UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

ROBÉRIO ALEXANDRE COELHO

A CONJECTURA DE GAUSS E OS CORPOS DE CLASSES DE HILBERT

FORTALEZA

2014

ROBÉRIO ALEXANDRE COELHO

A CONJECTURA DE GAUSS E OS CORPOS DE CLASSES DE HILBERT

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do título de Mestre em Matemática. Área de Concentração: Teoria dos Números.

Orientador: Prof. Dr. José Othon Dantas Lopes

FORTALEZA

2014

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C619c Coelho, Robério Alexandre.
A Conjectura de Gauss e os Corpos de Classes de Hilbert / Robério Alexandre Coelho. – 2014.
142 f. : il.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Matemática, Fortaleza, 2014.
Orientação: Prof. Dr. José Othon Dantas Lopes.

1. Corpos Quadráticos. 2. Discriminante. 3. Grupo de Classes. 4. Corpos de Classes de Hilbert. I. Título.

CDD 510

ROBÉRIO ALEXANDRE COELHO

A CONJECTURA DE GAUSS E OS CORPOS DE CLASSES DE HILBERT

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do título de Mestre em Matemática. Área de Concentração: Teoria dos Números

Aprovada em: 06/11/2014

BANCA EXAMINADORA

_____

Prof. Dr. José Othon Dantas Lopes (Orientador)

Universidade Federal do Ceará – UFC

_____

Prof. Dr. José Robério Rogério

Universidade Federal do Ceará – UFC

_____

Prof. Dr. Trajano Pires da Nóbrega Neto

Universidade Estadual Paulista – UNESP

Dedico a todos os meus familiares

AGRADECIMENTOS

Obrigado a Deus e a meus familiares: tio Amaro Coelho da Silva, prima Eveline Ferreira Lima, tia Maria Elza de Almeida, tia Maria de Fátima Coelho, tia Maria Socorro de Jesus, pai Paulo Coelho da Silva, mãe Rozaria Alexandre Coelho, irmão Rommel Alexandre Coelho, irmão Romário Alexandre Coelho.

Obrigado ao meu orientador: José Othon Dantas Lopes.

Obrigado aos examinadores da banca: José Robério Rogério, Trajano Pires da Nóbrega Neto.

Obrigado aos membros do projeto UAB do IFCE "Juazeiro do Norte e Fortaleza": Ana Paula Gomes "Paulinha", Cristina Alves Bezerra, Darlan Portela Veras, Francisca Venâncio da Silva, Julyane Silva de Souza, Júnio Moreira de Alencar, Maria das Dôres dos Santos Moreira "Dorys", Maria Irene Silva de Moura, Priscila Rodrigues de Alcantara.

Obrigado aos professores do departamento de matemática da UFC: Abdênago Alves de Barros, Antônio Caminha Muniz Neto, Darlan Rabelo Girão, Ernani de Sousa Ribeiro Júnior, Fernanda Ester Camillo Camargo, Francesco Mercuri, João Lucas Marques Barbosa, Jorge Herbert Soares de Lira, José Alberto Duarte Maia, José Fábio Bezerra Montenegro, Levi Lopes de Lima, Luquésio Petróla de Melo Jorge, Marcos Ferreira de Melo.

Obrigado aos atuais e ex-professores dos departamentos de matemática da URCA e IFCE: Alexandro Coelho Alencar, Bárbara Paula B. Leite Lima, Francisco Valdemiro Braga, Flávio França Cruz, Jocel Faustino Norberto de Oliveira, José Alves Francisco, José Tiago Nogueira Cruz, Juscelino Perreira Silva, Luiz Antônio da Silva Medeiros, Marcos Antônio de Macedo, Maria Engrácia Loiola, Maria Vanda Silvino da Silva, Mário de Assis Oliveira, Paulo César Cavalcante de Oliveira, Regilânia da Silva Lucena, Ricardo Rodrigues de Carvalho, Tiago da Silva Alencar, Valéria Gerônimo Pedrosa Alencar, Zelálber Gondim Guimarães.

Obrigado aos amigos: Francisco de Assis Benjamim Filho, Maria Selene Bezerra de Carvalho.

Obrigado aos colegas e amigos de moradia: Antônio Airton Freitas Filho, Antônio Kelson Vieira da Silva, Antônio Wilson Rodrigues da Cunha, Augusto "Tchan", Elaine Sampaio de Sousa Carlos, Expedito, Cícero Tiarlos Nogueira Cruz, Francisco

Pereira Chaves, João Nunes de Araújo Neto, João Vítor da Silva, José Anastácio de Oliveira, Kelton Silva Bezerra, Renivaldo Sodré de Sena, Rondinelle Marcolino Batista, Upa Gomes.

Obrigado aos colegas e amigos de sala: Acácio Bizarria Neves, Breno Rafael Pinheiro Sampaio, Davi Ribeiro dos Santos, Diego de Sousa Rodrigues, Eddygledson Souza Gama, Elano Caio do Nascimento, Elisafã Braga dos Santos, Fábio da Costa Ribeiro, Francisca Damiana Vieira, Francisco Valber Parente Júnior, Gilson Granja Ferreira Filho, Helano dos Santos Campelo Rego, Janielly Gonçalves Araújo, João Luiz Batista de Melo Júnior, João Victor Maximiano Albuquerque, José Eduardo Moura Garcez, José Ilhano da Silva Pereira, Léo Ivo da Silva Souza, Marlon de Oliveira Gomes, Narcélio Silva de Oliveira Filho, Nícolas Alcântara de Andrade, Pereira Eufrazio, Raimundo Nonato Rodrigues da Cunha, Roger Oliveira Sousa, Wanderley de Oliveira Pereira, Henrique Blanco da Silva.

Obrigado aos demais colegas, alunos e ex-alunos do departamento da pós-graduação em matemática: Adenilson Arcanjo de Moura Júnior, Adriano Alves de Medeiros, Alex Sandro Lopes Santos, Alexandre de Sousa Mota, Antônio Diego Silva Farias, Antônio Edinardo de Oliveira, Cleiton Lira Cunha, Davi Lustosa da Silva, Diego Eloi Mesquita Gomes, Disson Soares dos Prazeres, Edvalter da Silva Sena Filho, Emanuel Mendonça Viana, Eraldo Almeida Lima Júnior, Fabiana Alves dos Santos, Fabrício de Figueredo Oliveira, Franciane de Brito Vieira, Francisco Yuri Alves Fernandes, Israel de Sousa Evangelista, Ivaldo Tributino de Sousa, João Francisco da Silva Filho, José Edson Sampaio, José Gleison Carneiro da Silva, José Ivan Mota Nogueira, José Loester Sá Carneiro, Leandro de Freitas Pessoa, Oslenne Nogueira de Araújo, Laerte Gomes Prado, Luiz Antônio Caetano Monte, Luiz Leonardo Duarte Garcia, Leonardo Tavares de Oliveira, Maria de Fátima Cruz Tavares, Neilha Marcia Pinheiro, Raquel Costa da Silva, Rodrigo Bezerra de Matos, Rafael Alves da Ponte, Rafael Jorge Pontes Diógenes, Ravik Mesquita Moreira da Rocha, Renan da Silva Santos, Rui Eduardo Brasileiro Paiva, Thadeu Ribeiro Benicio Milfont, Weslley Marinho Lozório.

Obrigado colegas e amigos de trabalho da URCA da unidade de Campos Sales: Adílio Junior de Souza, Cecília Rejane Duarte, Claudener Souza Teixeira, Daniel Batista Carneiro, Denise Aparecida Eneis Ribeiro, Francisco de Assis Gonçalves Dias Ferreira “Di Assis”, Francisco Ronald Feitosa, Francisco Vagner Gurgel Maia, Felipe Ridalgo Silvestre Soares, Moraes, Jackson “Mostorista”, Josafá Justino Barbosa, José Rafael da Cruz Souza,

Leila Kelly Pereira Dutra Taveira, Manoel Nilvan Macedo Oliveira Silva, Marcos Aurélio Figueiredo F. dos Santos, Maria das Graças Rodrigues Cabral, Maria Goretti de Sousa Alencar, Miguel Ângelo Monteiro Lessa, Nara Kelly Albuquerque Santos, Pedro Hudson Rodrigues Teixeira, Rafael Celestino Soares, Renato Juciano Ferreira, Rosa Carolline de Alencar, Samya de Oliveira Lima, Teresinha Pereira de Caldas Machado “Dona Teresinha”, Thiago do Nascimento Thel, Van Eudes Farias do Nascimento.

Obrigado aos demais funcionários do departamento e da PGMAT da UFC: Andréa Costa Dantas, Antônia Catarina Gomes Vieira Castelo Branco, Jéssyca Soares da Silva, Rocilda Maria Cavalcante Sales.

Obrigado aos funcionários do Alfa-Ômega: Evandro “Seu Diniz” e a Márcia.

Obrigado ao Google “pesquisa e tradutor”, ao Library Genesis e ao Wikipédia pelo auxílio a pesquisa.

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

“Eureka!” (Arquimedes)

“Se cheguei até aqui foi porque me apoiei em ombros de gigantes” (Isaac Newton)

“A Matemática é a rainha das Ciências e a Teoria dos Números é a rainha das Matemáticas” (Carl F. Gauss)

“Não tentes ser bem sucedido, tenta antes ser um homem de valor” (Albert Einstein)

“Qualidade significa fazer certo quando ninguém está olhando” (Henry Ford)

“Os homens de poucas palavras são os melhores” (William Shakespeare)

“Treinamento difícil, combate fácil” (Provérbio Militar)

“O destino de um é partilhado por todos” (Mestre dos Magos)

“As pessoas boas devem amar seus inimigos” (Seu Madruga)

“Independência ou Morte!” (D. Pedro I)

“Talvez possa descrever melhor a minha maneira de fazer matemática comparando-a com a entrada numa mansão escura. Entra-se na primeira divisão e está escuro, completamente escuro, tropeça-se e bate-se na mobília. Gradualmente, vai-se aprendendo onde está cada peça da mobília, e passados uns seis meses encontra-se o interruptor, liga-se a luz, e de repente está tudo iluminado, pode ver-se então exatamente onde se estava”. (Andrew Wiles)

RESUMO

A proposta principal do trabalho é baseada no artigo On the Class Number of Hilbert Class Fields do autor Farshid Hajir. Para isso são necessárias algumas noções preliminares da Teoria dos Números Algébricos que estão disponíveis no início do trabalho. A discussão é apresentar um caminho alternativo ao estudo do problema que ainda continua em aberto sobre a existência de infinitos corpos quadráticos reais com número de classe igual a 1, conhecido como a Segunda Conjectura de Gauss. Através do estudo dos Corpos de Classes de Hilbert obtemos alguns resultados relacionados a essa conjectura. Vamos também comentar o resultado particular publicado por Heegner-Stark-Baker, que foi o primeiro avanço obtido para o Problema do Número de Classe de Gauss.

Palavras-Chave: Corpos Quadráticos. Discriminante. Grupo de Classes. Corpos de Classes de Hilbert.

ABSTRACT

The main work proposal is based on Article On the Class Number of Hilbert Class Fields author Farshid Hajir. This requires some preliminary notions of the Theory of Algebraic Numbers are available at the beginning of the work. The discussion is to present an alternative way to study the problem still remains open on the existence of infinite real quadratic bodies with class number equal to 1, known as the Second Conjecture Gauss. Through the study of Hilbert Class Bodies get some results related to this conjecture. We will also comment on the particular result published by Heegner-Stark-Baker, who was the first advance made to the Issue Number Gauss class.

Keyword: Fields Quadratic. Discriminant. Group Class. Class Fields of Hilbert.

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{Q}$	Conjunto dos Números Racionais
$\mathbb{R}$	Conjunto dos Números Reais
$\mathbb{C}$	Conjunto dos Números Complexos
$\mathrm{M}_n(\mathrm{R})$	Conjunto das Matrizes com Entradas em R
$\mathbb{Z}_n$	Conjunto das Classes Módulo n
$\mathbb{Z}[i]$	Conjunto dos Inteiros Gaussiano
$\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}: \mathrm{K})$	Conjunto dos $\mathrm{K} - homorfismo$ de L em K
$dim_{\mathrm{K}}(\mathrm{V})$	Dimensão de V sobre K
$a \mid b$	a divide b
$a \nmid b$	a não divide b
$a \equiv b\ mod(n)$	a é côngruo a b módulo n
$\lvert x \rvert$	Módulo ou Valor Absoluto de x
$\mathrm{R} \leq \mathrm{S}$	R é subanel de S
$\mathrm{J} \trianglelefteq \mathrm{A}$	J é Ideal de A
$x\mathrm{R}$	Ideal Principal Gerado por x
$\langle x \rangle$	Ideal Principal Gerado por x
$\#(\mathrm{X})$	Cardinalidade de X
■	Fim da Demonstração
$\mathrm{I}_{\mathrm{S}}(\mathrm{R})$	Anel dos Inteiros de S sobre R
$\mathrm{K}_f(\mathrm{A})$	Corpo de Frações do Domínio A
$car(\mathrm{A})$	Característica de A
$\mathrm{R}[\alpha]$	Adjunção de α
$\mathrm{R}[x]$	Anel dos Polinômios na Indeterminada x sobre R
$m_\alpha(x)$	Polinômio Minimal do Elemento α
$\mathrm{P}_{(\alpha,\mathrm{L}\mid\mathrm{K})}(x)$	Polinômio Característico de φ_α
$\partial(p)$	Grau do Polinômio p
$\mathcal{U}(\mathrm{S})$	Conjunto das Unidades do Anel S
$\mathrm{R}/_{\mathrm{J}}$	Anel Quociente

$\preccurlyeq$	Ordem Parcial
$\mathrm{M} \lhd_{Sm} \mathrm{E}$	M é submódulo do Anel Noetheriano E
$\varphi\vert_{\mathrm{X}}$	Restrição ao Conjunto X
$ker(\varphi)$	Kernel ou Núcleo do Homomorfismo φ
$\mathrm{A} \cong \mathrm{B}$	A e B são Isomorfos
$\mathrm{Aut(K)}$	Conjunto dos Automorfismos de K
$\mathfrak{n}_{\mathfrak{p}}(\mathfrak{b})$	Expoente do Ideal Primo $\mathfrak{p}$ na Fatoração de $\mathfrak{b}$
$\mathrm{C}\ell_{\mathrm{K}}$	O Grupo de Classes de Ideais de K
h_{K}	Número de Classe do Corpo K
$f(\mathfrak{p})$	Grau de Inércia do Ideal Primo $\mathfrak{p}$
$\mathcal{F}(\mathrm{L})$	Grupo dos Ideais Fracionários
$\mathcal{P}(\mathrm{L})$	Grupo dos Ideais Fracionários Principais
$\mathrm{Tr}_{(\mathrm{L}\vert\mathrm{K})}(\alpha)$	Traço do Elemento α
$\mathcal{N}_{(\mathrm{L}\vert\mathrm{K})}(\alpha)$	Norma do Elemento α
$\mathcal{N}_{(\mathrm{L}\vert\mathrm{K})}(\mathfrak{a})$	Norma do Ideal $\mathfrak{a}$
$disc(\mathrm{K})$	Discriminante de K
d_{K}	Discriminante de K
$det(\mathrm{X})$	Determinante da Matriz X
δ_{K}	Número de Divisores de $disc(\mathrm{K})$
L|K	L é Extensão do Corpo K
$[\mathrm{L} : \mathrm{K}]$	O Grau da Extensão L|K
Gal(L|K)	Grupo de Galois de L sobre K
H(K)	Corpo de Classe de Hilbert de K
$\ell(\mathrm{K})$	Comprimento da Cadeia de Corpos
$\mathrm{H}^{p}(\mathrm{K})$	Corpo $p - classe$ de Hilbert de K
S_n	Grupo de Permutações
A_n	Grupo de Permutações Pares

SUMÁRIO

1 INTRODUÇÃO

A Teoria dos Números é um dos ramos da Matemática Pura em que muitos problemas se encontram em aberto, alguns deles clássicos.

Discutir sobre uma dessas conjecturas que ainda continua sem resposta é uma das propostas desse trabalho.

O problema em encontrar um algoritmo eficiente que forneça para cada $h \geq 1$ uma lista completa de todos os corpos quadráticos imaginários com o determinado número de classe h é conhecido como o problema do número de classes de Gauss.

Este problema tem uma longa história, que não fazemos a reprodução aqui, mas os primeiros passos importantes foram obtidos pelos matemáticos Kurt **Heegner** em 1952 Harold **Stark** em 1967 e Alan **Baker** em 1966 cujos trabalhos levaram a solução do problema do número de classe igual a 1 e 2.

Mais tarde foi resolvido o problema do número de classes igual a 3 por Kenneth **Ireland** e Mchael **Rosen** em 1993 e para o número de classes até 100 por Mark **Watkins** em 2004.

Problema do Número de Classes: Para um dado número de classes pequeno "como $h = 1, 2, 3$" encontrar a tabela dos corpos quadráticos imaginários com número de classes h.

O problema foi escrito em 1801 na Seção V, entre os artigos 303 e 304 de Disquisitiones Arithmeticae.

No artigo 303 Gauss discute corpos quadráticos imaginários e no artigo 304 discute corpos quadráticos reais, enunciando duas conjecturas.

Primeira Conjectura: $h(d) \longrightarrow \infty$ quando $d \longrightarrow -\infty$. Onde $h(d)$ é o número de classes dos corpos $\mathbb{Q}(\sqrt{d})$ e d é inteiro livre de quadrados.

Segunda Conjectura: Existem infinitos corpos quadráticos reais com número de classe igual a 1.

A primeira conjectura encontra-se resolvida por Hans **Heilbronn**, 1934, porém o segundo enunciado encontra-se ainda sem resposta.

O capítulo 01 é destinado a conceitos, definições e alguns resultados básicos da Teoria dos Números Algébricos.

O capítulo 02 é onde estão concentrados os propósitos do referido trabalho que envolve o artigo publicado pelo autor Farshid **Hajir** em 1997. Nesse capítulo são

discutidas questões relacionadas a Segunda Conjectura de Gauss, bem como a ferramenta alternativa “Corpos de Classes de Hilbert” mais indicada na tentativa de chegar a avanços significativos. São apresentadas novas questões ainda desconhecidas, computações e evidências que se mostram provavelmente verdadeiras.

2 PRELIMINARES, CONCEITOS E DEFINIÇÕES

2.1 Módulos

Nesta seção são apresentadas as definições e as propriedades elementares sobre módulos em Álgebra Abstrata que é um conceito central para Álgebra Comutativa.

A noção de módulo é a generalização do conceito de espaço vetorial em Álgebra Linear, ao em vez de corpo, tomamos um anel para o conjunto de escalares.

2.1.1 Módulos e Submódulos

Considere $(\mathrm{A}, +, \cdot)$ um anel com identidade e $(\mathrm{M}, +)$ um grupo abeliano. M é denominado de $\mathrm{A} - m\acute{o}dulo$ quando há uma operação

$$\begin{aligned} * : \mathrm{A} \times \mathrm{M} &\longrightarrow \mathrm{M} \\ (a, m) &\longmapsto a * m \end{aligned}$$

tal que, dados $a, b \in \mathrm{A}$ e $m, n \in \mathrm{M}$, tem-se:

$(i)\ a * (b * m) = (ab) * m$

$(ii)\ a * (m + n) = a * m + a * n$

$(iii)\ (a + b) * m = a * m + b * m$

$(iv)\ 1_{\mathrm{A}} * m = m$

Exemplo 01: O grupo $\{0\}$ é um $\mathrm{A} - m\acute{o}dulo$, com $(\mathrm{A}, +, \cdot)$ um anel.

Exemplo 02: Espaços vetoriais $(\mathrm{V}, +, \cdot)$ sobre um corpo K são $\mathrm{K} - m\acute{o}dulos$.

Exemplo 03: Todo anel $(\mathrm{A}, +, \cdot)$ é um $\mathrm{A} - m\acute{o}dulo$. Nesse caso $\mathrm{M} = (\mathrm{A}, +)$.

Exemplo 04: O conjunto $(\mathrm{M}, +)$ e $\{0\}$ são $\mathrm{A} - m\acute{o}dulo$ denominados triviais.

Quando N é um subconjunto não vazio de M, N é denominado $\mathrm{A}-$ *submódulo* de M quando:

(i) N é subgrupo abeliano de M

(ii) Para $n \in \mathrm{N}$ e $a \in \mathrm{A}$ quaisquer implique $a * n \in \mathrm{N}$

Proposição 01: Considere $(\mathrm{M}, +)$ um $\mathrm{A}-$ *módulo* e N um subconjunto não vazio de M. Então N é $\mathrm{A}-$ *submódulo* de M se e somente se satisfazer as condições:

$(i) \ \forall \ x, y \in \mathrm{N} \Longrightarrow x + y \in \mathrm{N}$

$(ii) \ \forall \ a \in \mathrm{A}, \forall \ n \in \mathrm{N} \Longrightarrow a * n \in \mathrm{N}$

Demonstração:

Se N é um $\mathrm{A}-$ *submódulo* de M, então vale (i) e (ii) de acordo com a definição.

Reciprocamente se N é subconjunto não vazio de M, então existe um elemento $n \in \mathrm{N}$. Mas de acordo com o item (ii) $0_{\mathrm{A}} = 0_{\mathrm{A}} * n \in \mathrm{N}$ e $-n = -1_{\mathrm{A}} * n \in \mathrm{N}$. Por outro lado N herda a associatividade e comutatividade de M, significando que N é subgrupo abeliano de M. Com isso segundo o item (ii) da definição, resulta que N é $\mathrm{A}-$ *submódulo* de M.

■

Exemplo 05: Dado o $\mathrm{A}-$ *módulo* $(\mathrm{M}, +)$ e o ideal à esquerda J de A, o conjunto $\mathrm{J}m = \{am : a \in \mathrm{A}\}$ é $\mathrm{A}-$ *submódulo* de M.

Proposição 02: Se $(\mathrm{M}, +)$ é um $\mathrm{A}-$ *módulo*, então a interseção arbitrária de $\mathrm{A}-$ *submódulos* N de M é um $\mathrm{A}-$ *submódulo* de M.

Demonstração:

Considere $\{\mathrm{N}_i\}_{i \in \Gamma}$ uma família de submódulos de M e o conjunto $\mathrm{N} = \bigcap_{i \in \Gamma} \mathrm{N}_i$.

Dados $x, y \in \mathrm{N}$, tem-se que $x, y \in \mathrm{N}_i$ para todo $i \in \Gamma$, donde $x + y \in \mathrm{N}_i$ para todo $i \in \Gamma$, consequentemente $x + y \in \bigcap_{i \in \Gamma} \mathrm{N}_i$. Por outro lado, para qualquer $a \in \mathrm{A}$ e $n \in \mathrm{N}$ tem-se que $a * n \in \mathrm{N}_i$ para todo $i \in \Gamma$, donde $a * n \in \bigcap_{i \in \Gamma} \mathrm{N}_i$. Portanto N é $\mathrm{A}-$ *submódulo* de M.

■

Exemplo 06: Se N e P são $A-$ *submódulos* de um $A-$ *módulo* $(M,+)$, então o conjunto $N+P=\{n+p : n \in N, p \in P\}$ é um $A-$ *submódulo* de M.

Note que para $x, y \in N+P$ tal que $x=n+p$, $y=\tilde{n}+\tilde{p}$ e $a \in A$ tem-se:

$$x+y=(n+p)+(\tilde{n}+\tilde{p})=(n+\tilde{n})+(p+\tilde{p}) \in N+P$$
$$a*x=a*n+a*p \in N+P$$

Considere o $A-$ *submódulo* N do $A-$ *módulo* $(M,+)$. Para $x, y \in M$ define-se a relação $x \equiv y\ mod(N)$ se e somente se $x-y \in N$. Esta relação é uma relação de equivalência. A classe de equivalência para cada $m \in M$ é o conjunto

$$[m]=\{x \in M : x \equiv m\ mod(N)\}$$

Assim:

$$[m]=\{x \in M : x-m \in N\} \Leftrightarrow$$
$$[m]=\{x \in M : x=m+n, \text{com } n \in N\} \Leftrightarrow$$
$$[m]=\{m+n : n \in N\}=m+N$$

Como $(M,+)$ é grupo abeliano, segue que todo seu submódulo N é um subgrupo normal e com isso as classes laterais $m+N$, $N+m$ são iguais.

Proposição 03: Para $x, y \in M$, tem-se que $x+N=y+N$ se e somente se $x \equiv y\ mod(N)$.

Demonstração:

Dados $x, y \in M$ tal que $x+N=y+N$, segue que $x=y+n$ para algum $n \in N$ donde $x-y=n \in N$, ou seja $x \equiv y\ mod(N)$.

Reciprocamente para $x, y \in M$ tal que $x \equiv y\ mod(N)$, então $x-y \in N$ donde $x=y+n \in y+N$. Assim para todo $z \in x+N$ implica $z=x+\tilde{n}=y+(n+\tilde{n}) \in y+N$, significando que $x+N \subseteq y+N$. De modo análogo $y+N \subseteq x+N$.

■

O conjunto quociente é denotado e definido por:

$$\mathrm{M}/_{\mathrm{N}} = \{[x] : x \in \mathrm{M}\} = \{x + \mathrm{N} : x \in \mathrm{M}\}$$

Proposição 04: O conjunto quociente $\mathrm{M}/_{\mathrm{N}}$ é um grupo abeliano com a operação

$$\oplus : \frac{\mathrm{M}}{\mathrm{N}} \times \frac{\mathrm{M}}{\mathrm{N}} \longrightarrow \frac{\mathrm{M}}{\mathrm{N}}$$

definida por $(x + \mathrm{N}, y + \mathrm{N}) \longmapsto (x + \mathrm{N}) \oplus (y + \mathrm{N}) = (x + y) + \mathrm{N}$

Demonstração:

Primeiramente a operação está bem definida, porque tomando $x, y, z, w \in \mathrm{M}$ tal que $(x + \mathrm{N}, y + \mathrm{N}) = (z + \mathrm{N}, w + \mathrm{N})$ implica $x + \mathrm{N} = z + \mathrm{N}$ e $y + \mathrm{N} = w + \mathrm{N}$ donde, $x - z \in \mathrm{N}$ e $y - w \in \mathrm{N}$ logo $(x - z) + (y - w) = (x + y) - (z + w) \in \mathrm{N}$ significando que $(x + y) + \mathrm{N} = (z + w) + \mathrm{N}$.

Como M é associativo segue que para todo $x, y, z \in \mathrm{M}$ tem-se:

$$\begin{aligned}
&(x + \mathrm{N}) \oplus [(y + \mathrm{N}) \oplus (z + \mathrm{N})] = \\
&(x + \mathrm{N}) \oplus (y + z) + \mathrm{N} = \\
&(x + y + z) + \mathrm{N} = \\
&[(x + y) + \mathrm{N}] \oplus (z + \mathrm{N}) = \\
&[(x + \mathrm{N}) \oplus (y + \mathrm{N})] \oplus (z + \mathrm{N})
\end{aligned}$$

logo $\mathrm{M}/_{\mathrm{N}}$ é associativo.

Sendo 0_{M} elemento neutro de M, então $0_{\mathrm{M}} + \mathrm{N} = \mathrm{N}$ é o elemento neutro de $\mathrm{M}/_{\mathrm{N}}$, porque para todo $x \in \mathrm{M}$, tem-se:

$$(0_{\mathrm{M}} + \mathrm{N}) \oplus (x + \mathrm{N}) = x + \mathrm{N} = (x + \mathrm{N}) \oplus (0_{\mathrm{M}} + \mathrm{N})$$

Sendo $-x$ o elemento inverso de $x \in \mathrm{M}$, segue que $-x + \mathrm{N}$ é o elemento inverso de $x + \mathrm{N}$ uma vez que:

$$(-x + \mathrm{N}) \oplus (x + \mathrm{N}) = \mathrm{N} = (x + \mathrm{N}) \oplus (-x + \mathrm{N})$$

Por fim como M é abeliano então para todo $x, y \in \mathrm{M}$, tem-se:

$$(x + \mathrm{N}) \oplus (y + \mathrm{N}) = (y + x) + \mathrm{N} = (y + \mathrm{N}) \oplus (x + \mathrm{N})$$

■

Proposição 05: Dado o grupo abeliano $^{\mathrm{M}}/_{\mathrm{N}}$ com a operação $\oplus$ definida anteriormente, $^{\mathrm{M}}/_{\mathrm{N}}$ é um $\mathrm{A} - \textit{módulo}$ com a operação multiplicativa

$$\odot : \mathrm{A} \times \frac{\mathrm{M}}{\mathrm{N}} \longrightarrow \frac{\mathrm{M}}{\mathrm{N}}$$

definida por $(a, x + \mathrm{N}) \longmapsto a \odot (x + \mathrm{N}) = a * x + \mathrm{N}$ para $x \in \mathrm{M}$.

