert, parte da Teoria de Corpos de Classes) que substitui o grupo de classes por um grupo de Galois de uma extensão finita de Galois.

4.1 Definição, Exemplos e Propriedades

Dado um corpo de números $\mathbb{K}$, denotamos por $\mathbb{H}_{\mathbb{K}}$ o Corpo de Hilbert de $\mathbb{K}$, $h_{\mathbb{K}}$ o número de classes e $Cl(\mathbb{K})$ o grupo de Galois de de $\mathbb{H}_{\mathbb{K}}/\mathbb{K}$.

Teorema 4.1.1 (Corpo de Hilbert)**.** *Seja $\mathbb{K}$ um corpo de números. Existe uma única extensão $\mathbb{H}_{\mathbb{K}}/\mathbb{K}$ finita, abeliana, não ramificada que é maximal e é tal que*

$$Gal(\mathbb{H}_{\mathbb{K}}/\mathbb{K}) \simeq Cl(\mathbb{K}).$$

Demonstração. Veja NEUKIRCH, 1999 páginas 399 e 400. □

No Teorema acima "não ramificada", possui dois significados:

1. os ideais primos de $\mathbb{K}$ não se ramificam em $\mathbb{H}_{\mathbb{K}}$;
2. se σ é uma imersão de $\mathbb{K}$ em $\mathbb{C}$ com $\sigma(\mathbb{K}) \subset \mathbb{R}$ e se σ' é uma imersão de $\mathbb{H}_{\mathbb{K}}$ que estende σ, então
$$\sigma'(\mathbb{K}) \subset \mathbb{R}.$$

Antes de usarmos o Corpo de Hilbert, vejamos alguns exemplos:

Exemplo 4.1.1. *Seja $\mathbb{K} = \mathbb{Q}\left(\sqrt{-1}\right)$, então*

$$\mathbb{H}_{\mathbb{K}} = \mathbb{K}.$$

Demonstração. O anel de inteiros de $\mathbb{K}$ é $\mathbb{Z}[i]$, os inteiros de Gauss, que são um domínio Euclidiano, portanto,

$$1 = h_{\mathbb{K}} = [\mathbb{H}_{\mathbb{K}} : \mathbb{K}]$$

ou seja,

$$\mathbb{H}_{\mathbb{K}} = \mathbb{K}.$$

□

Para o próximo exemplo, precisaremos de alguns resultados.

Definição 4.1.1. *O ideal diferente de uma extensão finita de corpos de números* $\mathbb{E}/\mathbb{F}$*, denotado por* $d\left(B_{\mathbb{E}}/B_{\mathbb{F}}\right)$ *ou* $d\left(\mathbb{E}/\mathbb{F}\right)$ *é o inverso do ideal fracionário*

$$I_{\mathbb{E}/\mathbb{F}} = \{x \in \mathbb{E} \mid T_{\mathbb{E}/\mathbb{F}}(xy) \in B_{\mathbb{F}},\ \forall\ y \in B_{\mathbb{E}}\}.$$

Teorema 4.1.2. *Sejam* $\mathbb{K}_1$ *e* $\mathbb{K}_2$ *extensões finitas de um corpo de número* $\mathbb{K}$*, então*

$$d\left(\mathbb{K}_1/\mathbb{K}\right) \subset d\left(\mathbb{K}_1\mathbb{K}_2/\mathbb{K}_2\right).$$

Demonstração. Veja RIBENBOIM, 2001 página 253. □

Podemos obter o discriminante do corpo a partir do diferente.

Proposição 4.1.1. *Se* $\mathbb{K} = \mathbb{Q}$ *e* $\mathbb{L}$ *é um corpo de números, então*

$$N\left(d\left(\mathbb{L}/\mathbb{K}\right)\right) = |\Delta_{\mathbb{L}}|.$$

Além disso, se J *é um ideal de* $B_{\mathbb{L}}$*, então*

$$N(J) \in J.$$

Demonstração. Veja RIBENBOIM, 2001 , página 247 e ASH, 2003 seção 4.29 □

Teorema 4.1.3. *Seja* $\mathbb{L}/\mathbb{K}$ *uma extensão finita de corpos de números. Dado um ideal primo,* Q *de* $B_{\mathbb{L}}$*, então,* Q *se ramifica, se e somente se,* Q *divide* $d\left(B_{\mathbb{L}}/B_{\mathbb{K}}\right)$*.*

Demonstração. Daremos a demonstração nesse capítulo. □

No Teorema acima. Se $Q \cap B_{\mathbb{K}} = \mathfrak{P}$. Dizer que Q se ramifica significa que $\mathfrak{P}B_{\mathbb{L}} \subset Q^2$.

Exemplo 4.1.2. *Se* $\mathbb{K} = \mathbb{Q}\left(\sqrt{-5}\right)$*, então*

$$\mathbb{L} = \mathbb{Q}\left(\sqrt{-5}, \sqrt{-1}\right)$$

é o corpo de Hilbert de $\mathbb{K}$*.*

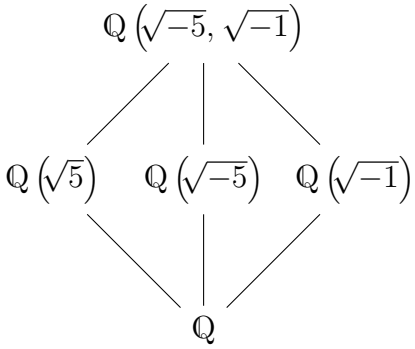
Demonstração. Temos que $h_{\mathbb{K}} = 2$. Assim,

$$[\mathbb{H}_{\mathbb{K}} : \mathbb{K}] = 2.$$

Vamos mostrar que $\mathbb{L}/\mathbb{K}$ é não ramificada e como

$$[\mathbb{L} : \mathbb{K}] = 2,$$

concluímos o resultado. $\mathbb{K}$ não possui imersões reais, assim precisamos verificar apenas que nenhum primo de $B_{\mathbb{K}}$ se ramifica.



Sejam $\mathbb{M} = \mathbb{Q}\left(\sqrt{5}\right)$ e $\mathbb{F} = \mathbb{Q}\left(\sqrt{-1}\right)$. Pela Proposição 4.1.1

$$4 = |\Delta_{\mathbb{F}}| = N\left(d\left(B_{\mathbb{F}}/B_{\mathbb{Q}}\right)\right).$$

Por outro lado, pelo Teorema 4.1.2 e Proposição 4.1.1,

$$N\left(d\left(B_{\mathbb{F}}/B_{\mathbb{Q}}\right) \subset d\left(B_{\mathbb{F}}/B_{\mathbb{Q}}\right) \subset d\left(B_{\mathbb{L}}/B_{\mathbb{K}}\right).\right.$$

Daí,

$$4 \in d\left(B_{\mathbb{L}}/B_{\mathbb{K}}\right).$$

Analogamente,

$$5 = \Delta_{\mathbb{M}} = N\left(d\left(B_{\mathbb{M}}/B_{\mathbb{Q}}\right)\right),$$

$$5 \in d\left(B_{\mathbb{L}}/B_{\mathbb{K}}\right).$$

Portanto,

$$1 \in d\left(B_{\mathbb{L}}/B_{\mathbb{K}}\right) = B_{\mathbb{L}}.$$

Portanto, $\mathbb{L}/\mathbb{K}$ é não ramificada, pelo Teorema 4.1.3. □

Não usaremos diretamente o Teorema do Corpo de Hilbert, mas um Corolário. Vamos precisar de uma proposição:

Proposição 4.1.2. *Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ corpos de números que contêm o corpo de números $\mathbb{K}$. Sejam $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$ e $\mathfrak{P}$ um ideal primo de $B_{\mathbb{K}}$, então, $\mathfrak{P}$ não se ramifica em $\mathbb{L}/\mathbb{K}$ se e somente se $\mathfrak{P}$ não se ramifica em $\mathbb{K}_1/\mathbb{K}$ e em $\mathbb{K}_2/\mathbb{K}$.*

Demonstração. Veja RIBENBOIM, 2001 , página 253. □

Corolário 4.1.1. *Seja $\mathbb{K}$ um corpo de números e $\mathbb{L}/\mathbb{K}$ extensão de Galois finita não ramificada(no sentido dos ideais primos e das imersões reais), então*

$$\mathbb{L} \subset \mathbb{H}_{\mathbb{K}}.$$

Demonstração. Temos que $\mathbb{L}\mathbb{H}_{\mathbb{K}}/\mathbb{K}$ é de Galois, pois a composição de extensões de Galois é de Galois e também é não ramificada, pois a composição de extensões não ramificada (no sentido dos primos finitos) é não ramificada, pela Proposição 4.1.2. É fácil ver que a composição de extensões não ramificadas (no sentido dos primos infinitos, das imersões) também é não ramificada. Como $\mathbb{H}_{\mathbb{K}}$ é maximal, temos

$$\mathbb{L}\mathbb{H}_{\mathbb{K}} = \mathbb{H}_{\mathbb{K}}.$$

Portanto,

$$\mathbb{L} \subset \mathbb{H}_{\mathbb{K}}.$$

□

O Teorema abaixo nos dá um critério muito simples de verificar a propriedade Euclidiana, pois envolve basicamente congruencia módulo 3.

Teorema 4.1.4. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt[q]{r})$ com q um primo ímpar e r livre de q-ésimas potências. Se r for divísivel por um primo, p, congruente a 1 mod q, então*

$$q \mid h_{\mathbb{K}}.$$

Demonstração. Sejam ζ_n uma n-ésima raiz primitiva da unidade, $\mathbb{L} \subset \mathbb{Q}(\zeta_p)$ com $[\mathbb{L} : \mathbb{Q}] = q$. Tal $\mathbb{L}$ existe, pois

$$G = Gal\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right),$$

é cíclico de ordem $p-1$, que é divisível por q. Portanto, G possui um único subgrupo G_q de ordem $\frac{p-1}{q}$. Assim, pela Teoria de Galois $\mathbb{L}$ é o corpo fixado por G_q.

Vamos mostrar que $\mathbb{K}\mathbb{L}/\mathbb{K}$ é de Galois de grau q, não ramificada, logo pelo Corolário 4.1.1

$$\mathbb{K}\mathbb{L} \subset \mathbb{H}_{\mathbb{K}}.$$

$$\begin{array}{c} \mathbb{H}_{\mathbb{K}} \\ | \\ | \\ \mathbb{K}\mathbb{L} \\ | \\ q \\ | \\ \mathbb{K} \end{array}$$

$$\#Cl\left(\mathbb{K}\right) = [\mathbb{H}_{\mathbb{K}}/\mathbb{K}] = [\mathbb{H}_{\mathbb{K}}/\mathbb{K}\mathbb{L}][\mathbb{K}\mathbb{L}/\mathbb{K}],$$

mas, como $[\mathbb{K}\mathbb{L}/\mathbb{K}] = q$, temos que

$$q \mid \#Cl\,(\mathbb{K})\,.$$

□

Esse Teorema é muito prático, pois é muito fácil verificar as suas hipóteses, no caso particular de corpos cúbicos complexo puros, $\mathbb{Q}(\sqrt[3]{d})$, basta verificar se d possui algum divisor primo congruente a 1 módulo 3. Usando esse Teorema, podemos descartar muitos dos corpos alistados no capítulo 3, reduzimos nossa lista a 42 corpos. São os corpos determinados por

$$d \in \{2,\ 3,\ 5,\ 11,\ 23,\ 29,\ 41,\ 47,\ 59,\ 17,\ 53,\ 71,\ 89,\ 107,\ 179,\ 197,\ 233,\ 6,$$

$$15,\ 33,\ 51,\ 69,\ 10,\ 46,\ 82,\ 118,\ 226,\ 55,\ 145,\ 235,\ 44,\ 116,\ 188,\ 332,\ 404,$$

$$575,\ 1025,\ 12,\ 45,\ 99,\ 153,\ 207\}.$$

Além disso, podemos retirar da nossa lista, os corpos determinados por

$$d \in \{11,\ 47,\ 89,\ 233,\ 15,\ 51,\ 118,\ 235,\ 1025,\ 153,\ 207\},$$

pois possuem número de classes $h_{\mathbb{K}} > 1$. De fato, a tabela abaixo, nos fornece o número de classes, $h_{\mathbb{K}}$, de cada um deles:

d	$h_{\mathbb{K}}$	d	$h_{\mathbb{K}}$	d	$h_{\mathbb{K}}$
11	2	89	2	233	4
15	2	118	2	235	7
47	2	153	9	1025	10
51	3	207	8		

Nessa dissertação não iremos nos delongar no cálculo do números de classes. Usamos o sofware SAGE para determiná-los.

Assim, podemos limitar nossa buscar aos trinta e um corpos determinados por

$$d \in \{2,\ 3,\ 5,\ 6,\ 10,\ 12,\ 17,\ 23,\ 29,\ 33,\ 41,\ 44,\ 45,\ 46,\ 53,\ 55,\ 59,\ 69$$

$$71,\ 82,\ 99,\ 107,\ 116,\ 145,\ 179,\ 188,\ 197,\ 226,\ 332,\ 404,\ 575\}.$$

Usando o SAGE, verificamos que $h_{\mathbb{K}} = 1$ para todos os 31 corpos listados acima.

No próximo capítulo, exibiremos outros métodos que também descartam a possibilidade de ser Euclidiano. No restante desse capítulo, iremos nos concentrar em mostrar que $\mathbb{K}\mathbb{L}/\mathbb{K}$ é não ramificada, no sentido do Corpo de Hilbert.

4.2 KL/K é não Ramificada nos Primos Finitos

Nesta seção, além dos resultados listados no início do capítulo precisaremos do Lema de Abhyankar e de outras propriedades básicas do ideal diferente, bem como das do discriminante.

O ideal diferente é multiplicativo:

Proposição 4.2.1. *Sejam* $\mathbb{K},\ \mathbb{L}, \mathbb{M}$ *corpos de números, tais que* $\mathbb{K} \subset\ \mathbb{L} \subset \mathbb{M}$*, então*

$$d(\mathbb{M}/\mathbb{K}) = d(\mathbb{M}/\mathbb{L})\, d(\mathbb{L}/\mathbb{K})\, B_{\mathbb{M}}.$$

Demonstração. Veja RIBENBOIM, 2001 , página 244, M. □

O discriminante do p-ésimo corpo cilotômico, p primo, se expressa de maneira bem simples em termos de p:

Proposição 4.2.2. *Seja* $\mathbb{K} = \mathbb{Q}(\zeta_p)$*, com p primo, então*

$$\Delta_{\mathbb{K}} = (-1)^{(p-1)/2} p^{p-2}.$$

Demonstração. Veja RIBENBOIM, 2001 , página 118, R. □

Vejamos a transitividade do discriminante

Proposição 4.2.3. *Sejam* $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ *extensões de corpos de números.*

$$\Delta(\mathbb{M}/\mathbb{K}) = \Delta(\mathbb{L}/\mathbb{K})^{[\mathbb{M}:\mathbb{L}]}\, N_{\mathbb{L}/\mathbb{K}}(\Delta(\mathbb{M}/\mathbb{L})).$$

Demonstração. Veja RIBENBOIM, 2001 , página 249,Q. □

Proposição 4.2.4. *Sejam* $\mathbb{L}/\mathbb{K}$ *uma extensão de Galois de corpos de números de grau n, P um primo de* $B_{\mathbb{K}}$*. Se*

$$PB_{\mathbb{K}} = Q_1^{e_1} \dots Q_g^{e_g}; \qquad f_i = [B_{\mathbb{L}}/Q_i : B_{\mathbb{K}}/P],$$

então

$$e = e_1 = \dots e_g; \qquad f = f_1 = \dots f_g; \qquad efg = n.$$

Demonstração. Veja RIBENBOIM, 2001 , página 192, F e página 193, G. □

Teorema 4.2.1 (Lema de Abhyankar)**.** *Sejam* $\mathbb{K}$*,* $\mathbb{F}$*,* $\mathbb{L}$ *corpos de números com* $\mathbb{K}$ *e* $\mathbb{L}$ *extensões disjuntas cíclicas de* $\mathbb{F}$ *de grau q, primo. Se P é um ideal primo de* $B_{\mathbb{F}}$ *acima de p primo,* $(p \in \mathbb{Z})$ *distinto de q, que se ramifica em* $\mathbb{K}/\mathbb{F}$ *e* $\mathbb{L}/\mathbb{F}$*, então, os primos de* $B_{\mathbb{K}}$ *acima de P não se ramificam em* $\mathbb{KL}/\mathbb{K}$*.*

Não podemos usar o Lema de Abhyankar com $\mathbb{K} = \mathbb{Q}\left(\sqrt[q]{r}\right)$, $\mathbb{L}$(como no Teorema 14) e $\mathbb{F} = \mathbb{Q}$, pois embora $\mathbb{L}/\mathbb{Q}$ seja cíclica de grau q (as extensões abelianas de $\mathbb{Q}$ estão contidas nas ciclotômicas), $\mathbb{K}/\mathbb{Q}$ não é de Galois.

Mas podemos usá-lo realizando algumas leves modificações. Sejam $\mathbb{K}_1 = \mathbb{K}\left(\zeta_q\right)$, $\mathbb{L}_1 = \mathbb{L}\left(\zeta_q\right)$, $\mathbb{Q}_1 = \mathbb{Q}\left(\zeta_q\right)$

Lema 4.2.1. $\mathbb{K}_1/\mathbb{Q}_1$, $\mathbb{L}_1/\mathbb{Q}_1$ *são cíclicas de grau q.*

Demonstração. $\mathbb{K}_1/\mathbb{Q}_1$ é de Galois, pois é o corpo de decomposição de $x^q - r \in \mathbb{Q}_1[x]$.

$$[\mathbb{K}_1 : \mathbb{K}][\mathbb{K} : \mathbb{Q}] = [\mathbb{K}_1 : \mathbb{Q}].$$

Mas $[\mathbb{K} : \mathbb{Q}] = q$, por isso

$$q \mid [\mathbb{K}_1 : \mathbb{Q}].$$

Por outro lado,

$$[\mathbb{K}_1 : \mathbb{Q}] = [\mathbb{K}_1 : \mathbb{Q}_1][\mathbb{Q}_1 : \mathbb{Q}].$$

Assim,

$$(q-1) \mid [\mathbb{K}_1 : \mathbb{Q}].$$

Como q e $q-1$ são coprimos, então

$$q\,(q-1) \mid [\mathbb{K}_1 : \mathbb{Q}].$$

Mas $[\mathbb{K}_1 : \mathbb{K}] \leq q - 1$, pois

$$[\mathbb{Q}\left(\zeta_q\right) : \mathbb{Q}] = [\mathbb{Q}_1 : \mathbb{Q}] = q - 1.$$

Portanto,

$$[\mathbb{K}_1 : \mathbb{Q}] = q\,(q-1)\,.$$

Assim,

$$[\mathbb{K}_1 : \mathbb{Q}_1] = q.$$

$\mathbb{L}/\mathbb{Q}$ é de Galois, pois

$$\mathbb{L} \subset \mathbb{Q}\left(\zeta_p\right)$$

Como $\mathbb{Q}\left(\zeta_q\right)/\mathbb{Q}$ é de Galois, temos que

$$\mathbb{L}_1/\mathbb{Q}_1$$

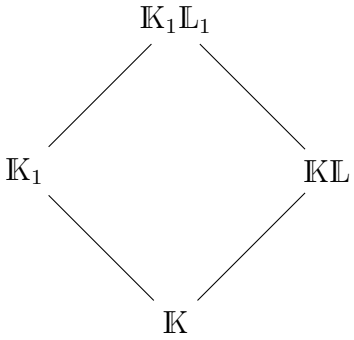
também é de Galois.

□

Com essas modificações, podemos usar o Lema de Abhyankar.

