UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

JOÃO VICTOR MAXIMIANO ALBUQUERQUE

FINITUDE DO GRUPO DAS CLASSES DE UM CORPO DE NÚMEROS VIA EMPACOTAMENTOS RETICULADOS

FORTALEZA
2013

JOÃO VICTOR MAXIMIANO ALBUQUERQUE

FINITUDE DO GRUPO DAS CLASSES DE UM CORPO DE NÚMEROS VIA EMPACOTAMENTOS RETICULADOS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de concentração: Álgebra.

Área de concentracão: Álgebra
Orientador: Prof. Dr. José Othon Dantas Lopes

FORTALEZA

2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

A310f Albuquerque, João Victor Maximiano.
Finitude do grupo das classes de um corpo de números via empacotamentos reticulados / João Victor Maximiano Albuquerque. – 2013.
51f.: il. enc.; 30 cm.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática, Fortaleza, 2013.
Área de Concentração: Álgebra.
Orientação: Prof. Dr. José Othon Dantas Lopes.

1. Corpos de números. 2. Grupo das classes. 3. Geometria de números. I. Título.

CDD 516.36

JOÃO VICTOR MAXIMIANO ALBUQUERQUE

FINITUDE DO GRUPO DAS CLASSES DE UM CORPO DE NÚMEROS VIA EMPACOTAMENTOS RETICULADOS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de concentração: Álgebra.

Aprovada em: 12/07/2013.

BANCA EXAMINADORA

_____

Prof. Dr. José Othon Dantas Lopes (Orientador)

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Trajano Pires da Nóbrega Neto

Universidade Estadual Paulista (UNESP)

_____

Prof. Dr. José Carmelo Interlando

San Diego State University

Dedico este trabalho à minha família.

“A Matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas.”

Gauss

AGRADECIMENTOS

Agradeço a Deus pelo dom da vida, por toda a força que ele me concede diante de todos os desafios que surgem e por todas as pessoas maravilhosas que ele colocou na minha vida, no caso, meus pais, minha avó (Maria Cristina), meu irmão (João Arthur), minha namorada (Yngrid Lohanne), minha família, meus amigos e os professores que marcaram toda minha carreira estudantil.

Ao meu pai José Josias e minha mãe Maria Erenilda que são as pessoas mais importantes da minha vida, e tudo que eu tenho e consegui até hoje se deve ao grande apoio e dedicação deles. Não há uma palavra no universo que possa expressar o amor e a gratidão que sinto por eles. Ao meu irmão, companheiro e melhor amigo João Arthur, que sempre esteve do meu lado em todas as madrugadas de estudo.

A minha namorada Yngrid Lohanne, bem como aos seus familiares, pelo constante apoio e ajuda em cuidar de mim e pela enorme paciência que teve comigo nos momentos mais dificeis, cabe a mim apenas agradecer pelo seu amor e carinho. Agradeço também a minha avó, e segunda mãe Maria Cristina, pelo carinho dedicado e todos os ensinamentos.

A todos os meus ex-alunos, professores companheiros do PNV e amigos, principalmente da escola Presidente Roosevelt, pelo apoio e amizade durante todo esse tempo.

Aos meus amigos, que considero meus irmãos, que contribuíram e ainda contribuem na minha vida e que devo grande parte desta vida acadêmica, especialmente, em ordem alfabética: Anderson Feitoza, Delson Barros, Ernando Carneiro, Francisco Yure, João Luiz, e Nicolas Alcântara.

Também não posso deixar de mencionar algumas pessoas que me ajudaram durantes os dois últimos anos com sua amizade e respeito: Breno Pinheiro, Diego Eloi, Edson Coutinho, Edson Sampaio, Eduardo Garcez(Zé), Fábio da Costa, Gilson Granja, Gisele Oliveira, Henrique Blanco, João Nunes, Kelma Gomes, Olavo Júnior, Renan Santos, Roger Oliveira, Robério Coelho, Rui Brasileiro, Wanderley de Oliveira e a todos aqueles que eu possa ter esquecido de mencionar.

Ao meu orientador José Othon Dantas Lopes, agradeço pela confiança depositada em mim, pelo incentivo e orientação nos meus estudos. Aos professores da Matemática em especial e em ordem alfabética: Afonso de Oliveira, Alberto Maia, Antonio Caminha, Fábio Montenegro, Lucas Barbosa, Luquésio Petrola, Marcos Melo, Pacelli Bessa, Romildo José e Válter Lopes pelo aprendizado proporcionado durante minha graduação e mestrado.

Aos membros da banca examinadora, Professor José Carmelo Interlando, Professor Trajano

Pires da Nóbrega Neto pela disponibilidade e pelas contribuições fornecidas. Aos membros da secretaria de pós-graduação em especial a Andrea.

Ao orgão financiador CNPQ pelo apoio financeiro.

RESUMO

Este trabalho é baseado no artigo *Finiteness of the class group of a number field via lattice packings*. Daremos aqui uma prova alternativa da finitude do grupo das classes de um corpo de números de grau n. Ela é baseada apenas no fato de que a densidade de centro de um empacotamento reticulado n-dimensional é limitado fora do infinito.

Palavras-Chaves: Corpo de números, grupo das classes, geometria de números.

ABSTRACT

This work is based on the article *Finiteness of the class group of a number field via lattice packings*. An alternative proof of the finiteness of the class group of a number field of the degree n is presented. It is based solely on the fact that the center density of an n-dimensional lattice packing is bounded away from infinity.

Keywords: Number fields, class groups, geometry of numbers.

SUMÁRIO

1 INTRODUÇÃO

Seja K um corpo de números algébricos de grau n com anel de inteiros algébricos $\mathfrak{D}_K$. A conhecida prova da finitude do grupo das classes $\mathcal{C}_K$ de um corpo de números K [ver seção 3.3] envolve o critério de Minkowski para um conjunto convexo que contém um ponto de um reticulado [ver teorema 2.9 e corolário 2.5] e a existência de um ideal inteiro $\mathfrak{b}$ cuja norma não excede M_K, o limitante de Minkowski de K.

O nosso próposito é apresentar uma prova alternativa para este teorema clássico da teoria dos números por meios de noções e resultados elementares de empacotamento esféricos. Uma consequência da nova prova é um limite inferior para a densidade de centro de empacotamentos reticulados associado com ideais inteiros $\mathfrak{b}$.

No capítulo de Preliminares, revisaremos os fatos necessários sobre a teoria algébrica dos números, corpos de números e reticulados em $\mathbb{R}^n$. O capítulo posterios será para falarmos sobre o mergulho canônico de um corpo de números, o grupo das classes, bem como dar algumas demonstrações deste resultado para efeito de comparação. Também servirá para estabelecermos a notação.

O último capítulo deste trabalho será destinado a provar o resultado principal usando o conceito de empacotamento reticulado, dado na primeira seção deste capítulo.

2 PRELIMINARES

Neste capítulo encontraremos os fundamentos básicos da Teoria Algébrica dos Números, a fim de identificar as hipóteses dos nossos resultados e obter um bom entendimento dos nossos cálculos, bem como os enunciados de alguns resultados conhecidos que usamos no trabalho.

2.1 Elementos inteiros sobre um anel R

Para os nossos própositos, nós assumiremos que é familiar as noções de grupo, anéis, corpos, espaços vetoriais e módulos, bem como algumas de suas propriedades.

Nesta dissertação, entenderemos por "anel" como um anel comutativo com elemento identidade.

Teorema 2.1. *Seja R um anel, A um subanel de R e x um elemento de R. As seguintes afirmações são equivalentes:*

(a) Existem $a_0, a_1, ..., a_{n-1} \in A$ *tais que*

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0 \tag{2.1}$$

(ou seja, x é uma raiz de um polinômio mônico com coeficientes em A).

(b) O anel A[x] é um A-módulo finitamente gerado.

(c) Existe um subanel B de R que contém A e x e que é um A-módulo finitamente gerado.

Demonstração. $(a) \Longrightarrow (b)$

Chame de M o A-submódulo de R gerado por 1, x, ..., x_{n-1}. Por (a), temos que $x^n \in M$. Multiplicando (2.1) por x^j, nós obtemos $x^{n+j} = -a_{n-1}x^{n+j-1} - ... - a_0x^j$. Usando indução em j, obteremos que $x^{n+j} \in M$, para todo $j \geq 0$. Como A[x] é o A-módulo gerado pelos $x^k (k \geq 0)$, nós vemos que A[x] = M. Assim, (a) implica (b).

$(b) \Longrightarrow (c)$

Isso é claro, basta tomar B = A[x].

$(c) \Longrightarrow (a)$

Seja $(y_1, y_2, ..., y_n)$ um conjunto finito de geradores para B como um A-módulo, ou seja, $B = Ay_1 + Ay_2 + ... + Ay_n$. Como $x \in B$ e B é um subanel de R, segue que $xy_i \in B$ para todo i = 1, 2, ..., n. Portanto:

$$xy_i = \sum_{j=1}^{n} a_{ij} y_j,$$

para qualquer $i = 1, ..., n,\ a_{ij} \in A,\ 1 \leq i,\ j \leq n$. Isto diz que

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0,\ \ i = 1, ..., n.$$

Considere este sistema de n equações lineares homogêneas em $(y_1, ..., y_n)$. Seja d o determinante da matriz $[\delta_{ij} x - a_{ij}]$. Se usarmos a Regra de Cramer, teremos que $dy_i = 0$ para todo i. Isto nos diz que $db = 0$ para todo $b \in B$; em particular, $d.1 = 0$, então $d = 0$. Mas d claramente é um polinômio mônico em x, pois o termo de maior grau aparece na expansão do produto $\prod_{i=1}^{n} (x - a_{ii})$ das entradas na diagonal principal. Assim, (c) implica (a). □

Definição 2.1. *Seja R um anel e seja A um subanel de R. Um elemento x de R é chamado inteiro sobre A se ele satisfaz uma, portanto todas, das condições (a), (b) e (c) do Teorema 2.1. Seja* $P \in A[x]$ *um polinômio mônico tal que* $P(x) = 0$ *(a condição (a) garante que tal polinômio existe). A relação* $P(x) = 0$ *é chamada de uma equação de dependência inteira de x sobre A.*

Um exemplo típico é $x = \sqrt{2}$ de $\mathbb{R}$. Veja que x é inteiro sobre $\mathbb{Z}$. A relação $x^2 - 2 = 0$ é uma equação de dependência inteira.

Proposição 2.1. *Seja R um anel, A um subanel de R e seja* $(x_i)_{1 \leq i \leq n}$ *um conjunto finito de elementos de R. Se para todo i,* x_i *é inteiro sobre* $A[x_1, ..., x_{i-1}]$ *(em particular, se todos os* $x_i's$ *são inteiros sobre A), então* $A[x_1, ..., x_n]$ *é um A-módulo finitamente gerado.*

Demonstração. Ver [11], Proposição 1 da página 28. □

Corolário 2.1. *Seja R um anel, A um subanel,* x *e* y *elementos de R que são inteiros sobre A. Então* $x + y,\ \ x - y$ *e* xy *são inteiros sobre A.*

Demonstração. Observe que $x + y,\ \ x - y,\ \ xy \in A[x, y]$. Pela Proposição 2.1, $A[x, y]$ é um A-módulo finitamente gerado. Pela parte (c) do Teorema 2.1, $x + y,\ \ x - y\ \ e\ \ xy$ são inteiros sobre A. □

Corolário 2.2. *Seja R um anel e seja A um subanel de R. O conjunto A' dos elementos de R que são inteiros sobre A é um subanel de R que contém A.*

Demonstração. O corolário 2.1 implica que A' é um subanel de R. Nós temos que $A \subset A'$, pois se $a \in A$, a é uma raiz do polinômio mônico $P(X) = X - a$, que tem coeficientes em A. □

Definição 2.2. *Seja R um anel e A um subanel de R. O anel A' dos elemento de R que são inteiros sobre A é chamado de fecho inteiro de A em R. Seja A um domínio de integridade e seja K o seu corpo de frações. O fecho inteiro de A em K é chamado de fecho inteiro de A. Seja B um anel e A um subanel de B. Nós dizemos que B é inteiro sobre A se todo elemento de B é inteiro sobre A (ou seja, o fecho inteiro de A em B é o próprio B).*

Proposição 2.2. *(Transitividade) Sejam C um anel, B um subanel de C e A um subanel de B. Se B é inteiro sobre A e se C é inteiro sobre B, então C é inteiro sobre A.*

Demonstração. Seja $x \in C$. Então x é inteiro sobre B, logo, existe uma equação de dependência inteira $x^n + b_{n-1}x^{n-1} + ... + b_0 = 0$ com $b_i \in B$, $i = 0, 1, ..., n-1$. Ponha $B' = A[b_0, ..., b_{n-1}, x]$. Então x é inteiro sobre B'. Como B é inteiro sobre A, os b_i's são inteiros sobre A. Portanto, pela Proposição 2.1 temos que $B' = A[b_0, ..., b_{n-1}, x]$ é um A-módulo finitamente gerado. Pela parte (c) do teorema 2.1, x é inteiro sobre A. Logo, C é inteiro sobre A. □

Proposição 2.3. *Seja B um domínio de integridade e A um subanel de B tal que B é inteiro sobre A. Para que B seja um corpo é necessário e suficiente que A seja um corpo.*

Demonstração. Suponha que A seja um corpo e seja $b \in B$, $b \neq 0$. então A[b] é um espaço vetorial sobre A de dimensão finita, pela parte (b) do teorema 2.1. Por outro lado, $y \mapsto by$ é uma transformação A-linear sobre A[b]. Essa transformação linear é injetiva pois A[b] é um domínio de integridade e $b \neq 0$. Como A[b] é de dimensão finita conclui-se que que a transformação linear é sobrejetiva. Logo, existe $b' \in A[b]$ tal que $bb' = 1$. Isto diz que, para qualquer $b \in B - (0)$, b é invertível em B, ou seja, B é um corpo.

Reciprocamente, suponha que B seja um corpo. Seja $a \in A - (0)$. Então a tem um inverso $a^{-1} \in B$ que satisfaz uma equação de dependência inteira

$$a^{-n} + a_{n-1}a^{-n+1} + ... + a_1a^{-1} + a_0 = 0, a_i \in A.$$

Multiplicando por a^{n-1}, nós obtemos

$$a^{-1} = -(a_{n-1} + ... + a_1a^{n-2} + a_0a^{n-1}),$$

que mostra que $a^{-1} \in A$. Assim A é um corpo. □

2.2 Anéis integralmente fechados

Definição 2.3. *Um Anel A é chamdo integralmente fechado se ele é um domínio de integridade e se ele é o seu próprio fecho inteiro.*

Em outras palavras, cada elemento x do corpo de frações K de A que é inteiro sobre A pertence à A.

Exemplo 1 Seja A um domínio de integridade e seja K seu corpo de frações. Então o fecho inteiro de A' de A (isto é, o fecho inteiro de A em K) é integralmente fechado. Isto segue do fato de que o fecho inteiro de A' é inteiro sobre A', portanto sobre A, pela Proposição 2.2. Sendo assim igual a A'.