Demonstração:

Primeiramente a operação está bem definida, pois tomando $x, y \in \mathrm{M}$ e $a \in \mathrm{A}$ tal que $(a, x + \mathrm{N}) = (a, y + \mathrm{N})$, tem-se $x + \mathrm{N} = y + \mathrm{N}$ donde $x - y \in \mathrm{N}$. Assim $a * (x - y) = a * x - a * y \in \mathrm{N}$, significando que $a * x + \mathrm{N} = a * y + \mathrm{N}$.

Agora dados $a, b \in \mathrm{A}$ e $x, y \in \mathrm{M}$ tem-se que:

(i)

$$(ab) \odot (x + \mathrm{N}) =$$
$$(ab) * x + \mathrm{N} =$$
$$a(b * x) + \mathrm{N} =$$
$$a \odot (bx + \mathrm{N})$$

(ii)

$$(a + b) \odot (x + \mathrm{N}) =$$
$$(a + b) * x + \mathrm{N} =$$
$$(a * x + b * x) + \mathrm{N} =$$
$$(a * x + \mathrm{N}) \oplus (b * x + \mathrm{N})$$

(iii)

$$a \odot [(x + y) + \mathrm{N}] =$$

$$a * (x + y) + \mathrm{N} =$$
$$(a * x + a * y) + \mathrm{N} =$$
$$(a * x + \mathrm{N}) \oplus (a * y + \mathrm{N})$$

(iv)

$$1_{\mathrm{A}} \odot (x + \mathrm{N}) =$$
$$1_{\mathrm{A}} * x + \mathrm{N} =$$
$$x + \mathrm{N}$$

Portanto ${}^{\mathrm{M}}/_{\mathrm{N}}$ é $\mathrm{A} - \textit{módulo}$ denominado módulo quociente.

■

Exemplo 07: Dado um ideal I do anel A, o anel quociente ${}^{\mathrm{A}}/_{\mathrm{I}}$ tem estrutura de $\mathrm{A} - \textit{módulo}$. O anel A tem estrutura de $\mathrm{A} - \textit{módulo}$ com seus ideais sendo seus $\mathrm{A} - \textit{submódulos}$.

2.1.2 Homomorfismos

Um homomorfismo de $\mathrm{A} - \textit{módulos}$ $(\mathrm{M}, +)$ e $(\mathrm{N}, \dot{+})$ é a aplicação $f : \mathrm{M} \longrightarrow \mathrm{N}$ tal que para todo $x, y \in \mathrm{M}$ e $a \in \mathrm{A}$ valem as condições:

$(i)\ f(x + y) = f(x) \dot{+} f(y)$
$(ii)\ f(ax) = a * f(x)$

Proposição 06: Considere os $\mathrm{A} - \textit{módulos}$ $(\mathrm{M}, +)$ e $(\mathrm{N}, \dot{+})$, o homomorfismo $f : \mathrm{M} \longrightarrow \mathrm{N}$ satisfazem as condições:

$(i)\ f(0_{\mathrm{M}}) = 0_{\mathrm{N}}$
$(ii)\ f(-x) = -f(x)$

Demonstração:

(i) Segue que $f(0_{\mathrm{M}}) = f(0_{\mathrm{M}}) \dot{+} f(0_{\mathrm{M}})$ logo $f(0_{\mathrm{M}}) = 0_{\mathrm{N}}$.

(ii) Sendo $f(0_{\mathrm{M}}) = 0_{\mathrm{N}}$ segue que $0_{\mathrm{N}} = f(x - x) = f(x) \dot{+} f(-x)$ resultando que $f(-x) = -f(x)$ para todo $x \in \mathrm{M}$.

■

Dado um homomorfismo de $\mathrm{A} - módulos$ $(\mathrm{M}, +)$ e $(\mathrm{N}, \dot{+})$ define-se os conjuntos $im(f) = \{f(x) : x \in \mathrm{M}\}$ e $ker(f) = \{x \in \mathrm{M} : f(x) = 0_{\mathrm{N}}\}$ denominados imagem e kernel ou núcleo respectivamente.

Proposição 07: O homomorfismo $f : \mathrm{M} \longrightarrow \mathrm{N}$ de $\mathrm{A} - módulos$ $(\mathrm{M}, +)$ e $(\mathrm{N}, \dot{+})$ é injetivo se e somente se $ker(f) = \{0_{\mathrm{M}}\}$.

Demonstração:

Suponha que $f : \mathrm{M} \longrightarrow \mathrm{N}$ é um homomorfismo injetivo. Escolhendo um $x \in ker(f)$ tem-se que $f(x) = 0_{\mathrm{N}}$ e por outro lado $f(0_{\mathrm{M}}) = 0_{\mathrm{N}}$, logo $x = 0_{\mathrm{M}}$.

Reciprocamente considere $ker(f) = \{0_{\mathrm{M}}\}$ e sejam $x, y \in \mathrm{M}$ quaisquer tal que $f(x) = f(y)$. Assim $f(x - y) = f(x) \dot{+} f(-y) = 0_{\mathrm{N}}$ resultando que $x - y = 0_{\mathrm{M}}$. Portanto f é injetivo.

■

Proposição 08: Sejam os homomorfismos $f : \mathrm{M} \longrightarrow \mathrm{N}$, $g : \mathrm{N} \longrightarrow \mathrm{P}$ de $\mathrm{A} - módulos$ $(\mathrm{M}, +)$, $(\mathrm{N}, \dot{+})$, $(\mathrm{P}, \ddot{+})$. A aplicação composta $g \circ f : \mathrm{M} \longrightarrow \mathrm{P}$ é um homomorfismo.

Demonstração:

Sejam $x, y \in \mathrm{M}$, assim

$$(g \circ f)(x + y) =$$
$$g\big(f(x + y)\big) =$$
$$g\big(f(x) \dot{+} f(y)\big) =$$
$$g\big(f(x)\big) \ddot{+} g\big(f(y)\big) =$$
$$(g \circ f)(x) \ddot{+} (g \circ f)(y)$$

Por fim para $x \in \mathrm{M}$ e $a \in \mathrm{A}$ tem-se que:

$$(g \circ f)(ax) =$$

$$g\big(f(ax)\big) =$$
$$g\big(a * f(x)\big) =$$
$$a * g\big(f(x)\big) =$$
$$a * (g \circ f)(x)$$

■

Proposição 09 "Teorema dos Isomorfismos de Módulos": Seja $f : \mathrm{M} \longrightarrow \mathrm{N}$ um homomorfismo de $\mathrm{A} - módulos$ $(\mathrm{M}, +)$ e $(\mathrm{N}, \dot{+})$. Então:

(i) $im(f)$ é $\mathrm{A} - submódulo$ de N

(ii) $ker(f)$ é $\mathrm{A} - submódulo$ de M

(iii) $\dfrac{\mathrm{M}}{ker(f)} \cong im(f)$

Demonstração:

(i) Segue que $im(f)$ é não vazio, uma vez que $f(0_{\mathrm{M}}) = 0_{\mathrm{N}}$. Para $x, y \in im(f)$ tem-se que $x = f(u)$, $y = f(v)$ com $u, v \in \mathrm{M}$. Assim $x + y = f(u) \dot{+} f(v) = f(u + v) \in im(f)$. Por outro lado, para todo $a \in \mathrm{A}$, $a * x = a * f(u) = f(au)$. Portanto $im(f)$ é $\mathrm{A} - submódulo$ de N.

(ii) Temos que $ker(f)$ é não vazio uma vez que $f(0_{\mathrm{M}}) = 0_{\mathrm{N}}$. Agora dados $x, y \in ker(f)$ tem-se que $x + y \in ker(f)$ pois $f(x + y) = f(x) \dot{+} f(y) = 0_{\mathrm{N}}$. Por fim para todo $a \in \mathrm{A}$, e segue que $a * x \in ker(f)$ uma vez que $f(ax) = a * f(x) = 0_{\mathrm{N}}$.

(iii) Primeiramente considere a aplicação

$$\varphi : \frac{\mathrm{M}}{ker(f)} \longrightarrow im(f)$$

dada por $x + ker(f) \mapsto \varphi\big(x + ker(f)\big) = f(x)$. A aplicação φ está bem definida, pois para $x + ker(f), y + ker(f) \in {}^{\mathrm{M}}/_{ker(f)}$ tal que $x + ker(f) = y + ker(f)$ resulta que $x - y \in ker(f)$ donde $f(x - y) = f(x) \oplus f(-y) = 0_{\mathrm{N}}$ e consequentemente $f(x) = f(y)$.

De fato φ é um homomorfismo visto que:

$$\varphi\Big(\big(x + ker(f)\big) \oplus \big(y + ker(f)\big)\Big) =$$
$$\varphi\big((x + y) + ker(f)\big) =$$
$$f(x + y) =$$
$$f(x) \dot{+} f(y) =$$
$$\varphi\big(x + ker(f)\big) \dot{+} \varphi\big(y + ker(f)\big)$$

e também

$$\varphi\Big(a \odot \big(x + ker(f)\big)\Big) =$$
$$\varphi\big(a * x + ker(f)\big) =$$
$$f(a * x) =$$
$$a \odot f(x) =$$
$$\varphi\big(x + ker(f)\big)$$

para todo $x, y \in \mathrm{M}$ e $a \in \mathrm{A}$.

Agora se $\varphi\big(x + ker(f)\big) = \varphi\big(y + ker(f)\big)$ com $x, y \in \mathrm{M}$, então $f(x) = f(y)$ se e somente se $f(x - y) = f(x) \oplus f(-y) = 0_{\mathrm{N}}$ significando que $x - y \in ker(f)$ ou seja $x + ker(f) = y + ker(f)$ e assim φ é injetiva.

Por outro lado φ também é sobrejetiva já que $im(\varphi) = \big\{\varphi\big(x + ker(f)\big) : x \in \mathrm{M}\big\} = \{f(x) : x \in \mathrm{M}\} = im(f)$.

Portanto φ é um isomorfismo.

■

Exemplo 08: Dado um $\mathrm{A} - submódulo$ N do $\mathrm{A} - módulo$ $(\mathrm{M}, +)$. Denomina-se projeção canônica a aplicação $\pi : \mathrm{M} \longrightarrow {}^{\mathrm{M}}/_{\mathrm{N}}$ dada por $\pi(x) = x + \mathrm{N}$ que é um homomorfismo sobrejetivo. Isso decorre que para todo $x, y \in \mathrm{M}$ e $a \in \mathrm{A}$ tem-se:

$$\pi(x+y) = (x+y) + \mathrm{N} = (x+\mathrm{N}) \oplus (y+\mathrm{N}) = \pi(x) \oplus \pi(y)$$
$$\pi(a * x) = ax + \mathrm{N} = a(x+\mathrm{N}) = a \odot \pi(x)$$

A sobrejetividade de π é imediata.

Exemplo 09: Se K for um corpo, os homomorfismos dos $\mathrm{K}-$*módulos* são transformações lineares.

2.1.3 Módulos Livres

Um $\mathrm{A}-$*módulo* $(\mathrm{M}, +)$ é denominado livre se existir uma família de elementos $\{e_i\}_{i\in\Gamma}$ de M satisfazendo as condições:

(a) $\{e_i\}_{i\in\Gamma}$ é linearmente independente sobre A, ou seja:

$$\sum_{i\in\Gamma} a_i e_i = 0_{\mathrm{M}} \Longrightarrow a_i = 0_{\mathrm{A}} \text{ com } i \in \Gamma$$

(b) Todo elemento $x \in \mathrm{M}$ é combinação linear de $\{e_i\}_{i\in\Gamma}$ ou seja:

$$x = \sum_{i\in\Gamma} a_i e_i \text{ , com } a_i \in \mathrm{A}$$

Tal família $\{e_i\}_{i\in\Gamma}$ é denominada base do $\mathrm{A}-$*módulo* livre A. Para um anel comutativo A, as bases terão mesma cardinalidade e o posto de M é definido como o número de elementos da base.

Quando o conjunto de índices Γ é finito dizemos que o $\mathrm{A}-$*módulo* M é finitamente gerado ou do tipo finito.

Para o anel comutativo A e um conjunto de índices Γ denota-se por $\mathrm{A}^{(\Gamma)}$ o conjunto $\{(a_i)_{i\in\Gamma} : a_i = 0$ exceto para um número finito de índices $i \in \Gamma\}$.

Dado o anel A e $(\mathrm{M}, +)$ um $\mathrm{A}-$*módulo*, $\{e_i\}_{i\in\Gamma}$ uma família em M, a aplicação $\varphi : \mathrm{A}^{(\Gamma)} \longrightarrow \mathrm{M}$ dada por:

$$(a_i)_{i\in\Gamma} \longmapsto \sum_{i\in\Gamma} a_i e_i$$

é linear.

Proposição 10: $\varphi : \mathrm{A}^{(\Gamma)} \longrightarrow \mathrm{M}$ é injetiva se e somente se $\{e_i\}_{i\in\Gamma}$ é linearmente independente.

Demonstração:

Dadas duas sequências indexadas $(a_i)_{i\in\Gamma}$ e $(b_i)_{i\in\Gamma}$ tal que

$$\sum_{i\in\Gamma} a_i e_i = \sum_{i\in\Gamma} b_i e_i \Leftrightarrow \sum_{i\in\Gamma} (a_i - b_i) e_i = 0_{\mathrm{M}}$$

Mas por hipótese $\{e_i\}_{i\in\Gamma}$ é linearmente independente donde $a_i - b_i = 0_{\mathrm{A}}$ ou seja $a_i = b_i$ para todo $i \in \Gamma$ é injetiva.

Reciprocamente admita que φ é injetiva e seja a combinação linear

$$\sum_{i\in\Gamma} a_i e_i = 0_{\mathrm{M}}$$

Então $(a_i)_{i\in\Gamma}$ é uma sequência no $ker(\varphi)$ e pela injetividade de φ, segue que $a_i = 0_{\mathrm{A}}$ para todo $i \in \Gamma$ e assim $\{e_i\}_{i\in\Gamma}$ é linearmente independente.

■

Proposição 11: $\varphi : \mathrm{A}^{(\Gamma)} \longrightarrow \mathrm{M}$ é sobrejetiva se e somente se $\{e_i\}_{i\in\Gamma}$ gera M.

Demonstração:

Suponha que $\{e_i\}_{i\in\Gamma}$ gere M, logo todo $y \in \mathrm{M}$ é da forma

$$y = \sum_{i\in\Gamma} a_i e_i$$

onde $a_i \in \mathrm{A}$ com $i \in \Gamma$ donde $(a_i)_{i\in\Gamma}$ está em $\mathrm{A}^{(\Gamma)}$. Portanto φ é sobrejetiva.

Reciprocamente se φ é sobrejetiva, dado qualquer $y \in \mathrm{M}$, existe $x = (a_i)_{i\in\Gamma}$ em $\mathrm{A}^{(\Gamma)}$ tal que

$$\varphi(x) = y = \sum_{i\in\Gamma} a_i e_i$$

logo $\langle e_i \rangle_{i\in\Gamma} = \mathrm{M}$.

■

Exemplo 10: $\{1, x, \cdots, x^n, \cdots\}$ é uma base do $\mathrm{A} - m\acute{o}dulo$ livre $\mathrm{A}[x]$.

Exemplo 11: $\{1, i\}$ é linearmente independente sobre $\mathbb{R}$ e consequentemente linearmente independente sobre $\mathbb{Z}$. Por outro lado $\langle 1, i\rangle = \mathbb{Z} + i\mathbb{Z} = \mathbb{Z}[i]$ é $\mathbb{Z} - m\acute{o}dulo$ livre.

2.2 Anéis Noetherianos e Domínios de Dedekind

A classe dos anéis Neotherianos é mais geral que a classe dos anéis de Dedekind. Iremos discutir o problema da fatoração única em anéis de Dedekind. No lugar da fatoração única em potências de elementos irredutíveis, válida somente no caso de domínios fatoriais, prova-se que em qualquer anel de inteiros algébricos $\mathrm{I_L}(\mathbb{Z})$ onde L é um corpo numérico, todo ideal não nulo possui uma fatoração única em potências de ideais primos, ou seja $\mathrm{I_L}(\mathbb{Z})$ pertence a classe dos domínios de Dedekind e portanto é Noetheriano.

O corpo quadrático $\mathrm{L} = \mathbb{Q}\left[\sqrt{-5}\right]$ mostra que o anel $\mathrm{I_L}(\mathbb{Z}) = \mathbb{Z}\left[\sqrt{-5}\right]$ não é fatorial apesar de ser integralmente fechado.

O principal objetivo por trabalhar com domínios de Dedekind R, é a verificação da existência e a unicidade na fatoração de ideais não nulos em ideais primos, já que a fatoração de elementos de $\mathrm{R} - \{0\}$ em elementos irredutíveis, embora sempre exista, porém nem sempre é única e que da mesma maneira que a fatoração em elementos irredutíveis é estendida aos elementos não nulos de $\mathrm{K}_f(\mathrm{R})$ "corpo de frações de R" admitindo potências negativas dos elementos irredutíveis, convém estender a fatoração em ideais primos aos ideais fracionários de R.

2.2.1 Anéis e Módulos Noetherianos

Dado um anel R, diremos que R é Noetheriano, quando todos os seus ideais são finitamente gerados ou do tipo finito. Convém estender para um $\mathrm{R}-$ *módulo* M.

Um $\mathrm{R}-$ *módulo* M é dito ser Noetheriano se todo $\mathrm{R}-$ *submódulo* N seu for finitamente gerado.

Em particular um anel R é chamado Noetheriano, se considerado como um $\mathrm{R}-$ *módulo* "seus submódulos são seus ideais" é Noetheriano.

Seja $(\Omega, \preccurlyeq)$ um conjunto parcialmente ordenado. Diremos que Ω satisfaz a condição maximal se todo subconjunto $\mathrm{X} \subset \Omega$ não vazio possuir pelo menos um elemento maximal ou seja existir $b_0 \in \mathrm{X}$ tal que não exista nenhum elemento $b \in \mathrm{X}$ com $b_0 \prec b$.

Diremos que $(\Omega, \preccurlyeq)$ satisfaz a condição de cadeia ascendente, se para toda sequência $(x_n)_{n\in\mathbb{N}}$ em Ω for estacionária, ou seja: se $x_1 \preccurlyeq x_2 \preccurlyeq \cdots \preccurlyeq x_{n-1} \preccurlyeq x_n \preccurlyeq \cdots$ então existe um $n_0 \in \mathbb{N}$ tal que $x_n = x_{n_0}$ para todo $n \geq n_0$.

Para dois ideais $\mathfrak{a}$ e $\mathfrak{b}$ de um anel A, definimos a soma $\mathfrak{a} + \mathfrak{b}$ dos ideais, como o conjunto dos elementos $a + b$ tal que $a \in \mathfrak{a}$ e $b \in \mathfrak{b}$. Ou seja:

$$\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a} \text{ e } b \in \mathfrak{b}\}$$

Diremos que dois ideais $\mathfrak{a}, \mathfrak{b}$ do anel A são comaximais quando $\mathfrak{a} + \mathfrak{b} = \mathrm{A}$.

Proposição 12: Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais comaximais de A, então $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.

Demonstração:

De fato, segue que $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Por outro lado dado $z \in \mathfrak{a} \cap \mathfrak{b}$ temos que $z \in \mathfrak{a}$ e como $\mathfrak{a} + \mathfrak{b} = \mathrm{A}$ existem $x \in \mathfrak{a}$ e $y \in \mathfrak{b}$ tal que $x + y = 1$. Logo $z = zx + zy \in \mathfrak{a} \cdot \mathfrak{b}$.

■

Proposição 13: Se $\mathfrak{a}_1, \mathfrak{a}_2$ são ideais de R com $r_1, r_2 \in \mathrm{R}$, então existe um $r \in \mathrm{R}$ tal que:

$$\begin{cases} r \equiv r_1 \ mod(\mathfrak{a}_1) \\ r \equiv r_2 \ mod(\mathfrak{a}_2) \end{cases}$$

se e somente se $r_1 \equiv r_2\ mod(\mathfrak{a}_1 + \mathfrak{a}_2)$.

Demonstração:

Suponhamos que exista um $r \in$ R tal que

$$\begin{cases} r \equiv r_1\ mod(\mathfrak{a}_1) \\ r \equiv r_2\ mod(\mathfrak{a}_2) \end{cases}$$

então $(r - r_1) - (r - r_2) = r_2 - r_1 \in \mathfrak{a}_1 + \mathfrak{a}_2$.

Reciprocamente se $r_1 \equiv r_2\ mod(\mathfrak{a}_1 + \mathfrak{a}_2)$ então existem $x \in \mathfrak{a}_1$ e $y \in \mathfrak{a}_2$ tal que $r_1 - r_2 = x - y$, logo $r = r_1 - x = r_2 - y \equiv r_j\ mod(\mathfrak{a}_j)$ "$j = 1, 2$".

■

Proposição 14: Para quaisquer ideais $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ de R, com $n \geq 2$ as seguintes condições são equivalentes:

(i) $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ são dois a dois comaximais.

(ii) $\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n$ e para quaisquer $r_1, r_2, \cdots, r_n \in$ R o sistema de congruências

$$\begin{cases} x \equiv r_1\ mod(\mathfrak{a}_1) \\ x \equiv r_2\ mod(\mathfrak{a}_2) \\ \quad\quad \vdots \\ x \equiv r_n\ mod(\mathfrak{a}_n) \end{cases}$$

possui uma única solução $r \in$ R congruente módulo $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n$.

(iii) O homomorfismo

$$\varphi : \mathrm{R} \longrightarrow \frac{\mathrm{R}}{\mathfrak{a}_1} \times \frac{\mathrm{R}}{\mathfrak{a}_2} \times \cdots \times \frac{\mathrm{R}}{\mathfrak{a}_n}$$

dado por

$$\varphi(r) = (r + \mathfrak{a}_1, r + \mathfrak{a}_2, \cdots, r + \mathfrak{a}_n)$$

é sobrejetivo e induz o isomorfismo

$$\frac{\mathrm{R}}{\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n} = \frac{\mathrm{R}}{\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n} \cong \frac{\mathrm{R}}{\mathfrak{a}_1} \times \frac{\mathrm{R}}{\mathfrak{a}_2} \times \cdots \times \frac{\mathrm{R}}{\mathfrak{a}_n}$$

$(i) \Longrightarrow (ii)$ A verificação da igualdade segue por indução em n.

De fato, a igualdade é verdadeira para $n = 2$ segundo o **Proposição 12**.

Suponha por hipótese de indução que

$$\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{n-1} = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1}$$

com $n > 2$, onde $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_{n-1}, \mathfrak{a}_n$ são dois a dois comaximais.

Agora resta verificar que $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{n-1}$ e $\mathfrak{a}_n$ são comaximais e a igualdade continua válida para n ideais. De fato, para todo $1 \leq i \leq n-1$ existem $r_i \in \mathfrak{a}_i$ e $s_i \in \mathfrak{a}_n$ tal que $r_i + s_i = 1$. Logo:

$$r_1r_2\cdots r_{n-1} = (1-s_1)(1-s_2)\cdots(1-s_{n-1}) = 1 - s$$

com $s \in \mathfrak{a}_n$ e onde s é uma soma de produtos dos $s_i's$, resultando

$$1 = r_1r_2\cdots r_{n-1} + s \in \mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{n-1} + \mathfrak{a}_n$$

logo $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{n-1} + \mathfrak{a}_n = \mathrm{R}$ e $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n = (\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{n-1})\mathfrak{a}_n = (\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n$.

Além disso $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{i-1}\mathfrak{a}_{i+1}\cdots\mathfrak{a}_n$ e $\mathfrak{a}_i$ para todo $1 \leq i \leq n$ são também comaximais seguindo o raciocínio semelhante ao anterior.

Existência:

Para verificar a existência da solução do sistema de congruências

$$\begin{cases} x \equiv r_1 \ mod(\mathfrak{a}_1) \\ x \equiv r_2 \ mod(\mathfrak{a}_2) \\ \quad\vdots \\ x \equiv r_n \ mod(\mathfrak{a}_n) \end{cases}$$

com $r_1, r_2, \cdots, r_n \in \mathrm{R}$ quaisquer, considere para todo $1 \leq j \neq i \leq n$

$$t_i = r_1 r_2 \cdots r_{i-1} r_{i+1} \cdots r_n \in \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_{i-1} \mathfrak{a}_{i+1} \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_j$$

com $1 - t_i \in \mathfrak{a}_i$. Por outro lado $\mathfrak{a}_j$ e $\mathfrak{a}_i$ são comaximais para $j \neq i$, logo

$$\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_{i-1} \mathfrak{a}_{i+1} \cdots \mathfrak{a}_n = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{i-1} \cap \mathfrak{a}_{i+1} \cap \cdots \cap \mathfrak{a}_n \subseteq \mathfrak{a}_j$$

Assim o elemento $r = r_1 t_1 + r_2 t_2 + \cdots + r_n t_n \in \mathrm{R}$ é a solução procurada, pois:

$$r - r_i = r_1 t_1 + \cdots + r_{i-1} t_{i-1} + r_i (t_i - 1) + r_{i+1} t_{i+1} + \cdots + r_n t_n \in \mathfrak{a}_i \Leftrightarrow$$
$$r - r_i = (r_1 t_1 + \cdots + r_{i-1} t_{i-1} + r_{i+1} t_{i+1} + \cdots + r_n t_n) + r_i (t_i - 1) \in \mathfrak{a}_i$$

Portanto $r \equiv r_i \; mod(\mathfrak{a}_i)$ pois para todo $i = 1, 2, \cdots, n$ tem-se $r_i (t_i - 1) \in \mathfrak{a}_i$ e $r_1 t_1 + \cdots + r_{i-1} t_{i-1} + r_{i+1} t_{i+1} + \cdots + r_n t_n \in \mathfrak{a}_i$.

Unicidade:

Sendo s uma outra solução do sistema de congruências, resulta que $r \equiv s \; mod(\mathfrak{a}_i)$ para todo $i = 1, 2, \cdots, n$ donde $r \equiv s \; mod(\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n)$ e consequentemente $r \equiv s \; mod(\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n)$.

$(ii) \Longrightarrow (i)$ Se para $r_1, r_2, \cdots, r_n \in \mathrm{R}$ existe $r \in \mathrm{R}$ tal que $r \equiv r_i \; mod(\mathfrak{a}_i)$, então segundo a **Proposição 13** $r_i \equiv r_j \; mod(\mathfrak{a}_i + \mathfrak{a}_j)$ para $i \neq j$ e com isso para $r_i = 1$ e $r_j = 0$ resulta que $\mathfrak{a}_i + \mathfrak{a}_j = \mathrm{R}$ significando que $\mathfrak{a}_i, \mathfrak{a}_j$ são comaximais.

$(ii) \Longrightarrow (iii)$ Dado um

$$(r_1 + \mathfrak{a}_1, r_2 + \mathfrak{a}_2, \cdots, r_n + \mathfrak{a}_n) \in \frac{\mathrm{R}}{\mathfrak{a}_1} \times \frac{\mathrm{R}}{\mathfrak{a}_2} \times \cdots \times \frac{\mathrm{R}}{\mathfrak{a}_n}$$

segue que existe $r \in \mathrm{R}$ tal que $\varphi(r) = (r_1 + \mathfrak{a}_1, r_2 + \mathfrak{a}_2, \cdots, r_n + \mathfrak{a}_n)$ e ainda vale a igualdade $\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n$. Por outro lado

$$ker(\varphi) = \{x \in \mathrm{R} : \varphi(x) = (0, 0, \cdots, 0)\} =$$
$$\{x \in \mathrm{R} : x \equiv 0\ mod(\mathfrak{a}_i), 1 \leq i \leq n\} =$$
$$\{x \in \mathrm{R} : x \in \mathfrak{a}_i, 1 \leq i \leq n\} = \left\{x \in \mathrm{R} : x \in \bigcap_{i=1}^{n} \mathfrak{a}_i\right\} =$$
$$\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n$$

Portanto pelo **Teorema dos Isomorfismos de Anéis** resulta

$$\frac{\mathrm{R}}{\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n} = \frac{\mathrm{R}}{\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n} \cong \frac{\mathrm{R}}{\mathfrak{a}_1} \times \frac{\mathrm{R}}{\mathfrak{a}_2} \times \cdots \times \frac{\mathrm{R}}{\mathfrak{a}_n}$$

$(iii) \Longrightarrow (ii)$ Se φ e induz o isomorfismo

$$\frac{\mathrm{R}}{\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n} = \frac{\mathrm{R}}{\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n} \cong \frac{\mathrm{R}}{\mathfrak{a}_1} \times \frac{\mathrm{R}}{\mathfrak{a}_2} \times \cdots \times \frac{\mathrm{R}}{\mathfrak{a}_n}$$

então

$$\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n = ker(\varphi) = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n$$

Por outro lado, para quaisquer $r_1, r_2, \cdots, r_n \in \mathrm{R}$ existe $r \in \mathrm{R}$ tal que

$$\begin{cases} r \equiv r_1\ mod(\mathfrak{a}_1) \\ r \equiv r_2\ mod(\mathfrak{a}_2) \\ \vdots \\ r \equiv r_n\ mod(\mathfrak{a}_n) \end{cases}$$

pois φ é sobrejetiva.