Teorema 4.2.2. *Se* $\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1$ *é não ramificada, então* $\mathbb{K}\mathbb{L}/\mathbb{K}$ *também é não ramificada (nos primos finitos, ou seja nos ideais).*

Demonstração. Considere as torres de corpos:



Como o diferente é multiplicativo, pela Proposição 4.2.1

$$d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}\right) = d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1\right) d\left(\mathbb{K}_1/\mathbb{K}\right) B_{\mathbb{K}_1\mathbb{L}_1} = d\left(\mathbb{K}_1/\mathbb{K}\right) B_{\mathbb{K}_1\mathbb{L}_1}.$$

Pois os ideais primos de $B_{\mathbb{K}_1\mathbb{L}_1}$ que dividem $d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1\right)$ são exatamente os primos que se ramificam (Teorema 4.1.3) em $\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1$. Mas essa extensão é não ramificada, assim

$$d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1\right) = B_{\mathbb{K}_1\mathbb{L}_1}.$$

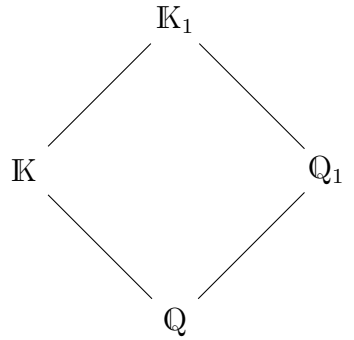
Por outro lado, novamente pela Proposição 4.2.1

$$d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}\right) = d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}\mathbb{L}\right) d\left(\mathbb{K}\mathbb{L}/\mathbb{K}\right) B_{\mathbb{K}_1\mathbb{L}_1}.$$

Daí,

$$d\left(\mathbb{K}_1/\mathbb{K}\right) B_{\mathbb{K}_1\mathbb{L}_1} \subset d\left(\mathbb{K}\mathbb{L}/\mathbb{K}\right) B_{\mathbb{K}_1\mathbb{L}_1}.$$

Na torre de corpos abaixo,



Obtemos, pelo Teorema 4.1.2

$$d\left(\mathbb{Q}_1/\mathbb{Q}\right) \subset d\left(\mathbb{K}_1/\mathbb{K}\right).$$

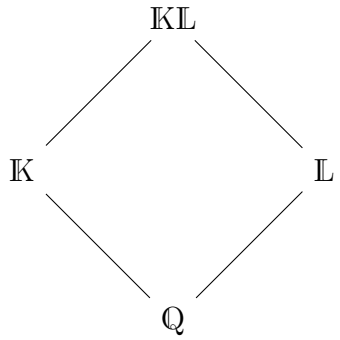
Mas pelas Proposições 4.1.1 e 4.2.2

$$N\left(d\left(\mathbb{Q}_1/\mathbb{Q}\right)\right) = \left|\Delta\left(\mathbb{Q}_1/\mathbb{Q}\right)\right| = q^{q-2}.$$

Assim,

$$q^s \in d\left(\mathbb{Q}_1/\mathbb{Q}\right) \subset d\left(\mathbb{K}_1/\mathbb{K}\right) B_{\mathbb{K}_1\mathbb{L}_1} \subset d\left(\mathbb{K}\mathbb{L}/\mathbb{K}\right) B_{\mathbb{K}_1\mathbb{L}_1}.$$

Além disso, pelo Teorema 4.1.2



$$d\left(\mathbb{L}/\mathbb{Q}\right) \subset d\left(\mathbb{K}\mathbb{L}/\mathbb{K}\right).$$

Mas, pela Proposição 4.1.1

$$N\left(d\left(\mathbb{L}/\mathbb{Q}\right)\right) = \left|\Delta\left(\mathbb{L}/\mathbb{Q}\right)\right|.$$

Temos também, pela Proposição 4.2.2

$$p^{p-2} = \left|\Delta\left(\mathbb{Q}\left(\zeta_p\right)/\mathbb{Q}\right)\right|.$$

Portanto, pela Proposição 4.2.3

$$\left|\Delta\left(\mathbb{L}/\mathbb{Q}\right)\right| = p^t \quad (t > 0).$$

Portanto,

$$p^t \in d\left(\mathbb{K}\mathbb{L}/\mathbb{K}\right).$$

Assim,

$$p^t, q^s \in d\left(\mathbb{K}\mathbb{L}/\mathbb{K}\right).$$

Como p e q são primos distintos, temos que

$$1 \in d\left(\mathbb{K}\mathbb{L}/\mathbb{K}\right).$$

Logo $\mathbb{K}\mathbb{L}/\mathbb{K}$ é não ramificada, pelo Teorema 4.1.3. □

Portanto, para mostrarmos que $\mathbb{K}\mathbb{L}/\mathbb{K}$ é não ramificada é suficiente mostrarmos que $\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1$ é não ramificada. Faremos isso no próximo Teorema.

Teorema 4.2.3. $\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1$ *não é ramificada.*

Demonstração. Pelas Proposições 4.1.1 e 4.2.2

$$N\left(d\left(\mathbb{L}/\mathbb{Q}\right)\right) = \left|\Delta\left(\mathbb{L}/\mathbb{Q}\right)\right| = p^{p-2} \Rightarrow$$

$$p^{p-2} \in d\left(\mathbb{L}/\mathbb{Q}\right) \subset d\left(\mathbb{L}_1/\mathbb{Q}_1\right) \subset d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1\right).$$

Seja

$$d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1\right) = I_1^{e_1}...I_r^{e_r},$$

com I_j ideal primo de $B_{\mathbb{K}_1\mathbb{L}_1}$.

$$p^{p-2} \in I_j \Rightarrow p \in I_j.$$

Mas os primos de $B_{\mathbb{K}_1\mathbb{L}_1}$ que se ramificam em $\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1$ são exatamente os que dividem o $d\left(\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1\right)$ (Teorema 4.1.3) . Assim, se mostrarmos que os ideais primos de $B_{\mathbb{K}_1}$, acima de p, não se ramificam em $\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1$, então mostramos que $\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1$ é não ramificada. Como $\mathbb{K}_1/\mathbb{Q}_1$ e $\mathbb{L}_1/\mathbb{Q}_1$ são cíclicas de grau q, se mostrarmos que os ideais primos acima de p em $B_{\mathbb{Q}_1}$ se ramificam em ambas as extensões, então pelo Lema de Abhyankar, Teorema 4.2.1, temos que nenhum primo de $B_{\mathbb{K}_1}$, acima de p, se ramifica em $\mathbb{K}_1\mathbb{L}_1/\mathbb{K}_1$.

Proposição 4.2.5. *Seja P um ideal de $\mathbb{Q}_1 = \mathbb{Q}\left(\zeta_q\right)$, acima de p, então P se ramifica totalmente em $\mathbb{K}_1/\mathbb{Q}_1$ e em $\mathbb{L}_1/\mathbb{Q}_1$.*

Demonstração. Vejamos que o resultado é válido para $\mathbb{K}_1/\mathbb{Q}_1$. De fato, p não se ramifica em $\mathbb{Q}_1/\mathbb{Q}$, pela Proposição 4.2.2 e o Teorema 3.2.2

$$p \nmid \left|\Delta\left(\mathbb{Q}_1/\mathbb{Q}\right)\right| = q^{q-2}.$$

Por isso, a fatoração, em primos, do ideal gerado por p em $\mathbb{Q}_1$ é:

$$pB_{\mathbb{Q}_1} = J_1 \ldots J_m, \qquad J_i \neq J_j,$$

$$pB_{\mathbb{K}_1} = J_1 B_{\mathbb{K}_1} \ldots B_{\mathbb{K}_1} J_m.$$

Precisamos mostrar que J_i se ramifica totalmente em $B_{\mathbb{K}_1}$.

Mas, pelo Teorema 3.2.2, temos que p se ramifica em $\mathbb{K}_1/\mathbb{Q}$, pois

$$p \mid \Delta\left(\mathbb{K}_1/\mathbb{Q}\right).$$

De fato, $\mathbb{K} = \mathbb{Q}(\alpha)$, $\alpha = \sqrt[q]{r}$, com r livre de q-ésimas potências divisível por p. Temos que

$$\mathbb{Q}\left(\alpha\right) = \mathbb{Q}\left(\alpha^j\right) \quad \text{com} \;\; 1 \leq j \leq q-1.$$

Claramente,

$$\mathbb{Q}\left(\alpha^{j}\right) \subset \mathbb{Q}\left(\alpha\right).$$

Por outro lado, seja $j^{'}$ com

$$jj^{'} \equiv 1 \pmod{q}; \qquad jj^{'} = tq + 1.$$

Assim,

$$\left(\alpha^{j}\right)^{j^{'}} = r^{t}\alpha \Rightarrow \alpha \in \mathbb{Q}\left(\alpha^{j}\right).$$

Agora, pelas Proposições 2.1.1, 2.1.2 e 2.1.3

$$|\Delta\left(1, \alpha, \ldots, \alpha^{q-1}\right)| = N\left(q\alpha^{q-1}\right) = q^{q}r^{q-1} = [B_{\mathbb{K}} : \mathbb{Z}[\alpha]]^{2}|\Delta_{\mathbb{K}}|.$$

Seja $r = p^{e_p}r^{'}$ e $\mathrm{mdc}(p, r^{'}) = 1$. Se $e_p > 1$, então existe t_p com

$$t_p e_p \equiv 1 \pmod{q}.$$

$$\mathbb{Q}\left(\alpha\right) = \mathbb{Q}\left(\alpha^{t_p}\right) = \mathbb{Q}\left(\sqrt[q]{pr^{''}}\right) \qquad \mathrm{mdc}(p, r^{''}) = 1.$$

Assim, podemos supor que $p^{2} \nmid r$. Dessa forma, α é de Eisenstein para p e, portanto, pelo Lema 2.1.1

$$p \nmid [B_{\mathbb{K}} : \mathbb{Z}[\alpha]].$$

Assim,

$$p^{q-1} \mid \Delta\left(\mathbb{K}/\mathbb{Q}\right).$$

Pela transitividade do discriminante, Proposição 4.2.3

$$\Delta\left(\mathbb{K}_1/\mathbb{Q}\right) = \Delta\left(\mathbb{K}/\mathbb{Q}\right)^{[\mathbb{K}_1:\mathbb{K}]} N_{\mathbb{K}/\mathbb{Q}}\left(\Delta\left(\mathbb{K}_1/\mathbb{K}\right)\right).$$

Em vista disso,

$$p \mid \Delta\left(\mathbb{K}_1/\mathbb{Q}\right).$$

Por isso, p se ramifica em $\mathbb{K}_1/\mathbb{Q}$, pelo Teorema 4.2.1. Além disso, $\mathbb{K}_1/\mathbb{Q}$ é de Galois (corpo de decomposição de $x^{q} - r$) . Disso e da Proposição 4.2.4, a fatoração, em primos, do ideal gerado por p em $B_{\mathbb{K}_1}$ é da seguinte forma:

$$pB_{\mathbb{K}_1} = I_1^{e} \ldots I_m^{e}, \qquad e > 1.$$

Por outro lado, já vimos a fatoração do ideal gerado por p em $B_{\mathbb{K}_1}$

$$pB_{\mathbb{K}_1} = J_1 B_{\mathbb{K}_1} \ldots B_{\mathbb{K}_1} J_m.$$

Logo,

$$I_1^{e} \ldots I_m^{e} = J_1 B_{\mathbb{K}_1} \ldots B_{\mathbb{K}_1} J_m.$$

Concluimos, então

$$J_i B_{\mathbb{K}_\mathbb{1}} = I_{\sigma_1}^e \dots I_{\sigma_g}^e,$$

já que cada ideal primo de $B_{\mathbb{K}_1}$ está acima de um único ideal de $B_{\mathbb{Q}_1}$. Também temos que $\mathbb{K}_\mathbb{1}/\mathbb{Q}_1$ é cíclica de grau q (primo), então pela equação fundamental de ramificação, Proposição 4.2.4

$$efg = q, \quad e > 1 \Rightarrow e = q.$$

Portanto, J_i se ramifica totalmente em $B_{\mathbb{K}_1}$.

Procederemos de maneira análoga na análise de $\mathbb{L}_1/\mathbb{Q}_1$. Temos que

$$\mathbb{Q} \subset \mathbb{L} \subset \mathbb{Q}(\zeta_p).$$

Pela Proposição 4.2.2,

$$|\Delta(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = p^{p-2}.$$

Então, pela Proposição 4.2.3

$$p \mid \Delta(\mathbb{L}/\mathbb{Q}).$$

Novamente pela Proposição 4.2.3

$$\Delta(\mathbb{L}_1/\mathbb{Q}) = \Delta(\mathbb{L}/\mathbb{Q})^{[\mathbb{L}_1:\mathbb{L}]} N_{\mathbb{L}/\mathbb{Q}}(\Delta(\mathbb{L}_1/\mathbb{L})).$$

Logo,

$$p \mid \Delta(\mathbb{L}_1/\mathbb{Q}).$$

Também temos que $\mathbb{L}_1/\mathbb{Q}$ é de Galois, pois $\mathbb{L}/\mathbb{Q}$ é de Galois ($\mathbb{L} \subset \mathbb{Q}(\zeta_p)$) bem como $\mathbb{Q}_1/\mathbb{Q}$ também é de Galois e a composição de extensões de Galois é de Galois. Além disso, $\mathbb{L}_1/\mathbb{Q}_1$ é cíclica de grau q. Portanto, de maneira análoga ao caso $\mathbb{K}_1/\mathbb{Q}_1$, os ideais primos de $B_{\mathbb{Q}_1}$, acima de p, se ramificam totalmente em $\mathbb{L}_1/\mathbb{Q}_1$. □

□

4.3 KL/K é não Ramificada nos Primos Infinitos

Na seção anterior provamos que os ideais primos de $\mathbb{K}$ não se ramificam em $\mathbb{KL}$, para $\mathbb{KL}/\mathbb{K}$ ser não ramifica no sentido do Corpo de Hilbert, precisamos mostrar que ela também é não ramificada no sentido dos primos infinitos. Ou seja, precisamos mostrar que dada uma imersão real de $\mathbb{K}$ sua extensão a $\mathbb{KL}$, σ' também é um imersão real.

Proposição 4.3.1. $\mathbb{KL}/\mathbb{K}$ *é não ramificada, no sentido das imersões.*

Demonstração. Seja $\mathbb{L}' = \mathbb{Q}(\zeta_p)$. Temos que

$$Gal\left(\mathbb{L}'/\mathbb{Q}\right) \simeq \mathbb{F}_p^*,$$

que é ciclico, pois é um subgrupo finito do grupo mulplicativo do corpo $\mathbb{F}_p$. Seja então, σ um gerador de $\mathbb{F}_p^* =< \sigma >$, pela teoria de Galois $\mathbb{L}$ é o corpo fixo de um subgrupo $G_{\mathbb{L}}$ de ordem $\frac{p-1}{q}$, assim

$$G_{\mathbb{L}} =< \sigma^q > .$$

Lema 4.3.1. *O corpo fixo por $G_{\mathbb{L}}$ é*

$$\mathbb{Q}\left(\sigma^q(\zeta), \sigma^{2q}(\zeta), \ldots, \sigma^{p-1}(\zeta)\right).$$

Demonstração. Inicialmente, note que $G_{\mathbb{L}}$ fixa

$$\alpha = \left(\sigma^q(\zeta) + \sigma^{2q}(\zeta) + \cdots + \sigma^{p-1}(\zeta)\right).$$

Só pecisamos verificar o resultado para os geradores $\mathrm{G}_{\mathbb{L}}$. De fato,

$$\sigma^q\left(\sigma^q(\zeta) + \sigma^{2q}(\zeta) + \cdots + \sigma^{p-1}(\zeta)\right) = \sigma^{2q}(\zeta) + \sigma^{3q}(\zeta) + \cdots + \sigma^q(\zeta),$$

pois σ^{p-1} é a identidade de $\mathrm{Gal}\left(\mathbb{L}'/\mathbb{Q}\right)$.

Como $[\mathbb{L} : \mathbb{Q}] = q$ (primo), então não existe corpos intermediários entre $\mathbb{L}$ e $\mathbb{Q}$, mas

$$\mathbb{Q} \subset \mathbb{Q}\left(\sigma^q(\zeta), \sigma^{2q}(\zeta), \ldots, \sigma^{p-1}(\zeta)\right) \subset \mathbb{L}.$$

Portanto,

$$\mathbb{Q}\left(\sigma^q(\zeta), \sigma^{2q}(\zeta), \ldots, \sigma^{p-1}(\zeta)\right) = \mathbb{L}.$$

ou

$$\mathbb{Q}\left(\sigma^q(\zeta), \sigma^{2q}(\zeta), \ldots, \sigma^{p-1}(\zeta)\right) = \mathbb{Q}.$$

Vamos mostrar que

$$\mathbb{Q} \neq \mathbb{Q}\left(\sigma^q(\zeta), \sigma^{2q}(\zeta), \ldots, \sigma^{p-1}(\zeta)\right).$$

Note que

$$\sigma^q(\zeta), \sigma^{2q}(\zeta), \ldots, \sigma^{p-1}(\zeta)$$

são todos distintos. De fato,

$$\{\sigma(\zeta), \sigma^2(\zeta), \ldots, \sigma^{p-1}(\zeta)\} = \{\zeta, \ldots, \zeta^{p-1}\}.$$

Por outro lado, $\mathbb{Z}[\zeta]$ é base inteira de $\mathbb{Q}(\zeta)$. Assim,

$$\sigma^q(\zeta) + \sigma^{2q}(\zeta) + \cdots + \sigma^{p-1}(\zeta) \neq \sigma^{q+1}(\zeta) + \sigma^{2q+1}(\zeta) + \cdots + \sigma^p(\zeta).$$

Por isso, $\sigma^q(\zeta) + \sigma^{2q}(\zeta) + \cdots + \sigma^{p-1}(\zeta)$ não é fixado por σ. □

Portanto,

$$\mathbb{KL} = \mathbb{Q}\left(\sqrt[q]{r},\ \alpha\right).$$

Se θ estende uma imersão real de $\mathbb{K}$ e $\theta(\alpha) \in \mathbb{R}$, então

$$\theta(\mathbb{KL}) \in \mathbb{R}.$$

Assim, é suficiente mostrarmos que todos os conjugados de α sobre $\mathbb{Q}$ são reais. Temos que $\sigma(\zeta) = \zeta^i$, então

$$\sigma^m(\zeta) = \zeta^{i^m}.$$

Como ζ é raiz primitiva p-ésima da unidade e σ é gerador de $G_{\mathbb{L}}$, temos que $p-1$ é o menor valor de m para o qual

$$\sigma^m(\zeta) = \zeta.$$

$$i^m \equiv 1 \pmod{p}.$$

Daí, i é uma raiz primitiva módulo p.

Lema 4.3.2. *Se existe m satisfazendo*

$$\sigma^{qm}(\zeta) = \zeta^j,$$

então existe $x \in \{1, \ldots, \frac{p-1}{q}\}$ *,satisfazendo*

$$\sigma^{qx}(\zeta) = \zeta^{-j}.$$

Demonstração. De fato,

$$\sigma^{qm}(\zeta) = \zeta^j,$$

com

$$i^{qm} \equiv j \pmod{p}.$$

Como i é uma raiz primitiva módulo p, i não é quadrado módulo p, então

$$i^{(p-1)/2} \equiv -1 (\mathrm{mod}\ p).$$

Mas $(p-1)/2$ é divisível q, ou seja, $(p-1)/2 = qa$, com a inteiro

$$i^{qa} i^{qm} = i^{q(a+m)} \equiv -j \pmod{p}.$$

Assim, podemos tomar

$$x \in \{1, \ldots, \frac{p-1}{q}\}$$

, pois os resíduos q-ésimos módulo p são

$$\{i^q, i^{2q} \ldots, i^{p-1}\}.$$

□

Usando os Lemas 4.3.1 e 4.3.2 , obtemos que

$$\mathbb{L} = \mathbb{Q}\left(\sum_{j\in J}\left(\zeta^{j} + \zeta^{-j}\right)\right).$$

Agora mostraremos que se $\alpha = \sum_{j\in J}(\zeta^{j} + \zeta^{-j})$, então os conjugados de α sobre $\mathbb{Q}$ são reais. Como $\zeta^{-1} = \overline{\zeta}$, temos que α é real. Note que cada imersão σ de $\mathbb{L}$ em $\mathbb{C}$ é a restrição de alguma imersão $\sigma^{'}$ de $\mathbb{L}^{'}$ em $\mathbb{C}$ (ASH, 2000 , seção 3.5.2.). Assim,

$$\sigma(\alpha) = \sigma^{'}(\alpha) = \sum_{j\in J}\left(\sigma(\zeta)^{j} + \sigma(\zeta)^{-j}\right).$$

Mas, $\sigma(\zeta)^{j} = \zeta^{tj}$, por isso,

$$\sigma(\zeta)^{-j} = \zeta^{-tj} = \overline{\zeta^{tj}} = \overline{\sigma(\zeta)^{j}}.$$

Assim, $\sigma^{'}(\alpha)$ é real.

□

4.4 O Lema de Abhyankar

O Lema de Abhyankar desempenhou um papel muito importante, na conexão entre corpos não Euclidianos e ramificação, via Corpo de Hilbert. Nesta seção, iremos apresentar uma demonstração para o Lema de Abhyankar.