Exemplo 2 Todo anel de ideais pricipais é integralmente fechado.

Demonstração. Por definição, um anel de ideais principais é um domínio de integridade. Seja x um elemento do corpo de frações de A que é inteiro sobre A. Seja

$$x^n + a_{n-1}x^{n-1} + \ ... \ a_1x + a_0 = 0 \quad (a_i \in A)$$

uma equação dependência inteira para x sobre A. Escreva $x = a/b$ com a e b elementos relativamente primos de A, afinal A é um domínio de ideais principais. Substituindo x na equação acima e multiplicando por b^n em ambos os lados, obtemos

$$a^n + b(a_{n-1}a^{n-1} + \ ... \ a_1ab^{n-2} + a_0b^{n-1}) = 0.$$

Assim, b divide a^n e aplicando repetidamente o lema de Euclides, temos que b divide a. Mas isto contradiz o fato de a e b serem relativamente ptimos. Assim, não há irredutíveis dividindo b e portanto b é uma unidade em A. Assim, $x = a/b \in A$ e A é integralmente fechado. □

O mesmo argumento mostra que todo domínio de fatoração única também é integralmente fechado. Mostraremos agora um exemplo de um anel que não é integralmente fechado.

Exemplo 3 Considere o anel A = $\mathbb{Z}[\sqrt{-3}]$. É elementar que A tem corpo de frações $K = \mathbb{Q}(\sqrt{-3})$. Observe que o elemento $\alpha = \dfrac{-1+\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3})$ é raiz do polinômio mônico $P(X) = X^2 + X + 1 \in \mathbb{Z}[X] \subset \mathbb{Z}[\sqrt{-3}][X]$. Mas $\alpha \notin \mathbb{Z}[\sqrt{-3}]$. Logo, A não pode ser integralmente fechado.

Neste exemplo vemos também outro fato: α é raiz de $P(X) = X^2 + X + 1$ que tem coeficientes inteiros. Logo α é inteiro sobre $\mathbb{Z}$ e estará no fecho inteiro de $\mathbb{Z}$ em $\mathbb{Q}(\sqrt{-3})$.

Observe que isso não contradiz a afirmação de $\mathbb{Z}$ ser integralmente fechado, pois $\mathbb{Q}(\sqrt{-3})$ não é o corpo de frações de $\mathbb{Z}$.

Uma pergunta interessante a se fazer é: Quem é o fecho inteiro de $\mathbb{Z}[\sqrt{-3}]$ no seu corpo de frações? Para responder tal pergunta, daremos aqui a indicação dos seguintes resultados:

(a) Seja K uma extensão de grau 2 sobre $\mathbb{Q}$, então K é da forma $\mathbb{Q}(\sqrt{d})$, onde d é livre de quadrados;

(b) Seja $K = \mathbb{Q}(\sqrt{d})$ uma extensão de grau 2 de $\mathbb{Q}$ com $d \in \mathbb{Z}$ livre de quadrados, ou seja, $d \not\equiv 0 \pmod 4$. Então:

i) Se $d \equiv 2$ ou $d \equiv 3 \pmod 4$, o fecho inteiro de $\mathbb{Z}$ em K consiste de todos os elementos da forma $a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$.

ii) Se $d \equiv 1 \pmod 4$, o fecho inteiro de $\mathbb{Z}$ em K consiste de todos os elementos da forma $\frac{1}{2}(u + v\sqrt{d})$, com $u, v \in \mathbb{Z}$ de mesma paridade.

As demonstrações destes resultados podem ser facilmente encontradas em [11] páginas 34 e 35 e a parte b) - ii) garante a resposta para o fecho inteiro de $\mathbb{Z}[\sqrt{-3}]$.

2.3 Elementos algébricos sobre um corpo. Extensões finitas e algébricas

Apresentaremos nesta seção alguns conceitos sobre elementos algébricos. Daremos também aqui uma rápida exposição sobre extensões finitas e algébricas.

Definição 2.4. *Sejam R um anel e K um subcorpo de R. Um elemento* $x \in R$ *é chamado de algébrico sobre K se existem elementos* $a_0, a_1, ..., a_n \in K$, *nem todos nulos, tais que* $a_n x^n + ... + a_1 x + a_0 = 0$. *Um elemento de R que não é algébrico sobre K é chamado de Transcendental sobre K.*

Na relação da definição anterior, nós podemos assumir que $a_n \neq 0$. Neste caso, $a_n^{-1} \in K$; multiplicando por a_n^{-1} nós obtemos uma equação de independência inteira. Com isso teremos a seguinte proposição:

Proposição 2.4. *Sejam R um anel e K um subcorpo de R. Então* $x \in R$ *é um elemento algébrico sobre K se e somente se, é inteiro sobre K.*

Dados um corpo L e um subcorpo K de L, podemos considerar L como um espaço vetorial sobre K, em relação a operação externa K x L $\to$ L, definida como restrição da mutiplicação em L. Como L é um espeço vetorial, faz sentido então falarmos de uma base para L. A dimensão do espaço vetorial L é denotado por [L:K] e é chamado de *grau* da extensão L sobre K. Diremos que a extensão L sobre K é finita quando $[L : K] < \infty$.

Nós dizemos que um anel R contendo um corpo K é *algébrico* sobre K se todo elemento de R é algébrico sobre K. Se R é um corpo, então R é chamado de uma *extensão algébrica* de K.

Proposição 2.5. *Seja K um corpo, L uma extensão algébrica de K e M uma extensão algébrica de L. Então M é uma extensão algébrica de L. Mais ainda,* $[M : K] = [M : L][L : K]$.

Demonstração. A primeira afirmação nada mais é do que um caso especial da Proposição 2.2. Além disso, se $(x_i)_{i\in I}$ é uma base de L sobre K e $(y_j)_{j\in J}$ é uma base de M sobre L, então $(x_i y_j)_{(i,j)\in IxJ}$ é uma base para M sobre K. Pela Proposição 2.1, nós temos que $(x_i y_j)_{(i,j)\in IxJ}$ gera M sobre K. A relação $\sum a_{ij}x_i y_j = 0$ com $a_{ij} \in K$ implica que $\sum(\sum a_{ij}x_i)y_j = 0$, quando $\sum a_{ij}x_i = 0$ para todo j, pois $\sum a_{ij}x_i \in L$ e consequetemente $a_{ij} = 0$ para todo $(i, j) \in IxJ$. Isto prova que $[M : K] = [M : L][L : K]$. □

Enunciaremos agora dois teoremas que relacionam extensões algébricas e finitas.

Teorema 2.2. *Sejam L um corpo, K um subcorpo de L e* $x \in L$. *São equivalentes:*

(i) x é algébrico sobre K;

(ii) K[x] é um corpo;

(iii) $[K[x] : K] < \infty$, *ou seja K[x] é uma extensão finita de K.*

Demonstração. Ver [5], página 34. □

Teorema 2.3. *Seja L um corpo e K um subcorpo de L. São equivalentes:*

(i) L é uma extensão finita de K;

(ii) L é uma extensão finitamente gerada e algébrica;

(iii) Existem $a_1, ..., a_r \in L$ *algébricos sobre K tais que* $L = K[a_1, ..., a_r]$.

Demonstração. Ver [5], página 35. □

Definição 2.5. *Qualquer extensão finita L sobre* $\mathbb{Q}$ *é chamado de corpo de números algébricos, ou simplesmente de corpo de números.*

Observe que faz sentido essa denotação já que, sendo L uma extensão finita de $\mathbb{Q}$, pelo Teorema 2.3 toda extensão finita é algébrica.

Agora nós estudaremos os elementos algébricos sobre um corpo em maiores detalhes. Seja R um anel, K um subcorpo de R e seja x um elemeto de R. Escreveremos K[X] para o anel de polinômios em uma variável sobre K. Existe um único homomorfismo $\varphi : K[X] \longrightarrow R$ tal que $\varphi(X) = x$ e tal que $\varphi(a) = a$ para todo $a \in K$. A imagem de φ é K[x]. Com isso, a definição de elemento algébrico pode ser reformulada como a seguir:

Um elemento x é algébrico sobre K se, e somente se $Ker(\varphi) \neq (0)$.

Para ver isto, observe que se x é um elemento transcendental sobre K, então é óbvio que $Ker(\varphi) = (0)$. Em qualquer caso, o ideal $Ker(\varphi)$ é um ideal principal (F(X)), pois K[X] é um anel de ideais principais. No caso em que x é algébrico sobre K, ele é gerado por um polinômio não-nulo F(X).

Nós podemos assumir que F(X) é mônico, pois K é um corpo. F(X) é unicamente determinado por K e x; nós chamaremos ele de *polinômio minimal* (ou mínimo) de x sobre K.

Propriedades importantes do polinômio minimal são:

a) Seja F(X) o polinômio minimal de x sobre K. Seja $G(X) \in K[X]$. $G(x) = 0$ se e somente se, F(X) divide G(X) em K[X].

b) Seja $K \subset L \subset \mathbb{C}$, onde L é uma extensão de um corpo de números algébricos K. Se $\alpha \in L$ é algébrico sobre K, então: [K(α):K] = grau(F(X)), onde F(X) é polinômio minimal de α em K.

Tais demonstrações podem ser vistas facilmente em [5], nas páginas 37 e 38.

Observe que passando para anéis quocientes, nós podemos obter um *isomorfismo canônico*:

$$K[X]/(F(X)) \longrightarrow K[x].$$

Para ver isto, defina a aplicação: $\varphi : K[X] \longrightarrow K[x]$, e ponha $\varphi(X) = x$. Claramente essa aplicação é um homomorfismo sobrejetivo e $Ker(\varphi) = (F(X))$ devido a propriedade [a] citado acima. Pelo teorema dos isomorfismos temos o resultado.

Com a mesma notação, suponha que x é algébrico sobre K e seja F(X) o seu polinômio minimal. Pelas propriedades acima citadas e a Proposição 2.3 , nós obtemos as seguintes equivalências:

$K[x]$ é um corpo $\Longleftrightarrow$ $K[x]$ é um domínio de integridade $\Longleftrightarrow$ $F(X)$ é irredutível.

Por outro lado, se K é um corpo e $F(X) \in K[X]$ é irredutível, então K[X]/(F(X)) é um corpo contendo K e escrevendo x para a projeção de $X \in K[X]$ neste corpo nós temos $F(x) = 0$. Assim $X - x$ divide F(X) no corpo K[x].

Proposição 2.6. *Seja K um corpo e seja* $P(X) \in K[X]$ *um polinômio não-constante. Existe uma extensão algébrica de grau finita K' de K tal que P(X) fatora-se, em K'[X], em um produto de polinômios de grau 1.*

Demonstração. Nós vamos provar a proposição por indução no grau d^o de P(X). Se $d^o = 1$, não há nada a se provar. Seja F(X) um fator irredutível de P(X). Nós acabamos de ver que existe uma extensão K"de grau finito sobre K, (no caso K[X]/(F(X))) contendo um elemento x tal que $X - x$ divide F(X) em K"[X]. Assim $P(X) = (X - x)P_1(X)$ com $P_1(X) \in K"[X]$. Pela hipótese de indução $P_1(X)$ fatora-se em um produto de polinômios lineares em alguma extensão K' de grau finito sobre K". Pela Proposição 2.5, K' é de grau finito sobre K e P(X) é um produto de fatores lineares em K'[X]. □

Um corpo K é chamado *Algebricamente Fechado* se cada polinômio não-constante $P(X) \in K[X]$ pode ser expresso como produto de fatores lineares, com todos os fatores em K[X]. Podemos provar por meio de técnicas de Análise Matemática que o corpo $\mathbb{C}$ é algebricamente fechado.

2.4 Elementos conjugados e corpos conjugados

Dados dois corpos L e L' ambos contendo um corpo K, chamaremos qualquer monomorfismo $\sigma : L \longrightarrow L'$ tal que $\sigma(a) = a$ para todo $a \in K$ de um K-isomorfismo de L em L'. Neste caso, dizemos que L e L' são K-isomorfos ou (se eles forem algébricos sobre K) conjugados sobre K, observando que "isomorfismo"no sentido que σ é bijetivo sobre a imagem. Dada duas extensões L e L' de K, diremos que dois elementos $x \in L$ e $x' \in L'$ são conjugados sobre K se existe um K-isomorfismo $\sigma : K(x) \longrightarrow K(x')$ tal que $\sigma(x) = x'$. Observe que tal σ é única. A existência de σ nos diz que ou x e x' são ambos transcedentais sobre K ou ambos são algébricos sobre K com o mesmo polinômio minimal.

Exemplo 4.1 - Considere L = $\mathbb{Q}(\sqrt{3})$ e L' = $\mathbb{C}$. Então as aplicações

$$\sigma_1 : \sqrt{3} \mapsto \sqrt{3} \ \ e \ \ \sigma_2 : \sqrt{3} \mapsto -\sqrt{3},$$

fixam os pontos de $\mathbb{Q}$.

Exemplo 4.2 - Sejam L = $\mathbb{Q}(\sqrt{-2})$ e L' = $\mathbb{C}$. As aplicações dadas por:

$$\sigma_1 : \sqrt{-2} \mapsto \sqrt{-2} \ \ e \ \ \sigma_2 \mapsto -\sqrt{-2}$$

também fixam o corpo $\mathbb{Q}$.

Lema 2.1. *Seja K um corpo de característica zero ou um corpo finito, seja* $F(X) \in K[X]$ *um polinômio mônico irredutível e seja* $F(X) = \prod_{i=1}^{n}(X - x_i)$ *sua decomposição em produto de fatores lineares em uma extensão de K' de K. Então as n raízes* $x_1, ..., x_n$ *de F(X) são distintas.*

Demonstração. Ver [11], Proposição 1 da página 36. □

Teorema 2.4. *Seja K um corpo de característica zero ou um corpo finito, seja K' uma extensão finita de grau n de K e seja C um corpo algebricamente fechado contendo K. Então existem n K-isomorfismos distintos de K' em C.*

Demonstração. Nossa afirmação é verdadeira para qualquer extensão K' de K que é da forma K[x] com $x \in K'$. De fato, o polinômio minimal F(X) de x sobre K é então de grau n. Ele tem n raízes $x_1, ..., x_n$ em C, dos quais todos distintos, devido ao lema anterior. Para qualquer $i = 1, 2, ..., n$ nós temos então um K-isomorfismo $\sigma_i : K' \longrightarrow C$ tal que $\sigma_i(x) = x_i$. Nós continuaremos por indução no grau n de K'. Seja $x \in K'$, considere os corpos $K \subset K[x] \subset K'$ e ponha $q = [K[x] : K]$. Nós podemos assumir $q > 1$. Nós vimos que existem q K-isomorfismos distintos $\sigma_1, ..., \sigma_q$ de K[x] em C. Como $K[\sigma_i(x)]$ e K[x] são isomorfos, é possivel construir uma extensão K_i' de $K[\sigma_i(x)]$ e um isomorfismo $\tau_i : K' \longrightarrow K_i'$ que extende σ_i. Claramente $K[\sigma_i(x)]$ é um corpo de característica zero ou um corpo finito. Visto que $[K_i' : K[\sigma_i(x)]] = [K' : K[x]] = n/q < n$, a hipótese de indução implica que existem n/q $K[\sigma_i(x)]$-isomorfismos θ_{ij} distintos de K_i' em C. Observe que eles são distintos, pois para $i \neq j$, $\theta_{ij} \circ \tau_i$ e $\theta_{i'j'} \circ \tau_{i'}$ diferem em K[x] quando $i = i'$, mas para $j \neq j'$, θ_{ij} e $\theta_{ij'}$ diferem em K_i'. □

Exemplo 4.3 - Considere o corpo $\mathbb{Q}(\sqrt[3]{2})$. Sabemos da teoria dos corpos que este corpo é uma extensão de grau 3 do corpo $\mathbb{Q}$. Pelo teorema anterior, existem 3 $\mathbb{Q}$-isomorfismos de $\mathbb{Q}(\sqrt[3]{2})$ em $\mathbb{C}$. São eles:

$$\sigma_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \ \ \sigma_2 : \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2} \ \ e \ \ \sigma_3 : \sqrt[3]{2} \mapsto \zeta_3^2\sqrt[3]{2},$$

onde ζ_3 é uma raiz primitiva cúbica da unidade.