■

Proposição 15: Sejam $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ ideais de R com $n \geq 2$ e que para quaisquer $r_1, r_2, \cdots, r_n \in \mathrm{R}$ tem-se $r_i \equiv r_j\ mod(\mathfrak{a}_i + \mathfrak{a}_j)$ "$1 \leq i, j \leq n$" $i \neq j$. A condição necessária e suficiente para que exista um $r \in \mathrm{R}$ tal que

$$\begin{cases} r \equiv r_1 \; mod(\mathfrak{a}_1) \\ r \equiv r_2 \; mod(\mathfrak{a}_2) \\ \quad \vdots \\ r \equiv r_n \; mod(\mathfrak{a}_n) \end{cases}$$

é que $(\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1}) + \mathfrak{a}_n = (\mathfrak{a}_1 + \mathfrak{a}_n) \cap (\mathfrak{a}_2 + \mathfrak{a}_n) \cap \cdots \cap (\mathfrak{a}_{n-1} + \mathfrak{a}_n)$.

Demonstração:

Suponhamos que para quaisquer, $r_1, r_2, \cdots, r_n \in$ R com $r_i \equiv r_j \; mod(\mathfrak{a}_i + \mathfrak{a}_j)$ "$1 \leq i \neq j \leq n$" exista um $r \in$ R tal que

$$\begin{cases} r \equiv r_1 \; mod(\mathfrak{a}_1) \\ r \equiv r_2 \; mod(\mathfrak{a}_2) \\ \quad \vdots \\ r \equiv r_n \; mod(\mathfrak{a}_n) \end{cases}$$

Então de imediato vale a inclusão

$$(\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1}) + \mathfrak{a}_n \subseteq (\mathfrak{a}_1 + \mathfrak{a}_n) \cap (\mathfrak{a}_2 + \mathfrak{a}_n) \cap \cdots \cap (\mathfrak{a}_{n-1} + \mathfrak{a}_n)$$

Seja $s \in (\mathfrak{a}_1 + \mathfrak{a}_n) \cap (\mathfrak{a}_2 + \mathfrak{a}_n) \cap \cdots \cap (\mathfrak{a}_{n-1} + \mathfrak{a}_n)$. Em particular quando $r_1 = r_2 = \cdots = r_{n-1} = s$ e $r_n = 0$ temos que $r_i \equiv r_j \; mod(\mathfrak{a}_i + \mathfrak{a}_j)$ "$1 \leq i \neq j \leq n$" e existe $r \in$ R tal que satisfaz o sistema de congruências, donde $r - s = r - r_t \in \mathfrak{a}_t$ para todo $1 \leq t \leq n-1$ e $r - r_n \in \mathfrak{a}_n$. Logo:

$$r - s \in \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1} \text{ e } r - r_n \in \mathfrak{a}_n$$

portanto

$$s = -(r - s) + r \in (\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1}) + \mathfrak{a}_n$$

valendo a outra inclusão.

Reciprocamente admita que para $n \geq 2$

$$(\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1}) + \mathfrak{a}_n = (\mathfrak{a}_1 + \mathfrak{a}_n) \cap (\mathfrak{a}_2 + \mathfrak{a}_n) \cap \cdots \cap (\mathfrak{a}_{n-1} + \mathfrak{a}_n)$$

A verificação da existência de $r \in \mathrm{R}$ é feita por indução.

Para $n = 2$, o resultado é válido pela **Proposição 13**.

Suponhamos por hipótese de indução que o resultado vale para $n - 1$ e $n \geq 2$.

Sejam $r_1, r_2, \cdots, r_n \in \mathrm{R}$ tal que $r_i \equiv r_j \, mod(\mathfrak{a}_i + \mathfrak{a}_j)$ "$1 \leq i \neq j \leq n$" e que exista $\tilde{r} \in \mathrm{R}$ com $\tilde{r} \equiv r_i \, mod(\mathfrak{a}_i)$ para $i = 1, 2, \cdots, n - 1$.

Então:

$$\tilde{r} - r_n = (\tilde{r} - r_j) + (r_j - r_n) \in \mathfrak{a}_i + \mathfrak{a}_j$$

para todo $1 \leq j \leq n - 1$. Portanto

$$\tilde{r} - r_n \in (\mathfrak{a}_1 + \mathfrak{a}_n) \cap (\mathfrak{a}_2 + \mathfrak{a}_n) \cap \cdots \cap (\mathfrak{a}_{n-1} + \mathfrak{a}_n) = (\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1}) + \mathfrak{a}_n$$

e da hipótese, existe um $r \in \mathrm{R}$ tal que

$$r \equiv \tilde{r} \equiv r_i \, mod(\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1})$$
$$r \equiv r_n \, mod(\mathfrak{a}_n)$$

donde $r \equiv r_i \, mod(\mathfrak{a}_i)$ para $1 \leq i \leq n$.

■

Proposição 16 "Teorema Chinês de Restos": Sejam $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ ideais de R com $n \geq 2$ e que para quaisquer $r_1, r_2, \cdots, r_n \in \mathrm{R}$. O sistema de congruências

$$\begin{cases} x \equiv r_1 \, mod(\mathfrak{a}_1) \\ x \equiv r_2 \, mod(\mathfrak{a}_2) \\ \vdots \\ x \equiv r_n \, mod(\mathfrak{a}_n) \end{cases}$$

possui solução $x = r \in \mathrm{R}$ quando $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ são dois a dois comaximais ou quando $r_i \equiv r_j \, mod(\mathfrak{a}_i + \mathfrak{a}_j)$ "$1 \leq i \neq j \leq n$" e $(\mathfrak{a}_1 + \mathfrak{a}_n) \cap (\mathfrak{a}_2 + \mathfrak{a}_n) \cap \cdots \cap (\mathfrak{a}_{n-1} + \mathfrak{a}_n) = (\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_{n-1}) + \mathfrak{a}_n$.

Esse nome é explicado pelo teorema tratar-se de uma generalização do sistema de congruências lineares resolvido pelos chineses para o caso $\mathrm{R} = \mathbb{Z}$. Em caso afirmativo diz-se que R satisfaz o Teorema Chinês de Restos para n ideais quaisquer.

Proposição 17: Seja $(\Omega, \preccurlyeq)$ um conjunto parcialmente ordenado. As afirmações são equivalentes.

(a) Ω satisfaz a condição maximal.

(b) Ω satisfaz a condição de cadeia ascendente.

Demonstração:

$(a) \Longrightarrow (b)$ Considere o elemento maximal x_q da sequência $(x_n)_{n\geq 1}$ em X. Como a sequência $(x_n)_{n\geq 1}$ é ascendente, então para $n \geq q$ implica $x_n \geq x_q$. Assim sendo x_q maximal, resulta que $x_n = x_q$ para todo $n \geq q$. Portanto a sequência $(x_n)_{n\geq 1}$ é estacionária.

$(b) \Longrightarrow (a)$ Suponha por absurdo que exista um subconjunto S de X que não contém um elemento maximal. Então para todo $x \in$ S, o conjunto dos elementos de S que são maiores do que x é não vazio.

De acordo com o Axioma da Escolha, existe uma aplicação $f : \mathrm{S} \longrightarrow \mathrm{S}$ tal que $f(x) > x$ para todo $x \in$ S. Sendo S não vazio, podemos tomar $x_0 \in$ S e definir por indução a sequência $(x_n)_{n\geq 0}$ da forma $f(x_n) = x_{n+1}$. Assim a sequência $(x_n)_{n\geq 0}$ é estritamente ascendente e não é estacionária, sendo uma contradição.

■

Proposição 18: Sejam $(\mathrm{M}, \subseteq)$ um $\mathrm{R} - m\acute{o}dulo$ parcialmente ordenado pela inclusão e $\mathcal{M}$ a coleção dos submódulos de M. As afirmações seguintes são equivalentes.

(i) M é um $\mathrm{R} - m\acute{o}dulo$ Neotheriano

(ii) $\mathcal{M}$ satisfaz a condição de cadeia ascendente

(iii) $\mathcal{M}$ satisfaz a condição maximal

Demonstração:

$(i) \Longrightarrow (ii)$ Seja $\mathrm{M}_1 \subseteq \mathrm{M}_2 \subseteq \cdots \subseteq \mathrm{M}_n \subseteq \cdots$ uma cadeia ascendente em $\mathcal{M}$ e seja $\mathrm{F} = \bigcup_{k\in\mathbb{N}} \mathrm{M}_k$. Então $\mathrm{F} \in \mathcal{M}$ e por hipótese é finitamente gerado ou seja $\mathrm{F} = \mathrm{R}x_1 + \cdots + \mathrm{R}x_n$.

Com isso existe $k \in \mathbb{N}$ tal que $x_i \in \mathrm{M}_k$ para todo $i \in [1, n] \cap \mathbb{N}$ pois $x_i \in \mathrm{F}$.

Portanto $\mathrm{F} \subseteq \mathrm{M}_k \subseteq \mathrm{M}_{k+1} \subseteq \cdots$ e vale a igualdade.

$(ii) \Longrightarrow (iii)$ Segue pela **Proposição 17**.

$(iii) \Longrightarrow (i)$ Dado um submódulo $\mathrm{F} \in \mathcal{M}$, considere $\mathcal{M}_\mathrm{F}$ o conjunto dos submódulos finitamente gerados de M que estão contidos em F.

Como $\mathcal{M}_\mathrm{F}$ é não vazio, pois $\langle 0 \rangle \in \mathcal{M}_\mathrm{F}$ segue que $\mathcal{M}_\mathrm{F}$ possui um elemento maximal S "pois $\mathcal{M}_\mathrm{F} \subseteq \mathcal{M}$".

Vamos verificar que $\mathrm{F} \subseteq \mathrm{S}$. De fato, para todo $y \in \mathrm{F}$, temos que $\mathrm{S} \subseteq \mathrm{S} + \mathrm{R}y \in \mathcal{M}_\mathrm{F}$ e pela maximalidade de S vale a igualdade. Portanto $y \in \mathrm{S} + \mathrm{R}y = \mathrm{S}$, logo $\mathrm{S} = \mathrm{F}$ é finitamente gerado, donde M é um $\mathrm{R} - \textit{módulo}$ Neotheriano.

■

Corolário 01: Todo ideal próprio $\mathfrak{i}$ de um anel Noetheriano A está contido num ideal maximal.

Demonstração:

Considere Γ o conjunto de todos os ideais próprios de A que contém $\mathfrak{i}$. De fato $\mathfrak{i} \in \Gamma$ e logo Γ é não vazio. Por outro lado, A é Noetheriano e portanto, Γ admite um ideal maximal $\mathfrak{m}$. Assim $\mathfrak{i} \subseteq \mathfrak{m} \subsetneq \mathrm{A}$ e pela maximalidade $\mathfrak{m}$ é ideal maximal.

■

Exemplo 12: Um anel de ideais principais é Noetheriano.

De fato, dado o $\mathrm{A} - \textit{módulo}$ considere a sequência de $\mathrm{A} - \textit{submódulos}$ $\mathrm{I}_1 \subseteq \mathrm{I}_2 \subseteq \cdots \subseteq \mathrm{I}_n \subseteq \cdots$

Por hipótese A é anel de ideais principais, logo seus submódulos são ideais principais. Assim a união

$$\mathrm{I} = \bigcup_{i \in \mathbb{N}} \mathrm{I}_i$$

é um ideal de A e $\mathrm{I}_n \subseteq \mathrm{I}$ para todo $i \in \mathbb{N}$.

Mas $\mathrm{I} = \langle x \rangle$ e com isso $x \in \mathrm{I}_{n_0}$ para algum $n_0 \in \mathbb{N}$, donde $\mathrm{I} = \langle x \rangle \subseteq \mathrm{I}_{n_0}$. Portanto $\mathrm{I} = \mathrm{I}_{n_0}$ e assim para todo $n \geq n_0$ implica $\mathrm{I} = \mathrm{I}_{n_0} \subseteq \mathrm{I}_n$ e a sequência é estacionária.

Exemplo 13: O anel $\mathrm{I}_{\mathrm{K}}(\mathbb{Z})$ "inteiros algébricos de um corpo de números algébricos ou corpo numérico K" é Noetheriano "$\mathrm{K} = \mathbb{Q}$ tome e $\mathrm{A} = \mathbb{Z}$".

Proposição 19: Sejam A um anel, M um $\mathrm{A} -$ *módulo* e N um $\mathrm{A} -$ *submódulo* de M. A condição necessária e suficiente para que M seja Noetheriano é que N e M/N sejam Noetherianos.

Demonstração:

Suponha que M seja Noetheriano e N um $\mathrm{A} -$ *submódulo* de M, então toda sequência $(\mathrm{N}_n)_{n \in \mathbb{N}}$ ascendente de $\mathrm{A} -$ *submódulos* de N é uma sequência ascendente de $\mathrm{A} -$ *submódulos* de M, logo estacionária. Portanto N é Noetheriano.

Agora considere o homomorfismo canônico $\mathrm{A} -$ *linear* $\varphi : \mathrm{M} \longrightarrow \mathrm{M}/\mathrm{N}$ dado por $\varphi(n) = n + \mathrm{N}$ e observe que o mesmo define uma correspondência bijetiva que preserva inclusão entre submódulos de M que contém N e submódulos de M/N ou seja os conjuntos $\Gamma = \{\mathrm{N} \subset \mathrm{E} \lhd_{Sm} \mathrm{M}\}$ e $\Omega = \{\mathrm{F} \lhd_{Sm} \mathrm{M}/\mathrm{N}\}$ estão em bijeção.

Então toda sequência $(\mathrm{F}_n)_{n \in \mathbb{N}}$ ascendente de $\mathrm{A} -$ *submódulos* de M/N corresponde por meio de φ a uma sequência $\left(\varphi^{-1}(\mathrm{F}_n)\right)_{n \in \mathbb{N}}$ ascendente de $\mathrm{A} -$ *submódulos* de M, que é estacionária. Portanto toda sequência $(\mathrm{F}_n)_{n \in \mathbb{N}}$ ascendente de $\mathrm{A} -$ *submódulos* de M/N também é estacionária e consequentemente M/N é Noetheriano.

Reciprocamente considere que N e M/N sejam Noetherianos e seja $(\mathrm{M}_n)_{n \in \mathbb{N}}$ uma sequência ascendente de $\mathrm{A} -$ *submódulos* de M. Então $(\mathrm{N} \cap \mathrm{M}_n)_{n \in \mathbb{N}}$ é uma sequência ascendente de $\mathrm{A} -$ *submódulos* de N e $(\varphi(\mathrm{M}_n))_{n \in \mathbb{N}}$ é uma sequência ascendente de $\mathrm{A} -$ *submódulos* de M/N.

Por hipótese existem $n_1, n_2 \in \mathbb{N}$ tal que $\mathrm{N} \cap \mathrm{M}_n = \mathrm{N} \cap \mathrm{M}_{n+1}$ para todo $n \geq n_1$ e $\varphi(\mathrm{M}_n) = \varphi(\mathrm{M}_{n+1})$ para todo $n \geq n_2$. Escolha $n_0 = máx.\{n_1, n_2\}$ e provemos que $\mathrm{M}_n = \mathrm{M}_{n+1}$ para todo $n \geq n_0$. É suficiente verificar que $\mathrm{M}_{n+1} \subset \mathrm{M}_n$ para todo $n \geq n_0$.

Assim seja $x \in \mathrm{M}_{n+1}$ qualquer, com $n \geq n_0$, logo existe um $y \in \mathrm{M}_n$ tal que $x + \mathrm{N} = y + \mathrm{N}$ daí $x - y \in \mathrm{N}$ e $x - y \in \mathrm{M}_{n+1}$ donde $x - y \in \mathrm{N} \cap \mathrm{M}_{n+1} = \mathrm{N} \cap \mathrm{M}_n$, portanto $x - y \in \mathrm{M}_n$ implicando que $x \in \mathrm{M}_n$. Com isso $(\mathrm{M}_n)_{n\in\mathbb{N}}$ é uma sequência ascendente de $\mathrm{A} - submódulos$ de M em que $\mathrm{M}_n = \mathrm{M}_{n+1}$ para todo $n \geq n_0$, logo $(\mathrm{M}_n)_{n\in\mathbb{N}}$ é estacionária e consequentemente M é Noetheriano.

■

Corolário 02: Sejam A um anel e $\mathrm{M}_1, \mathrm{M}_2, \cdots, \mathrm{M}_n$ $\mathrm{A} - módulos$ Noetherianos. Então o produto cartesiano $\mathrm{M}_1 \times \mathrm{M}_2 \times \cdots \times \mathrm{M}_n$ é um $\mathrm{A} - módulo$ Noetheriano.

Demonstração:

A verificação é feita através de indução matemática sobre o número n. A afirmação é imediata para $n = 1$.

Para $n = 2$ o resultado é válido, pois para $\mathrm{E}_1, \mathrm{E}_2$ $\mathrm{A} - módulos$ Noetherianos tem-se que $\mathrm{M}_1 \times \{0\} \cong \mathrm{M}_1$ e $\mathrm{M}_1 \times \{0\} \subseteq \mathrm{M}_1 \times \mathrm{M}_2$. Por outro lado $f : \mathrm{M}_1 \times \mathrm{M}_2 \longrightarrow \mathrm{M}_2$ definida por $f(0, y) = y$ é um homomorfismo sobrejetivo com $ker(f) = \mathrm{M}_1 \times \{0\}$ e pela **Proposição 09** segue que

$$\frac{\mathrm{M}_1 \times \mathrm{M}_2}{\mathrm{M}_1 \times \{0\}} \cong \mathrm{M}_2$$

donde $\mathrm{M}_1 \times \mathrm{M}_2$ é $\mathrm{A} - módulo$ Noetheriano pela **Proposição 19**.

Suponhamos por hipótese de indução que a afirmação é verdadeira para $n - 1$ $\mathrm{A} - módulos$ Noetherianos, com $n \geq 2$.

Sejam n $\mathrm{A} - módulos$ Noetherianos $\mathrm{M}_1, \mathrm{M}_2, \cdots, \mathrm{M}_{n-1}, \mathrm{M}_n$. O submódulo $\mathrm{N} = \langle 0 \rangle \times \cdots \times \langle 0 \rangle \times \mathrm{E}_n$ de $\mathrm{M}_1 \times \mathrm{M}_2 \times \cdots \times \mathrm{M}_{n-1} \times \mathrm{M}_n$ e o módulo quociente

$$\frac{\mathrm{M}_1 \times \mathrm{M}_2 \times \cdots \times \mathrm{M}_n}{\mathrm{N}}$$

são Noetheriano porque são isomorfos a M_n e a $M_1 \times M_2 \times \cdots \times M_{n-1}$ respectivamente por hipótese. Portanto pela **Proposição 19** $M_1 \times M_2 \times \cdots \times M_n$ é um $A-$*módulo* Noetheriano.

■

Corolário 03: Sejam A um anel Noetheriano e M um $A-$*módulo* finitamente gerado ou do tipo finito, então M é $A-$*módulo* Noetheriano "portanto todo $A-$*submódulo* de M é finitamente gerado".

Demonstração:

Seja $M = Ax_1 + Ax_2 + \cdots + Ax_{n-1} + Ax_n$ um $A-$*módulo* finitamente gerado e considere o homomorfismo $\psi : A^n \longrightarrow E$ sobrejetivo dado por:

$$\psi(a_1, a_2, \cdots, a_{n-1}, a_n) =$$
$$a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} + a_nx_n =$$
$$\sum_{i=1}^{n} a_ix_i$$

onde $A \times A \times \cdots \times A \times A = A^n$. Com isso pela **Proposição 09**

$$\frac{A^n}{ker(\psi)} \cong im(\psi) = E$$

Portanto M é Noetheriano, porque A^n é Noetheriano pelo **Corolário 02** e $A^n/_{ker(\psi)}$ é Noetheriano pela **Proposição 19** e pelo fato do $ker(\psi)$ ser um submódulo de A^n.

■

Um ideal $\mathfrak{p}$ de um anel A é dito ser primo quando o anel quociente $A/_{\mathfrak{p}}$ é um domínio de integridade. Isso é equivalentemente a dizer que $A - \mathfrak{p}$ é fechado para o produto, ou seja:

$$x \in A - \mathfrak{p} \text{ e } y \in A - \mathfrak{p} \Longrightarrow xy \in A - \mathfrak{p}$$

Um ideal $\mathfrak{m}$ de A é dito ser maximal, quando o anel quociente $^{A}/_{\mathfrak{m}}$ é um corpo. Daí cada ideal maximal de um anel A, é um ideal primo, porém a inversa é falsa, como por exemplo $\langle 0 \rangle$ é um ideal primo em $\mathbb{Z}$, mas não é ideal maximal.

Proposição 20: Sejam A um anel, com $\mathfrak{p}$ e S seu ideal primo e subanel de A respectivamente. Então $\mathfrak{p} \cap S$ é um ideal primo de S.

Demonstração:

Seja $i : S \hookrightarrow A$ a aplicação inclusão e o homomorfismo canônico $\varphi : A \longrightarrow {}^{A}/_{\mathfrak{p}}$ dado por $\varphi(a) = a + \mathfrak{p}$. Com isso a composição $\varphi \circ i : S \longrightarrow {}^{A}/_{\mathfrak{p}}$ ainda é um homomorfismo e sobrejetivo, cujo $ker(\varphi \circ i) = \{x \in S : (\varphi \circ i)(x) = 0\} = \{x \in S : x \in \mathfrak{p}\} = \mathfrak{p} \cap S$.

Então pelo Teorema dos Isomorfismos para Anéis, tem-se que ${}^{S}/_{ker(\varphi \circ i)} = {}^{S}/_{\mathfrak{p} \cap S} \cong im(\varphi \circ i) = {}^{A}/_{\mathfrak{p}}$. Logo ${}^{S}/_{\mathfrak{p} \cap S}$ é um subanel de ${}^{A}/_{\mathfrak{p}}$ que é um domínio de integridade, pois $\mathfrak{p}$ é ideal primo.

Portanto ${}^{S}/_{\mathfrak{p} \cap S}$ também é um domínio de integridade, consequentemente $\mathfrak{p} \cap S$ é um ideal primo.

■

Para dois ideais $\mathfrak{a}$ e $\mathfrak{b}$ do anel A, definimos o produto $\mathfrak{ab}$ dos ideais, não como o conjunto dos produtos ab tal que $a \in \mathfrak{a}$ e $b \in \mathfrak{b}$, mas como o conjunto de todas as somas finitas dos produtos de elementos dos ideais $\mathfrak{a}$ e $\mathfrak{b}$. Ou seja:

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathfrak{a} \text{ e } b_i \in \mathfrak{b} \right\}$$

É de imediato que $\mathfrak{ab}$ é um ideal de A e $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. A igualdade não é necessariamente verdadeira.

A multiplicação de ideais é associativa e comutativa. O anel A age como o elemento identidade, no monóide de ideais.

Dado um $A-$ *módulo* M, um $A-$ *submódulo* N é um ideal de A. Define-se $\mathfrak{a}N$ do mesmo modo como o produto de ideais. $\mathfrak{a}N$ é um $A-$ *submódulo* de M.

Proposição 21: Sejam $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_r$ ideais do anel R e $\mathfrak{p}$ um ideal primo de R. Se $\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_r \subset \mathfrak{p}$ "respectivamente $\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_r = \mathfrak{p}$" então $\mathfrak{a}_i \subset \mathfrak{p}$ "respectivamente $\mathfrak{a}_i = \mathfrak{p}$" para algum $i = 1, 2, \cdots, r$.

Demonstração:

Suponhamos por absurdo que para todo $i = 1, 2, \cdots, r$ tenhamos $\mathfrak{a}_i \nsubseteq \mathfrak{p}$, então existem $a_i \in \mathfrak{a}_i - \mathfrak{p}$ para todo $i = 1, 2, \cdots, r$. Mas como $\mathfrak{p}$ é um ideal primo implica $a_1a_2 \cdots a_n \in \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n \subset \mathfrak{p}$ e $a_1a_2 \cdots a_r \notin \mathfrak{p}$ o que é uma contradição.

Por outro lado se $\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_r = \mathfrak{p}$, então $\mathfrak{p} \subset \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_r \subseteq \mathfrak{a}_j$ para todo $j = 1, 2, \cdots, r$ e $\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_r \subset \mathfrak{p}$ donde $\mathfrak{a}_i \subset \mathfrak{p}$ para algum $j = 1, 2, \cdots, r$, valendo a igualdade.

■

Proposição 22: Em um anel Noetheriano R. Para todo ideal $\mathfrak{a}$ de R existem n ideais primos $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ de R tal que $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n \subset \mathfrak{a} \subset \mathfrak{p}_1 \cap \mathfrak{p}_2 \cdots \cap \mathfrak{p}_n$. Em um domínio de integridade Noetheriano D, todo ideal próprio não nulo $\mathfrak{a}$ de D, contém um produto finito de ideais primos não nulos.

Demonstração:

Suponhamos por absurdo que o conjunto Γ da família dos ideais não nulos de R que não contém um produto de ideais primos não nulos seja diferente do conjunto vazio. Como R é Neotheriano, Γ possui um elemento maximal $\mathfrak{a}$.

Esse ideal $\mathfrak{a}$ não pode ser primo, pois do contrário $\mathfrak{a}$ não pertenceria a Γ. Nesse caso $\mathfrak{a}$ não sendo primo, existem $x, y \in R - \mathfrak{a}$ cujo $xy \in \mathfrak{a}$. De fato $\mathfrak{a} + x\mathrm{A}$ e $\mathfrak{a} + y\mathrm{A}$ contém propriamente o ideal $\mathfrak{a}$, pois $x \in \mathfrak{a} + x\mathrm{A}$ e $y \in \mathfrak{a} + y\mathrm{A}$, mas $x, y \notin \mathfrak{a}$.

Pela maximalidade do elemento $\mathfrak{a}$ na família, segue que os ideais $\mathfrak{a} + x\mathrm{A}$ e $\mathfrak{a} + y\mathrm{A}$ não pertencem a família Γ, logo os mesmos contém um produto de ideais primos não nulos, ou seja existem ideais primos $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n, \mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_n$ de R tais que:

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a} + x\mathrm{A} \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cdots \cap \mathfrak{p}_n$$

$$\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_n \subseteq \mathfrak{a} + y\mathrm{A} \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$$

Mas como $xy \in \mathfrak{a}$ obtemos que

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_n \subseteq (\mathfrak{a} + x\mathrm{A})(\mathfrak{a} + y\mathrm{A}) \subseteq \mathfrak{a} \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cdots \cap \mathfrak{p}_n \cap \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$$

isso quer dizer que $\mathfrak{a} \notin \Gamma$, o que uma contradição ou absurdo. Portanto Γ é o conjunto vazio.

Em particular quando R é um domínio de integridade e $\mathfrak{a} \neq \langle 0 \rangle$, temos que $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a} \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cdots \cap \mathfrak{p}_n$, resultando que $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ são não nulos, pois do contrário se pelo menos um dos $\mathfrak{p}_i's = \langle 0 \rangle$ então $\mathfrak{a} = \langle 0 \rangle$ o que geraria uma contradição.

■

Seja A um domínio de integridade e $\mathrm{K}_f(\mathrm{A})$ seu corpo de frações. Chama-se um ideal fracionário de A "ou ideal fracionário de $\mathrm{K}_f(\mathrm{A})$ com respeito a A", qualquer $\mathrm{A} - submódulo$ I de $\mathrm{K}_f(\mathrm{A})$ em que exista um $d \in \mathrm{A} - \langle 0 \rangle$ tal que $d\mathrm{I} \subset \mathrm{A}$.

Neste caso $d\mathrm{M} = \mathfrak{a}$ é ideal de A e $\mathrm{M} = d^{-1}\mathfrak{a}$.

Qualquer $\mathrm{R} - módulo$ $\mathfrak{a}$ do tipo finito em $\mathrm{K}_f(\mathrm{R})$ é um ideal fracionário. Isto segue do fato que se $\{e_1, e_2, \cdots, e_{n-1}, e_n\}$ é um conjunto de geradores de $\mathfrak{a}$, os $e_i's$ tem um denominador comum d "produto dos $d_i's$ onde $e_i = a_i d_i^{-1}$ com $a_i, d_i \in \mathrm{R}$" e d é um denominador comum para $\mathfrak{a}$.