Precisaremos de alguns resultados.

Proposição 4.4.1. *Se* $\mathbb{K}/\mathbb{F}$ *e* $\mathbb{L}/\mathbb{F}$ *são extensões de Galois então* $\mathbb{KL}/\mathbb{F}$ *também é de Galois. Além disso, se* $\mathbb{K}/\mathbb{F}$ *e* $\mathbb{L}/\mathbb{F}$ *são disjuntas, então*

$$Gal(\mathbb{KL}/\mathbb{F}) \simeq Gal(\mathbb{K}/\mathbb{F}) \times Gal(\mathbb{L}/\mathbb{F}).$$

Em particular, se $\mathbb{K}/\mathbb{F}$ *e* $\mathbb{L}/\mathbb{F}$ *são disjuntas e cíclicas de grau* q *, então*

$$\mathbb{KL}/\mathbb{F} \simeq \mathbb{Z}_q \times \mathbb{Z}_q.$$

(que não é cíclico).

.

Definição 4.4.1. *Seja* $\mathbb{K}/\mathbb{F}$ *uma extensão de Galois e* P *um ideal fixado de* $B_{\mathbb{K}}$*, o grupo de decomposição,* D*, de* P *na extensão* $\mathbb{K}/\mathbb{F}$ *é*

$$D = \{\sigma \in Gal(\mathbb{K}/\mathbb{F}) \mid \sigma(P) = P\}.$$

O i*-ésimo grupo de inércia de* P *na extensão* $\mathbb{K}/\mathbb{F}$ *é*

$$V_i = \{\sigma \in D \mid \sigma(x) \equiv x \ (mod\ P^{i+1})\ \forall\, x \in B_{\mathbb{K}}\}.$$

Proposição 4.4.2. *Se* $\mathbb{K}$ *é um corpo, então qualquer subgrupo finito do grupo multiplicativo de* $\mathbb{K}$ *é cíclico.*

Definição 4.4.2. *Se* A *é um anel e* P *um ideal primo de* A*, denotamos por* A_P *a localização de* P *em* A

$$A_P = S^{-1}A \quad onde \quad S = A \backslash P.$$

A seguinte proposição mostra a importância da localização.

Proposição 4.4.3. *Se* A *é domínio de Dedekind, então* A_P *é um domínio de ideais principais.*

Demonstração. Veja RIBENBOIM, 2001 página 211, G. □

Algo muito interesante é que os grupos de inércia também se expressam em termos da Localização de maneira simples.Nas proposições abaixo, denotaremos $B_{\mathbb{K}}$ por A. A proposição que segui é uma maneira prática de determinar se um elemento do grupo de decomposição de uma extensão de Galois está no i-ésimo grupo de inércia, não precisamos verificar para todo x no anel de inteiros, basta verificar apenas para um único elemento.

Proposição 4.4.4. *Seja* $\mathbb{K}/\mathbb{F}$ *uma extensão finita de Galois, e* P *um ideal primo de* A *com* $t \in A$ *tal que*

$$A_P P = A_P t,$$

então

$$V_i = \{\sigma \in D \mid \sigma(x) \equiv x \ (mod\ A_P P^{i+1}) \ \forall\ x \in A_P\}.$$

Além disso,

$$V_i = \{\sigma \in D \mid \sigma(t)\, t^{-1} \equiv 1 \ (mod\ A_P P^{i})\}.$$

Demonstração. Veja RIBENBOIM, 2001 página 266, G. □

Proposição 4.4.5. *Seja* $\mathbb{K}/\mathbb{F}$ *uma extensão finita de Galois, e* P *um ideal primo de* A*. Para cada* $i = 0, 1, 2, ...$ *Temos que* V_{i+1} *é subgrupo normal de* V_i *e existe um isomorfismo de* V_i/V_{i+1} *no grupo aditivo do corpo finito* $\frac{A_P}{A_P P}$ *(o qual possui característica p, portanto é um espaço vetorial sobre* $\mathbb{F}_p$*) e assim,* V_i/V_{i+1} *é um p-grupo. Além disso, existe* r *tal que*

$$I_d = V_r \subseteq \cdots \subseteq V_0.$$

Demonstração. Veja RIBENBOIM, 2001 página 266, G e pagina 267,Teorema 2. □

Proposição 4.4.6. *Seja* $\mathbb{K}/\mathbb{F}$ *uma extensão de corpos de números de Galois,* P *um ideal primo de* A *com índice de ramificação* e*, então* $\#V_0 = e$*. Além disso,* V_0/V_1 *é um grupo cíclico e* V_1 *é um p-grupo.*

Demonstração. Mostraremos que

$$V_0/V_1 \simeq \left(\frac{A_P}{A_P P}\right)^*$$

Grupo multiplicativo de um corpo finito, portanto V_0/V_1 é cíclico, pela proposição 4.4.2.

Como A é um domínio de Dedenkind, pela Proposição 4.4.3, temos que A_P é um domínio de ideais principais. Assim,

$$A_P P = A_P t', \quad t' \in A_P P.$$

Mas podemos supor $t' \in A$, pois se $t' = \frac{t}{s}$ com $(t \in A$ e $s \in A \backslash P)$

$$A_P t' = A_P t,$$

já que $\frac{1}{s} A_P = A_P$.

Assim,

$$t \ \in A_P \cap A = P.$$

Se $\sigma \in D$, então $\sigma(P) = P$, assim

$$\sigma(t) \in P \subset A_P P = A_P t.$$

Por isso, existe $c_\sigma \in A_P$ tal que

$$\sigma(t) = c_\sigma t.$$

Mas, para qualquer $\sigma \in D$, temos que $\sigma^{-1} \in D$, e dessa maneira

$$\sigma^{-1}(t) = c_{\sigma^{-1}} t, \quad c_{\sigma^{-1}} \in A_P.$$

Temos, então

$$t = \sigma\left(\sigma^{-1}(t)\right) = \sigma\left(c_{\sigma^{-1}}\right)\sigma(t) = \sigma\left(c_{\sigma^{-1}}\right) c_\sigma t.$$

Por isso,

$$\sigma\left(c_{\sigma^{-1}}\right) c_\sigma = 1.$$

Portanto,

$$c_\sigma \notin A_P P.$$

Agora, vamos construir um isomorfismo entre V_0/V_1 e $\left(\frac{A_P}{A_P P}\right)^*$.

Seja

$$\theta \colon V_0 \to \left(\frac{A_P}{A_P P}\right)^*$$

$$\sigma \longmapsto \overline{c_\sigma}.$$

Onde $\overline{c_\sigma}$, a redução de c_σ módulo $A_P P$.

Vamos mostrar que θ está bem definida e é um homormofismo sobrejetivo cujo núcleo é V_1.

Suponha que

$$A_P t = A_P P = A_P t', \quad t, t' \in A.$$

Assim, existe $u \in A_P$ tal que $t' = ut$, então dado $\sigma \in V_0$, temos

$$\sigma(u)\,\sigma(t) = \sigma(ut) = c'_\sigma t' = c'_\sigma tu.$$

Por outro lado,

$$\sigma(u) - u \in A_P t.$$

O que resulta em

$$\sigma(u) = u + vt, \quad v \in A_P$$

$$\sigma(ut) = (u + vt)\, c_\sigma t.$$

Assim,

$$\overline{c'_\sigma u} = \overline{(u + vt)\, c_\sigma} = \overline{c_\sigma u}.$$

Como $u \notin A_P t$, obtemos

$$\overline{c_\sigma} = \overline{c'_\sigma}.$$

Portanto, θ está bem definida.
Agora, vamos mostrar que θ é um homomorfismo. Queremos mostrar que

$$\theta(\sigma\varphi) = \theta(\sigma)\,\theta(\varphi).$$

Temos que $\theta(\sigma) = \overline{c_\sigma}$, $\theta(\varphi) = \overline{c_\varphi}$. Daí,

$$\sigma(\varphi(t)) = \sigma(c_\varphi t) = \sigma(c_\varphi)\,\sigma(t) = \sigma(c_\varphi)\, c_\sigma t.$$

Assim,

$$c_{\sigma\varphi} = \sigma(c_\varphi)\, c_\sigma.$$

Por outro lado,

$$\sigma(c_\varphi) = c_\varphi + vt, \quad v \in A_P.$$

Daí,

$$\overline{c_{\sigma\varphi}} = \overline{(c_\varphi + vt)\, c_\sigma} = \overline{c_\varphi c_\sigma} = \overline{c_\varphi}\ \overline{c_\sigma}.$$

Temos, então o homomorfismo desejado.

Agora vejamos que o núcleo desse homomorfismo é V_1. De fato, se $\sigma \in V_1$, então

$$\sigma(t) - t \in A_P t^2.$$

Assim, existe $b \in A_P$

$$\sigma(t) = t + bt^2 = (1 + bt)\, t \Rightarrow c_\sigma = 1 + bt.$$

Logo,

$$\theta(\sigma) = \overline{1 + bt} = \overline{1}.$$

Reciprocamente, suponha que σ está no núcleo de θ, ou seja,

$$\overline{c_\sigma} = \overline{1},$$

então

$$c_\sigma - 1 \in A_P t.$$

Daí, multiplicando por t, obtemos

$$\sigma(t) - t = (c_\sigma - 1)\, t \in A_P t^2$$

$$\frac{\sigma(t)}{t} \in A_P t.$$

Portanto, $\sigma \in V_1$ pela Proposição 4.4.4.
Por fim, vejamos que V_1 é um p-grupo. Temos V_i/V_{i+1} é um p-grupo pela Proposição 4.4.5 Como existe m com $V_m = I_d$, temos que

$$\#V_1 = \#V_1/V_2 \ldots \#V_{m-1}/\{I_d\} = p^y,$$

já que cada fator é potência de p, portanto V_1 é um p-grupo.

Aqui, seguimos fielmente o RIBENBOIM, 2001. Para $\#V_0 = e$, veja ASH, 2003 seção 8.1.9. □

Agora, podemos demonstrar o Lema de Abhyankar (Teorema 4.2.1).

Demonstração. [Abhyankar]

Desde que $\mathbb{K}/\mathbb{F}$ e $\mathbb{L}/\mathbb{F}$ são extensões de Galois, então pela Proposição 4.4.1

$$\mathbb{KL}/\mathbb{F}$$

também é de Galois. Como P se ramifica nas extensões de Galois de grau $q : \mathbb{L}/\mathbb{F}$ e $\mathbb{K}/\mathbb{F}$. Então, pela equação geral de ramificação (Proposição 4.2.4), temos

$$PB_{\mathbb{K}} = P_{\mathbb{K}}^q.$$

Assim, queremos mostrar que $P_{\mathbb{K}}$ não se ramifica em $\mathbb{KL}/\mathbb{K}$. Suponhamos, por absurdo que que ele se ramifica, então

$$PB_{\mathbb{KL}} = P_{\mathbb{KL}}^{q^2}.$$

Além disso,

$$V_0 \subset Gal\left(\mathbb{KL}/\mathbb{F}\right).$$

Pela Proposição 4.4.6

$$\#V_0 = q^2 = \#Gal\left(\mathbb{KL}/\mathbb{F}\right).$$

Portanto,

$$V_0 = Gal\left(\mathbb{KL}/\mathbb{F}\right).$$

Temos pela Proposição 4.4.6,

$$G/V_1 = V_0/V_1,$$

é cíclico e V_1 é um p-grupo. Mas V_1 é subgrupo de $Gal\left(\mathbb{KL}/\mathbb{F}\right)$, grupo com q^2 elementos. Assim, V_1 também é um q-grupo, portanto V_1 é o grupo trivial. Daí,

$$G/V_1 = G.$$

Isso garante que G é cíclico. Mas isso é um absurdo, pois pela Proposição 4.4.1

$$G \simeq \mathbb{Z}_q \times \mathbb{Z}_q,$$

que não é cíclico. □

4.5 Ideal Diferente e Ramificação

Dada $\mathbb{E}/\mathbb{F}$ uma extensão de corpos de números, caracterizamos, precisamente, os primos de $B_{\mathbb{E}}$ que se ramificam como sendo os que dividem o ideal diferente da extensão. Esse resultado foi muito importante para mostrar que $\mathbb{KL}/\mathbb{K}$ é não ramificada. Nessa seção faremos a demonstração dessa propriedade tão importante do ideal diferente.

No Teorema seguinte, usaremos as notações: Sejam $\mathbb{E}/\mathbb{F}$ uma extensão de corpos de números, $\mathscr{S}$ o conjunto dos ideais primos de $B_{\mathbb{E}}$. Façamos $B = B_{\mathbb{E}}$, $A = B_{\mathbb{F}}$. Dado um ideal Q_1 de B $P = Q_1 \cap A$ e $\mathscr{I}$ o conjunto dos ideais de B que estão acima de P.

$$d\left(B/A\right) = \prod_{Q \in \mathscr{S}} Q^{s_Q}, \qquad PB = \prod_{Q \in \mathscr{I}} Q^{e_Q}.$$

Teorema 4.5.1. *Para cada ideal primo Q_1 de B, nós temos $s_{Q_1} \geq e_{Q_1} - 1$ e $s_{Q_1} = e_{Q_1} - 1$ se e somente se a característica de $\frac{B}{Q_1}$ não divide o índice de ramificação de Q_1, e_{Q_1}.*

Demonstração . Sejam $S = A \backslash P$, $A' = A_P$ e $B' = S^{-1}B$. Por RIBENBOIM, 2001 páginas 210, (F) e 245 (N), temos

$$d\left(B'/A'\right) = B'd\left(B/A\right) = \prod_{Q \in \mathscr{I}} B'Q^{s_Q}.$$

Temos que $s_Q \geq e_Q - 1$ é equivalente a

$$Q^{s_Q} \subset Q^{e_Q - 1},$$

pois B é domínio de Dedenkind. Assim, é equivalente mostrar que

$$\prod_{Q \in \mathscr{I}} B^{'} Q^{s_Q} \subset \prod_{Q \in \mathscr{I}} B^{'} Q^{e_Q - 1} \Longleftrightarrow \prod_{Q \in \mathscr{I}} B^{'} Q^{1 - e_Q} \subset \prod_{Q \in \mathscr{I}} B^{'} Q^{-s_Q}$$

$$\Longleftrightarrow \prod_{Q \in \mathscr{I}} B^{'} Q^{1 - e_Q} \subset d\left(B^{'}/A^{'}\right)^{-1}.$$

Tome

$$x \in \prod_{Q \in \mathscr{I}} B^{'} Q^{1 - e_Q}.$$

Como $A^{'}$ é domínio de ideais principais (Proposição 4.4.3), $P^{'} = A^{'}P$ é um ideal principal. Assim, existe $t \in A^{'}$ tal que

$$P^{'} = tA^{'}.$$

Por isso,

$$t \in P^{'}B^{'} = \prod_{Q \in \mathscr{I}} B^{'} Q^{e_Q}.$$

Portanto,

$$tx \in \prod_{Q \in \mathscr{I}} B^{'} Q^{1 - e_Q} \prod_{Q \in \mathscr{I}} B^{'} Q^{e_Q} = \prod_{Q \in \mathscr{I}} B^{'} Q \subset B^{'} Q \ (\ \forall\ Q \in \mathscr{I}).$$

Resultando em

$$\prod_{Q \in \mathscr{I}} (tx)^{e_Q} \subset \prod_{Q \in \mathscr{I}} B^{'} Q^{e_Q}.$$

Assim, $\overline{tx}$ é um elemento nilpotente do anel $\frac{B^{'}}{P^{'}B^{'}}$, que é um espaço vetorial de dimensão finita sobre $\frac{A^{'}}{P^{'}}$ (Veja RIBENBOIM, 2001ágina 212, I). Além disso, $B^{'}$ é um $A^{'}$-módulo livre, pois $A^{'}$ é domínio de ideias principais. Dessa maneira, podemos definir, $T_{B^{'}/A^{'}}$, o traço da extensão $B^{'}/A^{'}$ de maneira análoga ao traço de extensões de corpos (veja RIBENBOIM, 2001 página 212, 213). Logo, temos

$$\overline{T_{B^{'}/A^{'}}(tx)} = T_{\left(B^{'}/B^{'}P^{'}\right)|\left(A^{'}/P^{'}\right)}(\overline{tx}) = \overline{0}.$$

Veja RIBENBOIM, 2001ágina 218, N.
Por isso,

$$T_{B^{'}/A^{'}}(tx) \in P^{'} = A^{'}t.$$

Mas

$$T_{B^{'}/A^{'}}(tx) = T_{\mathbb{E}/\mathbb{F}}(tx)$$

(RIBENBOIM, 2001 página 216, L).

Daí,

$$T_{\mathbb{E}/\mathbb{F}}(x) \in A^{'}$$

e dado qualquer $z \in B$, temos que

$$zx \in \prod_{Q \in \mathscr{I}} B^{'} Q^{1-e_Q}$$

e portanto,

$$T_{\mathbb{E}|\mathbb{F}}(zx) \in A^{'}.$$

Logo,

$$x \in d\left(B^{'}/A^{'}\right)^{-1}.$$

Agora vejamos quando $s_{Q_1} = e_{Q_1} - 1$. Inicialmente suponha que a característica de $\frac{B^{'}}{B^{'}P}$ divide e_{Q_1}, mostraremos que $s_{Q_1} \geq e_{Q_1}$ e dessa forma, não podemos ter a igualdade. Temos que

$$J = B^{'} Q_1^{-e_{Q_1}} \prod_{Q \neq Q_1} B^{'} Q^{1-e_Q} \subset d\left(B^{'}/A^{'}\right)^{-1} \Longleftrightarrow s_{Q_1} \geq e_{Q_1}.$$

Tome $x \in J$. Temos $PA^{'} = A^{'}t$, então

$$t \in B^{'}P^{'} = \prod_{Q \in \mathscr{I}} B^{'} Q^{e_Q}.$$

Assim, $tx \in \prod_{Q \neq Q_1} B^{'} Q$, ou seja, $tx \in Q$ para todo Q acima de P em B diferente de Q_1.

$$\Psi\left(T_{\mathbb{E}/\mathbb{F}}(tx)\right) = \sum_{Q_i \in \mathscr{I}} \left[e_{Q_i} T_{\left(B^{'}/B^{'}P^{'}\right)|\left(A^{'}/P^{'}\right)}\left(\Psi_i(tx)\right)\right] \tag{4.1}$$

.

Veja RIBENBOIM, 2001 página 221. Onde Ψ e Ψ_i são, respectivamennte, os homomorfismos canônicos:

$$\Psi \colon A^{'} \to \frac{A^{'}}{P^{'}}$$

$$\Psi_i \colon B^{'} \to \frac{B^{'}}{B^{'}Q_i}$$

Mas

$$tx \in B^{'}Q$$

para todo ideal Q_i diferente de Q_1 acima de P em B. Por isso

$$\Psi_i(tx) = 0.$$

Além disso, a característica de $\frac{B^{'}}{B^{'}P}$ que é igual a característica de $\frac{A^{'}}{P^{'}}$ divide e_{Q_1}. Assim,

$$\Psi\left(T_{\mathbb{E}/\mathbb{F}}(tx)\right) = \overline{0}.$$

Portanto,

$$T_{\mathbb{E}/\mathbb{F}}(tx) \in P' = A't$$

$$T_{\mathbb{E}/\mathbb{F}}(x) \in A'.$$

Por outro lado, dado qualquer z em B', temos que

$$xz \in J = B'Q_1^{-e_{Q_1}} \prod_{Q \in \mathscr{I};\ Q \neq Q_1} B'Q^{1-e_Q}$$

e

$$T_{\mathbb{E}/\mathbb{F}}(zx) \in A'.$$

Portanto

$$x \in d\left(B'/A'\right)^{-1}.$$

Agora suponha que a característica de $\frac{B'}{B'P}$ não divide e_{Q_1}. Seja $x \in B'$ tal que a imagem de $\Psi_1(x)$ possui traço não nulo. Por (RIBENBOIM, 2001 página 131, L) existe $y \in B'$ tal que $y - x \in B'Q_1$ e $y \in B'Q^{e_Q}$ para todo ideal $Q \neq Q_1$ acima de P em B.