Teorema 2.5. *Se* $E \subset \mathbb{C}$ *é uma extensão finita do corpo F, então cada monomorfismo de F em* $\mathbb{C}$ *extende-se a exatamente* $[E : F]$ *monomorfismos de E em* $\mathbb{C}$*. Em particular, existem* $[E : F]$ *F-isomorfismos de E.*

Demonstração. Nós usaremos indução em [E:F]. Se $E = F$, então o resultado é claro, então nós podemos asumir que toda extensão K de F com $[K : F] \leq [E : F]$ satisfaz a propriedade que cada monomorfismo de F em $\mathbb{C}$ extende-se a [K:F] monomorfismos de K em $\mathbb{C}$. Seja $\alpha \in E - F$ e seja $m_{\alpha,F}(x)$ o polinômio minimal de α sobre F. Denotemores ele por $m(x)$. Se σ é um monomorfismo de F em $\mathbb{C}$, seja $m^{\sigma}(x)$ o polinômio obtido aplicando σ aos coeficientes de $m(x)$. Assim, $m^{\sigma}(x)$ é irredutível sobre $\sigma(F)$. Se α_j é uma raiz de $m(x)$, nós podemos definir o isomorfismo σ_j por:

$$\sigma_j|_F = \sigma, \quad e \quad \sigma_j : \alpha \mapsto \alpha_j,$$

tal que nós temos o isomorfismo entre corpos

$$\sigma_j : F(\alpha) \mapsto F(\alpha_j).$$

Existem

$$n = grau(m(x)) = [F(\alpha) : F]$$

escolhas para σ_j. Daí, existem *exatamente* n extensões distintas de σ a $F(\alpha)$ pois um monomorfismo de $F(\alpha)$ em $\mathbb{C}$ é completamente determinada por suas ações em F e em α. Por hipótese de indução, cada um destes monomorfismos extende-se a exatamente $[E:F(\alpha)]$ monomorfismos de E em $\mathbb{C}$. Portanto, existem

$$[E : F(\alpha)] \cdot [F(\alpha) : F] = [E : F]$$

monomorfismos distintos de E em $\mathbb{C}$ que extende σ. Finalmente, toda extensão de σ a E deve ser um destes, uma vez que não pode haver mais do que [E:F] de tais monomorfismos, considerando as restrições dos monomorfismos já existentes. □

O Teorema 2.5 motiva o seguinte link entre o polinômio minimal de qualquer número algébrico $\beta \in F = \mathbb{Q}(\alpha)$ e o polinômio

$$f(x) = \prod_{j=1}^{n} (x - \sigma_j(\beta)),$$

chamado *corpo polinomial* de β sobre F, onde os σ_j são todos monomorfismos de F em $\mathbb{C}$.

Teorema 2.6. *Seja F um corpo de números de grau n com monomorfismos σ_1, ..., σ_n de $\mathbb{Q}$ em $\mathbb{C}$. Se $\beta \in F$ é um número algébrico de grau d sobre $\mathbb{Q}$, com polinômio minimal $m(x) = m_{\beta,\mathbb{Q}}(x)$, nós temos a seguinte fatoração do corpo polinomial de β sobre $\mathbb{Q}$:*

$$f(X) = \prod_{j=1}^{n}(X - \sigma_j(\beta)) = m^{n/d}(X),$$

onde $n/d \in \mathbb{N}$. Assim, os $\sigma_j(\beta)$ são raízes de m(x), repetida n/d vezes na fatoração de $f(x) \in \mathbb{Q}[X]$. Também $F = \mathbb{Q}(\beta)$ se, e somente se, d = n.

Demonstração. Como $\mathbb{Q}(\beta)$ é um subcorpo de F, então:

$$n = [F : \mathbb{Q}] = [F : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = [F : \mathbb{Q}(\beta)] \cdot d.$$

Assim, $n/d \in \mathbb{N}$ e $F = \mathbb{Q}(\beta)$ se, e somente se, d = n.

Pela definição de $\mathbb{Q}$-isomorfismo, a restrição de σ_j a $\mathbb{Q}(\beta)$ continua sendo um $\mathbb{Q}$-isomorfismo. Portanto, podemos arranjar os σ_j's tais que os primeiros d deles são os distintos de $\mathbb{Q}(\beta)$ em $\mathbb{C}$, quando considerado como restição a ele. Assim,

$$m(x) = \prod_{j=1}^{n}(x - \sigma_j(\beta)) = \prod_{j=1}^{n}(x - \beta_j). \tag{2.2}$$

Observe que $m(x)|f(x)$, pois $f(\beta) = f(\sigma_1(\beta)) = 0$. Assim, para algum $N \in \mathbb{N}$ e algum polinômio mônico $g(X) \in F[X]$, nós temos $f(x) = m^N(x)$, onde $m.d.c.(m(x), g(x)) = 1$. Se g(x) não é constante, existe um inteiro algébrico γ tal que $g(\gamma) = 0$. Assim, $f(\gamma) = 0$, então, $\gamma = \sigma_j(\beta)$, para algum $j = 1, 2, ..., d$. Portanto pela equação (2.2), $\sigma_j(\beta) = \beta_j$, então $m(x)|g(x)$, uma contradição. Assim, $f(x) = m^N(x) \in \mathbb{Q}[X]$, então $n = grau(f) = grau(m^N) = dN$. Portanto, $N = n/d$

□

2.5 O discriminante

Nesta seção nós introduziremos um conceito importantíssimo na Teoria Algébrica dos Números que é o conceito de *discriminante*. Para tanto, precisamos rever algumas noções de Álgebra linear, tais como *traço*, *determinante* e o *polinômio característico*.

Sejam A um anel, E um A-módulo livre finitamente gerado e seja *u* um endomorfismo de E. Seja (e_i) uma base escolhida para E e seja (a_{ij}) a matriz de *u* com respeito a esta base. Então o traço, o determinante e o polinômio característico de *a* são respectivamente:

$$Tr(u) = \sum_{i=1}^{n} a_{ii},\ \ det(u) = det(a_{ij})\ \ e\ \ det(X \cdot I_E - u) = det(X\delta_{ij} - a_{ij}).$$

É possível verificar que estas quantidades independem da escolha da base.

As fórmulas acima implicam: (i) $Tr(u+u') = Tr(u) + Tr(u')$;
(ii) $det(uu') = det(u)det(u')$;
(iii) $det(X_E - u) = X^n - (Tr(u))X^{n-1} + ... + (-1)^n det(u)$.

Agora nós vamos falar de normas e traços em uma extensão.

Seja B um anel e seja A um subanel de B tal que B é um A-módulo livre de grau n (por exemplo, A pode ser um corpo e B uma extensão finita de grau n de A). Para $x \in B$, a multiplicação m_x por x (ou seja, $y \mapsto xy$) é um endomorfismo do A-módulo B.

Definição 2.6. *Nós chamamos de traço (respectivamente norma e polinômio característico) de* $x \in B$ *relativo a B e A, o traço (respectivamente determinante e polinômio característico) do endomorfismo* m_x.

O traço (respectivamente norma) de x é denotado por $Tr_{B/A}(x)$ (respectivamente $N_{B/A}(x)$) ou Tr(x) (respectivamente N(x)) quando não há possibilidade de confusão. Eles são elementos de A. Para $x, x' \in B$ e $a \in A$ nós temos $m_x + m_{x'} = m_{x+x'},\ \ m_x \circ m_{x'} = m_{xx'}\ \ e\ \ m_{ax} = am_x$. Portanto, a matriz de m_a com respeito a qualquer base para B, é a matriz diagonal cujas entradas são a. Podemos verificar facilmente que:

$$Tr(x+x') = Tr(x) + Tr(x'),\ \ Tr(ax) = aTr(x),\ \ Tr(a) = na$$
$$N(xx') = N(x)N(x'),\ \ N(a) = a^n\ \ \ e\ \ \ N(ax) = a^n N(x).$$

Demonstração. Ver [11]. □

Assim, o polinômio característico é a [L:K[x]]-ésima potência do polinômio minimal de x sobre K.

Proposição 2.7. *Sejam K um corpo de característica 0 ou um corpo finito, L uma extensão algébrica de grau* n *de K,* x *um elemento de L e* $x_1, ..., x_n$ *as* n *raízes do polinômmio minimal de* x *sobre K, cada uma repetida* $[L : K[x]]$ *vezes. Então* $Tr_{L/K}(x) = x_1 + ... + x_n,\ \ N_{L/K}(x) = x_1...x_n$. *O polinômio característico de* x *relativo a L e K é* $(X - x_1)...(X - x_n)$.

A Proposição 2.7 nos diz que poderíamos ter definido a norma e o traço de um elemento x como a seguir:

$$Tr_{L|K}(x) = \sum_{i=1}^{n} \sigma_i(x)\ \ e\ \ N_{L|K}(x) = \prod_{i=1}^{n} \sigma_i(x), \tag{2.3}$$

onde os σ_i's são definidos como no inicio da seção 2.4.

Proposição 2.8. *Sejam A um domínio de integridade, K seu corpo de frações, L uma extensão finita de grau n de K e x um elemento de L inteiro sobre A. Assuma que K tem característica 0. Então os coeficientes do polinômio característico P(X) de x relativo a L e K, em particular,* $Tr_{L/K}(x)$ *e* $N_{L/K}(x)$, *são inteiros sobre A.*

Demonstração. Ver [11], ver Proposição 2 da página 38. □

Corolário 2.3. *Suponha que A é integralmente fechado. então os coeficientes do polinômio característico de x, em particular o* $Tr_{L/K}(x)$ *e* $N_{L/K}(x)$ *são elementos de A.*

Demonstração. Pela definição, estes coeficientes são elementos de K. Pela Proposição 2.8, eles são inteiros sobre A. □

A partir dos conceitos citados, podemos agora definir o discriminante de um conjunto de elementos de um anel A.

Definição 2.7. *Seja B um anel e seja A um subanel de B tal que B é um A-módulo livre de grau n. Para* $(x_1,...,x_n) \in B^n$ *nós chamamos o discriminante do conjunto* $(x_1,...,x_n)$ *o elemento de A definido pela relação*

$$D(x_1,...,x_n) = \det(Tr_{B/A}(x_i x_j)). \tag{2.4}$$

Proposição 2.9. *Se* $(y_1,...,y_n) \in B^n$ *é um outro conjunto de elementos de B tais que* $y_i = \sum_{i=1}^{n} a_{ij}x_j$ *com* $a_{ij} \in A$, *então*

$$D(y_1,...,y_n) = (\det(a_{ij}))^2 D(x_1,...,x_n). \tag{2.5}$$

Demonstração.

$$Tr(y_p y_q) = Tr(\sum_{i,j} a_{pi}a_{qj}x_{ij}) = \sum_{i,j} a_{pi}a_{qj}Tr(x_i y_j).$$

Isto dá a matriz: $(Tr(y_p yq)) = (a_{pi})(Tr(x_i x_j) \cdot {}^t(a_{qj})$, onde ${}^tM$ denota a matriz transposta de M. Assim, tomando determinantes em ambos os lados e usando propriedades dos determinantes, chegaremos no resultado. □

A Proposição 2.8 implica que o discriminante de bases de B sobre A são *associados* em A, ou seja, a matriz mudança de base (a_{ij}) tem uma inversa com entradas em A. Portanto ambos os $\det(a_{ij})$ *e* $\det(a_{ij})^{-1}$ são unidades em A. Nós podemos assim formular a seguinte definição:

Definição 2.8. *Sob as hipóteses da Definição 2.7, nós chamaremos o ideal principal de A gerado pelo discriminante de qualquer base B sobre A o discriminante de B sobre A. Nós denotaremos ele por* $\mathcal{D}_{B/A}$.

Proposição 2.10. *Suponha que* $\mathcal{D}_{B/A}$ *contém um elemento que não é um divisor de zero. Então, a fim de que o conjunto* $(x_1,...,x_n) \subset B^n$ *seja uma base para B sobre A, é necessário e suficiente que* $D(x_1,...,x_n)$ *gere* $\mathcal{D}_{B/A}$.