Reciprocamente se R é Neotheriano, todo ideal fracionário $\mathfrak{a}$ é um $\mathrm{R} - módulo$ finitamente gerado porque $\mathfrak{a} \subset d^{-1}\mathrm{R}$ e $d^{-1}\mathrm{R}$ é um $\mathrm{R} - módulo$ isomorfo a R.

Definimos o produto de dois ideais fracionários, como sendo o conjunto

$$f_1 f_2 = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in f_1 \text{ e } y_i \in f_2 \right\}$$

Se f_1, f_2 são ideais fracionários com os denominadores comuns d_1, d_2 respectivamente, então os conjuntos $f_1 + f_2$, $f_1 \cap f_2$ e $f_1 f_2$ são ideais fracionários. São também $\mathrm{R} - módulo$ de $\mathrm{K}_f(\mathrm{R})$ e tem como denominadores comuns d_1 ou d_2, $d_1 + d_2$ e $d_1 d_2$, respectivamente.

Denotamos por $\mathcal{M}(\mathrm{A})$ o conjunto de todos os $\mathrm{A}-$ *módulo* de $\mathrm{K}_f(\mathrm{A})$ não nulos munido da multiplicação, respectivamente $\mathcal{F}(\mathrm{A})$ o conjunto dos ideais fracionários de A.

Diremos que $\mathrm{M} \in \mathcal{M}(\mathrm{A})$ possui inverso se existir $\mathrm{N} \in \mathcal{M}(\mathrm{A})$ tal que $\mathrm{MN} = \mathrm{A}$. Nesse caso pode ser verificado que o inverso N de M é unicamente determinado e será denotado por M^{-1}.

Um monóide $(\mathrm{G},*)$ com a operação

$$\begin{aligned} * : \mathrm{G} \times \mathrm{G} &\longrightarrow \mathrm{G} \\ (a, b) &\longmapsto a * b \end{aligned}$$

é uma estrutura algébrica que satisfaz as condições:

Associatividade: $x * (y * z) = (x * y) * z$ para cada $x, y, z \in \mathrm{G}$.

Elemento Neutro: existe um único elemento $e \in \mathrm{G}$ tal que $x * e = e * x = x$ para todo $x \in \mathrm{G}$

A multiplicação de ideais é associativa e comutativa. O ideal A atua como elemento neutro no monóide dos ideais de A.

O monóide G passa a ser denominado grupo quando satisfaz a propriedade:

Elemento Inverso: para todo $x \in \mathrm{G}$ existe um $y \in \mathrm{G}$ tal que $x * y = y * x = e$

$\mathcal{M}(\mathrm{A})$ é um monóide comutativo e $\mathcal{F}(\mathrm{A})$ é um submonóide de $\mathcal{M}(\mathrm{A})$, ambos tendo A como elemento neutro.

Proposição 23: Se A é um domínio Noetheriano, então todo ideal fracionário I de A é um $\mathrm{A}-$ *módulo* finitamente gerado ou do tipo finito.

Demonstração:

Considere o ideal fracionário I. Assim existe um $d \in \mathrm{A} - \{0\}$ tal que $d\mathrm{I} \subset \mathrm{A}$ e consequentemente $\mathrm{I} \subset d^{-1}\mathrm{A}$. Por outro lado $d^{-1}\mathrm{A}$ é um $\mathrm{A}-$ *módulo* e a aplicação $f : \mathrm{A} \longrightarrow d^{-1}\mathrm{A}$ dada por $f(x) = d^{-1}x$ é um isomorfismo.

Portanto d^{-1}A é Noetheriano, donde I é um A $-$ *módulo* finitamente gerado ou do tipo finito.

■

Corolário 04: Sejam A um domínio e $K_f(A)$ o seu corpo de frações. Todo A $-$ *submódulo* I de $K_f(A)$ do tipo finitamente gerado é um ideal fracionário.

Demonstração:

Se $\{x_1, x_2, \cdots, x_n\}$ é um conjunto finito de geradores de I, então $I = x_1A + x_2A + \cdots + x_nA$. Cada x_i possui um denominador comum $d = d_1 d_2 \cdots d_n$ onde $x_i = a_i {d_i}^{-1}$ com $a_i d_i \in A$. Portanto dI $\subset$ A e consequentemente I é um ideal fracionário.

■

Proposição 24: Dado o anel de ideais principais A, M um A $-$ *módulo* livre de posto n e N um A $-$ *submódulo* de M. Então:

(a) N é A $-$ *submódulo* livre de posto q, com $0 \leq q \leq n$.

(b) Se N $\neq \langle 0 \rangle$ existe uma base $\{e_1, e_2, \cdots, e_n\}$ de M e elementos não nulos $a_1, a_2, \cdots, a_q \in A$ tais que $\{a_1 e_1, a_2 e_2, \cdots, a_q e_q\}$ é uma base de N e $a_i | a_{i+1}$ para $i = 1, 2, \cdots, q-1$.

Demonstração:

Suponha então que N $\neq \langle 0 \rangle$ e seja $\mathcal{L}(M, A)$ o conjunto das formas lineares em M. Para $\varphi \in \mathcal{L}(M, A)$ tem-se que φ(N) é um submódulo de A e portanto, um ideal de A que é do tipo principal, $\varphi(N) = Aa_\varphi$ para algum a_φ em A.

De acordo com o **Exemplo 12** e a **Proposição 18** o anel A é Noetheriano existe $\psi \in \mathcal{L}(M, A)$ tal que Aa_ψ é maximal.

Considere a base $\{x_1, x_2, \cdots, x_n\}$ de M identificada com A^n e seja a projeção π_i : M $\longrightarrow$ A da $i-$*ésima* coordenada dada por $\pi_i(x_i) = \delta_{ij}$. E como N $\neq \langle 0 \rangle$ segue que $\pi_i(N) \neq \langle 0 \rangle$ para algum $1 \leq i \leq n$ e assim $a_\psi \neq 0$.

Pela construção existe $\theta \in \mathrm{N}$ tal que $\psi(\theta) = a_\psi$. Vamos verificar que a_ψ divide $\phi(\theta)$ seja qual for $\phi \in \mathcal{L}(\mathrm{M}, \mathrm{A})$. Tomando $d = mdc\left(a_\psi, \phi(\theta)\right)$ resulta que $d = \alpha a_\psi + \beta\phi(\theta) = \alpha\varphi(\theta) + \beta\phi(\theta) = (\alpha\varphi + \beta\phi)(\theta)$ para algum α, β em A.

Assim $\alpha\varphi + \beta\phi \in \mathcal{L}(\mathrm{M}, \mathrm{A})$ e $\mathrm{A}a_\psi \subseteq \mathrm{A}d$ e vale a igualdade pela maximalidade de $\mathrm{A}a_\psi$ e consequentemente a_ψ divide d que por transitividade divide $\phi(\theta)$. Em particular a_ψ divide $\pi_i(\theta)$ significando que $\pi_i(\theta) = a_\psi b_i$ para algum $b_i \in \mathrm{A}$.

Agora fazendo

$$\delta = \sum_{i=1}^{n} b_i x_i$$

tem-se que $\theta = a_\psi\delta$ e como $a_\psi = \psi(\theta) = a_\psi\,\psi(\delta)$ conclui-se que $\psi(\delta) = 1$.

Mostremos agora as somas diretas:

(i) $\mathrm{M} = ker(\psi) \oplus \mathrm{A}\delta$

Note que para $x \in \mathrm{M}$ temos $x = \psi(x)\delta + [x - \psi(x)\delta]$ e $\psi(x - \psi(x)\delta) = \psi(x) - \psi(x)\psi(\delta) = \psi(x) - \psi(x)1 = 0$ significando que $x - \psi(x)\delta \in ker(\psi)$ e $\psi(x)\delta \in \mathrm{A}\delta$. Além disso $\delta \neq 0$ e $x \in ker(\psi) \cap \mathrm{A}\delta$ se só se $\psi(x = a\delta) = 0$ donde $a = 0$.

(ii) $\mathrm{N} = [\mathrm{N} \cap ker(\psi)] \oplus \mathrm{A}\theta$ onde $\theta = a_\psi\delta$

Note que para $y \in \mathrm{N}$ temos $\psi(y) = ba_\psi$ para algum $b \in \mathrm{A}$. Logo $y = ba_\psi\delta + \left[y - ba_\psi\delta\right] = ba_\psi\delta + [y - \psi(y)\delta] = b\theta + [y - \psi(y)\delta]$ e veja que $\psi(y - \psi(y)\delta) = \psi(y) - \psi(y)\psi(\delta) = \psi(y) - \psi(y)1 = 0$ significando que $y - \psi(y)\delta \in ker(\psi)$ e $y - \psi(y)\delta = y - b\theta \in \mathrm{N}$. Portanto $y - \psi(y)\delta \in \mathrm{N} \cap ker(\psi)$ e $b\theta \in \mathrm{A}\theta$. Além disso $[\mathrm{N} \cap ker(\psi)] \cap \mathrm{A}\theta = \{0\}$.

(a) Por indução sobre o posto de N.

Para $q = 0$ de imediato $\mathrm{N} = \langle 0 \rangle$ e o resultado é direto.

Para $q > 0$ tem-se $\mathrm{N} \cap ker(\psi)$ de posto $q - 1$ por (ii) e é livre de acordo com a hipótese de indução.

Mas sendo N uma soma direta por (ii) uma base para N é formada com os $q - 1$ elementos de $\mathrm{N} \cap ker(\psi)$ somado com θ no que resulta em N livre de posto q.

(b) Por indução sobre o posto de M.

Para $n = 0$ o resultado é direto.

Supondo que $n > 0$ e de acordo com o (i) $ker(\psi)$ é livre de posto $n - 1$ pela soma direta. A hipótese de indução será aplicada para $ker(\psi)$ e o submódulo $\mathrm{N} \cap ker(\psi)$ de M.

Se $\mathrm{N} \cap ker(\psi) \neq \langle 0 \rangle$, existe uma base $\{e_2, \cdots, e_n\}$ de $ker(\psi)$ e elementos não nulos $a_2, \cdots, a_q \in \mathrm{A}$ tais que $\{a_2 e_2, \cdots, a_n e_n\}$ é base de $\mathrm{N} \cap ker(\psi)$ com $a_i | a_{i+1}$ para $i = 2, \cdots, q-1$ para $q \leq n$. Mantendo a notação anterior e fixando $a_1 = a_\psi$ e $e_1 = \delta$ o conjunto $\{e_1, e_2, \cdots, e_n\}$ é base de M de acordo com (i) e também o conjunto $\{e_1, e_2, \cdots, e_q\}$ é base de N de acordo com (ii) e do fato $a_1 e_1 = a_\psi \delta = \theta$.

Resta provar que $a_1 | a_2$. Assim seja a forma linear $\varphi \in \mathcal{L}(\mathrm{M}, \mathrm{A})$ definida por

$$\varphi(e_i) = \begin{cases} 1, \text{se } i = 1 = 2 \\ 0, \text{se } i \geq 3 \end{cases}$$

Assim por um lado $a_\psi = a_1 = \varphi(a_1 e_1) = \varphi(\theta) \in \varphi(\mathrm{N}) \Longrightarrow \mathrm{A}a_\psi = \mathrm{A}a_1 \subseteq \varphi(\mathrm{N})$ valendo a igualdade segundo a maximalidade de $\mathrm{A}a_\psi$.

Por outro lado $a_2 = \varphi(a_2 e_2) \in \varphi(\mathrm{N}) = \mathrm{A}a_1 \Longrightarrow a_1 | a_2$

■

Corolário 05: Se A é um anel de ideais principais e M um $\mathrm{A} - módulo$ finitamente gerado onde $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_n$ são ideais de A. Então:

$$\mathrm{M} \cong \frac{\mathrm{A}}{\mathfrak{a}_1} \times \frac{\mathrm{A}}{\mathfrak{a}_2} \times \cdots \times \frac{\mathrm{A}}{\mathfrak{a}_n}$$

Demonstração:

Sendo M um $\mathrm{A} - módulo$ finitamente gerado então existe um conjunto gerador $\{u_1, \cdots, u_n\}$ de M. Logo pela **Proposição 11** $\varphi : \mathrm{A}^{(n)} \longrightarrow \mathrm{M}$ é homomorfismo sobrejetivo e consequentemente segundo a **Proposição 09**

$$\frac{\mathrm{A}^{(n)}}{ker(\varphi)} \cong \mathrm{M}$$

Por outro lado, da **Proposição 24** existe uma base $\{e_1, e_2, \cdots, e_n\}$ de $\mathrm{A}^{(n)}$ e elementos não nulos $a_1, a_2, \cdots, a_q \in \mathrm{A}$ tais que $\{a_1e_1, a_2e_2, \cdots, a_qe_q\}$ é uma base de $ker(\varphi)$ e $a_i | a_{i+1}$ para $i = 1, 2, \cdots, q-1$. Fazendo $a_p = 0$ para $q+1 \leq p \leq n$ resulta que:

$$\frac{\mathrm{A}^{(n)}}{ker(\varphi)} \cong \prod_i \frac{\mathrm{A}e_i}{\mathrm{A}a_ie_i} \Longrightarrow \frac{\mathrm{A}^{(n)}}{ker(\varphi)} \cong \prod_i \frac{\mathrm{A}}{\mathrm{A}a_i}$$

uma vez que

$$\frac{\mathrm{A}e_i}{\mathrm{A}a_ie_i} \cong \frac{\mathrm{A}}{\mathrm{A}a_i}$$

Portanto tomando $\mathrm{A}a_i = \mathfrak{a}_i$ resulta

$$\mathrm{M} \cong \frac{\mathrm{A}^{(n)}}{ker(\varphi)} \cong \frac{\mathrm{A}}{\mathfrak{a}_1} \times \frac{\mathrm{A}}{\mathfrak{a}_2} \times \cdots \times \frac{\mathrm{A}}{\mathfrak{a}_n}$$

■

2.2.2 Domínios de Dedekind

Um domínio de Integridade R é chamado um **Domínio ou Anel de Dedekind**, se R for Noetheriano, integralmente fechado "no corpo de frações $\mathrm{K}_f(\mathrm{R})$ ou em alguma extensão finita L de $\mathrm{K}_f(\mathrm{R})$" e cada ideal primo não nulo de R é um ideal maximal.

O anel $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$ dos inteiros $\mathbb{Z}$ e mais geralmente qualquer anel de ideais principais é um domínio de Dedekind, assim como os corpos também são domínios de Dedekind.

Proposição 25: Seja A um anel Neotheriano integralmente fechado, $\mathrm{K}_f(\mathrm{A})$ seu corpo de frações, L uma extensão finita de $\mathrm{K}_f(\mathrm{A})$ e $\mathrm{I}_{\mathrm{L}}(\mathrm{A})$ o fecho inteiro de A em L. Suponha que $\mathrm{K}_f(\mathrm{A})$ tem característica nula. Então $\mathrm{I}_{\mathrm{L}}(\mathrm{A})$ é um anel Neotheriano e um $\mathrm{A} - m\acute{o}dulo$ finitamente gerado.

Demonstração:

Iremos admitir a afirmação de que $I_L(A)$ é um $A-$ *submódulo* de um $A-$ *módulo* livre de posto n cuja mesma será provada mais adiante de acordo com o item (a) da **Proposição 16 do Capítulo 3.**

Como A é Noetheriano e $I_L(A)$ é um $A-$ *submódulo* segue-se que $I_L(A)$ é um $A-$ *módulo* do tipo finito. Agora, pelo **Corolário 03** temos que $I_L(A)$ é um $A-$ *módulo* Noetheriano. Por outro lado, os ideais de $I_L(A)$ são $A-$ *submódulo* de $I_L(A)$, eles satisfazem a condição maximal. Portanto $I_L(A)$ é um anel Neotheriano.

■

A proposição seguinte diz que o anel dos inteiros em um corpo de números é um domínio de Dedekind.

Proposição 26: Seja A um domínio de Dedekind, $K_f(A)$ seu corpo de frações e L uma extensão de grau finito de $K_f(A)$ e $I_L(A)$ o fecho inteiro de A em L. Assuma que $K_f(A)$ tem característica nula. Então $I_L(A)$ é um domínio de Dedekind e um $A-$ *módulo* finitamente gerado.

Demonstração:

Sabemos que $I_L(A)$ é integralmente fechado, pois A é um domínio de Dedekind, é Noetheriano e é um $A-$ *módulo* finitamente gerado pela **Proposição 25**.

Resta verificarmos que todo ideal primo $\mathfrak{p} \neq \langle 0 \rangle$ não nulo de $I_L(A)$ é ideal maximal. Sabemos pela **Proposição 20** que $\mathfrak{p} \cap A$ é um ideal primo de A.

Vejamos primeiro que: para $x \in \mathfrak{p} - \langle 0 \rangle$ e considerando a equação de dependência inteira de x sobre A dada por $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ com $a_i \in$ A onde $i = 1, 2, \cdots, n-1$ "nem todos nulos, cujo o grau é mínimo" segue que $a_0 \neq 0$, pois do contrário obteríamos uma equação de grau menor. Portanto temos que $a_0 = -x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2 x + a_1) \in I_L(x) \cap A \subset \mathfrak{p} \cap A$, ou seja $\mathfrak{p} \cap A \neq \langle 0 \rangle$.

Como por hipótese A é um domínio de Dedekind, acarreta que $\mathfrak{p} \cap A$ é um ideal primo e maximal de A, logo $A/\mathfrak{p} \cap A$ é um corpo o qual pode ser identificado com algum subanel de $I_L(A)/\mathfrak{p} \cap A$ e por $I_L(A)$ ser um inteiro sobre A, acarreta $I_L(A)/\mathfrak{p} \cap A$ ser inteiro

sobre ${\mathrm{A}}/{\mathfrak{p} \cap \mathrm{A}}$. Mas ${\mathrm{I_L(A)}}/{\mathfrak{p}}$ é um corpo "cuja verificação é feita pela **Proposição 07** do **Capítulo 3**". Portanto $\mathfrak{p}$ é ideal maximal.

■

A característica de um anel A é o menor inteiro positivo n tal que $nx = 0$ para todo $x \in \mathrm{A}$, se tal elemento não existe diz-se que A tem característica nula, ou seja:

$$car(\mathrm{A}) = \begin{cases} mín.\{n \in \mathbb{N} : nx = 0 \ \forall \ x \in \mathrm{A}\} \\ 0, \text{caso contrário} \end{cases}$$

O interesse em anéis de Dedekind decorre do fato de que o anel de números inteiros em um corpo de números algébricos é um anel de Dedekind, mas nem sempre é um anel de ideais principais. Por exemplo, considere o anel dos inteiros $\mathrm{I_L}(\mathbb{Z}) = \mathbb{Z}\left[\sqrt{-5}\right]$ e o corpo de números algébricos $\mathrm{L} = \mathbb{Q}\left[\sqrt{-5}\right]$.

Proposição 27: Se A é um domínio de Dedekind que não é corpo, $\mathrm{K}_f(\mathrm{A})$ seu corpo de frações e $\mathfrak{m}$ um ideal maximal de A, então $\mathfrak{m}' = \left\{x \in \mathrm{K}_f(\mathrm{A}) : x\mathfrak{m} \subset \mathrm{A}\right\}$ é um ideal fracionário de A.

Demonstração:

Como por hipótese A não é um corpo então $\langle 0 \rangle$ não é ideal maximal de A e consequentemente temos que $\mathfrak{m} \neq \langle 0 \rangle$. Além disso $\mathfrak{m}' \neq \emptyset$ pois $0 \in \mathfrak{m}'$.

Se $x, y \in \mathfrak{m}'$, então $x\mathfrak{m}, y\mathfrak{m} \subset \mathrm{A}$ donde $x + y \in \mathfrak{m}'$ haja vista que $y\mathfrak{m} + x\mathfrak{m} = (x + y)\mathfrak{m} \subset \mathrm{A}$.

Agora se $x \in \mathfrak{m}'$ e $a \in \mathrm{A}$, daí segue que $ax\mathfrak{m} = (ax)\mathfrak{m} \subset \mathrm{A}$. Portanto $ax \in \mathfrak{m}'$. Consequentemente $d\mathfrak{m}' \subset \mathrm{A}$ para todo $d \in \mathrm{A} - \{0\}$, portanto $\mathfrak{m}'$ é ideal fracionário de A.

■

Proposição 28: Se A um domínio de Dedekind que não é um corpo, então cada ideal maximal de A, possui inverso no monóide $\mathcal{F}(\mathrm{A})$ de ideais fracionários de A.

Demonstração:

Pois bem, seja $\mathfrak{m}$ um ideal maximal de A. De acordo com o **Proposição 27** foi visto que $\mathfrak{m}' = \{x \in \mathrm{K}_f(\mathrm{A}) : x\mathfrak{m} \subset \mathrm{A}\}$ é um ideal fracionário de $\mathrm{K}_f(\mathrm{A})$ e segundo a sua construção, podemos ver que $\mathfrak{m}'\mathfrak{m} \subset \mathrm{A}$ e mais ainda, como $\mathfrak{m}$ é ideal de A, então $\mathfrak{m}\mathrm{A} = \mathfrak{m} \subset \mathfrak{m}'\mathfrak{m} \subset \mathrm{A}$ no que acarreta $\mathfrak{m}'\mathfrak{m} = \mathrm{A}$ ou $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ devido $\mathfrak{m}$ ser ideal maximal de A.

Iremos verificar que $\mathfrak{m}'\mathfrak{m} \neq \mathfrak{m}$. Pois suponhamos por absurdo que $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$. Para $x \in \mathfrak{m}'$ implica $x\mathfrak{m} \subset \mathfrak{m}$ e que $x^n\mathfrak{m} \subset \mathfrak{m}$ com $n \in \mathbb{N}$ qualquer.

Por outro lado, se $d \in \mathfrak{m}$ então $x^n d \in \mathrm{A}$ para todo $n \in \mathbb{N}$.

Logo $\mathrm{A}[x]$ é um ideal fracionário de A e como A é Noetheriano, então pela **Proposição 02**, segue que $\mathrm{A}[x]$ é um $\mathrm{A} - m\acute{o}dulo$ do tipo finito, logo $x \in \mathrm{I}_{\mathrm{K}_f(\mathrm{A})}(\mathrm{A})$ e como A é integralmente fechado $\mathrm{I}_{\mathrm{K}_f(\mathrm{A})}(\mathrm{A}) = \mathrm{A}$ segue que, $x \in \mathrm{A}$, portanto $\mathfrak{m}' \subset \mathrm{A}$. Como $\mathrm{A} \subset \mathfrak{m}'$ resulta que $\mathrm{A} = \mathfrak{m}'$.

Por outro lado, se $a \in \mathfrak{m} - \{0\}$ então pela **Proposição 22** o ideal $a\mathrm{A}$ contém um produto mínimo $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n$ de ideais primos não nulos de A. Assim $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n \subset a\mathrm{A} \subset \mathfrak{m}$. Logo pela **Proposição 21** segue que $\mathfrak{p}_i \subset \mathfrak{m}$ para algum $i \in [1, n] \cap \mathbb{N}$. Sem perda de generalidade podemos supor que $\mathfrak{p}_1 \subset \mathfrak{m}$. Como $\mathfrak{p}_1$ é maximal em A "A é domínio de Dedekind", então $\mathfrak{p}_1 = \mathfrak{m}$. Escolhendo $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$, temos que $\mathfrak{m}\mathfrak{b} \subset a\mathrm{A}$ e $\mathfrak{b} \subsetneq a\mathrm{A}$ devido a minimalidade de n.

Com isso existe $z \in \mathfrak{b}$ tal que $z \notin a\mathrm{A}$. Como $\mathfrak{m}\mathfrak{b} \subset a\mathrm{A}$ segue que $(z/a)\mathfrak{m} \subset \mathrm{A}$ e daí $z/a \in \mathfrak{m}'$, mas por outro lado temos que $z/a \notin \mathrm{A}$ e assim $\mathfrak{m}' \neq \mathrm{A}$ donde obtemos uma contradição com o fato de $\mathfrak{m}' = \mathrm{A}$.

Portanto essa contradição segue do fato de termos admitido que $\mathfrak{m}' = \mathrm{A}$. Com isso somos forçados a aceitar que $\mathfrak{m}'\mathfrak{m} = \mathrm{A}$ e isso quer dizer que $\mathfrak{m}'$ é o inverso de $\mathfrak{m}$.

■

Proposição 29 "Dedekind": Seja A um domínio de Dedekind e seja $\mathcal{P}$ o conjunto de todos os ideais primos não nulos de A. Então:

(a) Cada ideal fracionário não nulo $\mathfrak{b}$ de A, pode ser unicamente expresso na forma:

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})}$$

onde cada $n_{\mathfrak{p}}(\mathfrak{b}) \in \mathbb{Z}$ e $n_{\mathfrak{p}}(\mathfrak{b}) = 0$ para quase todos os $\mathfrak{p} \in \mathcal{P}$.

(b) O monóide $\mathcal{F}(\mathrm{A})$ "dos ideais fracionários não nulos de A" é um grupo abeliano.

Demonstração:

(a) Segue que da **Proposição 22** que existem ideais primos $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ não nulos de A tal que $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{n-1}\mathfrak{p}_n \subset \mathfrak{a}$. Provemos que $\mathfrak{a}$ é um produto de ideais primos por indução sobre o número n de ideais contidos em $\mathfrak{a}$.

Para $n = 1$ a proposição é válida, pois temos que $\mathfrak{a} \subset \mathfrak{p}_1$, mas como $\mathfrak{p}_1$ é ideal maximal "haja vista que A é domínio de Dedekind" segue que $\mathfrak{a} = \mathfrak{p}_1$ e assim $\mathfrak{a}$ é primo. Agora vamos admitir por hipótese de indução que todo ideal que contém um produto de $n-1$ ideais primos não nulos de A é escrito como um produto de ideais de A.

Seja agora $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{n-1}\mathfrak{p}_n \subset \mathfrak{a}$ "n ideais primos não nulos de A", como A é domínio de Dedekind então $\mathfrak{a}$ está contido em um ideal maximal $\mathfrak{m}$ de A.

Seja $\mathfrak{m}^{-1}$ o ideal fracionário inverso de $\mathfrak{m}$. Como $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{n-1}\mathfrak{p}_n \subset \mathfrak{a} \subset \mathfrak{m}$ segue que $\mathfrak{m}$ contém um dos $\mathfrak{p}_i$'s para algum $i \in [1, n] \cap \mathbb{N}$. Sem perda de generalidade suponhamos que $\mathfrak{p}_n \subset \mathfrak{m}$ asssim $\mathfrak{p}_n = \mathfrak{m}$ pois $\mathfrak{m}$ é maximal, logo $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{n-1}\mathfrak{p}_n \subset \mathfrak{a}\mathfrak{m}^{-1} \subset \mathfrak{m}\mathfrak{m}^{-1} = \mathrm{A}$. Pela hipótese de indução decorre que $\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$, onde $\mathfrak{q}_{1 \le i \le s}$ são ideais primos não nulos de A e daí $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$.

A prova da unicidade decorre da seguinte maneira, suponhamos que

$$\prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\mathfrak{n}_\mathfrak{p}(\mathfrak{b})} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\mathfrak{m}_\mathfrak{p}(\mathfrak{b})} \Longrightarrow \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\mathfrak{n}_\mathfrak{p}(\mathfrak{b}) - \mathfrak{m}_\mathfrak{p}(\mathfrak{b})} = \mathrm{A}$$

Se $\mathfrak{n}_\mathfrak{p}(\mathfrak{b}) - \mathfrak{m}_\mathfrak{p}(\mathfrak{b}) \neq 0$, para algum $\mathfrak{p} \in \mathcal{P}$ podemos separar os expoentes positivos e negativos e reescrevê-los como ${\mathfrak{p}_1}^{\alpha_1}{\mathfrak{p}_2}^{\alpha_2} \cdots {\mathfrak{p}_r}^{\alpha_r} = {\mathfrak{q}_1}^{\beta_1}{\mathfrak{q}_2}^{\beta_2} \cdots {\mathfrak{q}_s}^{\beta_s}$ com $\mathfrak{p}_i, \mathfrak{q}_i \in \mathcal{P}$, $\alpha_i, \beta_i < 0$, $\mathfrak{p}_i \neq \mathfrak{q}_j$ para todo i e j.

Logo $\mathfrak{p}_1$ contém ${\mathfrak{q}_1}^{\beta_1}{\mathfrak{q}_2}^{\beta_2} \cdots {\mathfrak{q}_s}^{\beta_s}$ e daí $\mathfrak{p}_1 \supset \mathfrak{q}_j$ para algum j. Suponhamos, sem perda de generalidade que $\mathfrak{p}_1 \supset \mathfrak{q}_1$, mas como os mesmos são ideais maximais segue que $\mathfrak{p}_1 = \mathfrak{q}_1$ e assim $\mathfrak{n}_\mathfrak{p}(\mathfrak{b}) = \mathfrak{m}_\mathfrak{p}(\mathfrak{b})$ ou seja $\mathfrak{n}_\mathfrak{p}(\mathfrak{b}) - \mathfrak{m}_\mathfrak{p}(\mathfrak{b}) = 0$, o que é uma contradição.