Logo,

$$\Psi\left(T_{\mathbb{E}/\mathbb{F}}(y)\right) = \sum_{Q_i \in \mathscr{I}} e_{Q_i} T_{\left(B'/B'P'\right)/\left(A'/P'\right)}\left(\Psi_i(y)\right) = e_{Q_1} T_{\left(B'/B'P\right)/\left(A'/P'\right)}\left(\Psi_1(y)\right) \neq 0.$$

Assim,

$$T_{\mathbb{E}/\mathbb{F}}(y) \notin A't.$$

$$T_{\mathbb{E}\mathbb{F}}\left(\frac{y}{t}\right) \notin A' \Rightarrow \frac{y}{t} \notin d\left(B'/A'\right)^{-1}.$$

Desde que

$$B't = B'P, \quad y \in B'Q^{e_Q} \ \text{ com } \ Q \neq Q_1.$$

Obtemos,

$$y \in B'Q_1^{-e_{Q_1}} \prod_{Q \in \mathscr{I}} B'Q^{e_Q} = B'Q_1^{-e_{Q_1}} t.$$

Daí,

$$\frac{y}{t} \in B'Q_1^{-e_{Q_1}}.$$

Por isso,

$$B'Q_1^{-e_{Q_1}} \nsubseteq d\left(B' \mid A'\right)^{-1}.$$

Agora, suponha por absurdo que $s_{Q_1} \geq e_{Q_1}$. Então

$$B'Q_1^{s_1} \subset B'Q_1^{e_1} \Rightarrow B'Q_1^{-e_{Q_1}} \subset B'Q_1^{-s_{Q_1}} \subset d\left(B'/A'\right)^{-1}.$$

Absurdo, assim temos que $e_{Q_1} > s_{Q_1} \geq e_{Q_1} - 1$. O que garante que $s_{Q_1} = e_{Q_1} - 1$. □

Agora, nós podemos concluir que os primos de B que se ramificam em B/A são exatamente, os que dividem o diferente.

De fato, se Q se ramifica, $e_Q \geq 2$, assim $s_Q \geq e_Q - 1 \geq 1$, portanto Q divide o diferente. Reciprocamente, se $e_Q = 1$ desde que a característica de $\frac{B'}{B'Q}$ não divide $e_Q = 1$, temos que $s_Q = e_Q - 1 = 0$.

Ao findar esse capítulo temos uma lista de 31 possíveis corpos cúbicos puros. No Próximo capítulo, mostraremos outros métodos que nos permitirão reduzir o tamanho da nossa lista de possíveis corpos Euclidianos.

5 Norma, Ramificação e Corpos não Euclidianos

Nesse capítulo, faremos uso mais uma vez da existência de primos que se ramificam totalmente. Consideraremos o fecho normal de uma extensão de corpos de números e usaremos as propriedades especiais do levantamento de ideais em extensões de Galois. Também precisaremos determinar se um inteiro racional, m, é ou não a norma de algum elemento do anel de inteiros algébricos, para isso recorremos a fatoração do ideal gerado por m.

Definição 5.0.1. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita de corpos, definimos o fecho normal de $\mathbb{E}/\mathbb{F}$ como sendo o menor corpo $\mathbb{N}$ que contém $\mathbb{E}$ e $\mathbb{N}/\mathbb{F}$ é normal.*

Teorema 5.0.1. *Sejam $\mathbb{K}$ um corpo de números de grau q, q primo ímpar, e p um primo que se ramifica totalmente em $\mathbb{K}$, com*

$$p \not\equiv 1 \ (mod\ q).$$

Se existe inteiro positivo $e < p$ tal que nem e nem $p - e$ são normas de elementos de $B_{\mathbb{K}}$, então $\mathbb{K}$ não é Euclidiano.

Demonstração. Seja

$$pB_{\mathbb{K}} = \mathfrak{P}^q.$$

Desde que $p \not\equiv 1 \pmod{q}$, pelo Lema 2.2.1, existe um único c

$$c \in \{0, 1, \ldots, p-1\},$$

tal que

$$c^q \equiv e \pmod{p}.$$

Suponha que existe $u \in B_{\mathbb{K}}$ tal que

$$u \equiv c \pmod{\mathfrak{P}},$$

com

$$|N(u)| < N(\mathfrak{P}) = p.$$

Seja $\mathbb{N}$ um fecho normal de $\mathbb{K}/\mathbb{Q}$ (ou seja, um corpo de decomposição do polinômio mínimo de um gerador de $\mathbb{K}$ sobre $\mathbb{Q}$). Temos

$$pB_{\mathbb{K}} = \mathfrak{P}^q,$$

então

$$(\mathfrak{P}B_{\mathbb{N}})^q = \mathfrak{P}^q B_{\mathbb{N}} = \mathfrak{P}^q B_{\mathbb{K}} B_{\mathbb{N}} = pB_{\mathbb{K}} B_{\mathbb{N}} = pB_{\mathbb{N}}.$$

Assim,

$$pB_{\mathbb{N}} = (\mathfrak{P}B_{\mathbb{N}})^q .$$

Por outro lado, se σ é um automorfismo de $\mathbb{N}/Q$, então

$$\sigma(B_{\mathbb{N}}) = B_{\mathbb{N}}, \quad \text{pois } \mathbb{N}/\mathbb{Q} \text{ é de Galois.}$$

Veja ASH, 2003 seção 8.1.1 . O que nos dá

$$pB_{\mathbb{N}} = \sigma(p)\,\sigma(B_{\mathbb{N}}) = \sigma(pB_{\mathbb{N}}) = \sigma\left((\mathfrak{P}B_{\mathbb{N}})^q\right) = \left(\sigma(\mathfrak{P})\,B_{\mathbb{N}}\right)^q .$$

Portanto,

$$(\mathfrak{P}B_{\mathbb{N}})^q = \left(\sigma(\mathfrak{P})\,B_{\mathbb{N}}\right)^q .$$

Como $B_{\mathbb{N}}$ é domínio de Dedekind, temos fatoração única de ideais em ideais primos (ASH, 2003 seção 3.3.1)

$$\sigma(\mathfrak{P})\,B_{\mathbb{N}} = \mathfrak{P}B_{\mathbb{N}}.$$

Portanto, $\mathfrak{P}B_{\mathbb{N}}$ é invariante pelo grupo de Galois de $\mathbb{N}/\mathbb{Q}$. Sejam $\sigma_1, \ldots, \sigma_q$ as $\mathbb{Q}-$imersões de $\mathbb{K}$ em $\mathbb{C}$ com

$$\sigma_i(u) = u_i,$$

onde $u_1, \ldots, u_q$ são os conjuados de u sobre $\mathbb{Q}$. Como $\mathbb{N}/\mathbb{K}$ é uma extensão finita e separável cada σ_i pode ser estendida a uma imersão $\sigma_i^{'}$ de $\mathbb{N}$ em $\mathbb{C}$, (veja ASH, 2000 , seção 3.5.2.). Temos que

$$u \equiv c \pmod{\mathfrak{P}}$$

$$u - c \in \mathfrak{P} \subset \mathfrak{P}B_{\mathbb{N}}.$$

Aplicando $\sigma_i^{'}$, obtemos

$$\sigma_i^{'}(u-c) = \sigma_i^{'}(u) - c \in \sigma_i^{'}(\mathfrak{P}B_{\mathbb{N}}) = \mathfrak{P}B_{\mathbb{N}},$$

$$u_i \equiv c \pmod{\mathfrak{P}B_{\mathbb{N}}}.$$

Com isso, podemos calcular a norma

$$N_{\mathbb{K}/\mathbb{Q}}(u) = u_1 \ldots u_q \equiv c^q \pmod{\mathfrak{P}B_{\mathbb{N}}}.$$

Agora podemos voltar a trabalhar nos inteiros

$$N_{\mathbb{K}/\mathbb{Q}}(u) \equiv c^q \pmod{p},$$

já que

$$\mathfrak{P}B_{\mathbb{N}} \cap \mathbb{Z} = p\mathbb{Z}.$$

Assim, $N(u) = e$ ou $N(u) = e - p$. Mas nem e, nem $p - e$ são normas de elementos de $B_{\mathbb{N}}$, absurdo.

Suponha que $B_{\mathbb{K}}$ seja Euclidiano, portanto domínio de ideais principais, assim

$$\mathfrak{P} = bB_{\mathbb{K}},$$

com $b \in B_{\mathbb{K}}$. Vamos mostrar que não conseguimos encontrar $t, r \in B_{\mathbb{K}}$ tais que

$$u = tb + r,$$

$$|N(b)| < |N(r)|.$$

De fato, isso resultaria em

$$r \equiv u \pmod{\mathfrak{P}}.$$

Assim,

$$|N(r)| \geq p = N(\mathfrak{P}) = |N(b)|$$

Portanto, $\mathbb{K}$ não é Euclidiano. □

Vamos aplicar esse resultado para descartar nove corpos satisfazendo a cota de Cassels. Precisaremos de mais um resultado:

Proposição 5.0.1. *Seja $\mathbb{L}$ um corpo de números, então*

- *Se $x \in B_{\mathbb{L}}$, então $|N(x)| = |N(xB_{\mathbb{L}})|$;*
- *Sejam I e J ideais de $B_{\mathbb{L}}$. Se $I \subset J$, então $J \mid I$.*

Demonstração. Veja ASH, 2003 , 3.3.5; 4.2.6 . □

Corolário 5.0.1. *Se $d \in \{59, 71, 82, 107, 179, 197, 226, 332, 404\}$, então $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$ não é Euclidiano.*

Demonstração. Pelo Teorema 3.2.2, podemos procurar os primos que se ramificam dentre os divisores do discriminante. Determinadas as possibilidades para p, precisamos verificar se algum inteiro positivo $e < p$ tal que nem e nem $p - e$ é a norma de algum elemento de $B_{\mathbb{K}}$. Para isso, usamos a fatoração de $eB_{\mathbb{K}}$ (No capítulo 2 encontrarmos como fatorar).

Vejamos um exemplo, $d = 59$. Vamos mostrar que 7 não é norma de nenhum inteiro de $\mathbb{K}$. Inicialmente, precisamos fatorar $7B_{\mathbb{K}}$. Temos que

$$59 = \sqrt[3]{59}^3.$$

Por isso,

$$59B_{\mathbb{K}} = \left(\sqrt[3]{59}B_{\mathbb{K}}\right)^3.$$

Assim, 59 é um primo que se ramifica totalmente. Vamos mostrar que podemos tomar $e = 7$. O resultado decorre diretamente da fatoração de $7B_{\mathbb{K}}$. Desde que $59 \not\equiv 1 \pmod 9$, pelo Teorema 2.1.2, temos que

$$\Delta_{\mathbb{K}} = -27.59^2.$$

Como 7 não divide 59, podemos usar o Corolário 2.2.3. O que nos dá que

$$7B_{\mathbb{K}} \quad \text{é primo,}$$

pois $7 \equiv 1 \pmod 3$ e 59 não é cubo módulo 7. Agora suponha, por absurdo, que exista um inteiro de $\mathbb{K}$ tal que

$$|N(x)| = 7.$$

Pela Proposições 4.1.1 e 5.0.1

$$|N(xB_{\mathbb{K}})| = 7,$$

$$7B_{\mathbb{K}} \subset xB_{\mathbb{K}}$$

e $xB_{\mathbb{K}}$ divide $7B_{\mathbb{K}}$. Mas como $7B_{\mathbb{K}}$ é primo, temos

$$xB_{\mathbb{K}} = 7B_{\mathbb{K}}.$$

Absurdo, pois

$$|N(xB_{\mathbb{K}})| = 7, \quad \text{enquanto} \quad |N(7B_{\mathbb{K}})| = 7^3.$$

A tabela abaixo nos dá nove corpos que não são Euclidianos.

d	p	e	p-e
59	59	7	52
71	71	19	52
82	41	13	28
107	107	14	91
179	179	7	172
197	197	39	158
226	113	37	76
332	83	7	76
404	101	28	73

□

Com isso, nossa lista de possíveis corpos Euclidianos fica com vinte e dois corpos.

$$d \in \{2,\ 3,\ 5,\ 6,\ 10,\ 12,\ 17,\ 23,\ 29,\ 33,\ 41,\ 44,\ 45,\ 46,\ 53,\ 55,\ 69$$

$$99,\ 116,\ 145,\ 188,\ 575\}.$$

Podemos generalizar o Teorema anterior e limitar ainda mais a nossa lista. A prova é inteiramente análoga ao caso anterior.

Teorema 5.0.2. *Sejam p_1 e p_2, primos que se ramificam totalmente no corpo cúbico puro $\mathbb{K}$ e*

$$p_1 \not\equiv 1 \ (mod\ 3) \quad p_2 \not\equiv 1 \ (mod\ 3).$$

Se existe um inteiro positivo $e < p_1p_2$ tal que nem e nem $p_1p_2 - e$ sejam normas de elementos de $B_{\mathbb{K}}$, então $\mathbb{K}$ não é Euclidiano.

Demonstração. Pelo Lema 2.2.1 existem inteiros c_1 e c_2 tais que

$$c_1^3 \equiv e \ (\text{mod } p_1)$$

$$c_2^3 \equiv e \ (\text{mod } p_2).$$

Assim, pelo teorema do Resto Chinês existe um inteiro c tal que

$$c^3 \equiv e \ (\text{mod } p_1)$$

$$c^3 \equiv e \ (\text{mod } p_2).$$

Portanto,

$$c^3 \equiv e \ (\text{mod } p_1p_2).$$

Sejam

$$p_1B_{\mathbb{K}} = \mathfrak{P}_1^3, \qquad p_2B_{\mathbb{K}} = \mathfrak{P}_2^3.$$

Temos que $\mathfrak{P}_1$, $\mathfrak{P}_2$ são coprimos, pois são ideais primos distintos. Novamente, pelo teorema do resto chinês, temos que existe $u \in B_{\mathbb{K}}$ tal que

$$u \equiv c \ (\text{mod } \mathfrak{P}_1)$$

$$u \equiv c \ (\text{mod } \mathfrak{P}_2).$$

Assim, $\mathfrak{P}_1$ e $\mathfrak{P}_2$ dividem $u - c$, portanto $\mathfrak{P}_1\mathfrak{P}_2$ dividem $u - c$

$$u \equiv c \ (\text{mod } \mathfrak{P}_1\mathfrak{P}_2).$$

Suponha que existe

$$v \equiv u \ (\text{mod } \mathfrak{P}_1\mathfrak{P}_2); \quad |N(v)| < p_1p_2 = N(\mathfrak{P}_1\mathfrak{P}_2).$$

Agora, considere $\mathbb{L}$, o fecho normal de $\mathbb{K}/\mathbb{Q}$, então $\mathbb{L}/\mathbb{Q}$ é uma extensão de Galois finita. Seja $\sigma \in \text{Gal}(\mathbb{L}/\mathbb{Q})$

$$\sigma(B_{\mathbb{L}}) = B_{\mathbb{L}} \quad \text{pois} \ \ \mathbb{L}/\mathbb{Q} \ \ \text{é de Galois.}$$

Veja ASH, 2003 8.1.1. Temos que

$$p_1p_2B_{\mathbb{L}} = p_1p_2B_{\mathbb{K}}B_{\mathbb{L}} = \mathfrak{P}_1^3\mathfrak{P}_2^3B_{\mathbb{L}}.$$

Também,

$$p_1p_2B_{\mathbb{L}} = \sigma(p_1p_2B_{\mathbb{L}}) = \sigma\left(\left(\mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}\right)^3\right) = \left(\sigma\left(\mathfrak{P}_1\mathfrak{P}_2\right)B_{\mathbb{L}}\right)^3$$

Portanto,

$$\left(\mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}\right)^3 = \left(\sigma(\mathfrak{P}_1\mathfrak{P}_2)\,B_{\mathbb{L}}\right)^3.$$

Como $B_{\mathbb{L}}$ é domínio de Dedekind, temos fatoração única de ideais em ideais primos

$$\sigma(\mathfrak{P}_1\mathfrak{P}_2)\,B_{\mathbb{L}} = \mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}.$$

Veja ASH, 2003 3.3.1. Portanto, $\mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}$ é invariante pelo grupo de Galois de $\mathbb{L}/\mathbb{Q}$. Sejam $\sigma_1, \sigma_2, \sigma_3$ as $\mathbb{Q}-$imersões de $\mathbb{K}$ em $\mathbb{C}$

$$\sigma_i\left(v\right) = v_i,$$

onde v_1, v_2, v_3 são os conjugados de v sobre $\mathbb{Q}$. Como $\mathbb{L}/\mathbb{K}$ é uma extensão finita e separável cada σ_i pode ser estendido a uma imersão de $\sigma_i^{'}\ \mathbb{L}$ em $\mathbb{C}$, (veja ASH, 2000 seção 3.5.2). Temos que

$$v \equiv c \pmod{\mathfrak{P}_1\mathfrak{P}_2}$$

$$v - c \in \mathfrak{P}_1\mathfrak{P}_2 \subset \mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}$$

Aplicando $\sigma_i^{'}$, obtemos

$$\sigma_i^{'}(v-c) = \sigma_i^{'}(v) - c \in \sigma_i^{'}(\mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}) = \mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}$$

$$v_i \equiv c \pmod{\mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}}.$$

Com isso, podemos calcular a norma

$$N_{\mathbb{K}/\mathbb{Q}}(v) = v_1v_2v_3 \equiv c^3 \pmod{\mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}}}.$$

Agora, podemos voltar a trabalhar nos inteiros

$$N_{\mathbb{K}/\mathbb{Q}}(v) \equiv c^3 \pmod{p_1p_2}.$$

Já que

$$\mathfrak{P}_1\mathfrak{P}_2B_{\mathbb{L}} \cap \mathbb{Z} = p_1p_2\mathbb{Z}.$$

Assim, $N_{\mathbb{K}/\mathbb{Q}}(v) = e$ ou $N_{\mathbb{K}/\mathbb{Q}}(v) = e - p_1p_2$. Mas nem e, nem $p_1p_2 - e$ são normas de elementos de $B_{\mathbb{L}}$, absurdo.

Suponha que $B_{\mathbb{K}}$ seja Euclidiano, portanto domínio de ideais principais, assim

$$\mathfrak{P}_1\mathfrak{P}_2 = bB_{\mathbb{K}},$$

com $b \in B_{\mathbb{K}}$. Vamos mostrar que não conseguimos encontrar $t, r \in B_{\mathbb{K}}$ tais que

$$u = tb + r$$

$$|N(b)| < |N(r)\,|.$$

De fato,

$$r \equiv u \pmod{\mathfrak{P}_1\mathfrak{P}_2}.$$

O que garante que

$$|N(r)| \geq p_1p_2 = N(\mathfrak{P}_1\mathfrak{P}_2) = |N(b)|\,.$$

Portanto $\mathbb{K}$ não é Euclidiano. □

Com esse teorema conseguimos eliminar mais dez corpos.

Corolário 5.0.2. *Se* $d \in \{23,\ 29,\ 33,\ 41,\ 46,\ 69,\ 116,\ 145,\ 188,\ 575\}$*, então* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$ *não é Euclidiano.*

Demonstração. A tabela abaixo nos dá para cada d os valores para p_1, p_2, e que satisfazem as condições do Teorema 5.0.2. Construímos a tabela de maneira análoga a do Corolário 5.0.1, procuramos os primos que se ramificam entre os divisores do discriminante e para verificar se e é norma de algum inteiro de $\mathbb{K}$, olhamos para a fatoração de $eB_{\mathbb{K}}$.

d	p_1	p_2	e	p-e
23	3	23	13	56
29	3	29	26	61
33	3	11	7	26
41	3	41	19	104
46	2	23	7	39
69	3	23	26	43
116	2	29	21	37
145	5	29	26	119
188	2	47	37	57
575	5	23	37	78

□

Assim, nossa lista de possíveis corpos Euclidianos fica com doze elementos

$$d \in \{2,\ 3,\ 5,\ 6,\ 10,\ 12,\ 17,\ 44,\ 45,\ 53,\ 55,\ 99\}.$$

Usando esse método ainda podemos excluir mais um elemento da nossa lista.