Demonstração. A condição necessária já foi provada. Para a recíproca, suponha que $d = D(x_1,...,x_n)$ seja um gerador para $\mathcal{D}_{B/A}$. Seja $(e_1,...,e_n)$ uma base para B sobre A. Ponha $d' = D(e_1,...,e_n)$ e $x_i = \sum_{j=1}^{n} a_{ij}e_j$ com $a_{ij} \in A, 1 \leq i \leq n$. Então $d = det(a_{ij})^2 d'$. Por hipótese $Ad = \mathcal{D}_{B/A} = Ad'$. Assim, existe $b \in A$ tal que $d' = bd$. Segue que $d(1 - bdet(a_{ij})^2) = 0$. Veja que d não é um divisor de zero, pois se fosse, cada elemento de $Ad = \mathcal{D}_{B/A}$ seria um divisor de zero. Assim $1 - bdet(a_{ij})^2 = 0$. Isto nos diz que $det(a_{ij})$ é invertível, portanto a matriz (a_{ij}) deve ser invertível também. Consequentemente, $(x_1,...,x_n)$ é uma base de B sobre A. □

Lema 2.2. *(Lema de Dedekind) Sejam G um grupo, C um corpo e sejam* $\sigma_1,...,\sigma_n$ *homomorfismos distintos de G no grupo multiplicativo C*. Então os* $\sigma_i's$ *são linearmente independentes sobre C, ou seja,* $\sum u_i\sigma_i(g) = 0$, *para todo* $g \in G$ *implica que todos os* $u_i's$ *são zero.*

Demonstração. Suponha que os $\sigma_i's$ são linearmente dependentes e considere a relação não-trivial $\sum_i u_i\sigma_i = 0 \quad (u_i \in C)$ tal que o número q de $u_i's$ que são não-nulos é mínimo. Após um rearranjo de indíces, nós podemos supor que

$$u_1\sigma_1(g) + ... + u_q\sigma_q(g) = 0 \text{ para todo } g \in G. \tag{2.6}$$

Nós temos $q \geq 2$, pois os $\sigma_i's$ são não-nulos. Para *g* e *h* arbitrários em G, nós temos que $u_1\sigma_1(hg) + ... + u_q\sigma_q(hg) = u_1\sigma_1(h)\sigma_1(g) + ... + u_q\sigma_q(h)\sigma_q(g) = 0$. Mutiplicando (2.6) por $\sigma_1(h)$ e subtraindo da equação acima, temos:

$$u_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + ... + u_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0.$$

Como isto se verifica para qualquer $g \in G$ e como q foi escolhido o menor possível, segue que $u_2(\sigma_1(h) - \sigma_2(h)) = 0$. Assim $\sigma_1(h) = \sigma_2(h)$ para todo $h \in G$, pois $u_2 \neq 0$. Mas isto contradiz a hipótese de que os $\sigma_i's$ são distintos. Logo, os $\sigma_i's$ são linearmente independentes. □

Proposição 2.11. *Seja K um corpo que é finito ou de característica 0, seja L uma extensão de grau n de K e sejam* $\sigma_1,...,\sigma_n$ *os n K-isomorfismos distintos de L em um corpo algebricamente*

fechado C contendo K (ver Teorema 2.4). Então, se $(x_1,...,x_n)$ *é uma base para L sobre K,*

$$D(x_1,...,x_n) = \det(\sigma_i(x_j))^2 \neq 0. \tag{2.7}$$

Demonstração. A primeira igualdade segue do cálculo:
$D(x_1,...,x_n) = \det(\mathrm{Tr}(x_i x_j)) = \det(\sum_k \sigma_k(x_i x_j) = \det(\sum_k \sigma_k(x_i)\sigma_k(x_j))$

$$= \det(\sigma_k(x_i)) \cdot \det(\sigma_k(x_i)) = \det(\sigma_i(x_j))^2.$$

Agora, suponha que $\det(\sigma_i(x_j)) = 0$. Então existem $u_1,...,u_n \in C$, nem todos nulos, tais que $\sum_{i=1}^n u_i\sigma_i(x_j) = 0$ para todo j. Pela linearidade nós concluímos que $\sum_{i=1}^n u_i\sigma_i(x) = 0$ para todo $x \in L$. Mas isto contradiz justamente o lema de Dedekind. □

Sob as condições da Proposição 2.10, a relação $D(x_1,...,x_n) \neq 0$ nos diz que a forma bilinear $(x,y) \mapsto \mathrm{Tr}_{L/K}(xy)$ é *não-degenerada*, ou seja $\mathrm{Tr}_{L/K}(xy) = 0$ para todo $y \in L$ implica $x = 0$. Assim, a aplicação K-linear que associa cada $x \in L$ a forma K-linear $s_x : y \mapsto \mathrm{Tr}_{L/K}(xy)$ é uma injeção de L no seu dual $\mathrm{Hom}_K(L,K)$ (para estruturas de espaço vetorial sobre K). Como L e $\mathrm{Hom}_K(L,K)$ são de mesma dimensão finita n sobre K, segue que $x \mapsto s_x$ é uma bijeção. A existência da "base dual"de um espaço vetorial e seu dual implica que, para qualquer base $(x_1,...,x_n)$ de L sobre K, existe uma base $(y_1,...,y_n)$ tal que

$$\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij} \quad (1 \leq i,j \leq n). \tag{2.8}$$

Dada essa observação, teremos o seguinte teorema.

Teorema 2.7. *Seja A um anel integralmente fechado, seja K o seu corpo de frações, L um extensão de grau n de K e A' o fecho inteiro de A em L. Suponha que K é de característica 0. Então, A' é um A-submódulo de um A-módulo livre de grau n.*

Demonstração. Seja $(x_1,...,x_n)$ uma base de L sobre K. Cada x_i é algébrico sobre K, então, para qualquer i, nós temos uma equação da forma $a_n x_i^n + a_{n-1}x_i^{n-1} + ... + a_0 = 0$. ($a_j \in A$ para todo j). Nós podemos assumir que $a_n \neq 0$. Multiplicando essa equação por a_n^{n-1}, teremos que $a_n x_i$ é inteiro sobre A. Ponha $x_i' = a_n x_i$. Então $(x_1',...,x_n')$ é uma base para L sobre K contido em A'.

Pela observação que fizemos acima, existe uma outra base $(y_1,...,y_n)$ de L sobre K tal que $\mathrm{Tr}(x_i' y_i) = \delta_{ij}$, por (2.6). Seja $z \in A'$. Já que $(y_1,...,y_n)$ é uma base para L sobre K, nós podemos escrever $z = \sum_{j=1}^n b_j y_j$ com $b_j \in K$. Para qualquer i nós temos $x_i' z \in A'$, pois $x_i' \in A'$. Portanto, $\mathrm{Tr}(x_i' z) \in A$, pelo corolário 2.3. Assim, $\mathrm{Tr}(x_i' z) = \mathrm{Tr}(\sum_j b_j x_i' y_j) = \sum_j b_j \mathrm{Tr}(x_i' y_i) =$

$\sum b_j \delta_{ij} = b_i$. Nós podemos concluir que $b_i \in A$ para todo i, o que implica que A' é um submódulo do A-módulo livre $\sum_{j=1}^{n} A y_j$. □

Corolário 2.4. *Adicionando a hipótese de que A é principal ao Teorema 2.7, então A' é um A-módulo livre de grau n.*

Demonstração. Um submódulo de um A-módulo livre é, sob nossas hipóteses adicionais, livre de grau $\leq n$. Por outro lado, nós vimos na prova do Teorema 2.7 que A' contém uma base de L sobre K. Portanto, A' é de grau n. □

2.6 Terminologia de corpos de números

Definição 2.9. *Seja K um corpo de números. Os elementos de K que são inteiros sobre $\mathbb{Z}$ são chamados de inteiros de K e denotaremos o conjuntos desses elementos por $\mathfrak{D}_K$.*

Observe que pelo Corolário 2.2, $\mathfrak{D}_K$ é um subanel de K e ao mesmo tempo é um $\mathbb{Z}$-módulo livre de grau $[K : \mathbb{Q}]$ devido ao Corolário 2.4, ou seja, podemos pedir uma base para $\mathfrak{D}_K$ sobre $\mathbb{Z}$. Obtemos então a seguinte definição:

Definição 2.10. *Se $\mathfrak{D}_K$ é o anel de inteiros de um corpo de números K, então uma base para $\mathfrak{D}_K$ sobre $\mathbb{Z}$, ou simplesmente uma $\mathbb{Z}$-base, é chamada de base integral para K.*

Sendo K um corpo de números de grau n, o Teorema 2.7 em conjunto com o Corolário 2.4 nos garante a existência de uma base integral para K e que tal base é de fato uma base para K sobre $\mathbb{Q}$.

Exemplo 1 Se $K = \mathbb{Q}(\sqrt{2})$, então $\mathfrak{D}_K = \mathbb{Z}[\sqrt{2}]$, devido ao resultado b) - ii) na página 6. Assim, $\beta = \{1, \sqrt{2}\}$ é uma base integral para K.

Exemplo 2 Se $K = \mathbb{Q}(\sqrt{13})$, então

$$\mathfrak{D}_K = \mathbb{Z}[(\tfrac{1+\sqrt{13}}{2})] \neq \mathbb{Z}[\sqrt{13}].$$

Aqui $\alpha = \frac{1+\sqrt{13}}{2}$ é uma raiz de $P(X) = X^2 - X - 3$, enquanto $\beta = \sqrt{13}$ é uma raiz de $Q(X) = X^2 - 13$. Assim. embora que $\eta = \{1, \beta\}$ seja uma base para K consistindo de inteiros algébricos, β não é uma base integral para K. Uma base integral para K é $\tau = \{1, \alpha\}$.

Sendo $\beta = \{x_1, \ ..., \ x_n\}$ uma base integral para K, faremos a seguinte convenção para o discriminante da base β: Disc (β) = $D(x_1, \ ..., \ x_n)$.

Proposição 2.12. *Se* β *é uma base para um corpo de números* K *sobre* $\mathbb{Q}$*, com* $\beta \subset \mathfrak{D}_K$*, então* $Disc\,(\beta) \in \mathbb{Z}$*.*

Demonstração. Segue direto do Corolário 2.3. □

Corolário 2.5. *Sejam* β_1 *e* β_2 *duas bases integrais para um corpo de números K. Então*

$$Disc\,(\beta_1) = Disc\,(\beta_2).$$

Demonstração. Pela Proposição 2.9, temos que

$$\text{Disc}\,(\beta_2) = D^2\text{Disc}\,(\beta_1)$$

onde $D \in \mathbb{Z}$ é dado na proposição. Mas a observação feita logo após a Proposição 2.9, nos garante que D é uma unidade em $\mathbb{Z}$, ou seja, $D = \pm 1$. A igualdade acima conclui imediatamente o corolário. □

Definição 2.11. *Seja* β *uma base integral para um corpo de números K. Então o discriminante absoluto de* K*, denotado por d, é* $d = Disc\,(\beta)$*.*

Exemplo Seja $K = \mathbb{Q}(\sqrt{19})$. Então $\beta = \{1, \sqrt{19}\}$ é uma base integral para K. Portanto,

$$d = \text{Disc}\,(\beta) = \det \begin{pmatrix} 1 & 1 \\ \sqrt{19} & -\sqrt{19} \end{pmatrix}^2 = (-2\sqrt{19})^2 = 76.$$

Enunciaremos aqui dois resultados interessantes sobre discriminantes absolutos de corpos de números, apenas para efeito de curiosidade. São eles

Teorema 2.8. *Seja* $D \neq 1$ *um inteiro livre de quadrados e seja* $K = \mathbb{Q}(\sqrt{D})$*, com discriminante absoluto d. Então*

i. $d = D$*, se* $D \equiv 1$ *(mod 4) ou*

ii. $d = 4D$*, se* $D \equiv 2,3$ *(mod 4),*

onde D é chamado de Radicando de K. Também podemos concluir que

iii. $\mathfrak{D}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$*, se* $d \equiv 1$ *(mod 4) ou*

iv. $\mathfrak{D}_K = \mathbb{Z}[\sqrt{D}]$*, se* $d \equiv 0$ *(mod 4).*

Demonstração. Ver [8] páginas 41 e 42. □

Teorema 2.9. *(Critério de Stickelberger) Seja K um corpo de números. Então*

$$d \equiv 0 \text{ ou } 1 \text{ (mod 4).}$$

Demonstração. Ver [8] páginas 43 e 44. □

Para encerrar, frequentemente, por abuso de linguagem, atribuíremos para K noções que são definidas relativamente para $\mathfrak{D}_K$. Assim quando nós falarmos de ideais (ou unidades) de K, nós estamos nos referindo a ideais (ou unidades) de $\mathfrak{D}_K$.

2.7 Conceitos preliminares de subgrupos discretos do $\mathbb{R}^n$

Nessa seção apresentaremos os conceitos importantes sobre reticulados. Alguns teoremas, bem como suas respectivas provas, irão precisar de alguns conceitos básicos de Análise.

Um subgrupo H do $\mathbb{R}^n$ é dito ser *discreto* se e somente se, para qualquer subconjunto compacto K do $\mathbb{R}^n$, a interseção $H \cap K$ é finita. Um exemplo clássico de um subgrupo discreto do $\mathbb{R}^n$ é $\mathbb{Z}^n$.

Teorema 2.10. *Seja H um subgrupo discreto do $\mathbb{R}^n$. Então H é gerado (como um $\mathbb{Z}$-módulo por r vetores que são linearmente independentes sobre $\mathbb{R}$.*

Demonstração. Seja $(e_1, ..., e_r)$ um conjunto de elementos de H que são linearmente independentes sobre $\mathbb{R}$, onde r é o maior possível. Seja

$$P = \{x \in \mathbb{R}^n \mid x = \sum_{i=1}^{r} \alpha_i e_i,\ 0 \leq \alpha_i \leq 1\} \tag{2.9}$$

o paralelepípedo construído por esses vetores. Claramente, P é compacto, então $P \cap H$ é finito. Tome $x \in H$. Da maximalidade do conjunto $(e_1, ..., e_r)$ segue que $x = \sum_{i=1}^{n} \lambda_i e_i, \quad \lambda_i \in \mathbb{R}$. Para $j \in \mathbb{Z}$ temos

$$x_j = jx - \sum_{i=1}^{r} \lceil j\lambda_i \rceil e_i, \tag{2.10}$$

onde $\lceil \mu \rceil$ denota o maior inteiro menor ou igual a $\mu \in \mathbb{R}$. Assim,

$$x_j = \sum_{i=1}^{r} (j\lambda_i - \lceil j\lambda_i \rceil) e_i,$$

que no qual segue que $x_j \in P$ e por (2.10), $x_j \in P \cap H$. Perceba que $x = x_1 + \sum_{i=1}^{r} \lceil \lambda_i \rceil e_i$, vendo assim que o $\mathbb{Z}$-módulo H é gerado por $P \cap H$ e assim é finitamente gerado. Por outro lado, como $P \cap H$ é finito e $\mathbb{Z}$ é infinito, existem inteiros distintos j e k tais que $x_j = x_k$. Segue de (2.10) que $(j-k)\lambda_i = \lceil j\lambda_i \rceil - \lceil k\lambda_i \rceil$, que implica que os λ_i's são racionais. Assim o $\mathbb{Z}$-módulo H é gerado por um número finito de elementos que são combinações lineares com coeficientes racionais dos e_i's. Seja $d \in \mathbb{Z} - (0)$ um denominador comum destes coeficientes. Claramente, $dH \subset \sum_{i=1}^{r} \mathbb{Z} e_i$. Assim, existe uma base (f_i) do $\mathbb{Z}$-módulo $\sum_{i=1}^{r} \mathbb{Z} e_i$ e inteiros α_i tais que $(\alpha_1 f_1, ..., \alpha_r f_r)$ gera dH. Como o $\mathbb{Z}$-módulo dH tem o mesmo grau de H e $H \supset \sum_{i=1}^{r} \mathbb{Z} e_i$, o grau de dH é $\geq r$. Portanto, o grau de dH é igual a r e os α_i's são não-nulos. Nós podemos concluir que os f_i's são, como os e_i's, linearmente independentes sobre $\mathbb{R}$. O módulo dH, e consequentemente o próprio H, é gerado (sobre $\mathbb{Z}$) por r vetores linearmente independentes sobre $\mathbb{R}$. □

Como aplicação do teorema anterior, seja $t = (\theta_1, ..., \theta_n) \in \mathbb{R}^n$ tal que pelo menos um dos θ_i's é irracional. Seja $(e_1, ..., e_n)$ a base canônica do $\mathbb{R}^n$ e seja H o subgrupo do $\mathbb{R}^n$ gerado por $(\theta_1, ..., \theta_n, t)$. O grupo H não é discreto; se fosse, aplicando o método da demonstração do teorema acima, teríamos uma expressão para t como combinação linear com coeficientes racionais dos e_i's, que é um absurdo. Assim, para qualquer $\epsilon > 0$ existe um elemento não-nulo de H cuja distância desse elemento a 0 é menor que ϵ. Logo, existe um inteiro $p_i \in \mathbb{Z}$ e $q \in \mathbb{N}$, $q \neq 0$, tal que $|q\theta_i - p_i| \leq \epsilon$, que nos diz que

$$|\theta_i - \tfrac{p_i}{q}| \leq \tfrac{\epsilon}{q} \text{ para todo } i = 1, ..., n.$$

Vamos observar que, simplesmente escolhendo o múltiplo $\frac{n_i}{q}$ de $\frac{1}{q}$ mais próximo de θ_i, nós temos a aproximmação

$$|\theta_i - \tfrac{n_i}{q}| \leq \tfrac{1}{2q} \ (n_i \in \mathbb{Z}), \text{ para qualquer } q > 0.$$

O resultado provado acima é um teorema básico na rica teoria de aproximação de números irracionais por racionais.