Apresentamos outra segunda solução alternativa para esse item. Provemos a existência, ou seja, que qualquer ideal fracionário $\mathfrak{a}$ é um produto de potências "inteiras" de ideais primos.

Como $\mathfrak{a}$ é fracionário segue que existe um $d \in \mathrm{A} - \langle 0 \rangle$ tal que $d\mathfrak{a} \subset \mathrm{A}$, ou seja: $d\mathfrak{a}$ é um ideal inteiro e $\mathfrak{a} = (d\mathfrak{a})(\mathrm{A}d)^{-1}$.

Sem perda de generalidade podemos provar o item para ideais inteiros. Assim considere $\Lambda(\mathrm{A})$ a coleção dos ideais não nulos de A que não são produtos de ideais primos.

Suponhamos por absurdo que $\Lambda(\mathrm{A})$ seja diferente do conjunto vazio. Daí como A é Noetheriano, então a coleção possui um elemento maximal $\mathfrak{m}$. De fato $\mathfrak{m} \neq \mathrm{A}$, pois A é o produto da coleção vazia de ideais primos.

Logo $\mathfrak{m} \subset \mathfrak{n}$, onde $\mathfrak{n}$ é um ideal maximal, que é um elemento maximal na coleção de ideais não triviais de A que contém $\mathfrak{m}$.

Seja f o ideal fracionário inverso de $\mathfrak{n}$. Como $\mathfrak{m} \subset \mathfrak{n}$, então $\mathfrak{m}f \subset \mathfrak{n}f = \mathrm{A}$. Como $\mathrm{A} \subset f$, $f \subset \mathfrak{m}f$ de fato $\mathfrak{m}f \neq \mathfrak{m}$, pois se $\mathfrak{m}f = \mathfrak{m}$ e $x \in f$, então: $\mathfrak{m}x \subset \mathfrak{m}$, $\mathfrak{m}x^n \subset \mathfrak{m}$ para todo $n \in \mathbb{N}$ e $x \in \mathrm{A}$ que é inteiro sobre A de acordo com a **Proposição 26**. Mas isso é impossível, pois $f \neq \mathrm{A}$ "do contrário $f = \mathrm{A}$ e $f = f\mathfrak{n}$".

Pela maximalidade de $\mathfrak{m}$ em $\Lambda(\mathrm{A})$ tem-se que $\mathfrak{m}f \notin \Lambda(\mathrm{A})$ com isso $\mathfrak{m}f = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$ donde $\mathfrak{m}f = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k \Longrightarrow \mathfrak{m} = \mathfrak{m}f\mathfrak{n} = \mathfrak{n}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$. Portanto todo ideal inteiro de a é um produto de ideais primos. A prova da unicidade decorre como da maneira anterior.

(b) Segue que o inverso de $\mathfrak{b}$ é

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\mathfrak{n}_\mathfrak{p}(\mathfrak{b})} \Longrightarrow \mathfrak{b}^{-1} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{-\mathfrak{n}_\mathfrak{p}(\mathfrak{b})}$$

■

Como visto $\mathfrak{n}_\mathfrak{p}(\mathfrak{b})$ é o expoente de $\mathfrak{p}$ na fatoração de $\mathfrak{b}$ em um produto de ideais primos. Então:

$$\mathfrak{n}_\mathfrak{p}(xy) = \mathfrak{n}_\mathfrak{p}(x) + \mathfrak{n}_\mathfrak{p}(y)$$

$$x \subset \mathrm{A} \Leftrightarrow \mathfrak{n}_\mathfrak{p}(x) \geq 0 \ \forall\, \mathfrak{p} \in \mathcal{P}$$

$$x \subset y \Leftrightarrow \mathfrak{n}_\mathfrak{p}(x) \geq \mathfrak{n}_\mathfrak{p}(y) \ \forall\, \mathfrak{p} \in \mathcal{P}$$

$$\mathfrak{n}_\mathfrak{p}(x + y) = mín.\{\mathfrak{n}_\mathfrak{p}(x), \mathfrak{n}_\mathfrak{p}(y)\}$$

$$\mathfrak{n}_\mathfrak{p}(x \cap y) = máx.\{\mathfrak{n}_\mathfrak{p}(x), \mathfrak{n}_\mathfrak{p}(y)\}$$

3 TEORIA ALGÉBRICA DOS NÚMEROS

3.1 Corpos Numéricos e Anel dos Inteiros

A verificação que a soma, a diferença e o produto de números algébricos "respectivamente inteiros" também são números algébricos "respectivamente inteiros" não é imediata e é feita utilizando a noção de adjunção e de módulos finitamente gerados.

$\mathrm{I_S(R)} = \{\alpha \in \mathrm{S} : \exists\, p(x) \in \mathrm{R}[x]$ mônico com $p(\alpha) = 0\}$ será denotado o conjunto dos elementos do anel S que são inteiros sobre R "$\mathrm{R} \leq \mathrm{S}$".

Será provado que todo corpo numérico K "sendo extensão finita de $\mathbb{Q}$ e subcorpo de $\mathbb{C}$" possui um subanel denotado por $\mathrm{I_K}(\mathbb{C}) = \mathrm{I_K}$, cujo corpo de frações é o próprio corpo K, ou seja $\mathrm{K}_f(\mathrm{I_K}) = \mathrm{K}$, mais precisamente que $\mathrm{I_S(R)}$ é subanel de S. No geral não é válido que $\mathrm{I}_{\mathbb{Q}(\alpha)}(\mathbb{Z}) = \mathbb{Z}[\alpha]$.

3.1.1 Corpo de Números

Dado um anel S e o subanel R o elemento $\alpha \in \mathrm{S}$ é dito ser **inteiro** sobre R se existir um polinômio mônico

$$p(x) = \sum_{i=0}^{n} a_i x^i = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathrm{R}[x]$$

com $p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ "essa equação é chamada de equação de dependência inteira de α sobre R".

Em particular para todo $x \in \mathrm{R}$, x é inteiro sobre R.

Para um anel S e um corpo K tal que $\mathrm{K} \leq \mathrm{S}$ o elemento $\alpha \in \mathrm{S}$ é dito ser **algébrico** sobre K se existir um polinômio

$$q(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathrm{R}[x]$$

com $q(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$.

Em particular todo elemento algébrico sobre K é inteiro sobre K.

A extensão L de K é chamada algébrica se todo elemento de L é algébrico sobre K. Toda extensão finita de K é algébrica; trata-se de um Teorema da Teoria dos Corpos. Um corpo de números ou corpo numérico é uma extensão finita do conjunto dos racionais.

Exemplo 01: Os números

$$\sqrt{2}, \sqrt{3}, i, \sqrt[7]{12}, e^{\frac{2\pi i}{n}} = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right), \frac{1+\sqrt{5}}{2}$$

são inteiros algébricos, haja vista que são respectivamente raízes dos polinômios mônicos $\mathrm{X}^2 - 2, \mathrm{X}^2 - 3, \mathrm{X}^2 + 1, \mathrm{X}^7 - 12, \mathrm{X}^n + 1, \mathrm{X}^2 - \mathrm{X} - 1 \in \mathbb{Z}[\mathrm{X}]$.

3.1.2 Fecho Algébrico

Proposição 01: Seja S um anel e R um subanel de S, para qualquer $\alpha \in$ S as condições são equivalentes:

(a) α é um inteiro sobre R "$\alpha \in \mathrm{I_S(R)}$".

(b) R$[\alpha]$ é um R $-$ *módulo* finitamente gerado ou do tipo finito.

(c) Existe um subanel S′ de S que é um R $-$ módulo finitamente gerado e tal que $\alpha \in$ S′.

(d) Existe um R $-$ *módulo* finitamente gerado N tal que αN $\subseteq$ N e que λN $\neq \{0\}$ para todo $\lambda \in$ R$[\alpha] - \{0\}$.

Demonstração:

$(a) \Longrightarrow (b)$ Se $\alpha \in \mathrm{I_S(R)}$ então $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ com $a_i \in$ R para $i = 0, 1, \cdots, n-1$. Sejam o anel

$$\mathrm{R}[\alpha] = \left\{ \sum_{k\in\mathbb{N}} a_k \alpha^k : a_k \in \mathrm{R} \right\}$$

e N um $\mathrm{R} - \textit{módulo}$ finitamente gerado por $\{1, \alpha, \cdots, \alpha^{n-1}\}$, ou seja

$$\mathrm{N} = \langle 1, \alpha, \cdots, \alpha^{n-1} \rangle = \mathrm{R} + \alpha\mathrm{R} + \cdots + \mathrm{R}\alpha^{n-1}$$

Note que $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0$ significando que $\alpha^j \in \mathrm{N}$. Portanto $\mathrm{R}[\alpha] \subseteq \mathrm{N}$ para todo $j \leq n$. Por outro lado $\alpha^j \in \mathrm{N}$ para todo $j > n$. Isso segue por indução, suponha que

$$\alpha^j = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$$

com $b_i \in \mathrm{R}$, $0 \leq i \leq n-1$, então:

$$\alpha^{j+1} = \alpha^j\alpha = (b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0)\alpha =$$
$$b_{n-1}\alpha^n + \cdots + b_1\alpha^2 + b_0\alpha =$$
$$b_{n-1}\left(-\sum_{i=0}^{n-1} a_i\alpha^i\right) + \cdots + b_1\alpha^2 + b_0\alpha =$$
$$-\sum_{i=0}^{n-1} b_{n-1}a_i\alpha^i + \cdots + b_1\alpha^2 + b_0\alpha =$$
$$-a_0b_{n-1} + (b_{n-1}a_1 + b_0)\alpha + \cdots + (-b_{n-1}a_{n-1} + b_{n-2})\alpha^{n-1}$$

Portanto $\alpha^j \in \mathrm{N}$ para todo $j \in \mathbb{N}$, logo $\mathrm{R}[\alpha] \subseteq \mathrm{N}$. De imediato $\mathrm{N} \subseteq \mathrm{R}[\alpha]$ valendo a igualdade.

$(b) \Longrightarrow (c)$ Basta tomar $\mathrm{S}' = \mathrm{R}[\alpha] \leq \mathrm{S}$. Além disso: $\mathrm{R} \subset \mathrm{S}'$ e $\alpha \in \mathrm{S}'$.

$(c) \Longrightarrow (d)$ Basta tomar $\mathrm{N} = \mathrm{S}'$ e notar que $\alpha\mathrm{S}' \subset \mathrm{S}'$, $\lambda = 1_{\mathrm{R}}\lambda \in \mathrm{S}'$ para todo $\lambda \in \mathrm{R}[\alpha] - \{0\}$.

$(d) \Longrightarrow (a)$ Considere $\mathrm{N} = \langle n_1, n_2, \cdots, n_k \rangle = n_1\mathrm{R} + n_2\mathrm{R} + \cdots + n_k\mathrm{R}$ o $\mathrm{R}-$ *módulo* finitamente gerado. Como $\alpha\mathrm{N} \subseteq \mathrm{N}$ segue que existem $a_{ij} \in \mathrm{R}\ 1 \leq i, j \leq k$ tal que

$$\alpha n_i = \sum_{j=1}^{k} a_{ij} n_j$$

equivalentemente

$$\begin{cases} (\alpha - a_{11})n_1 - a_{12}n_2 - \cdots - a_{1k}n_k = 0 \\ -a_{21}n_1 + (\alpha - a_{22})n_2 - \cdots - a_{2k}n_k = 0 \\ \vdots \\ -a_{k1}n_1 - a_{k2}n_2 - \cdots + (\alpha - a_{kk})n_k = 0 \end{cases}$$

Na forma matricial fica

$$\begin{bmatrix} (\alpha - a_{11}) & -a_{12} & \cdots & -a_{1k} \\ -a_{21} & (\alpha - a_{22}) & \cdots & -a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{k1} & -a_{k2} & \cdots & (\alpha - a_{kk}) \end{bmatrix} \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

logo $(n_1, n_2, \cdots, n_k)$ é solução do sistema homogêneo

$$\sum_{j=1}^{k} \left(\delta_{ij}\alpha - a_{ij}\right) y_j = 0, \delta_{ij} = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

com $1 \leq i \leq k$. Assim segundo a Regra de Cramer se $d = det\left(\delta_{ij}\alpha - a_{ij}\right)$, então $dn_j = 0$ e como $d\mathrm{N} \neq \{0\}$ tem-se que $d = 0$. Por outro lado:

$$0 = d = det\left(\delta_{ij}\alpha - a_{ij}\right) =$$

$$det \begin{bmatrix} (\alpha - a_{11}) & -a_{12} & \cdots & -a_{1k} \\ -a_{21} & (\alpha - a_{22}) & \cdots & -a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{k1} & -a_{k2} & \cdots & (\alpha - a_{kk}) \end{bmatrix} \Leftrightarrow$$

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$$

com $b_i \in \mathrm{R}$. Portanto d é equação de dependência integral de α sobre R e assim $\alpha \in \mathrm{I_S(R)}$.

■

Corolário 01: Seja S um anel, R um subanel de S. Se $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathrm{S}$ com α_i inteiro $\mathrm{R}[\alpha_1, \alpha_2, \cdots, \alpha_{i-1}]$ então $\mathrm{R}[\alpha_1, \alpha_2, \cdots, \alpha_n]$ é um $\mathrm{R} - módulo$ finitamente gerado ou do tipo finito.

Demonstração:

A verificação é feita por indução em n.

Para $n = 1$ a verificação é imediata pelo item (b) da **Proposição 01**.Admita por hipótese de indução que $\mathrm{K} = \mathrm{R}[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}]$ é um $\mathrm{R} - módulo$ finitamente gerado com inteiro α_n sobre K. Então:

$$\mathrm{K} = \sum_{i=1}^{r} x_i \mathrm{R}$$

e $\mathrm{K}[\alpha_n] = \mathrm{R}[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}][\alpha_n] = \mathrm{R}[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n]$ é um $\mathrm{R} - módulo$ finitamente gerado. Logo:

$$\mathrm{K}[\alpha_n] = \sum_{j=1}^{s} y_j \mathrm{K}$$

donde

$$\mathrm{R}[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n] =$$

$$\sum_{j=1}^{s} y_j \mathrm{K} =$$

$$\sum_{j=1}^{s} y_j \left(\sum_{i=1}^{r} x_i \mathrm{R} \right) =$$

$$\sum_{j=1}^{s} \sum_{i=1}^{r} (x_i y_j) \mathrm{R}$$

Portanto $\{x_i y_j\}$ $1 \leq i \leq r,\ 1 \leq j \leq s$ gera $\{x_i y_j\}$ o $\mathrm{R} - módulo$ finitamente gerado $\mathrm{K}[\alpha_n]$. Então $\mathrm{R}[\alpha_1, \alpha_2, \cdots, \alpha_n]$ é um $\mathrm{R} - módulo$ finitamente gerado.

■

Corolário 02: Seja S um anel, R um subanel de S. Se $\alpha_1, \alpha_2, \cdots, \alpha_n \in$ S com α_i inteiro sobre R, então R$[\alpha_1, \alpha_2, \cdots, \alpha_n]$ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado ou do tipo finito.

Demonstração:

Se α_i inteiro sobre R, então α_i é inteiro sobre R$[\alpha_1, \alpha_2, \cdots, \alpha_{i-1}]$, com $1 \leq i \leq n$. Segundo o **Corolário 01** R$[\alpha_1, \alpha_2, \cdots, \alpha_n]$ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado.

■

Corolário 03: Seja S um anel, R um subanel de S, então:

(a) $x, y \in \mathrm{I_S(R)}$ implica $x + y, x - y, xy \in \mathrm{I_S(R)}$.

(b) $\mathrm{I_S(R)}$ é um subanel de S que contém R.

(c) Todo subanel S′ de S, que é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado está contido em $\mathrm{I_S(R)}$.

Demonstração:

(a) Segue que $x, y \in \mathrm{R}[x, y] \leq \mathrm{S}$ com $x + y, x - y, xy \in \mathrm{R}[x, y]$. Mas como $x, y \in \mathrm{I_S(R)}$ segundo o **Corolário 02** R$[x, y]$ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado.

Assim pelo item (c) da **Proposição 01** $x + y, x - y, xy \in \mathrm{I_S(R)}$.

(b) Segundo o item (a) $\mathrm{I_S(R)}$ é subanel de S que contém R, uma vez que para todo $r \in$ R, r é raiz do polinômio $p(x) = x - r$.

(c) Seja S′ subanel de S tal que S′ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado então todo $\alpha \in$ S′ implica $\alpha \in \mathrm{I_S(R)}$ segundo o item (c) da **Proposição 01**.

■

O subanel $\mathrm{I_S(R)}$ "anel dos inteiros de S sobre R" de S é chamado também fecho inteiro de R em S. Quando $\mathrm{I_S(R)} = \mathrm{S}$, S é dito inteiro sobre R. E quando $\mathrm{I_S(R)} = \mathrm{R}$, R é dito integralmente fechado em S e apenas integralmente fechado quando $\mathrm{I_{K_f(R)}(R)} = \mathrm{R}$ onde R é um domínio de integridade e

$$\mathrm{K}_f(\mathrm{R}) = \left\{\frac{x}{y} : x, y \in \mathrm{R}, y \neq 0\right\}$$

é o corpo de frações de R.

No caso de corpos $\mathrm{S} = \mathrm{L}, \mathrm{R} = \mathrm{K}, \mathrm{I}_\mathrm{L}(\mathrm{K})$ é subcorpo de L, a saber o fecho algébrico de K em L. Em particular, temos que $\mathrm{I}_\mathrm{L}(\mathrm{K}) = \mathrm{K}$ se e somente se K for algebricamente fechado em L e $\mathrm{I}_\mathrm{L}(\mathrm{K}) = \mathrm{L}$ se e somente se a extensão for algébrica.

Corolário 04: Seja o Ω_S conjunto dos subanéis de S. Então a aplicação

$$\begin{aligned} \mathrm{I}_\mathrm{S} : \Omega_\mathrm{S} &\longrightarrow \Omega_\mathrm{S} \\ \mathrm{R} &\longmapsto \mathrm{I}_\mathrm{S}(\mathrm{R}) \end{aligned}$$

é uma operação de fecho no conjunto dos subanéis de S, ou seja, satisfaz as condições:

(a) Se $\mathrm{R} \subseteq \mathrm{R}'$ então $\mathrm{I}_\mathrm{S}(\mathrm{R}) \subseteq \mathrm{I}_\mathrm{S}(\mathrm{R}')$

(b) $\mathrm{R} \subseteq \mathrm{I}_\mathrm{S}(\mathrm{R}) = \mathrm{I}_\mathrm{S}\big(\mathrm{I}_\mathrm{S}(\mathrm{R})\big)$

Demonstração:

(a) De fato, se $\mathrm{R} \subseteq \mathrm{R}'$ então $\mathrm{I}_\mathrm{S}(\mathrm{R}) \subseteq \mathrm{I}_\mathrm{S}(\mathrm{R}')$.

(b) Como $\mathrm{R} \subseteq \mathrm{I}_\mathrm{S}(\mathrm{R})$, pelo item (a) resulta que $\mathrm{I}_\mathrm{S}(\mathrm{R}) \subseteq \mathrm{I}_\mathrm{S}\big(\mathrm{I}_\mathrm{S}(\mathrm{R})\big)$. Se $\alpha \in \mathrm{I}_\mathrm{S}\big(\mathrm{I}_\mathrm{S}(\mathrm{R})\big)$ então $\mathrm{I}_\mathrm{S}(\mathrm{R})[\alpha]$ é um $\mathrm{I}_\mathrm{S}(\mathrm{R}) - m\acute{o}dulo$ finitamente gerado e como $\mathrm{R} \subseteq \mathrm{I}_\mathrm{S}(\mathrm{R})$ segue que $\mathrm{R}[\alpha]$ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado donde $\alpha \in \mathrm{I}_\mathrm{S}(\mathrm{R})$. Logo vale a igualdade.

■

Proposição 02: Sejam S um subanel de T e R um subanel do anel S. As seguintes condições são equivalentes:

(a) $\mathrm{I}_\mathrm{T}(\mathrm{S}) = \mathrm{T}$ e $\mathrm{I}_\mathrm{S}(\mathrm{R}) = \mathrm{S}$

(b) $\mathrm{I}_\mathrm{T}(\mathrm{R}) = \mathrm{T}$

Demonstração:

$(a) \Longrightarrow (b)$ Dado um $x \in \mathrm{T} = \mathrm{I_T(S)}$ tem-se que existem $a_0, a_1, \cdots, a_{n-1} \in \mathrm{S} = \mathrm{I_S(R)}$ tal que $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, daí x é inteiro sobre $\mathrm{S}' = \mathrm{R}[a_1, a_2, \cdots, a_{n-1}]$.

Logo $\mathrm{S}'[x] = \mathrm{R}[a_1, a_2, \cdots, a_{n-1}, x]$ é um $\mathrm{S}' - m\acute{o}dulo$ finitamente gerado segundo o item (b) da **Proposição 01** e S′ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado segundo o **Corolário 02**.

Portanto $\mathrm{S}'[x]$ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado e consequentemente $x \in \mathrm{I_T(R)}$ donde $\mathrm{T} \subseteq \mathrm{I_T(R)} \subseteq \mathrm{T}$.

$(b) \Longrightarrow (a)$ Se $x \in \mathrm{S}$, então $x \in \mathrm{T} = \mathrm{I_T(S)}$ donde $\mathrm{R}[x]$ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado, mas também R é subanel de S, logo $x \in \mathrm{I_S(R)} \subseteq \mathrm{S}$. Por outro lado $\mathrm{R} \subseteq \mathrm{S}$ implica $\mathrm{T} = \mathrm{I_T(R)} \subseteq \mathrm{I_T(S)} \subseteq \mathrm{T}$.

■

Proposição 03: Seja S um domínio de integridade e R um subanel de S tal que $\mathrm{I_S(R)} = \mathrm{S}$ então S é corpo se e somente se R é corpo.

Demonstração:

Suponha que S seja um corpo e que $a \in \mathrm{R}$, e $a \neq 0$ então a possui inverso $a^{-1} \in \mathrm{S} = \mathrm{I_S(R)}$, logo $a^{-n} + b_{n-1}a^{-n+1} + \cdots + b_1 a^{-1} + b_0 = 0$ onde $b_i \in \mathrm{R}$ para $0 \leq i \leq n-1$.

Agora tomando o produto por a^{n-1} na equação de dependência inteira fica $a^{-1} = -(b_{n-1} + \cdots + b_1 a^{n-2} + b_0 a^{n-1})$, significando que $a^{-1} \in \mathrm{R}$. Portanto R é corpo.

Reciprocamente se R é um corpo e $b \in \mathrm{S} - \{0\}$ então segundo o item (b) da **Proposição 01**, $\mathrm{R}[b]$ é um $\mathrm{R} - m\acute{o}dulo$ finitamente gerado logo um espaço vetorial de dimensão finita sobre R. Por outro lado, definindo a aplicação

$$\begin{aligned} \varphi : \mathrm{R}[b] &\longrightarrow \mathrm{R}[b] \\ y &\longmapsto yb \end{aligned}$$

tem-se que φ é transformação $\mathrm{R} - linear$, injetiva já que $\varphi(\lambda x + y) = (\lambda x + y)b = \lambda xb + yb = \lambda\varphi(x) + \varphi(y)$, $\mathrm{R}[b]$ é domínio de integridade e com isso $ker(\varphi) = \{0\}$.

Assim pelo Teorema do Núcleo e da Imagem φ é sobrejetiva e consequentemente bijetiva. Então $1_{\mathrm{R}} \in \mathrm{R}[b]$, portanto existe um único $b' \in \mathrm{R}[b]$ tal que $b'b = 1_{\mathrm{R}}$ donde S é corpo.

■

O operador tem a propriedade de fecho e a aplicação que cujo mesmo define é chamada operação de fecho.

Proposição 04: Todo domínio fatorial R é integralmente fechado.

Demonstração:

Seja $x \in \mathrm{K}_f(\mathrm{R})$ tal que $x \neq 0$, logo $x = {}^{a}/_{b} = ab^{-1}$ com $a, b \in \mathrm{R}$, $b \neq 0$ com o $mdc(a, b) = 1$.

Se $x \in \mathrm{I}_{\mathrm{K}_f(\mathrm{R})}(\mathrm{R})$ então existem constantes $c_i \in \mathrm{R}$ para $0 \leq i \leq n$ tal que

$$x^n + c_1 x^{n-1} + \cdots + c_{n-1}x + c_n =$$
$$\left(\frac{a}{b}\right)^n + c_1\left(\frac{a}{b}\right)^{n-1} + \cdots + c_{n-1}\left(\frac{a}{b}\right) + c_n = 0 \Leftrightarrow$$
$$a^n + bc_1a^{n-1} + \cdots + c_{n-1}a + b^n c_n = 0 \Leftrightarrow$$
$$a^n = -b(c_1a^{n-1} + \cdots + c_{n-1}a + b^{n-1}c_n)$$

donde b divide a^n e com isso b é invertível, pois do contrário, para um elemento irredutível p que divide b tem-se que p divide a^n, logo p dividirá a e isso é uma contradição com o fato do $mdc(a, b) = 1$.

Portanto $b \in \mathcal{U}(\mathrm{R})$ donde $x = {}^{a}/_{b} \in \mathrm{R}$ e consequentemente $\mathrm{I}_{\mathrm{K}_f(\mathrm{R})}(\mathrm{R}) = \mathrm{R}$.

■

Exemplo 02: $\mathrm{I}_{\mathbb{Q}}(\mathbb{Z}) = \mathbb{Z}$, porque $\mathbb{Z}$ é um domínio fatorial e $\mathbb{Q}$ é seu corpo de frações, donde vale a igualdade segundo a **Proposição 04**.

Proposição 05: Seja R um subanel de um corpo L. Então:

$$\mathrm{K}_f\big(\mathrm{I}_\mathrm{L}(\mathrm{R})\big) = \mathrm{I}_\mathrm{L}\left(\mathrm{K}_f(\mathrm{R})\right) = \mathrm{I}_\mathrm{L}(\mathrm{R})$$

Demonstração:

Seja $x \in \mathrm{K}_f\big(\mathrm{I}_\mathrm{L}(\mathrm{R})\big)$, logo $x = ab^{-1} = {}^{a}/_{b}$ onde $a, b \in \mathrm{I}_\mathrm{L}(\mathrm{R})$, $b \neq 0$. Mas $\mathrm{I}_\mathrm{L}\left(\mathrm{K}_f(\mathrm{R})\right)$ é um subcorpo de L que contém $\mathrm{I}_\mathrm{L}(\mathrm{R})$ "$\mathrm{R} \subseteq \mathrm{K}_f(\mathrm{R}) \Longrightarrow \mathrm{I}_\mathrm{L}(\mathrm{R}) \subseteq \mathrm{I}_\mathrm{L}\left(\mathrm{K}_f(\mathrm{R})\right)$".

Para um $x \in \mathrm{I}_\mathrm{L}\left(\mathrm{K}_f(\mathrm{R})\right)$, temos que existem elementos ${}^{c_i}/_{d_i} \in \mathrm{K}_f(\mathrm{R})$ em que $c_i, d_i \in \mathrm{R}$ com $d_i \neq 0$ para $1 \leq i \leq n$ tal que

$$x^n + \left(\frac{c_1}{d_1}\right)x^{n-1} + \cdots + \left(\frac{c_{n-1}}{d_{n-1}}\right)x + \left(\frac{c_n}{d_n}\right) = 0$$

Fazendo $d = d_1 d_2 \cdots d_n \in \mathrm{R}$ então $d \neq 0$ e

$$d^n x^n + d^{n-1} d_1' c_1 x^{n-1} + \cdots + d^{n-1} d_{n-1}' c_{n-1} x + d^{n-1} d_n' c_n = 0$$

onde para $1 \leq i \leq n$

$$d_i' = \frac{d}{d_i}$$

Assim $d^{i-1} d_i' c_i \in \mathrm{R}$ para $1 \leq i \leq n$. Portanto $dx \in \mathrm{I}_\mathrm{L}(\mathrm{R})$, porém como $d \in \mathrm{R} \subseteq \mathrm{I}_\mathrm{L}(\mathrm{R})$, $d \neq 0$ e $\mathrm{I}_\mathrm{L}(\mathrm{R})$ é subanel de L, resulta que $x = d^{-1} d \in \mathrm{I}_\mathrm{L}(\mathrm{R})$.

Finalmente observe que $\mathrm{I}_\mathrm{L}(\mathrm{R}) \subseteq \mathrm{K}_f\big(\mathrm{I}_\mathrm{L}(\mathrm{R})\big)$.