Proposição 5.0.2. $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{53}\right)$ *não é Euclidiano.*

Demonstração. Existe apenas um ideal com norma 53. Suponha que o ideal J possui norma 53. Então, $53B_{\mathbb{K}} \subset J$, Proposição 4.1.1. Assim, concluimos que J divide $53B_{\mathbb{K}}$,

Proposição 5.0.1. Mas $53 \equiv 2 \pmod 3$, assim a fatoração em primos de $53B_{\mathbb{K}}$ é

$$53B_{\mathbb{K}} = \mathfrak{P}\mathfrak{P}_1; \quad N(\mathfrak{P}) = 53; \quad N(\mathfrak{P}_1) = 53^2.$$

Portanto, há apenas uma possibilidade para J,

$$J = \mathfrak{P}.$$

Analogamente, existe um único ideal de norma 2 (veja o Corolário 2.2.2)

$$2B_{\mathbb{K}} = \mathfrak{Q}\mathfrak{Q}_1; \quad N(\mathfrak{Q}) = 2; \quad N(\mathfrak{Q}_1) = 2^2.$$

Temos que $\mathfrak{Q}$ é o único ideal com norma 2. Pelo Teorema do Resto Chinês, exite $u \in B_{\mathbb{K}}$, tal que

$$u \equiv -25 \pmod{\mathfrak{P}}; \quad u \equiv 1 \pmod{\mathfrak{Q}}.$$

Como $53 \not\equiv 1 \pmod 3$ e 53 se ramifica totalmente em $\mathbb{K}$, então

$$N(u) \equiv (-25)^3 \equiv -10 \pmod{53}.$$

Veja a demonstração dos Teoremas 5.0.1 e 5.0.2. Suponha que $|N(u)| < 106$, então

$$N(u) \in \{-63,\ -10,\ 43,\ 96\}.$$

Mas 43 e -63 não são normas de elementos de $B_{\mathbb{K}}$. De fato, $43 \equiv 1 \pmod 3$ e 53 não é resíduo cúbico módulo 43, portanto $43B_{\mathbb{K}}$ é um ideal primo (analogamente $7B_{\mathbb{K}}$ é primo). Se $N(u) = 43$, então $43B_{\mathbb{K}} \subset uB_{\mathbb{K}}$ (Proposição 4.1.1). Assim , $uB_{\mathbb{K}}$ divide $43B_{\mathbb{K}}$ pela Proposição 5.0.1. Logo

$$uB_{\mathbb{K}} = 43B_{\mathbb{K}}.$$

Absurdo, pois

$$N(43B_{\mathbb{K}}) = 43^3.$$

Analogamente, se

$$N(u) = 63,$$

então

$$uB_{\mathbb{K}} \mid (7B_{\mathbb{K}})(3B_{\mathbb{K}})^2.$$

Como $(7B_{\mathbb{K}})$ é primo, se

$$(7B_{\mathbb{K}}) \mid uB_{\mathbb{K}},$$

então

$$7^3 \mid N(u) = 63.$$

Por outro lado, se

$$(7B_{\mathbb{K}}) \nmid (uB_{\mathbb{K}}),$$

então

$$7 \nmid N(u) = 63,$$

que também não acontece. Por isso, 63 e 43 não são normas de elementos de $B_{\mathbb{K}}$. Como

$$u \equiv 1 \pmod{\mathfrak{Q}}, \quad N(u) \neq 10,\ 96,$$

pois os elementos x de $B_{\mathbb{K}}$ que possuem norma 10 ou 96, estão em $\mathfrak{Q}$. De fato, se $N(u) = 10$, então pelas Proposições 4.1.1 e 5.0.1

$$uB_{\mathbb{K}} \mid 10B_{\mathbb{K}} = 2B_{\mathbb{K}}5B_{\mathbb{K}}.$$

Assim $\mathfrak{Q}_1$ não pode aparecer na fatoração de $uB_{\mathbb{K}}$, pois $N(u)$ não é divisível por 4. Dessa forma, $\mathfrak{Q}$ divide $uB_{\mathbb{K}}$, pois se nem $\mathfrak{Q}$ nem $\mathfrak{Q}_1$ dividissem $uB_{\mathbb{K}}$, teríamos que

$$2 \nmid N(u) = 10.$$

Portanto, pela Proposição 5.0.1

$$\mathfrak{Q} \mid uB_{\mathbb{K}} \subset \mathfrak{Q}.$$

Analogamente, se $N(v) = 96$

$$\mathfrak{Q} \mid vB_{\mathbb{K}} \subset \mathfrak{Q}.$$

Agora suponha que $\mathbb{K}$ seja Euclidiano, então $B_{\mathbb{K}}$ é domínio de fatoração de ideais principais.

$$bB_{\mathbb{K}} = \mathfrak{P}\mathfrak{Q}.$$

Assim, se $a \equiv u \pmod{b}$, então $|N(a)| \geq |N(b)| = 106$. Dividindo u por b, obtemos

$$u = qb + r.$$

Como

$$r \equiv u \pmod{b},$$

então

$$|N(r)| \geq |N(b)| = 106.$$

Portanto, $\mathbb{K}$ não é Euclidiano. □

Concluimos esse capítulo com onze possíveis corpos Euclidianos:

$$d \in \{2,\ 3,\ 5,\ 6,\ 10,\ 12,\ 17,\ 44,\ 45,\ 55,\ 99\}.$$

6 Outras Técnicas e Corpos Euclidianos

Nesse capítulo, finalmente, concluiremos o resultado de Cioffari sobre corpos cúbicos puros Euclidianos. Iremos explorar a redução módulo o ideal gerado por 2, as classes ficam bem definidas em termos da base inteira. Também usaremos o valor absoluto e mostraremos os fundamentos técnicos do algoritmo implementado por Cioffari para mostrar que os corpos são Euclidianos.

6.1 Redução Módulo 2

Proposição 6.1.1. *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt[3]{d})$*, d ímpar livre de cubos. Se* $\alpha = \sqrt[3]{d}$*, então*

$$\{0,\ 1,\ \alpha,\ \alpha^2,\ 1+\alpha,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2\},$$

é um sistema completo de resíduos módulo 2*. Além disso, os elementos congruentes a* 1*,* α*,* α^2 *possuem norma ímpar, enquanto os demais possuem norma par.*

Demonstração. Temos uma fórmula para a norma e já determinamos as bases inteiras no capítulos 2.

$$N\left(x + y\alpha + z\alpha^2\right) = x^3 + dy^3 + d^2z^3 - 3dxyz.$$

□

O resultado a seguir é mais um exemplo que mostra o quanto as unidades estão relacionadas com a propriedade euclidiana.

Proposição 6.1.2. *Sejam* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$*, d livre de cubos e* ϵ *unidade fundamental de* $\mathbb{K}$*. Suponha que d é ímpar e que o número de classes,* $h_{\mathbb{K}} = 1$ *e que exista um primo ímpar, p, que se ramifica totalmente* ($p \neq d$)*, então*

$$\epsilon \equiv 1 \ (mod\ 2).$$

Demonstração. Como p se ramifica totalmente,

$$pB_{\mathbb{K}} = \mathfrak{P}^3.$$

Desde que o número de classes é 1, temos que $B_{\mathbb{K}}$ é domínio de ideais principais. Por isso

$$\mathfrak{P} = cB_{\mathbb{K}}, \quad c \in B_{\mathbb{K}}.$$

Então c^3 é gerador de $pB_{\mathbb{K}}$. Daí, c^3 e p são associados

$$c^3 = pu,$$

com u unidade. Mas, pelo Teorema das unidades de Dirichet (Teorema 3.2.1, Corolário 3.2.1), temos que $(r + s - 1 = 1)$ e toda unidade é da forma

$$\zeta\epsilon^m,$$

com ζ raiz da unidade. Mas as únicas raízes da unidade em K são ± 1, pois se ζ é raiz primitiva n-ésima da unidade, então o grau do polinômio mínimo de ζ é $\varphi(n)$, a função de Euler (veja ENDLER, 1986 página 32, Teorema 3.6). Se

$$\zeta \neq \pm 1 \Rightarrow \zeta \notin \mathbb{Q},$$

então

$$\varphi(n) = 3.$$

Mas, $\varphi(n) = 3$ não possui solução, pois se

$$\text{mdc}(a, n) = 1 \Rightarrow \text{mdc}(n - a, n) = 1.$$

± 1 são cubos, por isso podem ser absolvidos em c^3, podemos supor

$$c^3 = p\epsilon^{-1}, \quad c^3 = p\epsilon.$$

Pois se $m = 0$, então

$$\sqrt[3]{p} \in \mathbb{Q}\left(\sqrt[3]{d}\right) \Rightarrow \mathbb{Q}(\sqrt[3]{p}) = \mathbb{Q}(\sqrt[3]{d}),$$

absurdo, veja o discriminante. Trocando, se necessário, ϵ por ϵ^{-1}.

$$c^3 = p\epsilon \Rightarrow c^3 \equiv \epsilon \pmod 2.$$

Mas como c possui norma ímpar, temos

$$c \equiv 1,\ \alpha \quad \text{ou} \quad \alpha^2 (\text{mod } 2).$$

Assim, de qualquer forma

$$c^3 \equiv 1(\text{mod } 2) \Rightarrow \epsilon \equiv 1(\text{mod } 2) \Rightarrow \epsilon, -\epsilon, \epsilon^{-1}, -\epsilon^{-1} \equiv 1(\text{mod } 2).$$

□

Com a notação da Proposição 6.1.2

Corolário 6.1.1. *Se* $d = 5,\ 45,\ 55,\ 99$*, então*

$$1 \equiv \epsilon \ (mod\ 2),$$

Além disso, para qualquer unidade u

$$1 \equiv u \ (mod\ 2).$$

Demonstração. Já vimos, no capítulo 3, que os quatros corpos possuem número de classes 1. Pelo capítulo 2, corolário 2.2.1, o primo 5 se ramifica totalmente para $d = 5,\ 45,\ 55$. O primo 11 se ramifica totalmente para $d = 99$. Portanto, pela Proposição 6.1.2

$$1 \equiv \epsilon \ (\text{mod } 2).$$

Mas toda unidade é da forma

$$\pm\epsilon^m \equiv 1 \ (\text{mod } 2).$$

□

Dois elementos que geram o mesmo ideal diferem por unidade, assim são congruentes módulo 2. Essa proposição nos ajudará a descartar mais quatros corpos da nossa lista.

Teorema 6.1.1. *Se* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{5}\right)$, $\mathbb{Q}\left(\sqrt[3]{45}\right)$, $\mathbb{Q}\left(\sqrt[3]{55}\right)$, $\mathbb{Q}\left(\sqrt[3]{99}\right)$*, então* $\mathbb{K}$ *não é Euclidiano.*

Demonstração. Vejamos inicialmente $\mathbb{Q}\left(\sqrt[3]{5}\right)$. A ideia é usar módulo o ideal $2B_{\mathbb{K}}$, que possui norma 8. Vamos precisar determinar todos os ideais com norma menor que 8, para isso usamos os métodos do Corolário 5.0.1. Obtemos

$$\mathfrak{P}_2,\ \mathfrak{P}_3,\ \mathfrak{P}_2^2,\ \mathfrak{P}_4,\ \mathfrak{P}_5,\ \mathfrak{P}_2\mathfrak{P}_3,$$

tais que

$$2B_{\mathbb{K}} = \mathfrak{P}_2\mathfrak{P}_4, \quad N(\mathfrak{P}_2) = 2, \quad N(\mathfrak{P}_4) = 4;$$
$$3B_{\mathbb{K}} = \mathfrak{P}_3^3, \quad N(\mathfrak{P}_3) = 3;$$
$$5B_{\mathbb{K}} = \mathfrak{P}_5^3, \quad N(\mathfrak{P}_5) = 5.$$

Esses ideais estão num domínio de ideais principais, assim iremos exibir geradores para cada um deles.

De fato,

$$2 = 3^3 - \sqrt[3]{25}^3 = \left(3 - \sqrt[3]{25}\right)\left(3^2 + 3\sqrt[3]{25} + \sqrt[3]{5^4}\right).$$

Além disso,

$$\left|N\left(3 - \sqrt[3]{25}\right)\right| = 2 \Rightarrow \mathfrak{P}_2 = \left(3 - \sqrt[3]{25}\right) \equiv 1 + \theta^2 \ (\text{mod } 2);$$

$$\left|N\left(3^2+3\sqrt[3]{25}+\sqrt[3]{5^4}\right)\right|=4\Rightarrow\mathfrak{P}_4=\left(3^2+3\sqrt[3]{25}+\sqrt[3]{5^4}\right)\equiv 1+\theta+\theta^2\ (\text{mod } 2).$$

Fatoração do 3

$$3=2^3-\sqrt[3]{5}^3=\left(2-\sqrt[3]{5}\right)\left(2+2\sqrt[3]{5}+\sqrt[3]{5^2}\right).$$

De forma que

$$\left|N\left(2-\sqrt[3]{5}\right)\right|=3\Rightarrow\mathfrak{P}_3=\left(2-\sqrt[3]{5}\right)\equiv\theta\ (\text{mod } 2).$$

$$\mathfrak{P}_5=\left(\sqrt[3]{5}\right)\equiv\theta\ (\text{mod } 2).$$

$$\mathfrak{P}_2^2=\left(3-\sqrt[3]{25}\right)^2=\left(9+5\sqrt[3]{5}-6\sqrt[3]{25}\right)\equiv 1+\theta\ (\text{mod } 2).$$

$$\mathfrak{P}_2\mathfrak{P}_3=\left(6-5-2\sqrt[3]{25}-3\sqrt[3]{5}\right)\equiv 1+\theta(\text{mod } 2).$$

Portanto, pela Proposição 6.1.2 nenhum desses seis ideais possui um gerador que seja congruente a $\theta^2(\text{mod } 2)$, assim dividindo θ^2 por 2 nós temos:

$$\theta^2=2t+a\Rightarrow|N(aB_{\mathbb{K}})|\geq 8.$$

□

Esse método pode ser usados nos outros casos $d=45,\ 55,\ 99$. O método exemplificado no caso $d=5$ consiste em :

1. Encontrar todos os ideais com norma menor que oito;
2. Encontrar geradores para os ideais de norma menor que oito;
3. Os geradores dos ideais listados não formam um sistema completo de resíduos módulo $2B_{\mathbb{K}}$. Escolha uma das classes módulo $2B_{\mathbb{K}}$ que não seja atingida por nenhum dos geradores listados, pelo Corolário 6.0.1, sempre que dividirmos um representante dessa classe por 2, o resto terá norma maior ou igual a oito.

Com isso, nossa lista de possíveis corpos Euclidianos fica com sete elementos

$$d\in\{2,\ 3,\ 6,\ 10,\ 12,\ 17,\ 44\}.$$

Teorema 6.1.2. $\mathbb{Q}(\sqrt[3]{6})$ *não é Euclidiano.*

Demonstração. Seja $\alpha=\sqrt[3]{6}$. Temos pelo Teorema 2.1.2 que

$$B_{\mathbb{K}}=\mathbb{Z}[\alpha].$$

Assim, o conjunto

$$\{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\},$$

um sistema completo de resíduos módulo $2B_{\mathbb{K}}$. Além disso,

$$N\left(x+y\alpha+z\alpha^2\right) = x^3+6y^3+36z^3-18xyz.$$

Usamos o software Sage para encontrar a unidade fundamental de $B_{\mathbb{K}}$

$$\epsilon = 1-6\alpha+3\alpha^2.$$

Vamos mostrar que se

$$\alpha+\alpha^2 = 2t+r \Rightarrow |N(r)| \geq N(2) = 8.$$

Se

$$\alpha+\alpha^2 \equiv a \pmod 2,$$

então

$$a = 2x+(2y+1)\alpha+(2y+1)\alpha^2.$$

Dessa forma,

$$N(a) = N\left(2x+(2y+1)\alpha+(2y+1)\alpha^2\right)$$
$$= (2x)^3+6(2y+1)^3+6^2(2z+1)^3-18(2x)(2y+1)(2z+1).$$

Portanto,

$$N(a) \equiv 2 \pmod 4.$$

Vejamos os elementos u que possuem norma ± 2. Se

$$N(u) = \pm 2 \Rightarrow N(uB_{\mathbb{K}}) = 2,$$

assim

$$2B_{\mathbb{K}} \subset uB_{\mathbb{K}}.$$

Portanto,

$$uB_{\mathbb{K}} \mid 2B_{\mathbb{K}}.$$

Mas

$$2B_{\mathbb{K}} = (2-\alpha)\left(\alpha^2+2\alpha+4\right)B_{\mathbb{K}}.$$

Por isso,

$$uB_{\mathbb{K}} = (2-\alpha)B_{\mathbb{K}}.$$

Portanto, o único ideal de norma 2 é gerado por $2-\alpha$, logo os elementos com norma ± 2 são os associados de $2-\alpha$

$$u = (2-\alpha)\epsilon^m.$$

Como

$$\epsilon \equiv 1 + \alpha^2 \pmod 2.$$

Temos que

$$\epsilon^m \equiv 1 + m\alpha^2 \pmod 2.$$

Logo,

$$u \equiv (2 - \alpha)\left(1 + m\alpha^2\right) \equiv \alpha \pmod 2.$$

Agora vejamos os elementos u com norma ± 6. Se

$$N(u) = \pm 6 \Rightarrow 6B_{\mathbb{K}} \subset uB_{\mathbb{K}}.$$

Portanto,

$$uB_{\mathbb{K}} \mid 6B_{\mathbb{K}} = \left(\sqrt[3]{6}\right)^3.$$

Logo,

$$u = \sqrt[3]{6}\epsilon^m.$$

Assim,

$$u \equiv \sqrt[3]{6}\left(1 + m\alpha^2\right) \equiv \alpha \pmod 2.$$

Se

$$a \equiv \alpha \ + \alpha^2 (\mathrm{mod}\ 2),$$

então

$$N(u) \equiv 2 \pmod 4; \quad |N(u)| > 6.$$

Portanto,

$$|N(u)| \geq 8.$$

Se dividirmos $\alpha + \alpha^2$ por 2

$$\alpha + \alpha^2 = 2t + a \Rightarrow |N(a)| \geq 8.$$

Logo $\mathbb{K}$ não é Euclidiano. □

Neste momento, a nossa lista de possíveis corpos Euclidianos fica com apenas seis elementos.

$$\{2, 3, 10, 12, 17, 44\}.$$

6.2 Usando Valores Absolutos

Nessa seção descartaremos mais três corpos de nossa lista $d \in \{12,\ 17,\ 44\}$. A técnica utilizada mais uma vez envolve as unidades. Usaremos as unidades para limitar os valor absoluto do coeficientes em termos da base inteira das translações inteiras de um elemento especial x de $\mathbb{Q}(\sqrt[3]{d})$.

Proposição 6.2.1. *Seja* $\{1,\ \theta,\ \varphi\}$ *base inteira de* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$. *Dado* $x \in \mathbb{K}$, *satisfazendo:*

1. $x\epsilon \equiv \pm x\ (mod\ B)$;
2. *Suponha que exista* $y \equiv x\ (mod\ B)$ *com* $|N(y)| < 1$.

d	θ	φ
12	$\sqrt[3]{12}$	$\sqrt[3]{18}$
17	$\sqrt[3]{17}$	$\frac{1-\theta+\theta^2}{3}$
44	$\sqrt[3]{44}$	$\frac{-1+\theta+\frac{\theta^2}{2}}{3}$

Então existem $z = r + s\theta + t\varphi$ *e inteiros positivos* $a,\ b,\ c$, *tais que*

1. $z \equiv \pm x\ (mod\ B)$;
2. $|N(z)| < 1$;
3. $|r| < a,\ |s| < b,\ |t| < c$.