Definição 2.12. *Um subgrupo discreto de grau n do $\mathbb{R}^n$ é chamado de um reticulado do $\mathbb{R}^n$.*

Pelo Teorema 2.10, um reticulado é gerado sobre $\mathbb{Z}$ por uma base do $\mathbb{R}^n$, que é então uma $\mathbb{Z}$-base para um dado reticulado. Para cada $\mathbb{Z}$-base $e = (e_1, ..., e_n)$ de um reticulado H, nós escreveremos P_e para o semi-paralelepípedo aberto

$$P_e = \{x \in \mathbb{R}^n | \ x = \sum_{i=1}^{n} \alpha_i e_i, \text{ com } 0 \leq \alpha_i < 1\}.$$

Assim, cada ponto do $\mathbb{R}^n$ é congruente módulo H a um e apenas um ponto de P_e para qualquer base e fixada. Neste caso, nós diremos que P_e é um domínio fundamental para H. Nós iremos escrever μ para denotar a *medida de Lebesgue* em $\mathbb{R}^n$, ou seja, se S é um subconjunto mensurável do $\mathbb{R}^n$, $\mu(S)$ irá denotar sua medida, que nós iremos chamar aqui por *volume*.

Lema 2.3. *O volume $\mu(P_e)$ independe da escolha da base e de H.*

Demonstração. Seja $f = (f_1, ..., f_n)$ uma outra base de H. Então

$$f_i = \sum_{j=1}^{n} \alpha_{ij} e_j \text{ com } \alpha_{ij} \in \mathbb{Z}.$$

Nós sabemos do cálculo que: $\mu(P_f) = |\det(\alpha_{ij})|\mu(P_e)$. A matriz (α_{ij}), sendo associada com uma mudança de base, é invertível com uma matriz inversa inteira, então $\det(\alpha_{ij}) = \pm 1$. Assim, $\mu(P_f) = \mu(P_e)$. □

O volume do paralelepípedo P_e associado com qualquer base e de H é chamado de *volume do reticulado* H e é denotado por $\nu(H)$.

Teorema 2.11. *(Minkowski) Seja H um reticulado em $\mathbb{R}^n$ e seja S um subconjunto mensurável do $\mathbb{R}^n$ tal que $\mu(S) > \nu(H)$. Então existem dois pontos distintos $x, y \in S$ tais que $x - y \in H$.*

Demonstração. Seja $e = (e_1, ..., e_n)$ uma $\mathbb{Z}$-base de H e seja P_e o paralelepípedo associado a base e. Assim P_e é um domínio fundamental para H. Veja que S pode ser visto como a união disjunta de subconjuntos da forma $S \cap (h + P_e)$, com $h \in H$. Segue que

$$\mu(S) = \sum_{h \in H} \mu(S \cap (h + P_e)). \tag{2.11}$$

Como μ é invariante por translação,

$$\mu(S \cap (h + P_e)) = \mu((-h + S) \cap P_e).$$

Os conjuntos $(-h + S) \cap P_e$ $(h \in H)$ não podem ser todos disjuntos, pois se fossem, teríamos que $\mu(P_e) \geq \sum_{h \in H} \mu((-h + S) \cap P_e)$, que contradiz (2.11) e a hipótese de que $\mu(P_e) = \nu(H) < \mu(S)$. Consequentemente, existem dois elementos distintos h e h' de H tais que $P_e \cap (-h + S) \cap (-h' + S) \neq \emptyset$. Sejam x e y elementos de S tais que $-h + x = -h' + y$. Então $x - y = h - h' \in H$ e $x \neq y$, pois $h \neq h'$. □

Corolário 2.6. *Seja H um reticulado em $\mathbb{R}^n$ e seja S um subconjunto mensurável do $\mathbb{R}^n$ que é simétrico com respeito ao 0 e convexo. Assuma que S satisfaz pelo menos uma das sequintes condições:*

(a) $\mu(S) > 2^n \nu(H)$

(b) $\mu(S) \geq 2^n \nu(H)$ *e S é compacto.*

Então $S \cap (H - \{0\}) \neq \emptyset$.

Demonstração. No caso (a), vamos aplicar o Teorema de Minkowski (2.11) ao conjunto $S' = \frac{1}{2}S$, pois $\mu(S') = 2^{-n}\mu(S) > \nu(H)$. Seja então y e z pontos distintos de S' tais que $y - z \in H$. Então $y - z$ também pertencem a S pois, $y - z = \frac{1}{2}(2y + (-2z))$ (usando também a simetria e convexidade de S). Portanto, $y - z \in S \cap (H - \{0\})$. Para o caso (b), observe que $(1+\epsilon)S$ para $\epsilon > 0$ satisfaz todas as hipóteses de S e também a hipótese do caso (a). Perceba que, $(H - \{0\}) \cap (1+\epsilon)S$ é um subconjunto finito, pois $(1+\epsilon)S$ é compacto e H é um subgrupo discreto do $\mathbb{R}^n$. Logo o conjunto $(H - \{0\}) \cap (1+\epsilon)S$ é compacto. Além disso, $\bigcap_{\epsilon>0} (H - \{0\}) \cap (1+\epsilon)S \neq \emptyset$, pois uma interseção de conjuntos compactos não-vazios e "encaixados"nunca é vazia. Isto diz que existe um ponto de $H - \{0\}$ que pertence a $(1+\epsilon)S$ para todo $\epsilon > 0$; Portanto, como S é compacto, esse ponto também pertence a S também. □

2.8 Ideais fracionários e a norma de um ideal

Definição 2.13. *Seja A um domínio de integridade com corpo de frações K. Um A-módulo não-nulo I contido em K é chamado de um ideal fracionário de A (ou de K com respeito a A), se existe um elemento não-nulo* $d \in A$ *tal que* $dI \subset A$. *Se* $I \subset A$, *então I é um ideal fracionário se e somente se I é um ideal de A. Nós chamamos estes ideais de "inteiros"para distingui-los dos demais ideais fracionários.*

Qualquer A-submódulo I finitamente gerado contido em K é um ideal fracionário. Isto segue do fato de que, se $(x_1, ..., x_n)$ é um conjunto finito de geradores para I, os x_i's tem um denominador comum $d = \prod_{i=1}^{n} d_i$, onde d_i é o denominador de cada x_i e ao mesmo tempo, d é um denominador comum para I. Reciprocamente, se A é anel Noetheriano, cada ideal fracionário I é um A-módulo finitamente gerado, isto é, $I \subset d^{-1}A$, e $d^{-1}A$ é um A-módulo isomorfo a A, sendo então um módulo Noethereiano.

Nós definimos o *produto* II' de dois ideais fracionários I e I' como o conjunto das somas finitas $\sum x_i y_i$, onde $x_i \in I$ e $y_i \in I'$. Se I e I' são ideais fracionários com denominador comum d e d', respectivamente, então os conjuntos $I \cap I'$, $I + I'$ e II' são ideais fracionários. Claramente, eles são A-submódulos de K e eles tem denominador comum d (ou d'), dd' e dd',

respectivamente. Com a operação de produto de ideais, é fácil ver que os ideais fracionários de A constituem um *monóide*, com elemento identidade $e = A$.

O conceito de ideal inteiro é importantíssimo e será usado futuramente para podermos definir o grupo das classes de um corpo de números.

Nós já estamos familiarizados com o conceito de *norma* de um elemento de um corpo. Iremos extender esse conceito para ideais. Sejam K um corpo de números, n o seu grau e $\mathfrak{D}_K$ o anel de inteiros de K. Escreveremos $N(x)$ no lugar de $N_{K/\mathbb{Q}}(x)$.

Proposição 2.13. *Se* x *é um elemento não-nulo de* $\mathfrak{D}_K$*, então* $|N(x)| = card(\mathfrak{D}_K/<x>)$.

Antes de iniciarmos a prova desse resultado, observe primeiramente que faz sentido essa fórmula, pois note que $x \in \mathfrak{D}_K$ e assim $N(x) \in \mathbb{Z}$ pelo Corolário 2.3.

Demonstração. Pela seção 6 (mais precisamente, pelo Corolário 2.4) nós sabemos que $\mathfrak{D}_K$ é um $\mathbb{Z}$-módulo livre de grau n e <x> é um $\mathbb{Z}$-submódulo de $\mathfrak{D}_K$. Ele também é de grau n, pois a multiplicação por x aplica $\mathfrak{D}_K$ em <x> isomorficamente. Assim, existe uma base $(e_1, ..., e_n)$ do $\mathbb{Z}$-módulo $\mathfrak{D}_K$ junto com os elementos $c_i \in \mathbb{N}$ tais que $(c_1e_1, ..., c_ne_n)$ é uma base de <x>.

Assim, o grupo abeliano $\mathfrak{D}_K$/<x> é isomorfo ao grupo abeliano finito $\prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$, cuja ordem é $c_1...c_n$. Vamos escrever u para a aplicação $\mathbb{Z}$-linear de $\mathfrak{D}_K$ em <x> definido por $u(e_i) = c_ie_i$ para $i = 1, 2, ..., n$. Assim, teremos que $det(u) = c_1...c_n$. Por outro lado, $(xe_1, ..., xe_n)$ também é uma base para <x>. Existe assim um automorfismo v do $\mathbb{Z}$-módulo <x> tal que $v(c_ie_i) = xe_i$. Então, o det(v) é invertível em $\mathbb{Z}$ e assim $det(v) = \pm 1$. Mas, $v \cdot u$ é a multiplicação por x, e assim pela definição 2.6, o seu determinante é N(x). Como $det(v \cdot u) = det(v) \cdot det(u)$, nós podemos concluir que $N(x) = \pm\ c_1...c_n = \pm$ card($\mathfrak{D}_K$/<x>), aplicando a função módulo em ambos os lados, obtendo assim o nosso rsultado. □

Definição 2.14. *Dado um ideal inteiro não-nulo* I *de* $\mathfrak{D}_K$*, nós chamamos o número card*($\mathfrak{D}_K$*/I) de norma de* I *e denotaremos ele por N(I).*

Observe que N(I) é finito. De fato, se *a* é um elemento não-nulo de I, então $< a > \subset I$ e $\mathfrak{D}_K$/I pode ser identificado com um quociente de $\mathfrak{D}_K$/<a>. Assim, card($\mathfrak{D}_K$/I) $\leq$ card($\mathfrak{D}_K$/<a>), que é finito pela Proposição 2.13. Por outro lado, nós diremos que, para um ideal principal $< b >$, $N(< b >) = |N(b)|$.

Proposição 2.14. *Se* I *e* J *são ideais inteiros não-nulos de* $\mathfrak{D}_K$*, então* $N(IJ) = N(I)\ N(J)$.

Demonstração. Ver [11], Proposição 2 da página 52. □

Corolário 2.7. *Sejam* K *um corpo de números de grau* n *e* $\mathfrak{D}_K$ *o anel de inteiros de K. Considere I um ideal não-nulo de* $\mathfrak{D}_K$*. Se N(I) é primo, então I é um ideal primo de* $\mathfrak{D}_K$*.*

Demonstração. Sejam I_1 e I_2 dois ideais de $\mathfrak{D}_K$, onde $I_1 I_2 = I$. Pela Proposição 2.14, $N(I) = N(I_1)N(I_2)$. Por hipótese, $N(I)$ é primo, então, $N(I_1) = 1$ ou $N(I_2) = 1$. Suponha que $N(I_1) = 1$. Assim, pela definição de norma de ideal, temos que $|\mathfrak{D}_K \setminus I_1| = 1$. Ou seja, $\mathfrak{D}_K = I_1$ e assim $I_2 = I$. Mostrando que I é um ideal primo. Observe que usamos o fato elementar que P é um ideal primo se, e somente se, dados ideais A e B com $AB \subset P$ implica $A \subset P$ ou $B \subset P$. □

Proposição 2.15. *Sejam* K *um corpo de números,* $\mathfrak{D}_K$ *o seu anel de inteiros algébricos e I um ideal inteiro. Então* $N(I) \in I$*.*

Demonstração. Seja $N(I) = |\mathfrak{D}_K/I| = r$. Se $x \in \mathfrak{D}_K$, então $r(x + I)$ é 0 em $\mathfrak{D}_K/I$, porque a ordem de qualquer elemento de um grupo divide a ordem do grupo. Assim, $rx \in I$. Em particular, podemos tomar $x = 1$ e concluir que $r \in I$. □

Para o bom entendimento dos próximos resultados, precisaremos da seguinte definição

Definição 2.15. *Um ideal* I *diz-se dividir um outro ideal* J*, denotado* $I \mid J$*, em um anel comutativo com identidade R, quando existe um outro ideal* H *em R tal que* $J = IH$*. Um ideal primo* P *em um anel de inteiros R é um ideal que satisfaz propriedade que*

Quando $P \mid IJ$ *para dois ideais* I*,* J *em R, então* $P \mid I$ *ou* $P \mid J$*.*

Lema 2.4. *Sejam* I *e* J *dois ideais de um anel R. Se* $I \mid J$*, então* $J \subset I$*.*

Demonstração. Se $I \mid J$, por definição, existe um ideal H tal que $J = HI$. mas, pode definição de ideal $HI \subset I$, então $I \supset J$. □

Lema 2.5. *Um inteiro* m *pode pertencer apenas a uma quantidade finita de ideais de* $\mathfrak{D}_K$*.*

Demonstração. Nós temos que $m \in I$ se, e somente se, I divide $< m >$. Como $< m >$ fatora-se de maneira única em um produto finito de ideais, então temos apenas uma quantidade finita de divisores para $< m >$. Ou seja, m pertence apenas a uma quantidade finita de ideias. □

Proposição 2.16. *Dado* $m \in \mathbb{N}$*, existe apenas uma quantidade finita de ideais I de* $\mathfrak{D}_K$ *tais que* $N(I) = m$*.*

Demonstração. Se $N(I) = m$, pela Proposição 2.15, $m \in I$ e o resultado segue direto pelo lema 2.4. □

3 O MERGULHO CANÔNICO E O GRUPO DAS CLASSES

O objetivo deste capítulo é introduzir o conceito de grupos das classes de maneira geral, estabelecer a notação do mergulho canônico de um corpo de números K e por fim dar a prova clássica da finitude dos grupo das classes via o limitante de Minkowski.