■

Observe como caso particular que $\mathrm{K}_f\big(\mathrm{I}_\mathrm{L}(\mathrm{R})\big) = \mathrm{L}$ se e somente se L for uma extensão algébrica de $\mathrm{K}_f(\mathrm{R})$. Isso é consequência do fato que $\mathrm{I}_\mathrm{L}\left(\mathrm{K}_f(\mathrm{R})\right) = \mathrm{L}$ se e somente se L é uma extensão algébrica de R.

Corolário 05: Seja L um corpo de números algébricos. Então:

$$\mathrm{K}_f\big(\mathrm{I}_\mathrm{L}(\mathbb{Z})\big) = \big(\mathrm{I}_\mathrm{L}(\mathbb{Z})\big)_{\mathbb{Z}-\{0\}} = \mathrm{L}$$

Demonstração:

Seque da **Proposição 05** e que $\mathrm{I}_\mathrm{L}\left(\mathrm{K}_f(\mathbb{Z})\right) = \mathrm{I}_\mathrm{L}(\mathbb{Q}) = \mathrm{L}$

■

Dado um corpo L e um subanel R de L, seja $m_\lambda(x)$ o polinômio minimal de $\lambda \in \mathrm{I}_\mathrm{L}(\mathrm{R})$ sobre $\mathrm{K} = \mathrm{K}_f(\mathrm{R})$. Em geral $m_\lambda(x) \notin \mathrm{R}[x]$. Sobre esse fato segue o resultado.

Proposição 06: Seja R um subanel de L e $\mathrm{K} = \mathrm{K}_f(\mathrm{R})$.

(a) Se f, g são polinômios mônicos em $\mathrm{K}[x]$ e $fg \in \mathrm{R}[x]$ então $f, g \in \mathrm{I}_\mathrm{K}(\mathrm{R})[x]$.
(b) Para todo $\lambda \in \mathrm{I}_\mathrm{L}(\mathrm{R})$ tem-se que $m_\lambda(x) \in \mathrm{I}_\mathrm{K}(\mathrm{R})[x]$.

Demonstração:

(a) Segue que existem $\alpha_1, \alpha_2, \cdots, \alpha_m, \beta_1, \beta_2, \cdots, \beta_n$ no fecho algébrico de L $\Omega = \mathrm{I}_{\mathrm{K}_f(\mathrm{L})}(\mathrm{L})$ tal que:

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_m) \text{ e } g(x) = (x-\beta_1)\cdots(x-\beta_n)$$

logo resulta que $\alpha_1, \alpha_2, \cdots, \alpha_m, \beta_1, \beta_2, \cdots, \beta_n \in \mathrm{I}_\Omega(\mathrm{R})$ donde os coeficientes de f e g estão em $\mathrm{I}_\Omega(\mathrm{R}) \cap \mathrm{K}_f(\mathrm{R}) = \mathrm{I}_{\mathrm{K}_f(\mathrm{R})}(\mathrm{R})$.

Note que:

$$\mathrm{K}_f(\mathrm{R}) \subseteq \mathrm{K}_f(\mathrm{L}) \subseteq \mathrm{I}_{\mathrm{K}_f(\mathrm{L})}(\mathrm{L}) = \Omega \Longrightarrow$$
$$\Omega \cap \mathrm{K}_f(\mathrm{R}) = \mathrm{K}_f(\mathrm{R})$$

resultando que

$$x \in \mathrm{I}_\Omega(\mathrm{R}) \cap \mathrm{K}_f(\mathrm{R}) \Leftrightarrow x \in \mathrm{I}_\Omega(\mathrm{R}) \text{ e } x \in \mathrm{K}_f(\mathrm{R}) \Leftrightarrow$$
$$x \in \Omega \cap \mathrm{K}_f(\mathrm{R}) \text{ e existe } p(x) \in \mathrm{R}[x] \text{ mônico tal que } p(x) = 0 \Leftrightarrow$$
$$x \in \mathrm{K}_f(\mathrm{R}) \text{ e existe } p(x) \in \mathrm{R}[x] \text{ mônico tal que } p(x) = 0 \Leftrightarrow$$
$$x \in \mathrm{I}_{\mathrm{K}_f(\mathrm{R})}(\mathrm{R})$$

(b) Se $\lambda \in \mathrm{I_L(R)}$ tem-se que então existe um polinômio mônico $h \in \mathrm{R}[x]$ tal que $h(\lambda) = 0$. Daí existe um polinômio mônico $g \in \mathrm{K}_f(\mathrm{R})[x]$ tal que $h = g \cdot m_\lambda(x)$ donde pelo item (a) $m_\lambda(x) \in \mathrm{I_K(R)}[x]$.

■

Proposição 07: Seja S um domínio em que $\mathrm{I_S(R)} = \mathrm{S}$. Então:

(a) Para todo ideal J não nulo de S, J⋂S é um ideal não nulo de R.

(b) $\mathcal{U}(\mathrm{S})\bigcap\mathrm{R} = \mathcal{U}(\mathrm{R})$.

(c) S é um corpo se e somente se R for um corpo.

(d) Um ideal primo $\mathfrak{p}$ de S é ideal maximal de S se e somente se $\mathfrak{p}$⋂S for ideal maximal de R.

Demonstração:

(a) Seja $\alpha \in$ J não nulo então $\alpha \in \mathrm{S} = \mathrm{I_S(R)}$, logo suponha que

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathrm{R}[x]$$

seja um polinômio de menor grau que tem α como raiz. Assim:

$$a_0 = -\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_2\alpha + a_1)$$

e $a_0 \in \alpha\mathrm{S}\bigcap\mathrm{R} \subseteq \mathrm{J}\bigcap\mathrm{S}$. Donde J⋂S é ideal não nulo.

(b) De fato $\mathcal{U}(\mathrm{R}) \subseteq \mathcal{U}(\mathrm{S})\bigcap\mathrm{R}$. Por outro lado, se $\alpha \in \mathcal{U}(\mathrm{S})\bigcap\mathrm{R}$, então $\alpha^{-1} \in \mathrm{S} = \mathrm{I_S(R)}$ logo existem constantes $c_i \in \mathrm{R}$ para $0 \leq i \leq m$ tal que

$$\alpha^{-m} + c_1\alpha^{-m+1} + \cdots + c_m = 0$$

no que implica

$$\alpha^{-1} = -(c_1 + \cdots + c_m\alpha^{m-1}) \in \mathrm{R}[\alpha] \subseteq \mathrm{R}$$

logo $\alpha \in \mathcal{U}(\mathrm{R})$.

(c) Suponha que S seja um corpo então $\mathcal{U}(\mathrm{R}) = \mathrm{S} - \{0\}$, logo $\mathcal{U}(\mathrm{S}) \cap \mathrm{R} = \mathrm{R} - \{0\}$ donde R é corpo.

Reciprocamente se S não for corpo então S contém um ideal J não nulo em que $1_{\mathrm{S}} \notin \mathrm{J}$.

Mas pelo item (a) $1_{\mathrm{S}} \notin \mathrm{J} \cap \mathrm{S}$ que é ideal não nulo de R, consequentemente R não é corpo.

(d) Considere o homomorfismo canônico $\varphi : \mathrm{S} \longrightarrow {}^{\mathrm{S}}/_{\mathfrak{p}}$ dado por $\varphi(s) = s + \mathfrak{p}$ com $\mathfrak{p}$ ideal primo de S. Então:

(i) Se R é subanel de S então $\varphi(\mathrm{R})$ é subanel de $\varphi(\mathrm{S})$.

(ii) $\varphi(\mathrm{S}) = {}^{\mathrm{S}}/_{\mathfrak{p}}$

(iii) $\varphi(\mathrm{R}) \cong {}^{\mathrm{R}}/_{\mathrm{R} \cap \mathfrak{p}}$ "segundo o Teorema dos Isomorfismos"

(iv) $\mathrm{I}_{\varphi(\mathrm{S})}\big(\varphi(\mathrm{R})\big) = \varphi(\mathrm{S})$ "segundo $\mathrm{S} = \mathrm{I}_{\mathrm{S}}(\mathrm{R})$ e $\varphi(\mathrm{R})$ é subanel de $\varphi(\mathrm{S})$"

Portanto $\mathfrak{p}$ é ideal maximal de S se e somente se $\varphi(\mathrm{S}) = {}^{\mathrm{S}}/_{\mathfrak{p}}$ é corpo, equivalentemente a $\varphi(\mathrm{R}) \cong {}^{\mathrm{R}}/_{\mathrm{R} \cap \mathfrak{p}}$ ser corpo, significando que $\mathrm{R} \cap \mathfrak{p}$ é ideal maximal de R.

■

Corolário 06: Seja S um domínio de integridade em que $\mathrm{S} = \mathrm{I}_{\mathrm{S}}(\mathrm{R})$. Se todo ideal primo não nulo de R for maximal então todo ideal primo não nulo de S será maximal.

Demonstração:

Seja $\mathfrak{p}$ um ideal primo não nulo de S então pelo item (a) da **Proposição 07** $\mathrm{R} \cap \mathfrak{p}$ é um ideal primo não nulo de R que por hipótese é maximal.

Portanto segundo o item (d) da **Proposição 07**, $\mathfrak{p}$ é maximal de S.

■

Corolário 07: Se D um domínio em que $\mathrm{I}_{\mathrm{D}}(\mathbb{Z}) = \mathrm{D}$, então todo ideal primo não nulo de D é maximal.

Em particular se L é um corpo numérico, então todo ideal primo não nulo de $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$ é ideal maximal de $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$.

Demonstração:

Segue pelo **Corolário 06** que $\mathbb{Z}$ é um domínio de ideais principais, logo todo ideal primo não nulo é maximal. Por outro lado $\mathrm{I}_{\mathrm{I}_{\mathrm{L}}(\mathbb{Z})}(\mathbb{Z}) = \mathrm{I}_{\mathrm{L}}(\mathbb{Z})$.

■

3.2 Corpos Numéricos Quadráticos

Os corpos quadráticos são de uma importante classe de corpos numéricos que são subcorpos L de $\mathbb{C}$, ou extensões de $\mathbb{Q}$ tal que o grau é $[\mathrm{L} : \mathbb{Q}] = 2$. Há duas classificações para esses corpos, os corpos quadráticos reais e os corpos quadráticos complexos ou imaginários.

Para cada $r \in \mathbb{Q} - \{0\}$ denota-se por $\sqrt{r}, -\sqrt{r}$ as raízes do polinômio $\mathrm{P}(x) = x^2 - r \in \mathbb{Z}[x]$. Segue que para $\alpha \in \mathrm{L} - \mathbb{Q}$ tem-se que $1 < [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathrm{L} : \mathbb{Q}] = 2$ donde $\mathrm{L} = \mathbb{Q}(\alpha)$.

Assim corpos quadráticos são do tipo $\mathbb{Q}(\alpha) = \mathbb{Q} + \alpha\mathbb{Q}$ com elemento primitivo α e base $\{1, \alpha\}$ para L.

Os números $d \in \mathbb{Z} - \{0, 1\}$ que não são divisíveis por nenhum quadrado $c^2 \neq 1$ "$c \in \mathbb{Z} - \{0\}$" são chamados livre de quadrados. Em outras palavras d não é divisível por quadrado diferente de 1 ou então $d = -1$ ou $d = \pm p_1 p_2 \cdots p_n$, p_i com $1 \leq i \leq n$ primos distintos.

3.2.1 Corpos Quadráticos

Proposição 08: Os corpos quadráticos são da forma $\mathrm{L} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ com d livre de quadrados.

Demonstração:

Considere o corpo quadrático $\mathrm{K} = \mathbb{Q}(\alpha)$ para o elemento primitivo α. Então $2 = [\mathrm{K} : \mathbb{Q}] = \partial(m_\alpha)$, com $m_\alpha(x) = x^2 + bx + c \in \mathbb{Q}[x]$ o polinômio minimal de α sobre $\mathbb{Q}$. Assim:

$$\alpha^2 + b\alpha + c = 0 \Longrightarrow$$

$$\alpha = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}$$

donde

$$\mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{-b \pm \sqrt{b^2 - 4c}}{2}\right) = \mathbb{Q}\left(\sqrt{b^2 - 4c}\right)$$

Mas $b^2 - 4c \in \mathbb{Q}$ e com isso:

$$b^2 - 4c = \frac{u}{v}$$

com $u, v \in \mathbb{Z}$, $v \neq 0$ e o $mdc(u, v) = 1$.

Portanto:

$$\frac{u}{v} = \frac{uv}{v^2} \Longrightarrow \mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{\sqrt{uv}}{|v|}\right) = \mathbb{Q}\left(\sqrt{uv}\right) = \mathbb{Q}\left(\sqrt{d}\right)$$

Para verificar a unicidade, considere $d_1 \in \mathbb{Z}$ livre de quadrados tal que $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(\sqrt{d_1}\right)$ então $\sqrt{d} = u + v\sqrt{d_1}$ para algum $u, v \in \mathbb{Q}$. Por outro lado, se $uv \neq 0$, então

$$\sqrt{d_1} = \frac{d - u^2 - dv^2}{2uv} \in \mathbb{Q}$$

o que contradiz o fato de d_1 ser livre de quadrados. Logo $uv = 0$. Assim se $v = 0$ então $\sqrt{d} \in \mathbb{Q}$ o que contradiz que d é livre de quadrados.

Portanto $u = 0$ e $d = v^2 d_1$, donde $v^2 = 1$ uma vez que d, d_1 são livres de quadrados, consequentemente $d = d_1$.

■

Quando $d > 0$ o corpo quadrático é dito real e quando $d < 0$, o corpo quadrático é dito imaginário ou complexo.

Proposição 09: Aut(K) $= \{id_{\mathrm{K}}, \varphi\}$ "o conjunto dos automorfismos do corpo quadrático K", onde $\varphi : \mathrm{K} \longrightarrow \mathrm{K}$ é dado por $\varphi\left(a + b\sqrt{d}\right) = a - b\sqrt{d}$.

Demonstração:

Segue que $\varphi : \mathrm{K} \longrightarrow \mathrm{K}$ é um homomorfismo bijetivo e como K é corpo temos que $\varphi(1) = 1$.

Por outro lado, por indução matemática, para todo $m \in \mathbb{Z}$ temos que $\varphi(m) = \varphi(m-1+1) = \varphi(m-1) + \varphi(1) = m - 1 + 1 = m$.

Para todo $r \in \mathbb{Q}$ tem-se que $r = pq^{-1}$ onde $q \neq 0$, donde

$$\varphi(r) = \varphi(pq^{-1}) = \varphi(p)\varphi(q^{-1}) = \varphi(p)\varphi(q)^{-1} = \frac{\varphi(p)}{\varphi(q)} = \frac{p}{q} = r$$

Assim $\varphi\left(a + b\sqrt{d}\right) = \varphi(a) + \varphi(b)\varphi\left(\sqrt{d}\right) = a + b\varphi\left(\sqrt{d}\right)$. Mas observe que $\left(\sqrt{d}\right)^2 = d$ implica $\varphi\left(\sqrt{d}\right)^2 = \varphi(d) = d$, donde $\varphi\left(\sqrt{d}\right) = \pm\sqrt{d}$. E no caso positivo $\varphi = id_{\mathrm{K}}$.

■

Proposição 10: Seja $\mathrm{K} = \mathbb{Q}\left(\sqrt{d}\right)$ um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados. Se $\alpha = a + b\sqrt{d} \in \mathrm{I_K}(\mathbb{Z})$ então $a^2 - db^2, 2a \in \mathbb{Z}$

Demonstração:

Dado um $\alpha = a + b\sqrt{d} \in \mathrm{I_K}(\mathbb{Z})$ existem $a_0, a_1, \cdots, a_{n-1} \in \mathbb{Z}$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$.

Seja φ: K $\longrightarrow$ K o automorfismo dado por $\varphi\left(a + b\sqrt{d}\right) = a - b\sqrt{d}$. Então:

$$\varphi(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) =$$
$$\varphi(\alpha)^n + a_{n-1}\varphi(\alpha)^{n-1} + \cdots + a_1\varphi(\alpha) + a_0 = 0$$

donde $\varphi(\alpha) \in \mathrm{I_K}(\mathbb{Z})$ e com isso

$$\alpha + \varphi(\alpha) = a + b\sqrt{d} + a - b\sqrt{d} = 2a \in \mathrm{I_K}(\mathbb{Z})$$
$$\alpha\varphi(\alpha) = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = a^2 - db^2 \in \mathrm{I_K}(\mathbb{Z})$$

Por outro lado $\mathbb{Z}$ é integralmente fechado "$\mathrm{I_K}(\mathbb{Z}) = \mathbb{Z}$" e segue o desejado.

■

3.2.2 Anel dos Inteiros de Corpos Quadráticos

Proposição 11: Seja $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ o corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados.

(a) Se $d \equiv 2\ mod(4)$ ou $d \equiv 3\ mod(4)$ então:

$$\mathrm{I_K}(\mathbb{Z}) = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}]$$

(b) Se $d \equiv 1\ mod(4)$, então:

$$\mathrm{I_K}(\mathbb{Z}) = \left\{\frac{u}{2} + \frac{v}{2}\sqrt{d} : u, v \in \mathbb{Z} \text{ com mesma paridade}\right\} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

Demonstração:

(a) Seja $\alpha = a + b\sqrt{d} \in \mathrm{I_K}(\mathbb{Z})$, então segundo a **Proposição 10**, $a^2 - db^2, 2a \in \mathbb{Z}$. Por outro lado $4(a^2 - db^2) = (2a)^2 - d(2b)^2 \in \mathbb{Z}$, donde $(2a)^2 - [(2a)^2 - d(2b)^2] = d(2b)^2 \in \mathbb{Z}$.

Agora $d(2b)^2 \in \mathbb{Z}$ implica $2b \in \mathbb{Z}$, pois caso contrário existiria um primo p no denominador de $2b$ e com isso p^2 estaria no denominador de $(2b)^2$ mas como d é livre de quadrados, teríamos que $d(2b)^2 \notin \mathbb{Z}$ o que seria uma contradição.

Portanto $2a, 2b \in \mathbb{Z}$. Assim:

$$a = \frac{u}{2}, b = \frac{v}{2}$$

para $u, v \in \mathbb{Z}$.

Se v for ímpar, então $v = 2m + 1$, $m \in \mathbb{Z}$ donde $v^2 = 4m^2 + 4m + 1$ equivalentemente a $v^2 \equiv 1\ mod(4)$ e como $u^2 \equiv dv^2\ mod(4)$ tem-se que $u^2 \equiv d\ mod(4)$.

Por outro lado $u^2 \equiv 0\ mod(4)$ ou $u^2 \equiv 1\ mod(4)$ "quadrado de um inteiro" significando que $d \equiv 0\ mod(4)$ ou $d \equiv 1\ mod(4)$, o que é uma contradição. Então v é par, logo $v^2 \equiv 0\ mod(4)$ implicando $u^2 \equiv dv^2 \equiv 0\ mod(4)$ e portanto u é par, donde $a, b \in \mathbb{Z}$.

Assim $\alpha \in \mathbb{Z}[\sqrt{d}]$ donde $\mathrm{I_K}(\mathbb{Z}) \subseteq \mathbb{Z}[\sqrt{d}]$.

Agora se $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, então:

$$(\alpha - a)^2 = b^2 d \Longrightarrow$$
$$\alpha^2 - 2a\alpha + a^2 - b^2 d = 0$$

donde

$$m_\alpha(x) = x^2 - 2ax + a^2 - b^2 d$$

Portanto $\alpha \in \mathbb{Q}(\sqrt{d}) \cap \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[\sqrt{d}]$ de acordo com a **Proposição 10**, $a^2 - db^2, 2a \in \mathbb{Z}$, logo $\alpha \in \mathrm{I_K}(\mathbb{Z})$, significando que $\mathbb{Z}[\sqrt{d}] \subseteq \mathrm{I_K}(\mathbb{Z})$.

(b) Seja $\alpha \in \mathrm{I_K}(\mathbb{Z})$, então $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ e segundo a **Proposição 10** $a^2 - db^2, 2a \in \mathbb{Z}$ implicando $2a, 2b \in \mathbb{Z}$, daí para $u = 2a, v = 2b$ tem-se que:

(i) v par implica u par

(ii) v ímpar implica u ímpar

De fato:

$$v = 2m + 1 \Longrightarrow v^2 = 4m^2 + 4m + 1 \Leftrightarrow$$
$$v^2 \equiv 1\ mod(4) \Longrightarrow u^2 \equiv dv^2 \equiv d\ mod(4) \Longrightarrow$$
$$d \equiv 1\ mod(4)\ \text{“}u^2 \equiv 1\ mod(4) \text{ ou } u^2 \equiv 1\ mod(4)\text{”}$$

assim $u^2 \equiv 1\ mod(4)$ donde u é ímpar.

Portanto u e v tem a mesma paridade e com isso

$$\alpha \in \left\{\frac{u}{2} + \frac{v}{2}\sqrt{d} : u, v \in \mathbb{Z} \text{ com mesma paridade}\right\}$$

Assim:

$$\mathrm{I_K}(\mathbb{Z}) \subseteq \left\{\frac{u}{2} + \frac{v}{2}\sqrt{d} : u, v \in \mathbb{Z} \text{ com mesma paridade}\right\}$$

Por outro lado, um

$$\alpha = a + b\sqrt{d} = \frac{u}{2} + \frac{v}{2}\sqrt{d}$$

com

$$a = \frac{u}{2}, b = \frac{v}{2}$$

tem-se que se u e v são pares, então $a, b \in \mathbb{Z}$ e α é raiz de

$$m_\alpha(x) = x^2 - 2ax + a^2 - b^2 d$$

donde $\alpha \in \mathrm{I_K}(\mathbb{Z})$.

Se u, v são ímpares, então é raiz de

$$m_\alpha(x) = x^2 - ux + \frac{u^2 - dv^2}{4}$$

significando que $\alpha \in \mathrm{I_K}(\mathbb{Z})$.

Portanto de qualquer forma

$$\mathrm{I_K}(\mathbb{Z}) \subseteq \left\{\frac{u}{2} + \frac{v}{2}\sqrt{d} : u, v \in \mathbb{Z} \text{ com mesma paridade}\right\} \subseteq \mathrm{I_K}(\mathbb{Z})$$

Agora para verificar que

$$\mathrm{I_K}(\mathbb{Z}) = \mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right]$$

basta verificar que na base

$$\left\{1, \frac{1 + \sqrt{d}}{2}\right\}$$

$\mathrm{I_K}(\mathbb{Z})$ é um $\mathbb{Z} - m\acute{o}dulo$, ou seja, cada elemento de $\mathrm{I_K}(\mathbb{Z})$ é uma combinação $\mathbb{Z} - linear$ dessa base. Então:

$$\frac{u+v\sqrt{d}}{2} = (m-n) + n\left(\frac{1+\sqrt{d}}{2}\right) = \left(\frac{u}{2} - \frac{v}{2}\right) + v\left(\frac{1+\sqrt{d}}{2}\right)$$

com $u = 2m, v = 2n \in 2\mathbb{Z}$. Com isso:

$$\mathbb{Z}[\sqrt{d}] \subseteq \mathrm{I_K}(\mathbb{Z}) \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

■

3.2.3 Exemplos

Exemplo 03: Para $\mathrm{K} = \mathbb{Q}(i)$, com $i = \sqrt{-1}$, tem-se que:

$$\mathrm{I_K}(\mathbb{Z}) = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

uma vez que $d = -1 \equiv 3\ mod(4)$ haja vista o item (a) da **Proposição 11**.

Exemplo 04: Para $\mathrm{K} = \mathbb{Q}(\sqrt{6})$, segue que $6 \equiv 2\ mod(4)$ donde $\mathrm{I_K}(\mathbb{Z}) = \mathbb{Z}[\sqrt{6}]$.

Exemplo 05: Para $\mathrm{K} = \mathbb{Q}(\sqrt{-3})$, segue que $d = -3 \equiv 1\ mod(4)$ donde

$$\mathrm{I_K}(\mathbb{Z}) = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

3.3 Traço, Norma e Discriminante

As noções de norma, traço e polinômio característico de um endomorfismo $\varphi :$ $\mathrm{E} \longrightarrow \mathrm{E}$ com E um $\mathrm{A} - módulo$ livre de posto finito n, A um anel, são feitas de maneira semelhante, como se introduz na Álgebra Linear, ou seja dado um corpo K, $\mathrm{T} : \mathrm{V} \longrightarrow \mathrm{V}$ um operador linear, V um $\mathrm{K} - espaço$ vetorial de dimensão finita $n = dim_{\mathrm{K}}(\mathrm{V})$, existe uma matriz quadrada $n \times n$ associada a transformação T.

O conceito de discriminante também está ligado a determinante e ao traço de matrizes e é importante para verificar que $\mathrm{I_K}(\mathbb{Z})$ é um $\mathbb{Z}-$*módulo* livre onde K é corpo numérico.

3.3.1 Norma e Traço

Considere $\mathrm{R} \subseteq \mathrm{S}$ anéis, tal que S é $\mathrm{R}-$*módulo* livre de posto n. Sejam $\Gamma = \{e_1, \cdots, e_n\}$ uma base de S sobre R e $\varphi : \mathrm{S} \longrightarrow \mathrm{S}$ um homomorfismo. Então existem $a_{ij} \in \mathrm{R}$, $1 \leq i, j \leq n$ tal que:

$$\begin{cases} \varphi(e_1) = a_{11}e_1 + \cdots + a_{1n}e_n \\ \varphi(e_2) = a_{21}e_1 + \cdots + a_{2n}e_n \\ \vdots \\ \varphi(e_n) = a_{n1}e_1 + \cdots + a_{nn}e_n \end{cases} \Leftrightarrow \begin{bmatrix} \varphi(e_1) \\ \varphi(e_2) \\ \vdots \\ \varphi(e_n) \end{bmatrix} = \begin{bmatrix} a_{11}\, a_{12} \ldots a_{1n} \\ a_{21}\, a_{22} \ldots a_{2n} \\ \vdots \quad \vdots \quad \ddots \quad \vdots \\ a_{n1} a_{n2} \cdots a_{nn} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}$$

O traço a norma e o polinômio característico de φ são definidos respectivamente por:

$$\mathrm{Tr}_{(\mathrm{S|R})}(\varphi) = \sum_{i=1}^{n} a_{ii}$$

$$\mathcal{N}_{(\mathrm{S|R})}(\varphi) = det\big(a_{ij}\big)$$

$$\mathrm{P}_{(\mathrm{S|R})}(x) = det(xid_n - \varphi) = det\big(x\delta_{ij} - a_{ij}\big)$$

onde id_n é a matriz identidade.

Observações 01:

(i) Os valores definidos são independentes da base $\Gamma = \{e_1, \cdots, e_n\}$.

(ii) Como $\mathrm{T}r(\mathrm{X} + \mathrm{Y}) = \mathrm{T}r(\mathrm{X}) + \mathrm{T}r(\mathrm{Y})$ e o $det(\mathrm{XY}) = det(\mathrm{X})det(\mathrm{Y})$, onde $\mathrm{X}, \mathrm{Y} \in \mathrm{M}_n(\mathrm{R})$ são matrizes, temos que:

$$\mathrm{Tr}_{(\mathrm{S|R})}(\varphi + \psi) = \mathrm{Tr}_{(\mathrm{S|R})}(\varphi) + \mathrm{Tr}_{(\mathrm{S|R})}(\psi)$$

$$\mathcal{N}_{(\mathrm{S|R})}(\varphi \circ \psi) = \mathcal{N}_{(\mathrm{S|R})}(\varphi) \cdot \mathcal{N}_{(\mathrm{S|R})}(\psi)$$

quando $\varphi \circ \psi$ está bem definida.