Demonstração. Vejamos inicialmente a demonstração para $d = 12$. Usando software SAGE encontramos a unidade fundamental de $\mathbb{Q}\left(\sqrt[3]{12}\right)$

$$1 + 3\sqrt[3]{12} - 3\sqrt[3]{18} < 0,006.$$

Assim, existe inteiro n de forma que

$$0,006 < |y\epsilon^n| < 1.$$

Podemos ter $z = y\epsilon^n$. De fato,

$$z \equiv \pm y \equiv \pm x\ (\text{mod}\ B).$$

Como $|N(\epsilon)| = 1$, já que ϵ é unidade, temos

$$|N(z)| = |N(y)| < 1.$$

Assim, σ' e σ'' as imersões de $\mathbb{K}$ em $\mathbb{C}$ que mandam $\sqrt[3]{12}$ em $\sqrt[3]{12}\omega$ e $\sqrt[3]{12}\omega^2$, respectivamente, onde $\omega = e^{\frac{2\pi}{3}}$. Dado u, consideramos $u' = \sigma'(u)$ e $u'' = \sigma''(u)$ os conjugados de u.

$$|N(z)| = |z||z'||z''| = |z||z'|^2 < 1.$$

Assim,

$$|z'|^2 < \frac{1}{|z|} < \frac{1}{0,006} \quad \text{pois} \quad |z| > 0,006.$$

Portanto,

$$|z'| < \sqrt{\frac{1}{0,006}} < 13.$$

Pela desigualdade tringular,

$$|z - z'| \leq |z| + |z'| < 1 + 13 = 14.$$

Assim,

$$|Re\left(z - z'\right)| \leq |z - z'| < 14;$$
$$|Im\left(z - z'\right)| \leq |z - z'| < 14.$$

Com essas desigualdes podemos limitar o z. De fato,

$$z' = r + s\sqrt[3]{12}\omega + t\sqrt[3]{18}\omega^2.$$

Desde que $\sqrt[3]{18} = \frac{\sqrt[3]{12}^2}{2}$, temos que

$$\begin{array}{rcccccc} -10 & < & \sqrt[3]{12}s & + & \sqrt[3]{18}t & < & 10 \\ -10\sqrt{3} & < & \sqrt[3]{12}s & - & \sqrt[3]{18}t & < & 10\sqrt{3} \end{array}$$

$$\left(\sqrt[3]{12}s + \sqrt[3]{18}t\right) + \left(\sqrt[3]{12}s - \sqrt[3]{18}t\right) < 10 + 10\sqrt{3}.$$

Somando as desigualdades, temos

$$s < \frac{10 + 10\sqrt{3}}{2\sqrt[3]{12}} < 6.$$

Analogamente,

$$s > -\frac{10 + 10\sqrt{3}}{2\sqrt[3]{12}} > -6.$$

Agora subtraindo as desigualdes, obtemos

$$t < \frac{10 + 10\sqrt{3}}{2\sqrt[3]{18}} < 6;$$

$$t > -\frac{10 + 10\sqrt{3}}{2\sqrt[3]{18}} > -6.$$

Podemos limitar também o r, usando novamente a desigualdade triangular

$$|r| = |r + \sqrt[3]{12}s + \sqrt[3]{18}t - \left(\sqrt[3]{12}s + \sqrt[3]{18}t\right)| < |z| + |\sqrt[3]{12}s + \sqrt[3]{18}t| < 1 + 10 = 11.$$

Agora, vamos repetir o mesmo procedimento para limitar os coeficientes de z quando $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{17}\right)$. No Sage, encontramos a unidade fundamental de $\mathbb{Q}\left(\sqrt[3]{17}\right)$:

$$\epsilon = 7\sqrt[3]{17} - 18, \quad \text{ou seja} \quad |\epsilon| > 0,001.$$

Assim existe inteiro n de forma que

$$0,001 < |y\epsilon^n| < 1.$$

Podemos ter $z = y\epsilon^n$, de fato

$$z \equiv \pm y \equiv \pm x \pmod{B}.$$

Como $|N(\epsilon)| = 1$, já que ϵ é unidade, temos

$$|N(z)| = |N(y)| < 1.$$

Assim, $\sigma^{'}$ e $\sigma^{''}$ as imersões de $\mathbb{K}$ em $\mathbb{C}$ que mandam $\sqrt[3]{17}$ em $\sqrt[3]{17}\omega$ e $\sqrt[3]{17}\omega^2$, respectivamente, onde $\omega = e^{\frac{2\pi}{3}}$ Dado u, consideramos $u^{'} = \sigma^{'}(u)$ e $u^{''} = \sigma^{''}(u)$ os conjugados de u.

$$|N(z)| = |z||z^{'}||z^{''}| = |z||z^{'}|^2 < 1.$$

Assim,

$$|z^{'}|^2 < \frac{1}{|z|} < \frac{1}{0,001}, \quad \text{pois} \quad |z| > 0,001.$$

Portanto,

$$|z^{'}| < \sqrt{\frac{1}{0,001}} < 32.$$

Pela desigualdade tringular,

$$|z - z^{'}| \leq |z| + |z^{'}| < 1 + 32 = 33.$$

Portanto,

$$|Re\left(z - z^{'}\right)| \leq |z - z^{'}| < 33;$$
$$|Im\left(z - z^{'}\right)| \leq |z - z^{'}| < 33.$$

Seja

$$z = r + s\sqrt[3]{17} + t\frac{1 - \sqrt[3]{17} + \sqrt[3]{17}^2}{3}.$$

Assim, como $\omega^2 = \overline{\omega} = \frac{\left(-1-\sqrt{3}i\right)}{2}$, temos

$$z^{'} = r + s\frac{\left(-1 + \sqrt{3}i\right)}{2}\sqrt[3]{17} + t\frac{\left(1 - \frac{\left(-1+\sqrt{3}i\right)}{2}\sqrt[3]{17} + \frac{\left(-1-\sqrt{3}i\right)}{2}\sqrt[3]{17}^2\right)}{3}.$$

Com isso, podemos calcular as partes real e imaginária de $z - z^{'}$

$$|Re\left(z - z^{'}\right)| = |s\frac{3\sqrt[3]{17}}{2} + t\frac{\left(-3\sqrt[3]{17} + 3\sqrt[3]{17}^2\right)}{6}|;$$

$$|Im\left(z - z^{'}\right)| = |s\frac{\sqrt[3]{17}\sqrt{3}}{2} + t\frac{\sqrt[3]{17}\sqrt{3} - \sqrt[3]{17}^2\sqrt{3}}{6}|.$$

Daí,

$$-198 < 9\sqrt[3]{17}s + \left(-3\sqrt[3]{17} + 3\sqrt[3]{17}^2\right)t < 198;$$

$$-198\sqrt{3} < 9\sqrt[3]{17}s + \left(3\sqrt[3]{17} - 3\sqrt[3]{17}^2\right)t < 198\sqrt{3}.$$

Somando as inequações

$$\frac{-198 - 198\sqrt{3}}{18\sqrt[3]{17}} < s < \frac{198 + 198\sqrt{3}}{18\sqrt[3]{17}}.$$

Obtemos

$$|s| < 12.$$

Por outro lado,

$$|t| < \frac{198 + 198\sqrt{3}}{-6\sqrt[3]{17} + 6\sqrt[3]{17}^2} < 23.$$

Agora usamos os limites para $s,\ t$ para limitar o r

$$|r| < |z| + |s\sqrt[3]{17}| + |t\frac{1 - \sqrt[3]{17} + \sqrt[3]{17}^2}{3}| < 1 + 31 + 39 = 81.$$

Agora, vejamos o caso $\mathbb{Q}\left(\sqrt[3]{44}\right)$. Usando o SAGE novamente, encontramos a unidade fundamental

$$\epsilon = \frac{17}{6}\sqrt[3]{44}^2 + \frac{2}{3}\sqrt[3]{44} - \frac{113}{3},\ 1 > |\epsilon| > 0,0002.$$

Assim existe inteiro n de forma que

$$0,0002 < |y\epsilon^n| < 1.$$

Podemos ter $z = y\epsilon^n$. De fato,

$$z \equiv \pm y \equiv \pm x \pmod{B_{\mathrm{K}}}.$$

Como $|N(\epsilon)| = 1$, já que ϵ é unidade, temos

$$|N(z)| = |N(y)| < 1.$$

Sejam $\sigma^{'}$ e $\sigma^{''}$ as imersões de $\mathbb{K}$ em $\mathbb{C}$ que mandam $\sqrt[3]{44}$ em $\sqrt[3]{44}\omega$ e $\sqrt[3]{44}\omega^2$, respectivamente, onde $\omega = e^{\frac{2\pi}{3}}$. Dado u, consideramos $u^{'} = \sigma^{'}(u)$ e $u^{''} = \sigma^{''}(u)$ os conjugados de u.

$$|N(z)| = |z||z^{'}||z^{''}| = |z||z^{'}|^2 < 1.$$

Assim,

$$|z^{'}|^2 < \frac{1}{|z|} < \frac{1}{0,0002} \quad \text{pois} \quad |z| > 0,0002.$$

Portanto,

$$|z^{'}| < \sqrt{\frac{1}{0,0002}} < 71.$$

Pela desigualdade tringular,

$$|z - z^{'}| \leq |z| + |z^{'}| < 1 + 71 = 72.$$

Assim,

$$|Re\left(z - z^{'}\right)| \leq |z - z^{'}| < 72;$$
$$|Im\left(z - z^{'}\right)| \leq |z - z^{'}| < 72.$$

Seja

$$z = r + s\sqrt[3]{44} + t\frac{-1 + \sqrt[3]{44} + \frac{\sqrt[3]{44}^2}{2}}{3}.$$

Assim, como $\omega^2 = \overline{\omega} = \frac{\left(-1-\sqrt{3}i\right)}{2}$, temos

$$z^{'} = r + s\frac{\left(-1+\sqrt{3}i\right)}{2}\sqrt[3]{44} + t\frac{\left(-1 + \frac{\left(-1+\sqrt{3}i\right)}{2}\sqrt[3]{44} + \frac{\left(-1-\sqrt{3}i\right)\sqrt[3]{44}^2}{4}\right)}{3}.$$

Com isso, podemos calcular as partes real e imaginária de $z - z^{'}$

$$|Re\left(z - z^{'}\right)| = |\frac{6\sqrt[3]{44}}{4}s + \frac{\left(2\sqrt[3]{44} + \sqrt[3]{44}^2\right)}{4}t|;$$

$$|Im\left(z - z^{'}\right)| = |\frac{6\sqrt{3}\sqrt[3]{44}}{12}s + \frac{2\sqrt{3}\sqrt[3]{44} - \sqrt{3}\sqrt[3]{44}^2}{12}t|.$$

Portanto, temos as seguintes desigualdades

$$|6\sqrt[3]{44}s + \left(2\sqrt[3]{44} + \sqrt[3]{44}^2\right)t| < 288;$$
$$|6\sqrt[3]{44}s + \left(2\sqrt[3]{44} - \sqrt[3]{44}^2\right)t| < 288\sqrt{3}.$$

$$-288 < 6\sqrt[3]{44}s + \left(2\sqrt[3]{44} + \sqrt[3]{44}^2\right)t < 288$$
$$-288\sqrt{3} < 6\sqrt[3]{44}s + \left(2\sqrt[3]{44} - \sqrt[3]{44}^2\right)t| < 288\sqrt{3}.$$

Subtraindo as duas desigualdades, obtemos

$$|t| < \frac{288\sqrt{3} + 288}{2\sqrt[3]{44}^2} < 32.$$

Temos que

$$|6\sqrt[3]{44}s| < |6\sqrt[3]{44}s + \left(2\sqrt[3]{44} + \sqrt[3]{44}^2\right)t - \left(2\sqrt[3]{44} + \sqrt[3]{44}^2\right)t|$$
$$< |6\sqrt[3]{44}s + \left(2\sqrt[3]{44} + \sqrt[3]{44}^2\right)t| + |\left(2\sqrt[3]{44} + \sqrt[3]{44}^2\right)t|$$
$$< 288 + 32\left(2\sqrt[3]{44} + \sqrt[3]{44}^2\right) < 913.$$

Assim,

$$|s| < \frac{913}{6\sqrt[3]{44}} < 44.$$

Agora com os limites de $s,\ t$ consiguimos limitar r

$$|r| = |r + s\sqrt[3]{44} + t\frac{-1 + \sqrt[3]{44} + \frac{\sqrt[3]{44}^2}{2}}{3} - s\sqrt[3]{44} - t\frac{-1 + \sqrt[3]{44} + \frac{\sqrt[3]{44}^2}{2}}{3}|,$$
$$1 + |s\sqrt[3]{44}| + |t\frac{-1 + \sqrt[3]{44} + \frac{\sqrt[3]{44}^2}{2}}{3}| < 250.$$

□

Usaremos, esse resultado para descartar mais três corpos da nossa lista. Abaixo segui uma tabela com os limites que temos de verificar.

Proposição 6.2.2. $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{12}\right)$, $\mathbb{Q}\left(\sqrt[3]{17}\right)$ *e* $\mathbb{Q}\left(\sqrt[3]{44}\right)$ *não são Euclidianos.*

Demonstração. A tabela, fornece para cada d, o valor de x que satisfaz a Proposição 6.2.1. Verificamos todos as translações inteiras de x limitadas Pela Proposição 6.2.1, nenhuma delas possui norma menor que 1. Isso mostra que $\mathbb{K}$ não é Euclidiano, pela Proposição 3.1.1.

d	x
12	$(\frac{2}{3} + \frac{5}{6}\theta + \frac{4}{9}\varphi)$
17	$(-\frac{94}{257} + \frac{233}{514}\theta - \frac{19}{1028}\varphi)$
44	$(\frac{12}{5+2\theta+\varphi})$

□

Portanto, agora restam apenas três corpos na nossa lista :

$$d \in \{2,\ 3,\ 10\}.$$

6.3 Corpos Cúbicos Puros que são Euclidianos

Nesta seção estudaremos os três corpos cúbicos puros satisfazendo o limite de Cassels que restaram na nossa lista e mostraremos que, de fato, são Euclidianos. Daremos os resultados que tornam possível a implementação de um algoritmo. Usaremos basicamente as bases inteiras e uma equivalência de ser Euclidiano, Proposição 3.1.1.

Teorema 6.3.1. *Seja* $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{d}\right)$, *d livre de cubos, então* $\mathbb{K}$ *é Euclidiano, se e somente*

$$\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{2}\right),\ \mathbb{Q}\left(\sqrt[3]{3}\right), \quad \textit{ou} \quad \mathbb{Q}\left(\sqrt[3]{10}\right).$$

Demonstração. Vejamos inicialmente o caso $d = 2,\ 3.$ que possuem bases inteiras

$$\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}, \quad \{1, \sqrt[3]{3}, \sqrt[3]{3}^2\},$$

respectivamente. Nós iremos analizar o caso $d = 10$ ($d \equiv \pm 1 \pmod 9$) separadamente, pois $\{1, \sqrt[3]{10}, \sqrt[3]{10}^2\}$ não é base inteira de $\mathbb{Q}\left(\sqrt[3]{10}\right)$.

Nós associaremos a cada inteiro algébrico em $\mathbb{Q}\left(\sqrt[3]{d}\right)$ um ponto do $\mathbb{R}^3$ da seguinte forma:

$$x + y\sqrt[3]{d} + z\sqrt[3]{d}^2 \longrightarrow (x,\ y,\ z) \in \mathbb{Z}^3.$$

Nós definimos o cubo fundamental como sendo

$$C = \{(x,\ y,\ z)\,|\,(x,\ y,\ z) \in \mathbb{R}^3 \quad 0 \leq x,\ y,\ z < 1\}.$$

Definimos a norma em $\mathbb{R}^3$ como a extensão da norma em $\mathbb{Q}^3$

$$N(x,\ y,\ z) = N\left(x + y\sqrt[3]{d} + z\sqrt[3]{d}\right) = x^3 + dy^3 + d^2z^3 - 3xyzd.$$

Assim, mostrar que $\mathbb{K}$ é Euclidiano é equivalente a mostrar que cada ponto de C pode ser transladado por um vetor de coordenadas inteiras a um ponto com valor absoluto norma menor que 1, Proposição 3.1.1. O grande obstáculo desse método é que temos uma quantidade infinita de casos a verificar. Precisamos, então reduzir a um número finito de casos, para isso dividimos o cubo fundamental em uma quantidade grande o suficiente de cubinhos, de forma que cada cubinho possa ser translado por um vetor de coordenadas inteiras a uma região com valor absoluto da norma menor que 1. Daremos condições que garantem que $|N|$ sobre cada um dos cubos assume valor máximo nos vértices. Assim,

para saber se um cubo está numa região com norma menor que 1, basta verificar que cada um dos oito vértices do cubo possui norma com módulo menor que 1.

A partir dessas observações, podemos implementar um algoritmo. O programa inicialmente subdivide C em oito cubos através dos planos $x,\ y,\ z = \frac{1}{2}$. Efetuamos 1500 translações inteiras em cada cubinho e verificamos se alguma dessas translações esta numa região com $|N| < 1$ e neste caso, dizemos que o cubinho foi coberto. Se algum cubinho ainda não foi coberto após isso, novamente o subdividimos em oito cubinhos, continuamos repetindo esse processo sucessivamente. Se em alguma etapa desse processo, todos os cubos forem cobertos, então temos mostrado que cada ponto de C pode ser transladado a uma região de $|N| < 1$ e, portanto, temos mostrado que $\mathbb{K}$ é Euclidiano.

Façamos a mudança de variáveis: $u = x,\ \ v = \sqrt[3]{d}y,\ w = \sqrt[3]{d^2}$. Essa mundança de variavéis manda cada cubo c_i, com faces paralelas aos planos coordenados, em um paralelepípedo $c_i^{'}$ cujas faces também são paralelas aos planos coordenados.

$$N(x, y, z) = x^3 + dy^3 + d^2z^3 - 3xyzd,$$

$$= N(u, v, w) = u^3 + v^3 + w^3 - 3uvw.$$

Como essa transformação manda vértice em vértice, se os máximos de N ocorrem nos vértices de $c_i^{'}$, então o máximo de N ocorre nos vértices de c_i.

Proposição 6.3.1. *Seja E a região de $\mathbb{R}^3$ limitada pelos planos $u = a_1,\ u = a_2,\ v = b_1,\ v = b_2,\ w = c_1,\ w = c_2$ (ou seja o cubo com vértices (a_i, b_j, c_l)). Suponha ainda que E encontra-se inteiramente no primeiro octante de $\mathbb{R}^3$. Se $|N(u)| < 1$ nas arestas desse cubo, então $|N(u)| < 1$ em todo E.*

Demonstração. N é contínua e o cubo E é um compacto de $\mathbb{R}^3$. Seja S a intersecção de E com um plano paralelo a um plano coordenado, por exemplo, uv. Digamos que S seja a intersecção de E com o plano $w = a$. Vejamos os pontos críticos de E.

$$\frac{\partial N}{\partial v} = 3v^2 - 3au = 0; \qquad \frac{\partial N}{\partial u} = 3u^2 - 3av = 0.$$

Daí se $a = 0$, então

$$v = 0 = u.$$

Mas, $(0, 0, 0)$ não é ponto interior de S, já que o cubo está contido no primeiro octante de $\mathbb{R}^3$. Por isso, vamos supor que $a \neq 0$ e assim, pelas derivadas parciais

$$u \neq 0 \neq v.$$

Portanto,

$$\frac{u^2}{v^2} = \frac{v}{u} \Rightarrow \frac{u^3}{v^3} = 1 \Rightarrow \frac{u}{v} = 1 \Rightarrow u = v.$$

Substituindo, $v = u$, nas derivadas parciais, obtemos

$$u = v = w = a \neq 0,$$

já que $u \neq 0$. Mas, $N(a, a, a) = 0$ que claramente não é extremo, pois o único inteiro algébrico com norma zero é o zero. Como a norma é simétrica em relação a u, v, w esse argumento vale para todo S inclusive para as faces do cubo, precisamos procurar o máximo de N apenas nas arestas. Disso, decorre o resultado. □

Proposição 6.3.2. *Suponha que* $|N| < 1$ *em todos os oito vértices de um cubo e que todos os números a seguir são todos não negativos*

$$\left(a_1^2 - b_i c_j\right)\left(a_2^2 - b_i c_j\right) \quad i, j = 1, 2,$$

$$\left(b_1^2 - a_i c_j\right)\left(b_2^2 - a_i c_j\right) \quad i, j = 1, 2,$$

$$\left(c_1^2 - b_i a_j\right)\left(c_1^2 - b_i a_j\right) \quad i, j = 1, 2.$$

então $|N| < 1$ *em todo o cubo.*

Demonstração. Queremos condições que nos garantam que o máximo de $|N|$ seja assumido nos vértices. Podemos considerar a restrição da norma à aresta que passa pelos vértices (a_i, b_1, c_j), (a_i, b_2, c_j)

$$N : [b_1, b_2] \longrightarrow \mathbb{R}$$

$$v \longmapsto N(a_i, v, c_j) = v^3 + a_i^3 + b_j^3 - 3a_i c_j v.$$

Então,

$$\frac{\partial N}{\partial v} = 3v^2 - 3a_i c_j = 0,$$

que possui raízes $v = \pm\sqrt{a_i c_j}$. Queremos que $\frac{\partial N}{\partial v}$ não se anule no aberto (b_1, b_2). Como o cubo fundamental está inteiramente no primeiro octante de $\mathbb{R}^3$, precisamos verificar quando

$$\alpha = \sqrt{a_i c_j} \in (b_1, b_2).$$

Se $\alpha \in (b_1, b_2)$, então

$$b_1 - \alpha < 0, \quad b_2 - \alpha > 0 \Rightarrow (b_1 - \alpha)(b_2 - \alpha) < 0.$$

Se $\alpha \geq b_2$, então

$$b_1 - \alpha < 0, \quad b_2 - \alpha \leq 0 \Rightarrow (b_1 - \alpha)(b_2 - \alpha) \geq 0.$$

Se $\alpha \leq b_1$

$$b_1 - \alpha \geq 0, \quad b_2 - \alpha > 0 \Rightarrow (b_1 - \alpha)(b_2 - \alpha) \geq 0.$$

Como o paralelepípedo está no primeiro octante

$$(b_1 + \alpha)(b_2 + \alpha) \geq 0.$$

Portanto, se $|N|$ não possui máximo em (b_1, b_2), ou seja, $\alpha \notin (b_1, b_2)$

$$\left(b_1^2 - \alpha^2\right)\left(b_2^2 - \alpha^2\right) \geq 0.$$

Mas, $|N|$ possui máximo no compacto $[b_1, b_2]$, por isso eles são atingidos nos vértices.