3.1 Grupo das classes

Para começarmos, vamos introduzir os conceitos de Anéis Noetherianos e Anéis de Dedekind.

Teorema 3.1. *Sejam A um anel e M um A-módulo. São equivalentes:*

(a) Toda coleção, não-vazia, de submódulos de M contém um elemento maximal.

(b) Toda sequência crescente de submódulos de M é estacionária.

(c) Todo submódulo de M é finitamente gerado.

Definição 3.1. *Um A-módulo M é chamado Noetheriano se ele satisfaz as condições do teorema anterior. Um Anel A é chamado Noetheriano se, considerado como A-módulo, é Noetheriano.*

Uma prova do teorema acima pode ser visto em [2] ou em [9]. Anéis Noetherianos são de grande importância em Álgebra Comutativa e ótimas referências para o seu estudo são [2], [9] ou [13].

Proposição 3.1. *Seja A um anel integralmente fechado e Noetheriano. Sejam K seu corpo de frações, L uma extensão finita de K e A' o fecho inteiro de A em L. Suponha que K é de característica 0. Então A' é um A-módulo finitamente gerado e um anel Noetheriano.*

Demonstração. Nós sabemos que A' é um A-submódulo livre de grau n, pelo Teorema 2.7. Assim, A' é um A-módulo finitamente gerado, e portanto, Noetheriano. Por outro lado, os ideais de A' são casos especiais de A-submódulos de A'. Eles satisfazem a condição (a) do teorema anterior, então A' é um anel Noetheriano. □

Exemplo: O anel de inteiros de um corpo de números é Noetheriano, bastando fazer $A = \mathbb{Z}$ e K = $\mathbb{Q}$ como na proposição anterior.

O próximo lema será usado posteriormente para provarmos a existência de elementos invertíveis no monóide de ideais fracionários. Uma prova desse lema pode ser visto em [11], lema 3 da página 48.

Lema 3.1. *Em um anel Noetheriano, todo ideal contém um produto de ideais primos. Em um domínio de integridade Noetheriano, todo ideal não-nulo contém um produto de ideais primos não-nulos.*

Definição 3.2. *Um domínio de integridade A é chamado de anel de Dedekind (ou domínio de Dedekind) se:*

i. *É Noetheriano;*

ii. *É integralmente fechado e*

iii. *Todo ideal primo de A é maximal.*

O anel $\mathbb{Z}$ e mais precisamente qualquer anel de ideais principais é um anel de Dedekind. O seguinte teorema implicará que o anel de inteiros de um corpo de números é um anel de Dedekind.

Teorema 3.2. *Seja A um anel de Dedekind, K seu corpo de frações, L uma extensão finita de K e A' o fecho inteiro de A em L. Assuma que K é de característica 0. Então A' é um anel de Dedekind e um A-módulo finitamente gerado.*

Demonstração. Já sabemos que o anel A' é integralmente fechado pela sua própria contrução e também é Noetheriano e um A-módulo finitamente gerado pela Proposição 3.1. Agora, é suficiente mostrar que todo ideal primo $I' \neq (0)$ de A' é maximal. Assim, escolha $x \in I' - (0)$ e considere uma equação de independência inteira de x sobre A, com grau mínimo:

$$x^n + a_{n-1}x^{n-1} + \ ... \ + a_1x + a_0 = 0, \ \ (a_i \in A). \tag{3.1}$$

Então $a_0 \neq 0$, pois senão fosse, poderíamos por x em evidência e diminuir de uma unidade o grau da equação, deixando assim de ser mínimo. Por (3.1), nós temos que $a_0 \in A'x \cap A \subset I' \cap A$. Portanto, $I' \cap A \neq (0)$ é um ideal maximal de A e $A/I' \cap A$ é um corpo. Mas $A/I' \cap A$ pode ser identificado como um subanel de A'/I' e A'/I' é inteiro sobre $A/I' \cap A$, pois A' é inteiro sobre A. Assim, A'/I' é um corpo, devido a Proposição 2.3, e assim I' é maximal. $\square$

O interesse em anéis de Dedekind ressurge do fato de que o anel de inteiros de um corpo de números é um anel de Dedekind, mas nem sempre é um anel de ideais principais.

Exemplo. Considere o anel de inteiros $A = \mathbb{Z}[\sqrt{-5}]$ em $\mathbb{Q}[\sqrt{-5}]$. Observe que $(1+\sqrt{-5})(1-\sqrt{-5}) = 2\cdot 3$, ou seja, não é um DFU (Domínio de Fatoração Única). Suponha que A seja um domínio de ideais principais. Sendo A é um domínio de Dedekind, segue pelo Teorema 3.5, que veremos logo adiante, que A não é um DIP.

Exibiremos agora alguns resultados sobre ideais em anéis de Dedekind que serão úteis para o próximo capítulo.

Lema 3.2. *Seja* $I \neq R$ *um ideal, onde R é um anel de Dedekind com corpo de frações K. Então, existe* $\gamma \in K - R$ *tal que* $\gamma I \subset R$

Demonstração. Seja $\alpha \in I$ um elemento fixado não-nulo. Pelo lema 3.1, o ideal principal $< \alpha >$ contém um produto de ideais primos P_1, ..., P_r, digamos. Suponha que r seja mínimo no que diz respeito a ser um produto de primos em $< \alpha >$. Usaremos o fato elementar de que todo ideal próprio está contido em algum ideal maximal, portanto primo. Assim, $I \subset P$ para algum ideal primo P de R. Pela primalidade, $P_j \subset P$, para algum j, que nós podemos assumir ser $j = 1$. Pela condição (iii) da Definição 3.2, $P_1 = P$. Como $< \alpha >$ não pode conter um produto com menos que r ideais primos, existe um $\beta \in P_2 \cdots P_r - < \alpha >$. Portanto,

$$\beta \ / \ \alpha \in \frac{1}{< \alpha >} P_2 \cdots P_r - R \subset K - R.$$

Porém,

$$\beta P \subset P P_2 \cdots P_r \subset < \alpha >,$$

então se $\delta \in P$, então $\beta\delta \in < \alpha >$. Em particular, se $\delta \in I$, então

$$\frac{\beta}{\alpha}\delta \in R.$$

Em outras palavras,

$$\gamma I = \frac{\beta}{\alpha} I \subset R.$$

□

Teorema 3.3. *Seja R um anel de Dedekind e I um ideal não-nulo de R. Então, existe um ideal J não-nulo de R tal que* IJ *é principal.*

Demonstração. Seja I um ideal não-nulo de R com $\alpha \in I$ e seja

$$J = \{\beta \in R \ : \ \beta I \subset < \alpha >\}.$$

É fácil verificar J é um ideal não-nulo de R contendo α e

$$IJ \subset < \alpha > .$$

Mostraremos que de fato segue a igualdade. Seja

$$L = \frac{1}{\alpha} IJ.$$

Então $L \subset R$. Como I e J são ideais, então L também é. Assuma que L é um ideal próprio de R. Pelo lema anterior, existe um $\gamma \in K - R$ tal que $\gamma L \subset R$. Chegaremos num absurdo pela condição (ii) da Definição 3.2, se mostrarmos que γ é raiz de um polinômio mônico sobre R. Desde que $J \subset L$, dado que $\alpha \in I$, então $\gamma J \subset \gamma L \subset R$. Assim, $\gamma JI \subset RI \subset I$, o que implica que

$$\gamma J \subset J. \tag{3.2}$$

Seja $\{B_1, \ ..., \ \beta_r\}$ um conjunto de geradores para o ideal J. De (3.2), existe $z_{i,j} \in \mathbb{Z}$ tal que para i = 1, ..., r,

$$\gamma \beta_i = \sum_{j=1}^{r} z_{i,j} \beta_j.$$

Surgirá assim o sistema de equações homogêneas

$$\begin{aligned}
(z_{1,1} - \gamma)x_1 + z_{1,2}x_2 + ... + z_{1,r}x_r &= 0 \\
z_{2,1}x_1 + (z_{2,2} - \gamma)x_2 + ... + z_{2,r}x_r &= 0 \\
&..... \\
z_{r,1}x_1 + z_{r,2}x_2 + ... + (z_{r,r} - \gamma)x_r &= 0
\end{aligned}$$

que possui solução não trivial $x_j = \beta_j$. Então o determinante

$$\det \begin{bmatrix}
(z_{1,1} - \gamma) & z_{1,2} & \cdots & z_{1,r} \\
z_{2,1} & (z_{2,2} - \gamma) & \cdots & z_{2,r} \\
\vdots & \vdots & \ddots & \vdots \\
z_{r,1} & z_{r,2} & \cdots & (z_{r,r} - \gamma)
\end{bmatrix}$$

anula-se. Concluindo que γ satisfaz o polinômio mônico sobre R requerido. □

Corolário 3.1. *Se I, J e L são ideais de um anel de Dedekind R, com I não-nulo e* $IJ = LJ$*, então J = L.*

Demonstração. Se H é um ideal tal que $IH = <\alpha>$, então $J <\alpha>= L <\alpha>$. Daí

$$L \subset L <\alpha>= J <\alpha> \subset J,$$

e

$$J \subset J <\alpha>= L <\alpha> \subset L,$$

então L = J. □

Corolário 3.2. *Se I e J são ambos ideais de um anel de Dedekind, então* $I \mid J$ *se, e somente se,* $I \supset J$.

Demonstração. Pelo Lema 2.4, precisamos apenas provar uma das implicações. Se $I \supset J$, então seja L um ideal tal que LI é principal, ou seja, $LI =<\alpha>$. Então $H = \frac{1}{\alpha}LJ$ é um ideal e $IH = J$. □

Vimos na seção 2.8 o conceito de ideais fracionários e inteiros, este conceito será agora útil para definir o grupo das classes de ideais.

Teorema 3.4. *Seja A um anel de Dedekind que não é corpo e K o seu corpo de frações. Todo ideal primo (e portanto, maximal) de A é invertível no monóide dos ideais fracionários de A.*

Demonstração. Seja $\mathcal{M}$ um ideal maximal de A. Então $\mathcal{M} \neq (0)$, pois A não é um corpo. Defina:

$$\mathcal{M}' = \{x \in K | x\mathcal{M} \subset A\}. \tag{3.3}$$

Claramente, $\mathcal{M}$' é um A-submódulo de K; qualquer elemento não-nulo de $\mathcal{M}$ serve como um denominador comum para $\mathcal{M}$'. Assim, $\mathcal{M}$' é um ideal fracionário de A. É suficiente mostrar que $\mathcal{M}\mathcal{M}' = A$. Por (3.3) temos que $\mathcal{M}\mathcal{M}' \subset A$; por outro lado, $A \subset \mathcal{M}'$, pois $\mathcal{M}$ é um ideal, então $\mathcal{M} = A\mathcal{M} \subset \mathcal{M}\mathcal{M}'$. Como $\mathcal{M}$ é maximal e $\mathcal{M} \subset \mathcal{M}\mathcal{M}' \subset A$, temos que ou $\mathcal{M}\mathcal{M}' = A$ ou $\mathcal{M}\mathcal{M}' = \mathcal{M}$. É suficiente mostrar que $\mathcal{M}\mathcal{M}' = \mathcal{M}$ é impossível.

Agora, se $\mathcal{M}\mathcal{M}' = \mathcal{M}$ e se $x \in \mathcal{M}'$, então $x\mathcal{M} \subset \mathcal{M}$, $x^2\mathcal{M} \subset x\mathcal{M} \subset \mathcal{M}$ e por indução teremos que $x^n\mathcal{M} \subset \mathcal{M}$ para todo $n \in \mathbb{N}$. Segue que A[x] é um ideal fracionário de A. Como A é Noetheriano, A[x] é um A-módulo finitamente gerado, pelas observações no começo da seção 2.8, e então $x \in A$ é inteiro sobre A devido ao Teorema 2.1. Mas A é integralmente fechado;

portanto, $x \in A$; e consequentemente $\mathcal{M}'\mathcal{M} = A$ implica $\mathcal{M}' = A$. Com isso, vamos provar que $\mathcal{M}' = A$ é impossível.

Para isso, tome um elemento não-nulo $m \in \mathcal{M}$. O ideal Am contém um produto ideais $p_1p_2...p_n$ de ideais primos não-nulos pelo Lema 3.1. Sem perda de generalidade, podemos tomar n como o menor possivel. Nós temos que $\mathcal{M} \supset Am \supset p_1p_2...p_n$ que nos diz que $\mathcal{M} \supset p_i$ para algum i. Digamos que seja $i = 1$. Como p_1 é maximal por hipótese, $\mathcal{M} = p_1$. Ponha $I = p_2...p_n$. Então $Am \supset \mathcal{M}I$ e $Am \not\supseteq I$, pois n foi tomado como o menor possivel. Assim, existe $b \in I$ tal que $b \notin Am$. Assim, $\mathcal{M}I \subset Am$ e $\mathcal{M}b \subset Am$, donde $\mathcal{M}bm^{-1} \subset A$. Pela definição (3.3) de $\mathcal{M}$', temos que $bm^{-1} \in \mathcal{M}$'. Mas, como $b \notin Am$, então $bm^{-1} \notin A$. Assim $\mathcal{M}' \neq A$. □

Teorema 3.5. *Seja A um anel de Dedekind e seja* P *o conjunto de todos os ideais primos não-nulos de A. Então:*

(a) Todo ideal fracionário não-nulo I de A pode ser expresso de forma única como

$$I = \prod_{p \in P} p^{n_p(I)}, \tag{3.4}$$

onde, para qualquer $p \in P$, $n_p(I) \in \mathbb{Z}$ *e para apenas uma quantidade finita de* $p \in P$, *teremos* $n_p(I) \neq 0$.

(b) O monóide dos ideais fracionários não-nulos de A é um grupo.

Demonstração. Primeiro nós provaremos a existência de (a), ou seja, qualquer ideal fracionário I é um produto de de potências (≥ 0 ou $\neq 0$) de ideais primos. Existe $d \in A - (0)$ tal que $dI \subset A$, isto é, tal que dI é um ideal inteiro de A, $I = (dI) \cdot (Ad)^{-1}$. Nós podemos, sem perda de generalidade, provar (a) para ideais inteiros. Considere a coleção Φ de ideais não-nulos de A que não são produtos de ideais primos. Suponha que Φ é não-vazio. Seja $\mathcal{M}$ um elemento maximal de Φ (A é Noetheriano). Então $\mathcal{M} \neq A$, pois A é o produto da coleção vazia de ideais primos. Então $\mathcal{M}$ está contido em um ideal maximal p, que é assim um elemento maximal na coleção dos ideais primos não-triviais de A que contém $\mathcal{M}$. Seja p' o ideal fracionário inverso de p. Como $\mathcal{M} \subset p$, então $\mathcal{M}p' \subset pp' =$A. Como $p' \supset A$, então $\mathcal{M}p' \supset \mathcal{M}$; de fato, $\mathcal{M}p' \neq \mathcal{M}$ (se, $\mathcal{M}p' = \mathcal{M}$ e se $x \in p'$, então $x\mathcal{M} \subset \mathcal{M}$, $x^n\mathcal{M} \subset \mathcal{M}$ para todo n, x inteiro sobre A e $x \in A$ (como no Teorema 3.2). Mas isto é impossível, pois $p' \neq A$ (caso contrário, $p' = A$ e $pp' = p$).). Pela maximilidade de $\mathcal{M}$ em Φ, nós temos que $\mathcal{M}p' \notin \Phi$, então $\mathcal{M}p' = p_1$ ... p_n, um produto de ideais primos. Multiplicando por p, nós vemos que $\mathcal{M} = pp_1$ ... p_n. Assim todo ideal inteiro de A é um produto de ideais primos.