(iii) $\mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\varphi), \mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\varphi) \in \mathrm{R}$

(iv) O polinômio característico é um polinômio mônico com coeficientes em R e

$$det(xid_n - \varphi) = x^n - \mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\varphi)x^{n-1} + \cdots + (-1)^n \mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\varphi)$$

Para o endomorfismo multiplicativo $\varphi_\alpha : \mathrm{S} \longrightarrow \mathrm{S}$ dado $\varphi_\alpha(x) = \alpha x$ com $\alpha \in \mathrm{S}$ define-se:

(a) O traço de $\alpha \in \mathrm{S}$ relativo a R como sendo, o traço da matriz associada ao endomorfismo φ_α

$$\mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\alpha) = \mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\varphi_\alpha)$$

(b) A norma de $\alpha \in \mathrm{S}$ relativo a R, como sendo, o determinante da matriz associada ao endomorfismo φ_α

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\alpha) = \mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\varphi_\alpha)$$

(c) O polinômio característico de $\alpha \in \mathrm{S}$ relativo a R, como sendo o polinômio característico do endomorfismo φ_α denotado por

$$\mathrm{P}_{(\alpha,\mathrm{S}|\mathrm{R})}(x) = det(xid_n - \varphi_\alpha)$$

Observação 02: Dados os anéis $\mathrm{R} \subseteq \mathrm{S}$ tais que S é $\mathrm{R} - módulo$ é livre de posto finito. Para qualquer $x \in \mathrm{S}$, $\alpha, \beta \in \mathrm{S}$, $\delta \in \mathrm{R}$ tem-se que:

$$\begin{aligned}
&(\varphi_\alpha + \varphi_\beta)(x) = \alpha x + \beta x = (\alpha + \beta)x = \varphi_{\alpha+\beta}(x) \\
&(\varphi_\alpha \circ \varphi_\beta)(x) = \varphi_\alpha(\beta x) = \alpha(\beta x) = \varphi_{\alpha\beta}(x) \\
&\varphi_{\delta\alpha}(x) = \delta\alpha x = \delta\varphi_\alpha(x)
\end{aligned}$$

Também a matriz de φ_α em relação a base $\Gamma = \{e_1, \cdots, e_n\}$ de S sobre R é a matriz diagonal

$$a_{ij} = \begin{cases} \alpha, \text{para } i = j \\ 0, \text{para } i \neq j \end{cases}$$

ou seja:

$$\begin{cases} \varphi_\alpha(e_1) = \alpha e_1 = \alpha e_1 + 0e_1 + \cdots + 0e_n \\ \varphi_\alpha(e_2) = \alpha e_2 = 0e_1 + \alpha e_2 + \cdots + 0e_n \\ \vdots \\ \varphi_\alpha(e_n) = \alpha e_n = 0e_1 + 0e_1 + \cdots + \alpha e_n \end{cases} \Leftrightarrow \begin{bmatrix} \varphi_\alpha(e_1) \\ \varphi_\alpha(e_2) \\ \vdots \\ \varphi_\alpha(e_n) \end{bmatrix} = \begin{bmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}$$

Proposição 12: Dados os anéis R ⊆ S tais que S é R − *módulo* é livre de posto finito n. Se $\alpha, \beta \in$ S, $\delta \in$ R então:

$(i)\ \mathrm{Tr}_{(\mathrm{S|R})}(\alpha + \beta) = \mathrm{Tr}_{(\mathrm{S|R})}(\alpha) + \mathrm{Tr}_{(\mathrm{S|R})}(\beta)$

$(ii)\ \mathrm{Tr}_{(\mathrm{S|R})}(\delta\alpha) = \delta \mathrm{Tr}_{(\mathrm{S|R})}(\alpha)$

$(iii)\ \mathrm{Tr}_{(\mathrm{S|R})}(\delta) = n\delta$

$(iv)\ \mathcal{N}_{(\mathrm{S|R})}(\alpha\beta) = \mathcal{N}_{(\mathrm{S|R})}(\alpha)\mathcal{N}_{(\mathrm{S|R})}(\beta)$

$(v)\ \mathcal{N}_{(\mathrm{S|R})}(\delta) = \delta^n$

$(vi)\ \mathcal{N}_{(\mathrm{S|R})}(\delta\alpha) = \delta^n \mathcal{N}_{(\mathrm{S|R})}(\alpha)$

Demonstração:

(i)

$$\mathrm{Tr}_{(\mathrm{S|R})}(\alpha + \beta) =$$
$$\mathrm{Tr}_{(\mathrm{S|R})}(\varphi_{\alpha+\beta}) =$$
$$\mathrm{Tr}_{(\mathrm{S|R})}(\varphi_\alpha + \varphi_\beta) =$$
$$\mathrm{Tr}_{(\mathrm{S|R})}(\varphi_\alpha) + \mathrm{Tr}_{(\mathrm{S|R})}(\varphi_\beta) =$$
$$\mathrm{Tr}_{(\mathrm{S|R})}(\alpha) + \mathrm{Tr}_{(\mathrm{S|R})}(\beta)$$

(ii)

$$\mathrm{Tr}_{(\mathrm{S|R})}(\delta\alpha) =$$
$$\mathrm{Tr}_{(\mathrm{S|R})}(\varphi_{\delta\alpha}) =$$

$$\mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\delta\varphi_\alpha) =$$

$$\delta\mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\varphi_\alpha) =$$

$$\mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\alpha)$$

(iii)

$$\mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\delta) =$$

$$\mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\varphi_\delta) = n\delta$$

(iv)

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\alpha\beta) =$$

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}\left(\varphi_{\alpha\beta}\right) =$$

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}\left(\varphi_\alpha \circ \varphi_\beta\right) =$$

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\varphi_\alpha) \cdot \mathcal{N}_{(\mathrm{S}|\mathrm{R})}\left(\varphi_\beta\right) =$$

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\alpha)\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\beta)$$

(v)

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\delta) =$$

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\varphi_\delta) = \delta^n$$

(vi)

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\delta\alpha) =$$

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\varphi_{\delta\alpha}) =$$

$$\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\delta\varphi_\alpha) =$$

$$\delta^n\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\varphi_\alpha) =$$

$$\delta^n\mathcal{N}_{(\mathrm{S}|\mathrm{R})}(\alpha)$$

■

Proposição 13: Sejam K um corpo finito ou de característica nula, L uma extensão algébrica de K de grau $n = [\mathrm{L} : \mathrm{K}]$, $\alpha \in \mathrm{L}$. Se $\alpha_1, \alpha_2, \cdots, \alpha_n$ são raízes do polinômio minimal de α sobre K. Então:

$(a)\ \mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha) = \left[\mathrm{L} : \mathrm{K}[\alpha]\right] \cdot \mathrm{Tr}_{(\mathrm{K}[\alpha]|\mathrm{K})}(\alpha)$

$(b)\ \mathcal{N}_{(\mathrm{L}|\mathrm{K})}(\alpha) = \left(\mathcal{N}_{(\mathrm{K}[\alpha]|\mathrm{K})}(\alpha)\right)^{[\mathrm{L}:\mathrm{K}[\alpha]]}$

(c) O polinômio característico $\mathrm{P}_{(\alpha,\mathrm{L}|\mathrm{K})}(x)$ é a $\left[\mathrm{L}:\mathrm{K}[\alpha]\right]-$ésima potência do polinômio minimal $m_\alpha(x)$ de α sobre K.

Demonstração:

Primeiramente consideremos o caso particular, $\mathrm{L}=\mathrm{K}[\alpha]$ ou seja, quando α é elemento primitivo de L sobre K.

Considerando o polinômio minimal $m_\alpha(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ de α sobre K onde $a_i\in\mathrm{K}$ para $0\leq i\leq n$, tem-se:

$$\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0\Longrightarrow$$
$$\alpha^n=-a_{n-1}\alpha^{n-1}-\cdots-a_1\alpha-a_0$$

Por outro lado L é K − isomorfo a $\mathrm{K}[x]\Big/_{\langle m_\alpha(x)\rangle}$ e $\Gamma=\{1,\alpha,\cdots,\alpha^{n-1}\}$ é uma base de L sobre K. Então:

$$\varphi_\alpha(1)=\alpha=0\cdot1+1\cdot\alpha+0\cdot\alpha^2+\cdots+0\cdot\alpha^{n-1}$$
$$\varphi_\alpha(\alpha)=\alpha^2=0\cdot1+0\cdot\alpha+1\cdot\alpha^2+\cdots+0\cdot\alpha^{n-1}$$
$$\vdots$$
$$\varphi_\alpha(\alpha^{n-2})=\alpha^{n-1}=0\cdot1+0\cdot\alpha+\cdots+1\cdot\alpha^{n-2}+0\cdot\alpha^{n-1}$$
$$\varphi_\alpha(\alpha^{n-1})=\alpha^n=-a_0\cdot1-a_1\alpha-\cdots-a_{n-2}\alpha^{n-2}-a_{n-1}\alpha^{n-1}$$

e

$$\mathrm{M}=\begin{bmatrix}0&1&0&\cdots&0&0\\0&0&1&\cdots&0&0\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&\cdots&0&1\\-a_0&-a_1&-a_2&\cdots&-a_{n-2}&-a_{n-1}\end{bmatrix}$$

é a matriz associada ao endomorfismo φ_α em relação a Γ. Assim:

$$xid_n-\mathrm{M}=\begin{bmatrix}x&-1&0&\cdots&0&0\\0&x&-1&\cdots&0&0\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&\cdots&x&-1\\a_0&a_1&a_2&\cdots&a_{n-2}&x+a_{n-1}\end{bmatrix}$$

cujo polinômio característico é $\mathrm{P}_{(\alpha,\mathrm{L}|\mathrm{K})}(x) = det(xid_n - \mathrm{M})$ e é igual ao polinômio minimal $m_\alpha(x)$ de α, donde

$$det(xid_n - \mathrm{M}) =$$
$$x^n - \mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\varphi_\alpha)x^{n-1} + \cdots + (-1)^n \mathcal{N}_{(\mathrm{L}|\mathrm{K})}(\varphi_\alpha) =$$
$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

e com isso $\mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha) = -a_{n-1}$ e $\mathcal{N}_{(\mathrm{L}|\mathrm{K})}(\alpha) = (-1)^n a_0$. Mas como α é um elemento primitivo, tem-se:

$$m_\alpha(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) =$$
$$x^n - \left(\sum_{i=1}^{n} \alpha_i\right)x^{n-1} + \cdots + a_1 x + (-1)^n \prod_{i=1}^{n} \alpha_i$$

resultando

$$\mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha) = \sum_{i=1}^{n} \alpha_i$$
$$\mathcal{N}_{(\mathrm{L}|\mathrm{K})}(\alpha) = (-1)^n \prod_{i=1}^{n} \alpha_i$$

Agora vamos ao caso geral, tomando $\alpha \in \mathrm{L}$ arbitrário, algébrico sobre K, tem-se que $\mathrm{K} \subseteq \mathrm{K}[\alpha] \subseteq \mathrm{L}$. Então $[\mathrm{L} : \mathrm{K}] = \big[\mathrm{L} : \mathrm{K}[\alpha]\big] \cdot [\mathrm{K}[\alpha] : \mathrm{K}]$ com $\big[\mathrm{L} : \mathrm{K}[\alpha]\big] = r$, $[\mathrm{K}[\alpha] : \mathrm{K}] = q$ e $n = qr$.

Agora se $\Gamma_\alpha = \{\alpha_1, \alpha_2, \cdots, \alpha_r\}$ é uma base de $\mathrm{K}[\alpha]$ sobre K e $\Gamma_\beta = \{\beta_1, \beta_2, \cdots, \beta_q\}$ uma base de L sobre $\mathrm{K}[\alpha]$. Então $\Gamma_{\alpha\beta} = \{\alpha_1\beta_1, \alpha_2\beta_2, \cdots, \alpha_r\beta_q\}$ é uma base de L sobre K. Considere a matriz $\mathrm{M} = (a_{ij})$ do endomorfismo $\sigma_\alpha : \mathrm{K}[\alpha] \longrightarrow \mathrm{K}[\alpha]$ sobre K em relação a base. Assim:

$$\sigma_\alpha(\alpha_i) = \alpha\alpha_i = \sum_{t=1}^{r} a_{it}\alpha_t \Longrightarrow$$
$$\sigma_\alpha(\alpha_i\beta_j) = \alpha(\alpha_i\beta_j) = (\alpha\alpha_i)\beta_j =$$
$$\left(\sum_{t=1}^{r} a_{it}\alpha_t\right)\beta_j = \sum_{t=1}^{r} a_{it}(\alpha_t\beta_j)$$

com $1 \leq j \leq q$. Logo:

$$\begin{cases} \alpha\alpha_1\beta_1 = a_{11}\alpha_1\beta_1 + a_{11}\alpha_1\beta_1 + \cdots + a_{1r}\alpha_r\beta_1 \\ \alpha\alpha_2\beta_1 = a_{21}\alpha_1\beta_1 + a_{22}\alpha_2\beta_1 + \cdots + a_{2r}\alpha_r\beta_1 \\ \vdots \\ \alpha\alpha_r\beta_1 = a_{r1}\alpha_1\beta_1 + a_{r2}\alpha_2\beta_1 + \cdots + a_{rr}\alpha_r\beta_1 \end{cases}$$

Então reordenando a base $\Gamma_{\alpha\beta}$ de L sobre K de modo que a matriz do endomorfismo $\sigma_\alpha : \mathrm{L}[\alpha] \longrightarrow \mathrm{L}[\alpha]$ seja a matriz $n \times n$ em bloco

$$\mathrm{N} = \begin{bmatrix} \mathrm{M} & 0 & \cdots & 0 \\ 0 & \mathrm{M} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathrm{M} \end{bmatrix}$$

resulta que

$$xid_n - \mathrm{N} = \begin{bmatrix} xid_n - \mathrm{M} & 0 & \cdots & 0 \\ 0 & xid_n - \mathrm{M} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & xid_n - \mathrm{M} \end{bmatrix}$$

implicando

$$det(xid_n - \mathrm{N}) = det(xid_n - \mathrm{M})^r \Leftrightarrow$$

$$\mathrm{P}_{(\alpha,\mathrm{L}|\mathrm{K})}(x) = \left[\mathrm{P}_{(\alpha,\mathrm{K}[\alpha]|\mathrm{K})}(x)\right]^r = m_\alpha(x)^r$$

■

Proposição 14: Sejam A um domínio, $\mathrm{K}_f(\mathrm{A})$ seu corpo de frações de característica nula. Se L é uma extensão finita de $\mathrm{K}_f(\mathrm{A})$ e $\alpha \in \mathrm{L} \cap \mathrm{I}_\mathrm{L}(\mathrm{A})$, então os coeficientes do polinômio característico $\mathrm{P}_{\left(\alpha,\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(x)$ são inteiros sobre A. Em particular $\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha), \mathcal{N}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha) \in \mathrm{I}_\mathrm{L}(\mathrm{A})$.

Demonstração:

Segundo a **Proposição 13**, o polinômio característico de α é da forma

$$\mathrm{P}_{\left(\alpha,\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

onde $\alpha_1, \alpha_2, \cdots, \alpha_n$ são raízes do polinômio $m_\alpha(x)$ minimal de α.

Então os coeficientes de $P_{\left(\alpha,L|K_f(A)\right)}(x)$ são somas e produtos dos α_i. Portanto basta verificar que cada α_i é inteiro sobre A.

Segundo a Teoria dos Corpos, existem n $K_f(A) -$ isomorfismos

$$\sigma_i : K_f(A)[\alpha] \longrightarrow K_f(A)[\alpha_i]$$

tal que $\sigma_i(\alpha) = \alpha_i$ com $i = 1, \cdots, n$. Mas como $\alpha \in I_L(A)$, α admite a equação de dependência inteira

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

com $\alpha_i \in A$, donde

$$\sigma_i(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) = 0 \Leftrightarrow$$
$$\sigma_i(\alpha)^n + a_{n-1}\sigma_i(\alpha)^{n-1} + \cdots + a_1\sigma_i(\alpha) + a_0 = 0 \Longrightarrow$$
$$\alpha_i{}^n + a_{n-1}\alpha_i{}^{n-1} + \cdots + a_1\alpha_i + a_0 = 0$$

e assim $\alpha_i \in I_L(A)$ com $i = 1, 2, \cdots, n$.

■

Corolário 08: Se A é um domínio integralmente fechado, então os coeficientes do polinômio característico de α são elementos de A. Em particular $Tr_{\left(L|K_f(A)\right)}(\alpha)$, $\mathcal{N}_{\left(L|K_f(A)\right)}(\alpha) \in A$.

Demonstração:

Basta notar que $I_L(A) = A$ e usar a **Proposição 14.**

■

Proposição 15: Sejam A um anel integralmente fechado, $K_f(A)$ seu corpo de frações, L uma extensão finita de $K_f(A)$ com grau $n = [L : K_f(A)]$ e $I_L(A)$ o fecho inteiro de A em L. Sejam $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ uma base de L sobre $K_f(A)$ onde $det\left(Tr_{\left(L|K_f(A)\right)}(\alpha_i\alpha_j)\right) \neq 0$ e $\alpha \in L$. Se então $Tr_{\left(L|K_f(A)\right)}(\alpha\beta) = 0$ para todo $\beta \in L$ então $\alpha = 0$.

Demonstração:

Segue que $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$ com $\alpha_i \in \mathrm{K}_f(\mathrm{A})$ e $i = 1, 2, \cdots, n$.

Como por hipótese $\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha\beta) = 0$ para todo $\beta \in \mathrm{L}$ em particular $\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha\alpha_j) = 0$ para $j = 1, 2, \cdots, n$ segue

$$0 = \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha\alpha_j) = \sum_{i=1}^{n} a_i \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_i\alpha_j)$$

Na forma matricial fica:

$$\begin{bmatrix} \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_1\alpha_1) & \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_1\alpha_n) \\ \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_2\alpha_1) & \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_2\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_n\alpha_1) & \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_n\alpha_2) & \cdots & \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_n\alpha_n) \end{bmatrix} . \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n-1} \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

Por outro lado $det\left(\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_i\alpha_j)\right) \neq 0$ significando que $a_1 = a_2 = \cdots = a_n = 0$. Portanto $\alpha = 0$.

■

Dada uma extensão L|K de corpos de grau $n = [\mathrm{L} : \mathrm{K}]$. A aplicação $\mathrm{S}_\alpha : \mathrm{L} \longrightarrow \mathrm{K}$ definida por $\mathrm{S}_\alpha(\beta) = \mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha\beta)$ é $\mathrm{K}-$homorfismo pois

$$\mathrm{S}_\alpha(\beta + \lambda) =$$
$$\mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha(\beta + \lambda)) =$$
$$\mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha\beta + \alpha\lambda) =$$
$$\mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha\beta) + \mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha\lambda) =$$
$$\mathrm{S}_\alpha(\beta) + \mathrm{S}_\alpha(\lambda)$$

e

$$\mathrm{S}_\alpha(\delta\beta) =$$
$$\mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha\delta\beta) =$$

$$\delta \mathrm{Tr}_{(\mathrm{L}|\mathrm{K})}(\alpha\beta) =$$
$$\delta \mathrm{S}_{\alpha}(\beta)$$

para todo $\beta, \lambda, \delta \in \mathrm{L}$.

Denota-se e define $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L} : \mathrm{K}) = \{f : \mathrm{L} \longrightarrow \mathrm{H}, \mathrm{K} - \text{homorfismo}\}$.

Corolário 09: Sejam A um anel integralmente fechado, $\mathrm{K}_f(\mathrm{A})$ o corpo de frações, L|K uma extensão de grau n e $\mathrm{I}_{\mathrm{L}}(\mathrm{A})$ o fecho inteiro de A em L. Sejam $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ uma base de L sobre $\mathrm{K}_f(\mathrm{A})$ onde $det\left(\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha_i\alpha_j)\right) \neq 0$ e $\alpha \in \mathrm{L}$. Se $\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha\beta) = 0$ para todo $\beta \in \mathrm{L}$ então aplicação

$$\rho : \mathrm{L} \longrightarrow \mathrm{Hom}_{\mathrm{K}_f(\mathrm{A})}\left(\mathrm{L}: \mathrm{K}_f(\mathrm{A})\right)$$

com $\mathrm{S}_{\alpha}(\beta) = \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha\beta)$ é um isomorfismo.

Demonstração:

De fato ρ é um homomorfismo porque para todo $\lambda, \delta \in \mathrm{L}$ e $a \in \mathrm{K}_f(\mathrm{A})$ segue que

$$\rho(\lambda + \delta)(\beta) =$$
$$\mathrm{S}_{\lambda+\delta}(\beta) =$$
$$\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}\big((\lambda + \delta)\beta\big) =$$
$$\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\lambda\beta + \delta\beta) =$$
$$\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\lambda\beta) + \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\delta\beta) =$$
$$\mathrm{S}_{\lambda}(\beta) + \mathrm{S}_{\delta}(\beta) =$$
$$\rho(\lambda)(\beta) + \rho(\delta)(\beta)$$

e

$$\rho(a\lambda)(\beta) =$$
$$\mathrm{S}_{a\lambda}(\beta) =$$
$$\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(a\lambda\beta) =$$
$$a\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\lambda\beta) =$$

$$aS_{\lambda}(\beta) =$$
$$a\rho(\lambda)(\beta)$$

Para um $\alpha \in \mathrm{L}$ tal que $\rho(\alpha) = 0$, segue que $\rho(\alpha)(\beta) = S_{\alpha}(\beta) = \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha\beta) = 0$ para todo $\beta \in \mathrm{L}$, donde $\alpha = 0$ segundo a **Proposição 15**, logo ρ é injetiva.

Por outro lado ρ é sobrejetiva uma vez que

$$dim_{\mathrm{K}_f(\mathrm{A})}(\mathrm{L}) = dim_{\mathrm{K}_f(\mathrm{A})}\left(\mathrm{Hom}_{\mathrm{K}_f(\mathrm{A})}\left(\mathrm{L}: \mathrm{K}_f(\mathrm{A})\right)\right)$$

Portanto ρ é isomorfismo.

■

Proposição 16: Seja A um anel integralmente fechado $\mathrm{K}_f(\mathrm{A})$ seu corpo de frações, $\mathrm{L}|\mathrm{K}_f(\mathrm{A})$ uma extensão finita de grau n e $\mathrm{I}_{\mathrm{L}}(\mathrm{A})$ o fecho inteiro de A em L. Então:

(a) $\mathrm{I}_{\mathrm{L}}(\mathrm{A})$ é um $\mathrm{A} - submódulo$ de um $\mathrm{A} - módulo$ livre.

(b) Se A é domínio principal, então $\mathrm{I}_{\mathrm{L}}(\mathrm{A})$ é um $\mathrm{A} - módulo$ livre de posto n.

(c) Se A é um domínio principal e $\mathrm{J} \subseteq \mathrm{I}_{\mathrm{L}}(\mathrm{A})$ é um ideal, então J é um $\mathrm{A} - módulo$ livre de posto n.

Demonstração:

(a) Considere $\{e_1, e_2, \cdots, e_n\}$ uma base de L sobre $\mathrm{K}_f(\mathrm{A})$. Como toda extensão finita é algébrica tem-se que cada e_i é algébrico sobre $\mathrm{K}_f(\mathrm{A})$ com $1 \leq i \leq n$. Então:

$$a_n e_i^n + a_{n-1} e_i^{n-1} + \cdots + a_0 = 0$$

Suponhamos que $a_n \neq 0$ e multiplicando a equação de dependência inteira acima por a_n^{n-1} resulta:

$$a_n^{n-1}(a_n e_i^n + a_{n-1}e_i^{n-1} + \cdots + a_0) = 0 \Leftrightarrow$$
$$(a_n e_i)^n + a_{n-1}(a_n e_i)^{n-1} + \cdots + a_n^{n-1}a_0 = 0$$

donde $a_n e_i$ é inteiro sobre A.

Tomando $\varepsilon_i = a_n e_i \in \mathrm{I_L(A)}$, com $1 \leq i \leq n$, vamos verificar que $\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n\}$ é uma base de L sobre $\mathrm{K}_f(\mathrm{A})$.

Para isso sejam $b_1, b_2, \cdots, b_n \in \mathrm{A}$ tais que $b_1\varepsilon_1 + b_2\varepsilon_2 + \cdots + b_n\varepsilon_n = 0$. Assim $b_1 a_n e_1 + b_2 a_n e_2 + \cdots + b_n a_n e_n = 0$ e como $\{e_1, e_2, \cdots, e_n\}$ é uma base de L sobre $\mathrm{K}_f(\mathrm{A})$, segue que $b_i a_n = 0$ com $1 \leq i \leq n$, donde $b_i = 0$.

Logo $\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n\}$ é um conjunto linearmente independente com n elementos sendo uma base de L sobre $\mathrm{K}_f(\mathrm{A})$. Mas de acordo com o **Corolário 09** existe a base dual $\{y_1, y_2, \cdots, y_n\}$ tal que

$$\rho(\varepsilon_i)(y_j) = \mathrm{S}_{\varepsilon_i}(y_j) = \mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(y_j\varepsilon_i) = \delta_{ij} = \begin{cases} 0, i \neq j \\ 1, i = j \end{cases}$$

para $i, j = 1, 2, \cdots, n$.

Por outro lado se $\alpha \in \mathrm{I_L(A)}$ então $\alpha\varepsilon_i \in \mathrm{I_L(A)}$ para $1 \leq i \leq n$ e pelo **Corolário 08** temos que $\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha\varepsilon_i) \in \mathrm{A}$ para $1 \leq i \leq n$.

Mas também para $c_1, c_2, \cdots, c_n \in \mathrm{K}_f(\mathrm{A})$ tal que $\alpha = c_1y_1 + c_2y_2 + \cdots + c_ny_n$ resulta:

$$\alpha\varepsilon_i = c_1y_1\varepsilon_i + c_2y_2\varepsilon_i + \cdots + c_ny_n\varepsilon_i \Longrightarrow$$
$$\mathrm{Tr}_{\left(\mathrm{L}|\mathrm{K}_f(\mathrm{A})\right)}(\alpha\varepsilon_i) = c_1\delta_{i1} + c_2\delta_{i2} + \cdots + c_n\delta_{in} = c_i \in \mathrm{A}$$

para $1 \leq i \leq n$.

Portanto todo $\alpha \in \mathrm{I_L(A)}$ é combinação linear da base $\{y_1, y_2, \cdots, y_n\}$ sobre A, o que significa que $\mathrm{I_L(A)}$ é um submódulo de um $\mathrm{A} - m\acute{o}dulo$ livre gerado por $\{e_1, e_2, \cdots, e_n\}$.

(b) Pela **Proposição 24 do Capítulo 2** um submódulo de um $\mathrm{A} - m\acute{o}dulo$ livre é também livre e possui posto menor ou igual a n. Mas de acordo com o item (a) $\mathrm{I_L(A)}$ possui uma base com n elementos de L sobre $\mathrm{K}_f(\mathrm{A})$. Assim $\mathrm{I_L(A)}$ tem posto n.

(c) Pelo item (b), $\mathrm{I_L(A)}$ é um $\mathrm{A}-$*módulo* livre de posto n. Dada uma base $\{e_1, e_2, \cdots, e_n\}$ de $\mathrm{I_L(A)}$ e $\alpha \in \mathrm{J} - \{0\}$ tem-se que $\alpha e_1, \alpha e_2, \cdots, \alpha e_n \in \mathrm{J}$ e são lineamente independentes sobre A, pois se $a_1\alpha e_1 + a_2\alpha e_2 + \cdots + a_n\alpha e_n = 0$ com $a_i \in \mathrm{A}$, então $a_i\alpha = 0$ para $i = 1, 2, \cdots, n$. Mas como A é domínio principal, resulta $a_i = 0$ para $i = 1, 2, \cdots, n$.

■

Proposição 17: Sejam A um anel Noetheriano, integralmente fechado, $\mathrm{K}_f(\mathrm{A})$ seu corpo de frações, $\mathrm{L}|\mathrm{K}_f(\mathrm{A})$ uma extensão finita de grau n e $\mathrm{I_L(A)}$ o fecho inteiro de A em L. Então $\mathrm{I_L(A)}$ é um $\mathrm{A}-$*módulo* finitamente gerado e $\mathrm{I_L(A)}$ é anel Noetheriano.

Demonstração:

De acordo com a **Proposição 16**, $\mathrm{I_L(A)}$ é $\mathrm{A}-$*submódulo* de um $\mathrm{A}-$*módulo* livre de posto n.

Segundo o **Corolário 03 do Capítulo 2**, $\mathrm{I_L(A)}$ é $\mathrm{A}-$*módulo* Noetheriano finitamente gerado.

Por outro lado, os ideais de $\mathrm{I_L(A)}$ são $\mathrm{A}-$*submódulos* de $\mathrm{I_L(A)}$ e satisfazem a condição maximalidade de cadeia ascendente. Portanto $\mathrm{I_L(A)}$ é Noetheriano.