Como a norma é simétrica em relação a u, v e w, podemos usar o mesmo racíocinio com $(a_1,\ a_2)$ e (c_1, c_2) e obtemos o resultado.

□

Usando estes resultados, podemos montar um algoritmo que mostra que

$$\mathbb{Q}\left(\sqrt[3]{2}\right),\ \mathbb{Q}\left(\sqrt[3]{3}\right),$$

são Euclidianos.

Para o caso $\mathbb{Q}\left(\sqrt[3]{10}\right)$, veja TAYLOR, 1976.

□

7 Corpos Quárticos

Neste capítulo, iremos abordar os métodos que Cioffari usa para tratar os corpos da forma $\mathbb{Q}(\sqrt[4]{-d})$, d livre de 4-ésimas potências. Tais corpos possuem duas imersões complexas conjugadas, logo também possuem posto do grupo das unidades igual a um. As técnicas utilizadas serão semelhantes às do caso cúbico. Aqui também temos um resultado de finitude de Cassels. Para mostrar que os corpos são Euclidianos Cioffari faz novamente uso de computadores, usando a imersão de $\mathbb{Q}(\sqrt[4]{-d})$ no $\mathbb{R}^4$, via base inteira.

7.1 Quárticos não Euclidianos

Iniciamos com um Teorema que irá descatar a possibilidade de muitos corpos serem Euclidianos, reduzindo basicamente ao caso quadrático.

Teorema 7.1.1 (Chevalley)**.** *Seja* $\mathbb{K} = \mathbb{Q}\left(\sqrt[4]{-d}\right)$ *com* $d = sr^2$*, sendo* s *e* r *inteiros livres de quadrados e* $s \neq 1$*. Seja* $K = \mathbb{Q}(\sqrt{-s})$ *o único subcorpo quadrático de* $\mathbb{K}$*, então* $h_{\mathbb{K}} = 1$ *somente se* $h_K = 1$*.*

Demonstração. A ideia fundamental é considerar o corpo de Hilbert de $\mathbb{K}$ e de K, que são denotados, respectivamente, por

$$\mathbb{H}_{\mathbb{K}} \quad \text{e} \quad \mathbb{H}_K.$$

Temos que

$$\mathbb{H}_K \cap \mathbb{K} \subset \mathbb{K}.$$

Como $[\mathbb{K} : K] = 2$, então

$$\mathbb{H}_K \cap \mathbb{K} = \mathbb{K} \quad \text{ou} \quad \mathbb{H}_K \cap \mathbb{K} = K.$$

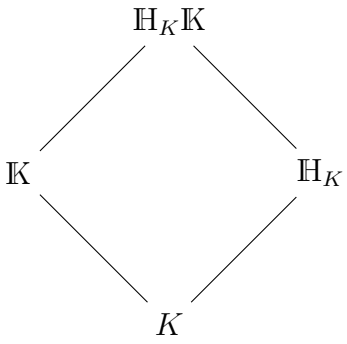
Vamos mostrar que a interseção é K. De fato, por definição, $\mathbb{H}_K/K$ é não ramificada. O Lema abaixo garante que $(\mathbb{H}_K \cap \mathbb{K})/K$ é não ramificada.

Lema 7.1.1. *Seja* $\mathbb{F}/\mathbb{E}$ *uma extensão de corpos de números que é não ramificada. Se* $\mathbb{F}' \subset \mathbb{F}$*, então* $\mathbb{F}'/\mathbb{E}$ *também é não ramificada.*

Mas $\sqrt{-s}B_K$ é um ideal primo de B_K que se ramifica em $\mathbb{K}/K$, portanto, pelo Lema 7

$$\mathbb{H}_K \cap \mathbb{K} = K.$$

Disso,



$$[\mathbb{H}_K\mathbb{K} : \mathbb{K}] = [\mathbb{H}_K : K] = h_K.$$

Temos que $\mathbb{H}_K/K$ é de Galois, então $\mathbb{H}_K\mathbb{K}/\mathbb{K}$ é de Galois, com grupo de Galois isomorfo a $Gal\left(\mathbb{H}_K/K\right)$ que é abeliano, assim $\mathbb{H}_K\mathbb{K}/\mathbb{K}$ é abeliana. Mostraremos também que ela é não ramificada. Para isso, vamos usar um pouco de corpos locais.

Seja $\mathbb{F}$ um corpo de números, para cada ideal primo $\mathfrak{P}$ de $B_{\mathbb{F}}$, obtemos uma norma para $\mathbb{F}$, a norma $\mathfrak{P}$-ádica:

$$|x|_{\mathfrak{P}} = N\left(\mathfrak{P}\right)^{-v(x)},$$

onde $v\left(x\right)$ é tal que

$$xB_{\mathbb{F}} = \mathfrak{P}^{v(x)}Q.$$

e $\mathfrak{P}$ não aparece na fatoração do ideal fracionário Q.

As sequências de Cauchy, $C_{\mathfrak{P}}$, em $\mathbb{F}$ (em relação) a $|.|_{\mathfrak{P}}$ formam um anel e as sequências que tendem a zero, $N_{\mathfrak{P}}$, formam um ideal maximal de $C_{\mathfrak{P}}$ e, portanto, $C_{\mathfrak{P}}/N_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{P}}$ é um corpo, o completamento $\mathfrak{P}$-ádico de $\mathbb{F}$.

Proposição 7.1.1. *Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos de números e $\mathfrak{P}$, β ideais primos de $B_{\mathbb{K}}$ e $B_{\mathbb{L}}$, respectivamente, com β acima de $\mathfrak{P}$. Então, existe uma cópia de $\mathbb{K}_{\mathfrak{P}}$ em $\mathbb{L}_{\beta}$, portanto, temos a extensão de corpos*

$$\mathbb{L}_{\beta}/\mathbb{K}_{\mathfrak{P}}.$$

Demonstração. Veja OGGIER, página página 81. □

Teorema 7.1.2. *Seja $\mathbb{K}$ um corpo local, com $\mathbb{L}/\mathbb{K}$ uma extensão que é não ramificada, finita e seja $\mathbb{K}'$ uma extensão finita arbitrária de $\mathbb{K}$. Se $\mathbb{L}' = \mathbb{K}'\mathbb{L}$, então $\mathbb{L}'/\mathbb{K}'$ também é não ramificada.*

Demonstração. Veja TENGAN, 2008 página 15, Teorema 5.1. □

Proposição 7.1.2. *Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos de números e $\mathfrak{P}$, β ideais primos de $B_{\mathbb{K}}$ e $B_{\mathbb{L}}$, respectivamente, com β acima de $\mathfrak{P}$. Seja $e_{\beta/\mathfrak{P}}$ o expoente da maior potência de β que divide $\mathfrak{P}B_{\mathbb{L}}$. Então $\mathbb{L}_\beta/\mathbb{K}_\mathfrak{P}$ é não ramificada, se e somente se,*

$$e_{\beta/\mathfrak{P}} = 1.$$

Demonstração. Veja OGGIER, página 81. □

Agora sejam

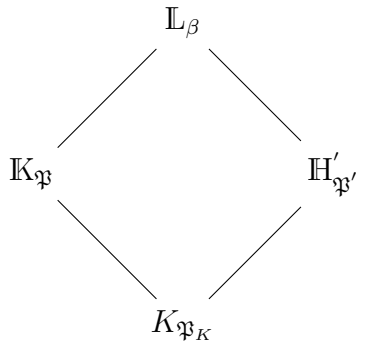
$$\mathbb{L} = \mathbb{H}_K\mathbb{K}, \quad \mathbb{H}' = \mathbb{H}_K, \quad \mathfrak{P}_K = \mathfrak{P} \cap B_K.$$

Tomamos $\mathfrak{P}'$ como sendo um ideal primo de $B_{\mathbb{H}'}$ acima de $\mathfrak{P}_K$.

Queremos mostrar que $\mathbb{L}/\mathbb{K}$ é não ramificada, ou seja, dado um ideal primo $\mathfrak{P}$ de $B_{\mathbb{K}}$ e outro ideal primo β de $B_{\mathbb{L}}$, acima de $\mathfrak{P}$

$$e_{\beta/\mathfrak{P}} = 1.$$

Pela Proposição 7.1.2 é suficiente mostrar que $\mathbb{L}_\beta/\mathbb{K}_\mathfrak{P}$ é não ramificada. Pela Proposição 7.1.1, temos as torres de corpos abaixo



Além disso, $\mathbb{H}'/K$ é não ramificada, pois $\mathbb{H}'$ é o corpo de Hilbert de K, assim

$$e_{\mathfrak{P}'/\mathfrak{P}_K} = 1.$$

Pela proposição 7.1.2, obtemos que

$$\mathbb{H}'_{\mathfrak{P}'}/K_{\mathfrak{P}_K}$$

é não ramificada. Agora, pelo Teorema 7.1.2, temos que

$$\mathbb{L}_\beta/\mathbb{K}_\mathfrak{P}$$

também é não ramificada. Assim, mostramos que $e_{\beta/\mathfrak{P}} = 1$ (Proposição 7.1.2). Como $\mathfrak{P}$ foi tomado de maneira arbitrária, temos que

$$\mathbb{L}/\mathbb{K}$$

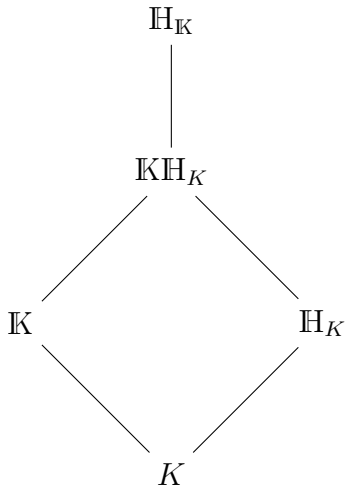
é não ramificada nos primos finitos.

Como $\mathbb{K} = \mathbb{Q}\left(\sqrt[4]{-d}\right)$ e os conjugados de $\sqrt[4]{-d}$ sobre $\mathbb{Q}$ são as raízes de $x^4 + d$ com $d > 0$, ou seja, são todos complexos. Assim, não existe imersão de $\mathbb{K}$ em $\mathbb{C}$ com

$$\sigma(\mathbb{K}) \subset \mathbb{R}.$$

Portanto, $\mathbb{K}\mathbb{H}_K/\mathbb{K}$ é uma extensão não ramificada, abeliana e finita, logo, pelo Corolário 4.1.1, obtemos

$$\mathbb{K}\mathbb{H}_K \subset \mathbb{H}_{\mathbb{K}}.$$



Portanto,

$$h_K \mid h_{\mathbb{K}}.$$

Assim, se $h_{\mathbb{K}} = 1$, então $h_K = 1$. □

Assim, precisamos nos concentrar apenas quando $K = \mathbb{Q}(\sqrt{-s})$ possui número de classes 1.

Teorema 7.1.3. *Seja $K = \mathbb{Q}(\sqrt{-m})$ com m inteiro positivo livre de quadrado, corpo quadrático imaginário, então $h_K = 1$ se, e somente se,*

$$m \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Demonstração. Não é difícil mostrar que esses corpos possuem número de classes 1, podemos fazer isso usando a cota de Minkowski, mas mostrar que essa lista está completa é bem mais difícil, veja STARK et al., 1967 □

Corolário 7.1.1. *Se $h_{\mathbb{K}} = 1$, então $s \in \{2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163\}$.*

Demonstração. Decorre diretamente dos Teoremas 7.1.1 e 7.1.3. □

A Proposição abaixo, enfatiza mais uma vez a ligação entre unidades, ramificação e ser Euclidiano.

Proposição 7.1.3. *Seja* $\mathbb{K} = \mathbb{Q}\left(\sqrt[4]{-d}\right)$ *e suponha que existem três primos distintos de* B_K *que se ramifica m em* $B_{\mathbb{K}}$*, então* $\mathbb{K}$ *não é Euclidiano.*

Demonstração. Inicialmente, note que s se ramifica totalmente em $B_{\mathbb{K}}$, pois s divide d

$$\mathfrak{P}_1^4 = sB_{\mathbb{K}}.$$

Por outro, lado s também se ramifica totalmente em B_K

$$sB_K = (\sqrt{-s}B_K)^2.$$

Assim,

$$sB_{\mathbb{K}} = sB_KB_{\mathbb{K}} = (\sqrt{-s}B_K)^2B_{\mathbb{K}}.$$

Disso, obtemos que

$$\sqrt{-s}B_{\mathbb{K}} = \mathfrak{P}_1^2.$$

Suponha que $\mathfrak{P}_2$ e $\mathfrak{P}_3$ sejam ideais de B_K que também se ramificam em $B_{\mathbb{K}}$

$$\mathfrak{P}_2B_{\mathbb{K}} = \mathfrak{Q}_2^2 \quad \text{e} \quad \mathfrak{P}_3B_{\mathbb{K}} = \mathfrak{Q}_3^2.$$

Suponha que $\mathbb{K}$ é Euclidiano, então

$$\mathfrak{Q}_2 = b_2B_{\mathbb{K}}; \quad \mathfrak{Q}_3 = b_3B_{\mathbb{K}} \quad \text{com} \quad b_2,\ b_3 \in B_{\mathbb{K}}.$$

Além disso, se $\mathbb{K}$ é Euclidiano, então $h_K = 1$, pelo Teorema 7.1.1

$$\mathfrak{P}_2 = a_2B_K;\ \mathfrak{P}_3 = a_3B_K \quad \text{com} \quad a_2,\ a_3 \in B_K.$$

Dessa maneira, b_i^2 e a_i são associados em $B_{\mathbb{K}}$. As imersões de $\mathbb{K}$ consistem de dois pares de imersões complexas conjugadas, portanto, pelo Teorema das Unidades de Dirichlet (Teorema 3.2.1), o grupo das unidades possui, exatamente, $0+2-1 = 1$ unidade fundamental. Como $\mathbb{K}$ não é um corpo ciclotômico e também não contém i, pois o seu único subcorpo quadrático é $\mathbb{Q}(\sqrt{-s})$. De fato, o fecho normal de $\mathbb{K}/\mathbb{Q}$ possui como grupo de Galois o diedral, o subgrupo que fixa $\mathbb{K}$ está contido em um único sugrupo de ordem 4. As únicas raízes da unidade em $\mathbb{K}$ são ± 1. Logo,

$$a_i = b_i\epsilon^{t_i}.$$

Dessa maneira, pelo menos um dentre

$$a_2 = b_2^2\epsilon^{t_2},\ a_3 = b_3^2\epsilon^{t_3},\ a_2a_3 = b_2^2b_3^2\epsilon^{t_2+t_3}$$

é um quadrado em $B_{\mathbb{K}}$. Assim, pelo menos um dentre

$$\sqrt{a_2},\ \sqrt{a_3},\ \sqrt{a_2a_3}\ \text{ está em }\ B_{\mathbb{K}}.$$

Se $\sqrt{a_i}$ ou$\sqrt{a_2a_3}$ está em $K \cap B_{\mathbb{K}} = B_K$, então

$$\mathfrak{P}_i = a_iB_K = \left(\sqrt{a_i}B_K\right)^2$$

ou

$$\mathfrak{P}_1\mathfrak{P}_2 = \left(\sqrt{a_2}B_K\right)^2\left(\sqrt{a_3}B_K\right)^2.$$

Nenhum dos dois casos acima pode acontecer, pois $\mathfrak{P}_i$ é um ideal primo. Por isso, pelo menos um dos casos abaixo ocorre

$$\mathbb{K} = K\left(\sqrt{a_2a_3}\right), \quad \mathbb{K} = K\left(\sqrt{a_2}\right)\ \text{ ou }\quad \mathbb{K} = K\left(\sqrt{a_3}\right).$$

Dessa maneira,

$$\mathbb{K} = K\left(\sqrt{x+\sqrt{-s}y}\right), \quad x,\ y \in \mathbb{Q}.$$

Mas, isso não pode acontecer, pois, o fecho normal de $\mathbb{K}/\mathbb{Q}$ é

$$F_N = \mathbb{Q}(\sqrt[4]{-sr^2}, i),$$

cujo grupo de Galois é o diedral. Temos que $\sqrt{x-\sqrt{-s}y} \in F_N$, pois é o conjugado de $\sqrt{x+\sqrt{-s}y}$ Logo,

$$\sqrt{x^2+sy^2} \in F_N.$$

Portanto, F_N, possui exatamente três corpos intermediários quadráticos. Mas nós temos quatro corpos quadráticos contidos em F_N :

$$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{-s}),\ \mathbb{Q}(\sqrt{s}),\ \mathbb{Q}(\sqrt{x^2+sy^2}).$$

Esses quatro corpos são distintos. De fato, basta mostrarmos que

$$\mathbb{Q}(\sqrt{s}) \neq \mathbb{Q}(\sqrt{x^2+sy^2}).$$

Suponha, por absurdo, que $\mathbb{Q}(\sqrt{s}) = \mathbb{Q}(\sqrt{x^2+sy^2})$, então $x^2+sy^2 = st^2$ $(t \in \mathbb{Z})$, mas sabemos que $x+y\sqrt{-s}$ é primo ou produto de dois primos em B_K (a_2, a_3 ou a_2a_3), tomando o conjugado complexo, vemos que o mesmo vale para $x-y\sqrt{-s}$. Como $\mathfrak{P}_2$ e $\mathfrak{P}_3$ são ambos distintos de$\sqrt{-s}B_K$, temos que $\sqrt{-s}$ não é associado de nenhum primo que aparece na fatoração de $x+y\sqrt{-s}$. Por outro lado,

$$(x+y\sqrt{-s})(x-y\sqrt{-s}) = st^2 = -(\sqrt{-s}t)^2.$$

Assim, $\sqrt{-s}$ aparece na fatoração de $x+y\sqrt{-s}$, absurdo. □

Com a notação da Proposição anterior

Corolário 7.1.2. *Se $h_{\mathbb{K}} = 1$ e $s \neq 2$, então*

$$d \in \{3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163,\ 12,\ 44,\ 76,\ 172,\ 652\}.$$

Demonstração. Já vimos no Corolário 7.1.1 que se $h_{\mathbb{K}} = 1$, então

$$s \in \{2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163\}.$$

Assim, se $s \neq 2$, temos que $s \equiv 3 \pmod 4$. Temos que $\mathfrak{P}_s = \sqrt{-s}B_K$ é um primo de B_K que se ramifica em $B_{\mathbb{K}}$. Além disso,

$$2 \mid \Delta_{\mathbb{K}},$$

veja HUARD; SPEARMAN; WILLIAMS, 1995 Corolário 2 página 91.

Portanto, se $s \neq 2$, concluímos que 2 não se ramifica em $\mathbb{Q}\left(\sqrt{-s}\right)$, pois

$$\begin{array}{c} \mathbb{Q}\left(\sqrt[4]{-sr^2}\right) \\ | \\ \mathbb{Q}\left(\sqrt{-s}\right) \\ | \\ \mathbb{Q} \end{array}$$

$$\Delta_K = -s, \quad -s \equiv 1 \pmod 4.$$

Assim, 2 não se ramifica em B_K, portanto $\mathfrak{P}_2 = 2B_K$ é um primo que se ramifica em $B_{\mathbb{K}}$. Se algum primo p diferente de 2 e de s dividisse r, então teríamos três ideais primos de B_K que se ramificam em $B_{\mathbb{K}}$

$$\mathfrak{P}_2,\ \mathfrak{P}_s,\ \mathfrak{P}_p = pB_K.$$

Portanto, pela Proposição 7.1.3, $\mathbb{K}$ não é Euclidiano. Dessa forma, se $h_{\mathbb{K}} = 1$ e $s \neq 2$, então $r \in \{1,\ 2\}$. Por isso,

$$d \in \{3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163,\ 12,\ 44,\ 76,\ 172,\ 652\}.$$

□

Vamos nos limitar a estudar o caso $s \neq 2$. A seguinte Proposição nos ajudará a descartar seis de tais corpos. Na seguinte Proposição mantemos a notação.