Vamos agora considerar a unicidade de (a). Suponha que

$$\prod_{p\in P} p^{n(p)} = \prod_{p\in P} p^{m(p)}, \text{ ou seja, } \prod_{p\in P} p^{n(p)-m(p)} = A.$$

Se $n(p) - m(p) \neq 0$ para algum dos ideais primos $p \in P$, nós podemos separar os expopentes positivos e negativos e escrever:

$$p_1^{\alpha_1} \dots p_r^{\alpha_r} = q_1^{\beta_1} \dots q_s^{\beta_s},$$

onde $p_i, q_j \in P$, $\alpha_i > 0$, $\beta_j > 0$, $p_i \neq q_j$ para todo i e j. Assim, p_1 contém $q_1^{\beta_1} \dots q_s^{\beta_s}$; $p_1 \supset q_j$ para algum j, digamos $p_1 \supset q_1$. Mas p_1 e q_1 são ambos maximais, que implica $p_1 = q_1$, que é uma contradição.

Finalmente, a expressão em (3.4) implica que $\prod_{p\in P} p^{-n_p(I)}$ é o inverso de I e isto prova (b). □

Assim, o Teorema 3.4 nos garante que se A é um anel de Dedekind, então o conjunto de todos os ideais fracionários formam um grupo abeliano multiplicativo, denotado por $\mathcal{F}_A$. O conjunto $\mathcal{P}_A$ consistindo de todos os ideais principais fracionários de A é um subgrupo de $\mathcal{F}_A$ já que, sendo $\alpha_1 A$ e $\alpha_2 A$ dois ideais fracionários principais não-nulos de A, temos $\alpha_1 A \alpha_2^{-1} A = \alpha_1 \alpha_2^{-1} A$.

Assim, podemos obter a seguinte definição:

Definição 3.3. *Seja A um anel de Dedekind. Então o grupo quociente $\mathcal{F}_A/\mathcal{P}_A$ é chamado de grupo das classes de A, denotado por $\mathcal{C}_A$. Quando A é o anel de inteiros algébricos de um corpo de números K, nós denotaremos por $\mathcal{C}_K$. Nós diremos que dois ideais fracionários são equivalentes se eles pertencem a uma mesma classe de $\mathcal{P}_A$ em $\mathcal{F}_A$. Em outras palavras, ideais fracionários I e J são equivalentes, denotados por $I \sim J$, quando $\psi(I) = \psi(J)$, onde ψ é o homomorfismo canônico $\psi : \mathcal{F}_A \longrightarrow \mathcal{F}_A/\mathcal{P}_A$.*

Dois resultados básicos envolvendo o grupo das classes são:

Teorema 3.6. *Se A é um anel de Dedekind, então A é um Domínio de Fatoração Única (DFU) se e somente se, A é um Domínio de Ideais Principais (DIP).*

Demonstração. Ver [8]. □

Teorema 3.7. *Suponha que A é um anel de Dedekind. Então A é um DFU se e somente se, $\mathcal{C}_A$ tem ordem 1.*

Demonstração. Pelo Teorema 3.6, A é um DFU se e somente se é um DIP, e ele é um DIP se e somente se, todos os seus ideais forem principais. Então $\mathcal{F}_A = \mathcal{P}_A$. Em outras palavras, a cardinalidade de $\mathcal{C}_A$ é 1. □

3.2 Mergulho canônico de um corpo de números

Seja K um corpo de números e seja n o seu grau. O Teorema 2.4 nos garante que existem n $\mathbb{Q}$-isomorfismos distintos $\sigma_i : K \longrightarrow \mathbb{C}$. Seja $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ a conjugação complexa. Então, para qualquer $i = 1, ..., n$, $\alpha \circ \sigma_i = \sigma_j$, $1 \leq j \leq n$ e $\sigma_i = \sigma_j$ se e somente se, $\sigma_i(K) \subset \mathbb{R}$. Vamos escrever r_1 para o número de índices tais que $\sigma_i(K) \subset \mathbb{R}$. Então $n - r_1$ é um número par, então nós podemos escrever:

$$r_1 + 2r_2 = n. \tag{3.5}$$

Nós vamos rearranjar os σ_i's tais que $\sigma_i(K) \subset \mathbb{R}$ para $1 \leq i \leq r_1$ e $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Então os primeiros $r_1 + r_2$ isomorfismos determinam os últimos r_2. Para $x \in K$ nós definimos

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

Nós chamamos σ de *mergulho canônico* de K em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$; Ele claramente é um homomorfismo injetivo entre anéis. Nós frequentemente identificaremos $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$ devido a (3.4). As notações σ, K, n, r_1 e r_2 serão usados até o término desta dissertação.

Proposição 3.2. *Se M é um $\mathbb{Z}$-submódulo livre de K de grau n e se $(x_i)_{1 \leq i \leq n}$ é uma $\mathbb{Z}$-base de M, então $\sigma(M)$ é um reticulado em $\mathbb{R}^n$, cujo volume é:*

$$\nu(\sigma(M)) = 2^{-r_2} |\det_{1 \leq i,j \leq n} (\sigma_i(x_j))|. \tag{3.6}$$

Demonstração. Para i fixado, as coordenadas de $\sigma(x_i)$ com respeito a base canônica do $\mathbb{R}^n$ são

$$\sigma_1(x_i), \ ... \ \sigma_{r_1}(x_i), \ \mathrm{Re}(\sigma_{r_1+1}(x_i)), \ \mathrm{Im}(\sigma_{r_1+1}(x_i)), \ ..., \ \mathrm{Re}(\sigma_{r_1+r_2}(x_i)), \ \mathrm{Im}(\sigma_{r_1+r_2}(x_i)), \tag{3.7}$$

onde Re e Im denotam, respectivamente, a parte real e imaginária. Nós vamos calcular o determinante D da matriz cuja i-ésima coluna é dada por (3.7). Fazendo o uso das fórmulas já conhecidas $\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z})$ e $\mathrm{Im}(z) = \frac{1}{2i}(z - \overline{z})$ para $z \in \mathbb{C}$ e da linearidade de Re e Im, nós teremos que $D = (2i)^{-r_2} \det(\sigma_j(x_i))$. Assim, pela Proposição 2.11, $\det(\sigma_j(x_i)) \neq 0$, assim, os x_i's formam uma base para K sobre $\mathbb{Q}$ e portanto $D \neq 0$. Assim os vetores $\sigma(x_i)$ são

linearmente independentes em $\mathbb{R}^n$ de modo que o $\mathbb{Z}$-módulos que eles geram (chamado $\sigma(M)$) é um reticulado em $\mathbb{R}^n$. O cálculo de D é justamente $\nu(\sigma(M))$. □

Proposição 3.3. *Seja d o discriminante absoluto de K, $\mathfrak{D}_K$ o anel de inteiros de K e I um ideal inteiro não-nulo de $\mathfrak{D}_K$, então $\sigma(\mathfrak{D}_K)$ e $\sigma(I)$ são reticulados. Mais ainda,*

$$\nu(\sigma(\mathfrak{D}_K)) = 2^{-r_2}|d|^{1/2} \ \text{ e } \ \nu(\sigma(I)) = 2^{-r_2}|d|^{1/2}N(I). \tag{3.8}$$

Demonstração. Já sabemos que $\mathfrak{D}_K$ e I são $\mathbb{Z}$-módulos livres de grau n, então, aplicando diretamente a proposição anterior, já teremos que $\sigma(\mathfrak{D}_K)$ e $\sigma(I)$ são reticulados. Por outro lado, se (x_i) é uma $\mathbb{Z}$-base para $\mathfrak{D}_K$, então $d = det(\sigma_i(x_j))^2$, novamente pela Proposição 2.11. Substituindo d na fórmula da proposição anterior, teremos a primeira fórmula em (3.8). A segunda fórmula vem do fato de que $\sigma(I)$ é um subgrupo de $\sigma(\mathfrak{D}_K)$ de índice $N(I)$, basta ver a Definição 2.14. Um domínio fundamental para $\sigma(I)$ pode ser contruído como a união disjunta de N(I) cópias de um domínio fundamental para $\sigma(\mathfrak{D}_K)$, assim:

$$\nu(\sigma(I)) = \mu(P_{\sigma(I)}) = \mu(\bigcup_{N(I)} P_{\sigma(\mathfrak{D}_K)}) = \mu(N(I)\ P_{\sigma(\mathfrak{D}_K)}) = N(I)\ \mu(P_{\sigma(\mathfrak{D}_K)}) =$$
$$= \ N(I)\ \nu(\sigma(\mathfrak{D}_K)) = 2^{-r_2}\ |d|^{1/2}\ N(I)$$

□

3.3 Prova da finitude dos grupo das classes

Esta seção é dada exclusivamente para darmos a prova clássica da finitude do grupo das classes.

Proposição 3.4. *Sejam K um corpo de números, n o seu grau, r_1 e r_2 os inteiros definidos na seção anterior, d o discriminante absoluto de K e I um ideal inteiro não-nulo de K. Então I contém um elemento não-nulo x tal que*

$$|N(x)| \ \leq \ (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}\sqrt{|d|}\ N(I). \tag{3.9}$$

Demonstração. Seja σ o mergulho canônico de K em $\mathbb{R}^{r_1}$ x $\mathbb{C}^{r_2}$. Seja t um número real positivo e seja B_t o conjuntos de todos os elementos $(y_1, ..., y_{r_1}, z_1, ..., z_{r_2}) \in \mathbb{R}^{r_1}$ x $\mathbb{C}^{r_2}$ tal que

$$\sum_{i=1}^{r_1}|y_i| + 2\sum_{j=1}^{r_2}|z_j| \leq t. \tag{3.10}$$

Então B_t é um conjunto compacto, convexo e simétrico com respeito a $0 \in \mathbb{R}^n$. Pode ser encontrado em [11] nas páginas 66 e 67 que

$$\mu(B_t) = 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{t^n}{n!}, \tag{3.11}$$

onde μ denota a medida de Lebesgue.

Agora, escolha t tal que $\mu(B_t) = 2^n\nu(\sigma(I))$, ou seja, tal que

$$2^{r_1}(\frac{\pi}{2})^{r_2}\frac{t^n}{n!} \overset{\text{prop.3.3}}{=} 2^{n-r_2}|d|^{1/2}\, N(I), \tag{3.12}$$

ou então, tal que $t^n = 2^{n-r_1}\ \pi^{-r_2}\ n!\ |d|^{1/2}\ N(I)$. Pelo Corolario 2.6, existe um elemento não-nulo $x \in I$ tal que $\sigma(x) \in B_t$. Sua norma tem valor absoluto:

$$|N(x)| = \prod_{i=1}^{r_1}|\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2}|\sigma_j(x)|^2. \tag{3.13}$$

Usando o fato de que a média geométrica é sempre menor ou igual que a média aritmética e também (3.10), nós temos que

$$|N(x)| \leq [\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(x)| + \frac{2}{n}\sum_{j=r_1+1}^{r_1+r_2}|\sigma_j(x)|\ ]^n \leq \frac{t^n}{n^n}$$

Consequentemente,

$$|N(x)| \leq \frac{1}{n^n}2^{n-r_1}\ \pi^{-r_2}\ n!\ |d|^{1/2}\ N(I),$$

que combinando com a relação $r_1 + 2r_2 = n$, nos dá (3.9). □

De (3.9) definimos por *Limitante de Minkowski* o número $M_K = (\frac{4}{\pi})^{r_2}\ \frac{n!}{n^n}\ |d|^{1/2}$.

Corolário 3.3. *Com a mesma notação, toda classe de ideais de* K*, contém um ideal inteiro* $\mathfrak{b}$ *tal que*

$$N(\mathfrak{b}) \leq M_K. \tag{3.14}$$

Demonstração. Seja J um ideal fracionário de uma dada classe. Nós podemos multiplicá-lo por um ideal principal de $\mathfrak{D}_K$ sem mudar a classe, então nós podemos assumir sem perda de generlidade que $I = J^{-1}$ é um ideal inteiro. Escolha um elemento não-nulo $x \in I$ tal que satisfaz (3.9). Nosso candidato é $\mathfrak{b} = xJ$. Primeiro, observe que $\mathfrak{b}$ é um ideal inteiro porque $x \in I$ e $IJ = \mathfrak{D}_K$. Agora, $< x >= \mathfrak{b}I$ e então, teremos

$$N(\mathfrak{b})\ N(I) = N(\mathfrak{b}I) = N(< x >) = N(x)\ \leq\ M_K\ N(I)$$

Cancelando N(I), teremos o resultado esperado. □

Teorema 3.8. *Para qualquer corpo de números* K*, o grupo das classes de ideais é finito.*

Demonstração. Pelo Corolário 3.1 é suficiente provar que, para todo inteiro q, o conjunto de todos os ideais inteiros I de K que tem q como norma é um conjunto finito. Mas pela proposição 2.16, o conjunto de todos os ideais inteiros I de K que tem q como norma é um conjunto finito. Logo, nossos ideais I estão entre aqueles que contém $< q >$, e existe apenas uma quantidade finita de tais ideais, dada a finitude de $\mathfrak{D}_K/ < q >$. □

Um outro raciocínio para uma prova seria o seguinte: Existe apenas uma quantidade finita de ideais com uma norma dada. Pelo corolario 3.1, nós podemos associar a cada classe de ideais a um ideal inteiro cuja norma é limitada por uma constante fixa. Se o grupo das classes de ideais fosse infinito, nós poderíamos eventualmente usar o mesmo ideal inteiro em duas classes distintas, o que seria impossível.

O raciocínio usando em [8] é o seguinte:

Demonstração. Seja H um ideal fracinário de $\mathfrak{D}_K$. Existe um ideal inteiro $I \in c_H$ (classe de ideais que contém H). Seja J um ideal inteiro, na mesma classe de H satisfazendo o Corolário 3.1. Como existe apenas uma quantidade finita de escolhas para J e $c_I = c_J = c_H$, então existe apenas uma quantidade finita de escolhas de classes c_H. Assim, $\mathcal{C}_K$ é um grupo finito. □

Vamos agora demonstrar o resultado seguindo os passos em [10]:

Demonstração. Se P é um ideal primo do anel de inteiros $\mathfrak{D}_K$ do corpo de números K e $P \cap \mathbb{Z} = p\mathbb{Z}$ para algum primo p. Então $\mathfrak{D}_K/P$ é um corpo finito e uma extensão de $\mathbb{Z}/p\mathbb{Z}$ de grau $f \geq 1$ e nós temos

$$N(P) = p^f.$$

Dado p, existe uma apenas uma quantidade finita de ideais primos P tais que $P \cap \mathbb{Z} = p\mathbb{Z}$, que significa que $P \mid < p >$. Segue que existe uma quantidade finita de ideais P de norma limitada. Como todo ideal inteiro admite uma representação $I = P_1^{\nu_1} \cdots P_r^{\nu_r}$, onde $\nu_i > 0$ e

$$N(I) = N(P_1)^{\nu_1} \cdots N(P_r)^{\nu_r},$$

existem apenas uma quantidade finita de ideais $I \in \mathfrak{D}_K$ com norma $N(I) \leq M_K$. Com isso é suficiente checar que toda classe $c_I \in \mathcal{C}_K$ contém um ideal inteiro J satisfazendo

$$N(J) \leq M_K.$$

Mas isto segue do Corolário 3.3. □

Uma consequência é que, sendo h_K o número de classes, ou seja, a ordem de $\mathcal{C}_K$ não pode exceder o número de ideais em A cuja norma não execede M_K, justificando assim o termo limitante de Minkowski.

A finitude do grupo das classes possio grandes aplicações. Kuumer provou o último teorema de Fermat no caso de um primo p que não é um divisor de $h_{\mathbb{Q}(\zeta_p)}$ e ele deu um critério para quando este é o caso. Por exemplo, para $p < 100$ existe apenas três números primos, 37, 59 e 67 para o qual $p \mid h_{\mathbb{Q}(\zeta_p)}$. Para ver a demonstração deste resultado, indicamos o primeiro capítulo de [12].

4 FINITUDE DO GRUPO DAS CLASSES DE UM CORPO DE NÚMEROS

Neste capítulo apresentaremos o resultado principal da dissertação. Antes faremos uma breve exposição sobre empacotamentos reticulados.

4.1 Empacotamentos reticulados

O objetivo desta seção é apenas citar os conceitos iniciais necessários de empacotamentos reticulados para demonstração do resultado principal. Uma teoria riquíssima deste assunto pode ser vista em [4] .

Definição 4.1. *Um empacotamento esférico em $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio ρ no $\mathbb{R}^n$ de forma que a interseção entre quaisquer duas esferas tenha no máximo um ponto.*

Definição 4.2. *Um empacatomento reticulado é um empacotamento esférico em que o conjunto dos centros das esferas formam um reticulado Λ em $\mathbb{R}^n$.*

Observe que, podemos descrever um empacotamento reticulado conhecendo apenas o centro e o raio das esferas. E além disso, se u e v são centro de esferas, existem também esferas de centro $u+v$ e $u-v$, em outras palavras o conjunto dos centros formam um grupo aditivo.

Podemos agora dar uma definição precisa do que seja a densidade Δ de um reticulado Λ.

Definição 4.3. *A densidade Δ de um reticulado Λ é a região do espaço ocupado pelas esferas. Em outros termos:*

$$\Delta = \frac{\text{volume de uma esfera}}{\text{volume da região fundamental}} = \frac{\rho^n V_n}{v(\Lambda)},$$

onde $\rho^n V_n$ é o volume de uma esfera n-dimensional de raio ρ e V_n é o volume da esfera n-dimensional do $\mathbb{R}^n$.

Claramente temos que $\Delta \leq 1$.

Definição 4.4. *A densidade de centro de um reticulado Λ é dada por:*

$$\delta = \frac{\Delta}{V_n}$$

Um fato interessante e de fundamental importância para os nossos propósitos é que:

$$\delta \leq \frac{1}{V_n},$$

visto que $\Delta \leq 1$.

4.2 Resultados e a prova do teorema principal

Seja K um corpo de números de grau n e seja $\mathfrak{D}_K$ o seu anel de inteiros. Seja σ o mergulho canônico como definido na seção anterior. Tomando a norma de $\sigma(x)$, para $x \in K$ não nulo, temos:

$$|\sigma(x)|^2 = \sigma_1(x)^2 + ... + \sigma_{r_1}(x)^2 + |\sigma_{r_1+1}(x)|^2 + ... + |\sigma_{r_1+r_2}(x)|^2. \tag{4.1}$$

Somando $|\sigma_{r_1+r_2+1}(x)|^2 + ... + |\sigma_{r_1+2r_2}(x)|^2$ em ambos lados da igualdade acima, teremos:

$$|\sigma(x)|^2 + |\sigma_{r_1+r_2+1}(x)|^2 + ... + |\sigma_{r_1+2r_2}(x)|^2 = \sum_{i=1}^{n} |\sigma_i(x)|^2. \tag{4.2}$$

Mas sabendo que $\sigma_{r_1+r_2+j}(x) = \overline{\sigma_{r_1+j}(x)}$, para todo $j = 1, ..., r_2$, conclui-se que para todo $j = 1, ..., r_2$:

$$|\sigma_{r_1+r_2+j}(x)|^2 = \sigma_{r_1+r_2+j}(x)\ \overline{\sigma_{r_1+r_2+j}(x)} = \overline{\sigma_{r_1+j}(x)}\ \sigma_{r_1+j}(x) = |\sigma_{r_1+j}(x)|^2.$$

Assim, substituindo esse valor no lado esquerdo da igualdade (4.2) teremos

$$|\sigma(x)|^2 + |\sigma_{r_1+1}(x)|^2 + ... + |\sigma_{r_1+r_2}(x)|^2 = \sum_{i=1}^{n} |\sigma_i(x)|^2.$$

Implicando, por (4.1), que:

$$|\sigma(x)|^2 + (|\sigma(x)|^2 - \sigma_1(x)^2 - ... - \sigma_{r_1}(x)^2) = \sum_{i=1}^{n} |\sigma_i(x)|^2.$$

Concluindo assim que:

$$2|\sigma(x)|^2 = 2(\sigma_1(x)^2 + ... + \sigma_{r_1}(x)^2) + |\sigma_{r_1+1}(x)|^2 + ... + |\sigma_{r_1+2r_2}(x)|^2. \tag{4.3}$$

Agora, observe que:

$$2|\sigma(x)|^2 \geq \sum_{i=1}^{n} |\sigma_i(x)|^2,$$

pois na igualdade (4.3) temos a soma $\sum_{i=1}^{r_1} \sigma_i(x)^2$, que claramente é maior ou igual a zero. Também temos que:

$$2|\sigma(x)|^2 \geq \sum_{i=1}^{n} |\sigma_i(x)|^2 \geq n \sqrt[n]{|\prod_{i=1}^{n} \sigma_i(x)|^2} = n \sqrt[n]{|N(x)|^2},$$

onde a última desigualdade segue diretamente de que a média aritmética é sempre maior ou igual que a média geométrica e a igualdade segue de 2.3 (ver Proposição 2.7). Simplificando, teremos a seguinte desigualdade:

$$|\sigma(x)| \geq \frac{\sqrt{2n}}{2} \sqrt[n]{|N(x)|}. \tag{4.4}$$

Agora, seja I um ideal inteiro de $\mathfrak{D}_K$ e seja também $I^* = I - \{0\}$. Vamos denotar $\Lambda(I) = \{\sigma(x)/x \in I\}$. Devido a proposição 3.3, $\Lambda(I)$ é um reticulado n-dimensional. Da definição 4.4, temos que:

$$\delta(\Lambda(I)) = \frac{\Delta}{V_n} = \frac{\rho^n V_n}{\nu(\Lambda)} \cdot \frac{1}{V_n} = \frac{\rho^n}{\nu(\Lambda(I))}, \tag{4.5}$$

onde, $\rho = \frac{1}{2} min\{|\sigma(x)| \ / \ x \in I^*\}$ é, por definição, o raio de empacotamento de $\Lambda(I)$.

Por (4.5) e pela Proposição 3.3, temos que:

$$\delta(\Lambda(I)) = \frac{2^{r_2}\rho^n}{\sqrt{|d|}N(I)} = \frac{2^{r_2}(\frac{1}{2} \min_{x \in I^*} |\sigma(x)|)^n}{\sqrt{|d|}N(I)},$$

ou seja,

$$\delta(\Lambda(I)) = \frac{1}{2^{r_1+r_2} \cdot \sqrt{|d|}} \cdot \frac{\min_{x \in I^*} |\sigma(x)|^n}{N(I)}. \tag{4.6}$$

De (4.4) e (4.6), nós obtemos

$$\delta(\Lambda(I)) \geq \frac{1}{2^{r_1+r_2}\cdot\sqrt{|d|}} \cdot \frac{\left(\frac{\sqrt{2n}}{2}\cdot \min\limits_{x\in I^*} \sqrt[n]{|N(x)|}\right)^n}{N(I)}$$

Assim, simplificando os termos e usando o fato de que $n = r_1 + 2r_2$, teremos

$$\delta(\Lambda(I)) \geq \frac{n^{n/2}}{2^{\frac{3}{2}r_1+2r_2}\cdot\sqrt{|d|}} \cdot \frac{\min\limits_{x\in I^*}|N(x)|}{N(I)}. \tag{4.7}$$

Agora, sejam $c_I \in \mathcal{C}_K$ a classe de ideais contendo I e $\overline{c_I}$ o conjunto de ideais inteiros contidos em c_I. Para $x \in I$, nós podemos escrever $< x >= I \cdot J_x$, onde J_x é um ideal inteiro, pois dado $x \in I$, temos: $< x > \subset I$; sabendo que o anel de inteiros de um corpo de números K é um anel de Dedekind, o corolário 3.2 garante a existência de J_x. Usando a proposição 2.14,

$$|N(x)| = N(< x >) = N(I)\cdot N(J_x).$$

Como $J_x =< x > \cdot I^{-1}$, então a classe de J_x é a mesma de I^{-1}, no caso, c_I^{-1}, já que estamos multiplicando por um ideal principal, concluindo assim que $J_x \in \overline{c_I^{-1}}$

Segue então que:

$$\frac{\min\limits_{x\in I^*}|N(x)|}{N(I)} = \min_{J_x\in\overline{c_I^{-1}}} \frac{N(I)\cdot N(J_x)}{N(I)} = \min_{J_x\in\overline{c_I^{-1}}} N(J_x). \tag{4.8}$$

Portanto, (4.8) e (4.7) implicam que:

$$\delta(\Lambda(I)) \geq \frac{n^{n/2}}{2^{\frac{3}{2}r_1+2r_2}\cdot\sqrt{|d|}} \cdot \min_{J_x\in\overline{c_I^{-1}}} N(J_x). \tag{4.9}$$

Agora, com a notação estabelecida acima, podemos provar o resultado:

Teorema 4.1. *O grupo das classes de ideais $\mathcal{C}_K$ é finito.*

Demonstração. Suponha que $\mathcal{C}_K$ tem uma quantidade infinita de classes. Seja i um inteiro positivo e defina

$$\mathcal{L}_i = \{c \in \mathcal{C}_K \mid \min_{J\in\overline{c}} N(J) = i\}.$$

Verifiquemos que:

a) $\mathcal{L}_i$ é um conjunto finito, para todo $i \in \mathbb{N}$.

Demonstração. Suponha que exista $i \in \mathbb{N}$ tal que $\mathcal{L}_i$ tenha cardinalidade infinita. Assim, existiria um ideal inteiro J_j para cada classe $c_j \in \mathcal{L}_i$ tal que $N(J_j) = i$, ou seja, existiria uma quantidade infinita de ideais com norma igual a i, contradizendo a Proposição 2.16. □

b) $\mathcal{L}_i \cap \mathcal{L}_j = \emptyset$ para todo $i \neq j$.

Demonstração. Suponha que existam $i \neq j$, onde $\mathcal{L}_i \cap \mathcal{L}_j \neq \emptyset$. Podemos supor que $i < j$. Seja $c \in \mathcal{L}_i \cap \mathcal{L}_j$. Como $c \in \mathcal{L}_j$, então para todo $J \in \overline{c}$, temos que $N(J) \geq j$. Por outro lado, $c \in \mathcal{L}_i$, ou seja, existe $I \in \overline{c}$, tal que $N(I) = i < j$, um absurdo. □

Observe que podemos escrever $\mathcal{C}_K = \bigcup_{i=1}^{\infty} \mathcal{L}_i$. Por hipótese, $\mathcal{C}_K$ tem uma quantidade infinita de elementos. Então, para todo $M \in \mathbb{N}$, existe $i > M$ tal que $\mathcal{L}_i \neq \emptyset$, ou seja, existe $c \in \mathcal{C}_K$ tal que $\min_{J \in \overline{c}} N(J) > M$. Escolha $s \in \overline{c^{-1}}$. De (4.9), nós temos

$$\delta(\Lambda(s)) \geq \frac{n^{n/2}}{2^{\frac{3}{2}r_1 + 2r_2} \cdot \sqrt{|d|}} \cdot M.$$

Assim, a densidade de centro do reticulado associado ao ideal inteiro pode se tornar arbitrariamente grande, gerando uma contradição a limitação de δ visto na Definição 4.4. Portanto, $\mathcal{C}_K$ tem apenas uma quantidade finita de elementos. □

REFERÊNCIAS

[1] ASH, R. B. **A Course In Algebraic Number Theory**, Books online, http://www.math.uiuc.edu/ r-ash/, Illinois, 2003.

[2] ATIYAH M. F.; MACDONALD, I. G. **Introduction to Commutative Algebra**, Addison-Wesley Publishing Company, London, 1969.

[3] BHATTACHARYA, P. B.; JAIN, S. K.; NAGPAUL, S. R. **Basic abstract algebra**,Cambridge University Press 2ed., New York, 1995.

[4] CONWAY J. H.; SLOANE N. J. A. **Spheres packings, Lattices and Groups**, Third Edition, Springer-Verlag, New York, 1999.

[5] ENDLER, O. **Teoria dos Corpos**, Rio de Janeiro: IMPA, Publicações matemáticas, 1987.

[6] INTERLANDO, J. C.; NÓBREGA NETO, T. P.; NUNES, J. V. L. . Finiteness of the class group of a number field via lattice packings. **JP Journal of Algebra, Number Theory and Applications**, v. 13, p. 1-5, 2009.

[7] KOCH, H. **Number Theory**: Algebraic Numbers and Functions, Graduate studies in mathematics, v. 24, Providence, 2000.

[8] MOLLIN R. A. **Algebraic Number Theory**, Chapman and Hall/CRC, New York, 1999.

[9] MATSUMURA, H. **Commutative Ring Theory**, Cambridge Studies in Advanced Mathematics, London, 1989.

[10] NEUKIRCH, J. **Algebraic Number Theory**, ed. Springer, A series of Comprehensive Studies in Mathematics, v. 322, Berlin, 1937.

[11] SAMUEL P. **Algebraic theory of numbers**, Dover ed., Paris, 1970.

[12] WASHINGTON, L. C. **Introduction to Cyclotomic Fields**, Graduate Texts in Mathematics, Springer, New York, 1982.

[13] ZARISKI, O.; SAMUEL. P. **Commutative Algebra**, Vol. I, Van Nostrand, Princeton, 1958.