Proposição 7.1.4. *Se $s \equiv 3 \pmod 4$ e se existe um primo $p < s$ tal que $p \equiv 1 \pmod 4$ e $-d$ é quadrado módulo p, mas não é uma quarta potência módulo p, então $\mathbb{K}$ não é Euclidiano.*

Demonstração. Suponha que $\mathbb{K}$ seja Euclidiano, pelo Corolário 7.1.1

$$s \in \{2, 3, 7, 11, 19, 43, 67, 163\}, \qquad \text{ou seja, } \ s \ \text{ é primo.}$$

Temos que s é um primo que se ramifica totalmente em $\mathbb{K}$. De, fato

$$sB_{\mathbb{K}}(rB_{\mathbb{K}})^2 = (\sqrt[4]{-sr^2}B_{\mathbb{K}})^4.$$

Mas os ideais primos em $B_{\mathbb{K}}$ acima de s são distintos dos ideais primos de $B_{\mathbb{K}}$ acima de p_i (p_i divide r). Portanto,

$$sB_{\mathbb{K}} = \mathfrak{Q}^4.$$

Como $p \equiv 1 \pmod 4$, então -1 é quadrado módulo p, então

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

Assim, pela Lei da Reciprocidade Quadrática

$$\left(\frac{s}{p}\right) = 1 \Rightarrow \left(\frac{p}{s}\right) = 1.$$

Em razão disso, existe $x \in \mathbb{Z}_s$ tal que

$$\bar{p} = x^2.$$

Seja g uma raiz primitiva módulo s, vamos mostrar que

$$\left(g^t\right)^4 \equiv p \pmod s,$$

possui solução. Seja y tal que

$$g^y \equiv x \pmod s.$$

Então é suficiente mostrar que

$$g^{2y} \equiv g^{4t} \pmod s,$$

possui solução. O que é equivalente, pelo Pequeno Teorema de Fermat, a

$$(s-1) \mid (4t - 2y)$$

se, e somente se,

$$2t \equiv y \pmod{\frac{s-1}{2}}$$

que possui solução, pois 2 é inversível módulo $\frac{s-1}{2}$ (que é ímpar). Seja, então, $b \in \mathbb{Z}$ satisfazendo

$$b^4 \equiv p \pmod{s}.$$

Suponha que existe $u \in B_{\mathbb{K}}$

$$u \equiv b \pmod{\mathfrak{Q}} \quad |N(u)| < s.$$

Se F_N é o fecho normal de de $\mathbb{K}/\mathbb{Q}$, então

$$\mathfrak{Q}B_{F_N} = \sigma(\mathfrak{Q})B_{\mathbb{F}_{\mathbb{N}}}.$$

Veja Teoremas 5.0.1, 5.0.2. Em razão disso,

$$N(u) \equiv b^4 \equiv p \pmod{s}.$$

Assim,

$$N(u) = p, \quad \text{pois} \quad 0 < p < s \quad \text{e} \quad N(x) = |x|^2|x_1|^2,$$

onde x, $\overline{x}$, x_1, $\overline{x_1}$ são os conjugados de x. Assim, existe um ideal $\mathfrak{P}$ com norma p (o ideal gerado por u). Por outro lado, existe $n \in \mathbb{Z}$ com

$$\sqrt[4]{-d} + n \in \mathfrak{P}.$$

De fato,

$$1 + \sqrt[4]{-d}, \ldots, p + \sqrt[4]{-d},$$

é um sistema completo de resíduos módulo $\mathfrak{P}$, pois se

$$\overline{j + \sqrt[4]{-d}} = \overline{i + \sqrt[4]{-d}}.$$

Então

$$p \mid (i - j), \quad \text{já que} \quad \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}.$$

Mas $i,\ j < p$, assim $i = j$, portanto, são p classes distintas, são todas as classes já que $N(\mathfrak{P}) = p$. Daí,

$$p = N(\mathfrak{P}) \mid N\left(\sqrt[4]{-d} + n\right) = d + n^4.$$

Logo,

$$n^4 \equiv -d \pmod{p},$$

que é um absurdo, por hipótese. Portanto,

$$\text{se} \quad u \equiv b \pmod{\mathfrak{Q}}, \quad \text{então} \quad |N(u)| \geq s.$$

Portanto, se $q \in B_{\mathbb{K}}$ é o gerador de $\mathfrak{Q}$, então não podemos dividir b por q

$$b = qt + u' \quad \text{com} \quad |N\left(u'\right)| < s.$$

□

Corolário 7.1.3. *Se*

$$d \in \{11,\ 19,\ 43,\ 76,\ 172,\ 268\}$$

então $\mathbb{K}$ *não é Euclidiano.*

Demonstração. A tabela abaixo fornece valores para d, s e p satisfazendo as condições da Proposição 7.1.4. A verificação de tais hipóteses são simples visto que só envolvem congruências módulo p.

d	s	p	d	s	p
11	11	5	76	19	5
19	19	17	172	43	13
43	43	17	268	67	29

□

Teorema 7.1.4 (Cassels)**.** *Se* $\mathbb{K}$ *é um corpo quártico totalmente complexo, com*

$$\Delta_{\mathbb{K}} > 28090000$$

então $\mathbb{K}$ *não Euclidiano.*

Demonstração. Veja CASSELS, 1952. □

Corolário 7.1.4. *Se*

$$d \in \{163,\ 652\}$$

então $\mathbb{K}$ *não é Euclidiano.*

Demonstração. Os corpos $\mathbb{Q}\left(\sqrt[4]{-163}\right)$ e $\mathbb{Q}\left(\sqrt[4]{-652}\right)$, posuem, respectivamente, discriminantes 69291952 e 277167808 (SAGE). □

Agora, temos apenas cinco possibilidades para $d \in \{3,\ 7,\ 12,\ 44,\ 67\}$, se $d \neq 2$.

7.2 Corpos Quárticos Euclidianos

Teorema 7.2.1. $\mathbb{Q}\left(\sqrt[4]{-2}\right)$ *é Euclidiano.*

Demonstração. Seja $\mathbb{K} = \mathbb{Q}\left(\sqrt[4]{-d}\right)$. Suponha que

$$\{1,\ \sqrt[4]{-d},\ \sqrt[4]{-d}^2,\ \sqrt[4]{-d}^3\}.$$

seja base inteira. Nós iremos seguir o mesmo procedimento do caso cúbico, iremos mergulhar $\mathbb{Q}(\sqrt[4]{-d})$ no $\mathbb{R}^4$ da seguinte forma

$$x + y\sqrt[4]{-d} + z\sqrt[4]{-d}^2 + w\sqrt[4]{-d}^3 \longmapsto (x, y, z, w) \in \mathbb{Z}^4.$$

Isso identifica os inteiros algébricos de $\mathbb{K}$ com $\mathbb{Z}^4$. Definimos o cubo fundamental como

$$C = \{(x, y, z, w) \,|\, (x, y, z, w) \in \mathbb{R}^4 \quad 0 \leq x,\ y,\ z,\ w < 1\}.$$

Para mostrar que $\mathbb{K}$ é Euclidiano é suficiente mostrar que cada ponto do domínio fundamental pode ser translado por um vetor de cordenadas inteiras a um ponto cujo valor absoluto da norma seja menor que 1, Proposição 3.1.1. Mas, o domínio fundamental possui infinitos pontos, para reduzir a um número finito de casos, usamos a continuidade da norma, como no caso cúbico. Daremos condições para que um 4-cubo esteja nunha região com $|N| < 1$. Mas, antes, vejamos como calcular a norma em $\mathbb{K}$. Dado $\alpha \in \mathbb{K}$

$$\alpha = x + y\sqrt[4]{-d} + z\sqrt[4]{-d}^2 + w\sqrt[4]{-d}^3.$$

Temos que

$$\left(x + y\sqrt[4]{-d} + z\sqrt[4]{-d}^2 + w\sqrt[4]{-d}^3\right)\left(x - y\sqrt[4]{-d} + z\sqrt[4]{-d}^2 - w\sqrt[4]{-d}^3\right)$$
$$= \left(\left(x + z\sqrt{-d}\right) + \sqrt[4]{-d}\left(y + w\sqrt{-d}\right)\right)\left(\left(x + z\sqrt{-d}\right) - \sqrt[4]{-d}\left(y + w\sqrt{-d}\right)\right)$$
$$= \left(x + z\sqrt{-d}\right)^2 - \sqrt{-d}\left(y + w\sqrt{-d}\right)^2 = \left(x^2 - dz^2 + 2ywd\right) + \left(-y^2 + dw^2 + 2xz\right)\sqrt{-d}.$$

Analogamente,

$$\left(x + iy\sqrt[4]{-d} - z\sqrt[4]{-d}^2 + -iw\sqrt[4]{-d}^3\right)\left(x - iy\sqrt[4]{-d} - z\sqrt[4]{-d}^2 + iw\sqrt[4]{-d}^3\right)$$
$$= \left(\left(x - z\sqrt{-d}\right) + i\sqrt[4]{-d}\left(y - w\sqrt{-d}\right)\right)\left(\left(x - z\sqrt{-d}\right) - i\sqrt[4]{-d}\left(y - w\sqrt{-d}\right)\right)$$
$$= \left(x - z\sqrt{-d}\right)^2 - i^2\sqrt{-d}\left(y - w\sqrt{-d}\right)^2 = \left(x^2 - dz^2 + 2ywd\right) - \left(-y^2 + dw^2 + 2xz\right)\sqrt{-d}.$$

Assim, se $N_1 = x^2 - z^2d + 2ywd$ e $N_2 = 2xz - y^2 + w^2d$, então

$$N\left(x + y\sqrt[4]{-d} + z\sqrt[4]{-d}^2 + w\sqrt[4]{-2}^3\right) = N_1^2 + dN_2^2.$$

Dessa forma, estendemos a norma para qualquer (x, y, z, w) em $\mathbb{R}^4$ de maneira natural

$$N(x, y, z, w) = N_1^2 + dN_2^2.$$

Proposição 7.2.1. *Seja S um $4-$cubo limitado por hiperplanos paralelos aos hiperplanos coordenados*

$$[a_1,\ a_2] \times [b_1,\ b_2] \times [c_1,\ c_2] \times [m_1,\ m_2]$$

e o interior de S não intersecta os planos coordenados. Se existe uma constante positiva $\lambda < 1$ tal que $|N_1| < \sqrt{\lambda}$ e $|N_2| < \sqrt{\frac{1-\lambda}{d}}$ em todos os dezesseis vértices de S, então

$$|N| < 1$$

em todo S.

Demonstração. S é um compacto em $\mathbb{R}^4$ e N_1 e N_2 são conínuas, assim admitem mínimo e máximo em S. Mostraremos que esses ocorrem nos vérices do $4-$cubo S. Vamos analizar as derivadas parciais de N_1. Suponha que $x,\ ,y,\ ,z,\ w$ seja um ponto crítico

$$\frac{\partial N_1}{\partial x} = 2x = 0, \qquad x = 0.$$

Mas $(\ 0,\ ,y,\ ,z,\ w)$ não está no interior de S, pois S não intersecta os eixos coordenados, portanto, o máximo de $|N_1|$ ocorre na fronteira de S.

A fronteira de S é

$$\{a_1\} \times [b_1,\ b_2] \times [c_1,\ c_2] \times [m_1,\ m_2] \cup \{a_2\} \times [b_1,\ b_2] \times [c_1,\ c_2] \times [m_1,\ m_2]$$

$$\cup\, [a_1,\ a_2] \times \{b_1\} \times [c_1,\ c_2] \times [m_1,\ m_2] \cup \times [a_1,\ a_2] \times \{b_2\} \times [c_1,\ c_2] \times [m_1,\ m_2]$$

$$\cup\, [a_1,\ a_2] \times [b_1,\ b_2] \times \{c_1\} \times [m_1,\ m_2] \cup\ [a_1,\ a_2] \times [b_1,\ b_2]\{c_2\} \times [m_1,\ m_2]$$

$$\cup [a_1,\ a_2] \times [b_1,\ b_2] \times [c_1,\ c_2]\ \times \{m_1\} \times \cup [a_1,\ a_2] \times [b_1,\ b_2] \times [c_1,\ c_2] \times \{m_2\}.$$

Chamemos cada uma das oito partes da união distintas acima de face de S, usando as derivadas parciais, verificaremos que o máximo de N_1 é atingindo nos vértices, portanto, o máximo de $|N_1|$ em S é menor que$\sqrt{\lambda}$. O mesmo acontece com N_2. O máximo de $|N_2|$ é atingindo nos vértices e, portanto, em todo S

$$|N_2| < \sqrt{\frac{1-\lambda}{d}}.$$

Logo,

$$|N| < \sqrt{\lambda}^2 + d\sqrt{\frac{1-\lambda}{d}}^2 = 1.$$

Agora, vamos verificar que o máximo de $|N_1|$ ocorre nos vértices para a face

$$\{a_1\} \times [b_1,\ b_2] \times [c_1,\ c_2] \times [m_1,\ m_2].$$

Podemos considerar

$$N_{a_1} = N_1\,(a_1,\ y,\ z,\ w) = a_1^2 - z^2 d + 2ywd,$$

que é uma função contínua em $\mathbb{R}^3$. Temos que

$$S_1 = [b_1,\ b_2] \times [c_1,\ c_2] \times [m_1,\ m_2]$$

é um compacto de $\mathbb{R}^3$, pelas derivadas parciais, o máximo de $|N_{a_1}|$ não ocorre em nenhum ponto interior de S, de fato

$$\frac{\partial N_1}{\partial z} = 2zd = 0, \qquad z = 0.$$

Mas $(y,\ 0,\ w)$ não é ponto interior de S_1, pois S_1 não intersecta os planos coordenados. Portanto, o máximo de $|N_{a_1}|$ em S_1 é atingindo na sua fronteira. Abaixo, segue a fronteira de S_1

$$\{(a_1, b_1)\}, \times[c_1,\ c_2] \times [m_1,\ m_2] \cup a_1 \times b_2 \times [c_1,\ c_2] \times [m_1,\ m_2]$$

$$\{a_1\} \times [b_1,\ b_2] \times \{c_1\} \times [m_1,\ m_2] \cup \{a_1\} \times [b_1,\ b_2] \times \{c_2\} \times [m_1,\ m_2]$$

$$\{a_1\} \times [b_1,\ b_2] \times [c_1,\ c_2] \times \{m_1\} \cup \{a_1\} \times [b_1,\ b_2] \times [c_1,\ c_2] \times \{m_2\}.$$

Continuando dessa maneira, considerando restrições de N_1, usando as derivadas parciais e lembrando da fronteira do produto de intervalos fechados no $\mathbb{R}^n$, encontramos que o máximo de N_1 ocorre nos vértices. O mesmo raciocínio aplica-se a N_2.

□

Usando o SAGE, obtemos que a base inteira de $\mathbb{Q}(\sqrt[4]{-2})$ é

$$\{1,\ \sqrt[4]{-2},\ \sqrt[4]{-2}^2,\ \sqrt[4]{-2}^3\}.$$

Implementando o algoritmo, mostramos que $\mathbb{Q}(\sqrt[4]{-2})$ é Euclidiano. □

Teorema 7.2.2. $\mathbb{Q}(\sqrt[4]{-7})$ *é Euclidiano.*

Demonstração. A demonstração é análoga ao caso $\mathbb{Q}(\sqrt[4]{-2})$. □

Teorema 7.2.3. $\mathbb{Q}(\sqrt[4]{-3})$ *é Euclidiano.*

Demonstração. veja LAKEIN, 1972. □

Teorema 7.2.4. $\mathbb{K} = \mathbb{Q}(\sqrt[4]{-sr^2})$*, com* s*,* r *livres de quadrados, é, Euclidiano, se e somente,*

$$\mathbb{K} = \mathbb{Q}(\sqrt[4]{-2}),\ \mathbb{Q}(\sqrt[4]{-3}),\ \mathbb{Q}(\sqrt[4]{-7}) \quad ou \quad \mathbb{Q}(\sqrt[4]{-12}).$$

Demonstração. Veja, LEMMERMEYER, 1995.

□

Referências

ASH, R. B. Ash. abstract algebra: the basic graduate year. Published online at http://www. math. uiuc. edu/˜ r-ash, 2000.

ASH, R. B. A course in algebraic number theory. Published online at http://www. math. uiuc. edu/˜ r-ash, 2003.

BARNES, E. S.; SWINNERTON-DYER, H. P. The inhomogeneous minima of binary quadratic forms (ii). *Acta Mathematica*, Springer, v. 88, n. 1, p. 279–316, 1952.

CASSELS, J. The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms. In: CAMBRIDGE UNIV PRESS. *Mathematical Proceedings of the Cambridge Philosophical Society*. [S.l.], 1952. v. 48, n. 01, p. 72–86.

CAVALLAR, S.; LEMMERMEYER, F. *The Euclidean Algorithm in Cubic Number Fields*. [S.l.], 2012.

CIOFFARI, V. G. The euclidean condition in pure cubic and complex quartic fields. *Mathematics of Computation*, v. 33, n. 145, p. 389–398, 1979.

COHEN, H. *Graduate Texts in Mathematics: A Course in Computational Algebraic Number Theory, vol. 138*. [S.l.]: Spring-Verlag, 1993.

DAVENPORT, H. Euclid's algorithm in cubic fields of negative discriminant. *Acta Mathematica*, Springer, v. 84, n. 1, p. 159–179, 1950.

ENDLER, O. *Teoria dos números algébricos*. [S.l.]: Instituto de Matemática Pura e Aplicada, CNPq, 1986.

HOURIET, J. Exceptional units and euclidean number fields. *Archiv der Mathematik*, Springer, v. 88, n. 5, p. 425–433, 2007.

HUARD, J. G.; SPEARMAN, B. K.; WILLIAMS, K. S. Integral bases for quartic fields with quadratic subfields. *Journal of Number Theory*, Elsevier, v. 51, n. 1, p. 87–102, 1995.

LAKEIN, R. B. Euclid's algorithm in complex quartic fields. *Acta Arithmetica*, Institute of Mathematics Polish Academy of Sciences, v. 20, n. 4, p. 393–400, 1972.

LEMMERMEYER, F. The euclidean algorithm in algebraic number fields. *Expositiones Mathematicae*, SPEKTRUM ACADEMISCHER VERLAG, v. 13, p. 385–416, 1995.

LEMMERMEYER, F. Euclid's algorithm in quartic cm-fields. *preprint*, 2011.

LENSTRA, H. W. Euclid's algorithm in cyclotomic fields. *Journal of the London Mathematical Society*, Wiley Online Library, v. 2, n. 4, p. 457–465, 1975.

LENSTRA, H. W. Euclidean number fields of large degree. *Inventiones mathematicae*, Springer, v. 38, n. 3, p. 237–254, 1976.

LENSTRA, H. W.; POORTEN, A. van der. Euclidean number fields 1. *The Mathematical Intelligencer*, Springer, v. 2, n. 1, p. 6–15, 1979.

LEUTBECHER, A.; MARTINET, J. Lenstra's constant and euclidean number fields. *Astérisque*, v. 94, p. 87–131, 1982.

MARCUS, D. A. *Number fields*. [S.l.]: Springer, 1977.

MASLEY, J. M.; MONTGOMERY, H. L. Cyclotomic fields with unique factorization. *Journal für die reine und angewandte Mathematik*, v. 286, p. 248–256, 1976.

MCKENZIE, R. G. *The ring of cyclotomic integers of modulus thirteen is norm-euclidean*. Tese (Doutorado) — Michigan State University. Dept. of Mathematics, 1988.

NEUKIRCH, J. Algebraic number theory. Springer, 1999.

OGGIER, F. http://www1.spms.ntu.edu.sg/ frederique/antchap7.pdf.

RIBENBOIM, P. *Classical Theory of Algebraic Numbers*. [S.l.]: Springer Science & Business Media, 2001.

STARK, H. M. et al. A complete determination of the complex quadratic fields of class-number one. *The Michigan Mathematical Journal*, The University of Michigan, v. 14, n. 1, p. 1–27, 1967.

TAYLOR, E. M. Euclid's algorithm in cubic fields with complex conjugates. *Journal of the London Mathematical Society*, Oxford University Press, v. 2, n. 1, p. 49–54, 1976.

TENGAN, E. An invitation to local fields. *Groups, Rings and Groups Rings*, 2008.