■

3.3.2 Discriminante

Considere $\mathrm{R} \subseteq \mathrm{S}$ anéis, tal que S é $\mathrm{R}-$*módulo* livre de posto finito n. Dado uma $n-upla$ $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathrm{S}^n = \mathrm{S} \times \mathrm{S} \times \cdots \times \mathrm{S}$ define-se seu discriminante e denota-se por:

$$disc_{(\mathrm{S}|\mathrm{R})}(\alpha_1, \alpha_2, \cdots, \alpha_n) = det\left(\mathrm{Tr}_{(\mathrm{S}|\mathrm{R})}(\alpha_i\alpha_j)\right)$$

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

Proposição 18: Sejam $\mathrm{R} \subseteq \mathrm{S}$ anéis, tais que S é $\mathrm{R}-$*módulo* livre de posto n. Dado a $n-upla$ $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathrm{S}^n$, se $(\beta_1, \beta_2, \cdots, \beta_n) \in \mathrm{S}^n$ tais que

$$\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$$

com $a_{ij} \in$ R, então:

$$disc_{(\mathrm{S|R})}(\beta_1, \beta_2, \cdots, \beta_n) = \left[det\left(a_{ij}\right)\right]^2 \cdot disc_{(\mathrm{S|R})}(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

Demonstração:

Segue por definição que

$$disc_{(\mathrm{S|R})}(\beta_1, \beta_2, \cdots, \beta_n) = det\left(\mathrm{Tr}_{(\mathrm{S|R})}(\beta_r \beta_s)\right)$$

onde

$$\beta_r = \sum_{i=1}^{n} a_{ri}\alpha_i \text{ e } \beta_s = \sum_{i=1}^{n} a_{sj}\alpha_j$$

implicando

$$\beta_r \beta_s = \sum_{j,i=1}^{n} \left(a_{ri}a_{sj}\right) \alpha_i \alpha_j$$

com $a_{ri}a_{sj} \in$ R. Então:

$$\mathrm{Tr}_{(\mathrm{S|R})}(\beta_r \beta_s) = \mathrm{Tr}_{(\mathrm{S|R})}\left(\sum_{i,j=1}^{n} \left(a_{ri}a_{sj}\right) \alpha_i \alpha_j\right) = \sum_{j,i=1}^{n} a_{ri}a_{sj}\mathrm{Tr}_{(\mathrm{S|R})}\left(\alpha_i \alpha_j\right)$$

Em forma matricial tem-se:

$$\left(\mathrm{Tr}_{(\mathrm{S|R})}(\beta_r \beta_s)\right) = (a_{ri}) \left(\mathrm{Tr}_{(\mathrm{S|R})}\left(\alpha_i \alpha_j\right)\right) \left(a_{sj}\right)^t$$

onde $\left(a_{sj}\right)^t$ representa a matriz transposta de $\left(a_{sj}\right)$. Portanto

$$disc_{(\mathrm{S|R})}(\beta_1, \beta_2, \cdots, \beta_n) = det\left(\mathrm{Tr}_{(\mathrm{S|R})}(\beta_r \beta_s)\right) =$$
$$det(a_{ri}) det\left(\mathrm{Tr}_{(\mathrm{S|R})}\left(\alpha_i \alpha_j\right)\right) det\left(a_{sj}\right)^t =$$
$$\left[det\left(a_{ij}\right)\right]^2 \cdot disc_{(\mathrm{S|R})}(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

■

O significado da proposição anterior é que a matriz que expressa uma base em termo da outra possui inversa.

Corolário 10: Sejam R ⊆ S anéis, tais que S é um R − *módulo* livre de posto finito n e R um domínio. Se $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ e $\{\beta_1, \beta_2, \cdots, \beta_n\}$ são bases de S, então $disc_{(S|R)}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ e $disc_{(S|R)}(\beta_1, \beta_2, \cdots, \beta_n)$ são associados ou ambos com determinantes nulos.

Demonstração:

Sendo $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, $\{\beta_1, \beta_2, \cdots, \beta_n\}$ bases de S, segue que existem elementos $a_{ij} \in$ R tais que

$$\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i$$

para $j = 1, 2, \cdots, n$ e de acordo com a **Proposição 18**

$$disc_{(S|R)}(\beta_1, \beta_2, \cdots, \beta_n) = \left[det\left(a_{ij}\right)\right]^2 \cdot disc_{(S|R)}(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

Por outro lado $\left(a_{ij}\right)$ é matriz inversível, logo $det\left(a_{ij}\right)$ é uma unidade de A. Logo $disc_{(S|R)}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ e $disc_{(S|R)}(\beta_1, \beta_2, \cdots, \beta_n)$ são associados ou ambos com determinantes nulos.

■

Proposição 19: Sejam R ⊆ S anéis, tais que S é R − *módulo* livre de posto finito n e R um domínio. Se o conjunto $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ de elementos em S é linearmente dependente sobre R, então:

$$disc_{(S|R)}(\alpha_1, \alpha_2, \cdots, \alpha_n) = 0$$

Demonstração:

Sendo $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ linearmente dependente sobre R, então existem $a_1, a_2, \cdots, a_n \in$ R nem todos nulos tal que $a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n = 0$.

Sem perda de generalidade, podemos e fazer $a_1 \neq 0$ e reordenar considerando o conjunto $\{\alpha_1', \alpha_2', \cdots, \alpha_n'\}$ de elementos de S onde $\alpha_1' = 0$ e $\alpha_i' = \alpha_i$ para $i = 2, 3, \cdots, n$.

Daí $\alpha_i' = a_{1i}\alpha_1 + a_{2i}\alpha_2 + \cdots + a_{ni}\alpha_n$ para $i = 2, 3, \cdots, n$ em que $a_{j1} = a_j$ e quando $i > 1$ tem-se:

$$a_{ji} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

Temos então que:

$$disc_{(\mathrm{S|R})}(\alpha_1', \alpha_2', \cdots, \alpha_n') = disc_{(\mathrm{S|R})}(0, \alpha_2, \cdots, \alpha_n) = 0$$

uma vez que a matriz $\left(\mathrm{Tr}_{\left(\mathrm{L|K}_f(\mathrm{A})\right)}(\alpha_i\alpha_j)\right)$ possui a primeira linha nula. Assim segundo a **Proposição 18** segue que:

$$0 = disc_{(\mathrm{S|R})}(0, \alpha_2, \cdots, \alpha_n) =$$
$$disc_{(\mathrm{S|R})}(\alpha_1', \alpha_2', \cdots, \alpha_n') =$$
$$\left[det(a_{ij})\right]^2 \cdot disc_{(\mathrm{S|R})}(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

Por outro lado

$$(a_{ij}) = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \Longrightarrow det(a_{ij}) = a_1 \neq 0$$

e como R é domínio segue o resultado esperado.

■

Proposição 20 "Lema de Dedekind": Se G é um grupo, K um corpo e $\sigma_1, \sigma_2, \cdots, \sigma_n$ homomorfismos distintos de G no grupo multiplicativo K^*, então os $\sigma_i's$ são linearmente independentes sobre K.

Demonstração:

Suponhamos por absurdo que $\sigma_i's$ sejam linearmente dependentes. Considere a combinação linear

$$\sum_{i=1}^{m} k_i\sigma_i = 0$$

com m mínimo, $k_i \in \mathrm{K}$ e $k_i \neq 0$ para $i = 1, 2, \cdots, m$. Assim para todo $x \in \mathrm{G}$ temos que

$$k_1\sigma_1(x) + \cdots + k_m\sigma_m(x) = 0_{\mathrm{G}}$$

Por outro lado, sendo os homomorfismos distintos segue que existe $\theta \in \mathrm{G}$ tal que $\sigma_1(\theta) \neq \sigma_m(\theta)$. Mas como $\theta x \in \mathrm{G}$ segue que:

$$k_1\sigma_1(\theta x) + \cdots + k_m\sigma_m(\theta x) = 0_{\mathrm{G}} \Longrightarrow$$
$$k_1\sigma_1(\theta)\sigma_1(x) + \cdots + k_m\sigma_m(\theta)\sigma_m(x) = 0_{\mathrm{G}}$$

Agora tomando o produto de $k_1\sigma_1(x) + \cdots + k_m\sigma_m(x) = 0_{\mathrm{G}}$ por $\sigma_1(\theta)$ e o resultante subtraindo de $k_1\sigma_1(\theta)\sigma_1(x) + \cdots + k_m\sigma_m(\theta)\sigma_m(x) = 0_{\mathrm{G}}$ tem-se a expressão:

$$k_2\sigma_2(x)[\sigma_2(\theta) - \sigma_1(\theta)] + \cdots + k_m\sigma_m(x)[\sigma_m(\theta) - \sigma_1(\theta)] = 0_{\mathrm{G}}$$

Portanto a expressão anterior valendo para todo $x \in \mathrm{G}$, sabendo que m é mínimo e por hipótese $k_i \neq 0$ para $i = 2, \cdots, m$ isso significa que $\sigma_2(\theta) - \sigma_1(\theta) = \cdots = \sigma_m(\theta) - \sigma_1(\theta) = 0$, gerando uma contradição.

■

Proposição 21: Sejam L uma extensão finita de grau n de um corpo K, onde K é finito ou de característica nula e $\sigma_1, \sigma_2, \cdots, \sigma_n$ os distintos de K − isomorfismos de L em um corpo algebricamente fechado F contendo K. Se $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ é uma base de L sobre K, então:

$$disc_{(\mathrm{L}|\mathrm{K})}(\alpha_1, \alpha_2, \cdots, \alpha_n) = det\left(\sigma_i(\alpha_j)\right)^2 \neq 0$$

Demonstração:

Observe que:

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j)$$

Como o $\mathrm{Tr}_{(\mathrm{S|R})}(\alpha_i \alpha_j)$ é a soma dos conjugados segue que:

$$disc_{(\mathrm{S|R})}(\alpha_1, \alpha_2, \cdots, \alpha_n) =$$

$$det\left(\mathrm{Tr}_{(\mathrm{S|R})}(\alpha_i \alpha_j)\right) =$$

$$det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j)\right) =$$

$$det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) =$$

$$det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) =$$

$$det(\sigma_k(\alpha_i))det\left(\sigma_k(\alpha_j)\right) =$$

$$det\left(\sigma_i(\alpha_j)\right)^2$$

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

Suponha por absurdo que $det\left(\sigma_k(\alpha_j)\right) = 0$ então existem $\lambda_1, \cdots, \lambda_n \in \mathrm{F}$ não todos nulos tal que:

$$\sum_{i=1}^{n} \lambda_i \sigma_i(\alpha_j) = 0$$

para todo $j = 1, 2, \cdots, n$. Se $\alpha \in \mathrm{L}$ então

$$\alpha = \sum_{i=1}^{n} \theta_i \alpha_i$$

onde $\theta_i \in \mathrm{K}$ e pela linearidade fica

$$\sum_{i=1}^{n} \lambda_i \sigma_i(\alpha) = \sum_{i=1}^{n} \lambda_i \sigma_i \left(\sum_{i=1}^{n} \theta_i \alpha_i \right) = \sum_{i=1}^{n} \theta_i \left(\sum_{i=1}^{n} \lambda_i \sigma_i(\alpha_i) \right) = 0$$

Porém $\sigma_i' s$ são linearmente independentes. Sendo uma contradição com a **Proposição 20**.

■

Proposição 22: Se K é um corpo finito ou de característica nula, $\mathrm{L} = \mathrm{K}[\alpha]$ uma extensão finita de K grau n e o $m_\alpha(x)$ polinômio minimal de α sobre K, então

$$disc_{(\mathrm{L}|\mathrm{K})}(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathcal{N}_{(\mathrm{L}|\mathrm{K})}\left(m_\alpha'(\alpha)\right)$$

onde $m_\alpha'(x)$ é a derivada de $m_\alpha(x)$.

Demonstração:

Se $\alpha_1, \alpha_2, \cdots, \alpha_n$ forem raízes de $m_\alpha(x)$ em alguma extensão $\mathrm{L} = \mathrm{K}[\alpha]$ então são conjugados de α e de acordo com a **Proposição 21**

$$disc_{(\mathrm{L}|\mathrm{K})}(1, \alpha, \cdots, \alpha^{n-1}) = det\left(\sigma_i\left(\alpha^j\right)\right)^2 = det\left(\alpha_i^j\right)^2$$

para $i = 1, 2, \cdots, n$ e $j = 1, 2, \cdots, n-1$. Portanto segundo o determinante de Vandermonde

$$det\left(\alpha_i^j\right)^2 =$$

$$\left[\prod_{1 \le k < i \le n} (\alpha_i - \alpha_k) \right]^2 =$$

$$\prod_{1 \le k < i \le n} (\alpha_i - \alpha_k)(\alpha_i - \alpha_k) =$$

$$(-1)^{\frac{n(n-1)}{2}} \prod_{1 \le k < i \le n} (\alpha_i - \alpha_k) =$$

$$(-1)^{\frac{n(n-1)}{2}} = \prod_{i=1}^{n} \left[\prod_{k=1, k \ne i}^{n} (\alpha_i - \alpha_k) \right] =$$

$$(-1)^{\frac{n(n-1)}{2}} = \prod_{i=1}^{n} m'_{\alpha}(\alpha_i) =$$

$$(-1)^{\frac{n(n-1)}{2}} \mathcal{N}_{(\mathrm{L}|\mathrm{K})}\left(m'_{\alpha}(\alpha)\right)$$

■

3.3.3 Exemplos

Exemplo 06: Seja o corpo quadrático $\mathrm{L} = \mathbb{Q}(i)$. Então $i, 1-i \in \mathbb{Q}(i)$ os polinômios minimais de i e $1-i$ são respectivamente

$$m_i(x) = x^2 + 1 = (x-i)(x+i) = \mathrm{P}_{(i,\mathrm{L}|\mathbb{Q})}(x)$$
$$m_{1-i}(x) = x^2 - 2x + 2 = (x-1-i)(x-1+i) = \mathrm{P}_{(1-i,\mathrm{L}|\mathbb{Q})}(x)$$

Assim:

$$\mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(i) = i - i = 0$$
$$\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(i) = i(-i) = -i^2 = 1$$
$$\mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(1-i) = -1 - i - 1 + i = -2$$
$$\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(i) = (-1-i)(-1+i) = 1 - i + i + 1 = 2$$

Exemplo 07: Sejam $\mathrm{L} = \mathbb{Q}\left(\sqrt{d}\right)$ o corpo quadrático com d livre de quadrados e $\alpha = a + b\sqrt{d} \in \mathrm{L}$. Assim:

(i) Se $b = 0$, então $\alpha \in \mathbb{Q}$ e $p_{\alpha}(x) = x - a$ é o polinômio minimal de α. Daí:

$$\mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(\alpha) = \mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\alpha) = a$$

(ii) Se $b \neq 0$, então o polinômio minimal de α é $q_{\alpha}(x) = x^2 - 2ax + a^2 - db^2 = \left(x - a - b\sqrt{d}\right)\left(x - a + b\sqrt{d}\right)$ com

$$\mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(\alpha) = 2a$$
$$\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\alpha) = a^2 - db^2$$

Exemplo 08: Seja $\mathrm{K} = \mathbb{Q}(\sqrt{d})$. Então:

(i) $\mathrm{I}_{\mathrm{K}}(\mathbb{Z}) = \mathbb{Z}[\sqrt{d}]$ quando $d \equiv 2\ mod(4)$ ou $d \equiv 3\ mod(4)$

(ii) $\mathrm{I}_{\mathrm{K}}(\mathbb{Z}) = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ quando $d \equiv 1\ mod(4)$

No caso (i) tem-se que $\Gamma = \{1, \sqrt{d}\}$ é uma base de $\mathrm{I}_{\mathrm{K}}(\mathbb{Z})$ e para $\alpha \in \mathrm{K}$ tem-se $\alpha = a + b\sqrt{d}$ donde

$$\varphi_\alpha(1) = a + b\sqrt{d}$$
$$\varphi_\alpha(\sqrt{d}) = a\sqrt{d} + bd$$

ou seja

$$\begin{bmatrix} \varphi_\alpha(1) \\ \varphi_\alpha(\sqrt{d}) \end{bmatrix} = \begin{bmatrix} a & b \\ bd & a \end{bmatrix} \cdot \begin{bmatrix} 1 \\ \sqrt{d} \end{bmatrix}$$

Assim:

$$\mathrm{Tr}_{(\mathrm{K}|\mathrm{I}_{\mathrm{K}}(\mathbb{Z}))}(\alpha) = 2a$$
$$\mathcal{N}_{(\mathrm{K}|\mathrm{I}_{\mathrm{K}}(\mathbb{Z}))}(\alpha) = a^2 - db^2$$

Exemplo 09: Considere um $\alpha \in \mathrm{L} = \mathbb{Q}(\sqrt{d})$ inteiro algébrico sobre $\mathbb{Z}$, com d livre de quadrados, segue que $\mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(\alpha), \mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\alpha) \in \mathrm{I}_{\mathrm{L}}(\mathbb{Z}) = \mathbb{Z}$.

Por outro lado se $p(x) = x^2 - \mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(\alpha)x + \mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\alpha) \in \mathbb{Z}[x]$ com $\alpha \in \mathrm{L} = \mathbb{Q}(\sqrt{d})$ segue que $p(\alpha) = 0$ e então $\alpha \in \mathrm{I}_{\mathrm{L}}(\mathbb{Z})$.

Portanto elementos de corpos quadráticos são inteiros algébricos se somente se seu traço e sua norma são números inteiros.

Exemplo 10: Seja $\mathrm{L} = \mathbb{Q}(\sqrt{d})$, sendo d um inteiro livre de quadrados. Para $\alpha = x + y\sqrt{d}$ com $x, y \in \mathbb{Q}$ temos que $\alpha^2 = (x^2 + y^2 d) + 2xy\sqrt{d}$, logo:

$$disc_{(\mathrm{L}|\mathbb{Q})}(1,\alpha) = det\begin{pmatrix} \mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(1) & \mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(\alpha) \\ \mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(\alpha) & \mathrm{Tr}_{(\mathrm{L}|\mathbb{Q})}(\alpha^2) \end{pmatrix} = \begin{vmatrix} 2 & 2x \\ 2x & 2(x^2+y^2d) \end{vmatrix} = 4y^2d$$

Em particular tem-se que

$$disc_{(\mathrm{L}|\mathbb{Q})}\left(1,\sqrt{d}\right) = 4d \text{ e } disc_{(\mathrm{L}|\mathbb{Q})}\left(1,\frac{1+\sqrt{d}}{2}\right) = d$$

Portanto como

$$\left\{1,\sqrt{d}\right\} \text{ e } \left\{1,\frac{1+\sqrt{d}}{2}\right\}$$

são bases integrais de L sobre $\mathbb{Q}$ quando $d \equiv 2$ ou $3\ mod(4)$ "respectivamente $d \equiv 1\ mod(4)$" segue que

$$d_{\mathrm{L}} = disc(\mathrm{L}) = \begin{cases} 4d, \text{quando } d \equiv 2 \text{ ou } 3\ mod(4) \\ d, \text{quando } d \equiv 1\ mod(4) \end{cases}$$

3.4 O Grupo de Classes de Ideais

Qualquer corpo numérico K, possui número de classe h_{K} "ordem do grupo abeliano $\mathrm{C}\ell_{\mathrm{K}}$ das classes de ideais de $\mathrm{I}_{\mathrm{K}}(\mathbb{Z})$" finito.

O principal objetivo do capítulo é verificar a finitude de h_{K}, por meio da existência de uma cota superior para a norma de ideais $\mathcal{N}$ "que generaliza a norma absoluta $\mathcal{N}_{(\mathrm{K}|\mathbb{Q})}$" aplicando o princípio das gavetas.

Tentar efetuar o cálculo de h_{K} para um certo corpo numérico K "em princípio por uma quantidade finita de etapas" é viável somente para casos bem simples. Em particular há uma cota ou desigualdade de Minkowski relacionada com o discriminante d_{K} de K, onde auxilia no cálculo de h_{K}.

Fórmulas básicas para obter h_{K} para qualquer corpo numérico K por métodos analíticos, por exemplo, são encontrados em BOREVICH, Z. I.; SHAFAREVICH, I. R. **Number theory.**

3.4.1 Normas de Ideais

Seja K uma extensão finita de $\mathbb{Q}$ e $\mathrm{I_K}(\mathbb{Z})$ o anel dos inteiros do corpo numérico K. Para um ideal não nulo $\mathfrak{a}$ de $\mathrm{I_K}(\mathbb{Z})$, a norma do ideal $\mathfrak{a}$ é denotada e definida como sendo

$$\mathcal{N}_{(\mathrm{K}|\mathbb{Q})}(\mathfrak{a}) = card\left(\frac{\mathrm{I_K}(\mathbb{Z})}{\mathfrak{a}}\right) = \#\left(\frac{\mathrm{I_K}(\mathbb{Z})}{\mathfrak{a}}\right)$$

ou seja, o número cardinal de $\mathrm{I_K}(\mathbb{Z})/\mathfrak{a}$. Também é comum escrever apenas $\mathcal{N}(\mathfrak{a})$ em vez de $\mathcal{N}_{(\mathrm{K}|\mathbb{Q})}(\mathfrak{a})$. Quando K for um corpo com o grau da extensão n, então para $x \in \mathrm{I_K}(\mathbb{Z})$, escrevemos $\mathcal{N}(x)$ para significar $\mathcal{N}_{(\mathrm{K}|\mathbb{Q})}\big(x\mathrm{I_K}(\mathbb{Z})\big)$.

Proposição 23: Se $x \in \mathrm{I_K}(\mathbb{Z})$ é um elemento não nulo de A, então:

$$|\mathcal{N}(x)| = card\left(\frac{\mathrm{I_K}(\mathbb{Z})}{x\mathrm{I_K}(\mathbb{Z})}\right)$$

Demonstração:

Seja $x \in \mathrm{I_K}(\mathbb{Z}) - \{0\}$. Então $\mathcal{N}(x) \in \mathbb{Z}$ segundo o item (v) da **Proposição 12.**

Também pelo item (b) da **Proposição 16**, temos que $\mathrm{I_K}(\mathbb{Z})$ é um $\mathbb{Z} - módulo$ livre de posto n e como $\psi : \mathrm{I_K}(\mathbb{Z}) \longrightarrow x\mathrm{I_K}(\mathbb{Z})$ dado por $\psi(\mathfrak{a}) = x\mathfrak{a}$ é um isomorfismo, consequentemente $x\mathrm{I_K}(\mathbb{Z})$ é um $\mathbb{Z} - módulo$ livre de $\mathrm{I_K}(\mathbb{Z})$ e de posto n.

Pela **Proposição 24 do Capítulo 2**, existe uma base $\{e_1, e_2, \cdots, e_n\}$ do $\mathbb{Z} - módulo$ livre de $\mathrm{I_K}(\mathbb{Z})$ e elementos $c_i \in \mathbb{Z}$ tal que $\{c_1e_1, c_2e_2, \cdots, c_ne_n\}$ é uma base de $\mathrm{I_K}(\mathbb{Z})$.

Temos também que o grupo abeliano $x\mathrm{I_K}(\mathbb{Z})$ é isomorfo ao grupo abeliano cuja ordem do mesmo é $c_1c_2 \cdots c_{n-1}c_n$.

Escreva agora a aplicação $\mathbb{Z} - linear\ \varphi : \mathrm{I_K}(\mathbb{Z}) \longrightarrow x\mathrm{I_K}(\mathbb{Z})$ com $\varphi(e_i) = c_ie_i$ para $i = 1, 2, \cdots, n$. Segue que o determinante $det(\varphi) = c_1c_2 \cdots c_{n-1}c_n$. Mas por outro lado, como $\{xe_1, xe_2, \cdots, xe_n\}$ também é uma base para $\mathrm{I_K}(\mathbb{Z})$ segue que existe um automorfismo $f : x\mathrm{I_K}(\mathbb{Z}) \longrightarrow x\mathrm{I_K}(\mathbb{Z})$ do $\mathbb{Z} - módulo\ x\mathrm{I_K}(\mathbb{Z})$ dado por $f(c_ie_i) = xe_i$ com $i = 1, 2, \cdots, n$.

Daí como o $det(f) \in \mathbb{Z}$ é invertível, implica que o $det(f) = \pm 1$, porém $f \circ \varphi$ é um homomorfismo multiplicado por x em que:

$$\mathcal{N}(x) = det(f \circ \varphi) = det(f) \cdot det(\varphi) = \pm c_1 c_2 \cdots c_{n-1} c_n = \pm card\left(\frac{\mathrm{I_K}(\mathbb{Z})}{x\mathrm{I_K}(\mathbb{Z})}\right)$$

■

Proposição 24: Seja $\mathrm{I_K}(\mathbb{Z})$ o anel dos inteiros de K, $[\mathrm{K} : \mathbb{Q}] < \infty$ e $\mathfrak{a}$ um ideal não nulo de $\mathrm{I_K}(\mathbb{Z})$. Se $\{e_1, e_2, \cdots, e_n\}$ é uma $\mathbb{Z} - base$ de $\mathrm{I_K}(\mathbb{Z})$ e $\{a_1 e_1, a_2 e_2, \cdots, a_n e_n\}$ é uma base de $\mathfrak{a}$, onde $a_{1 \le i \le n} \in \mathbb{Z} - \{0\}$, então $\mathcal{N}(\mathfrak{a}) = |a_1 a_2 \cdots a_n|$

Demonstração:

Considere a aplicação

$$\varphi : \mathrm{I_K}(\mathbb{Z}) \longrightarrow \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \frac{\mathbb{Z}}{a_2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}}$$

dada por

$$\varphi\left(\sum_{i=1}^{n} b_i e_i\right) = (b_1 + a_1\mathbb{Z}, b_2 + a_2\mathbb{Z}, \cdots, b_n + a_n\mathbb{Z})$$

Segue que φ é um homomorfismo sobrejetivo segundo a soma coordenada a coordenada e que $\mathrm{K}er(\varphi) = \mathfrak{a}$, pois para

$$b = \sum_{i=1}^{n} b_i e_i \in \mathrm{K}er(\varphi) \Longrightarrow$$

$$\varphi(b) = (b_1 + a_1\mathbb{Z}, b_2 + a_2\mathbb{Z}, \cdots, b_n + a_n\mathbb{Z}) = (a_1\mathbb{Z}, a_2\mathbb{Z}, \cdots, a_n\mathbb{Z})$$

donde $b_i \in a_i\mathbb{Z} \Leftrightarrow b_i = a_i c_i$ para algum $c_i \in \mathbb{Z}$ e $i = 1, \cdots, n$. Logo:

$$b = \sum_{i=1}^{n} b_i e_i = \sum_{i=1}^{n} (a_i c_i) e_i = \sum_{i=1}^{n} c_i (a_i e_i) \in \mathfrak{a}$$

significando que $\mathrm{K}er(\varphi) \subseteq \mathfrak{a}$.Por outro lado dado

$$c = \sum_{i=1}^{n} c_i(a_i e_i) \in \mathfrak{a} \text{ com } c_i \in \mathbb{Z}$$

tem-se que

$$\varphi(c) = \varphi\left(\sum_{i=1}^{n} c_i(a_i e_i)\right) = (c_1 a_1 + a_1\mathbb{Z}, \cdots, c_n a_n + a_n\mathbb{Z}) = (a_1\mathbb{Z}, \cdots, a_n\mathbb{Z})$$

implicando que $c \in \mathrm{K}er(\varphi)$. Logo $\mathfrak{a} \subseteq \mathrm{K}er(\varphi)$. Portanto $\mathrm{K}er(\varphi) = \mathfrak{a}$.

Então aplicando o Teorema dos Isomorfismos, tem-se que:

$$\frac{\mathrm{I_K}(\mathbb{Z})}{\mathfrak{a}} \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}} \Longrightarrow \mathcal{N}(\mathfrak{a}) = \left|\frac{\mathrm{I_K}(\mathbb{Z})}{\mathfrak{a}}\right| = \left|\frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}}\right| = |a_1 a_2 \cdots a_n|$$

■

Proposição 25: Seja $\mathfrak{p}$ um ideal primo não nulo de $\mathrm{I_L}(\mathbb{Z})$, com L um corpo numérico. Então:

(a) $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, sendo p o único número primo em $\mathfrak{p}$.

(b) $\mathrm{I_L}(\mathbb{Z})/\mathfrak{p}$ é uma extensão finita do corpo $\mathbb{Z}_p$ de grau $\left[\mathrm{I_L}(\mathbb{Z})/\mathfrak{p} : \mathbb{Z}_p\right] \leq n = [\mathrm{L} : \mathbb{Q}]$.

Demonstração:

(a) O ideal $\mathfrak{p} \cap \mathbb{Z}$ é não nulo segundo o item (a) da **Proposição 07**, que é primo em $\mathbb{Z}$ segundo a **Proposição 20 do Capítulo 2**. Logo os ideais primos de $\mathbb{Z}$ são $p\mathbb{Z}$ para algum primo p. Portanto $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ para p o único em $\mathfrak{p}$.

(b) Considere o homomorfismo canônico $\varphi : \mathrm{I_L}(\mathbb{Z}) \longrightarrow \mathrm{I_L}(\mathbb{Z})/\mathfrak{p}$, então o $ker(\varphi|_{\mathbb{Z}}) = p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

Logo pelo Teorema dos Isomorfismos tem-se que:

$$\mathbb{Z}_p \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \cong \varphi|_{\mathbb{Z}}(\mathbb{Z})$$

Portanto $\mathbb{Z}_p$ é um subcorpo de $\mathrm{I_L}(\mathbb{Z})/\mathfrak{p}$. Por outro lado $\mathrm{I_L}(\mathbb{Z})$ é um $\mathbb{Z} - módulo$ livre de posto n, donde L possui uma base integral $\{e_1, e_2, \cdots, e_n\}$.

Portanto $\{\varphi(e_1), \varphi(e_2), \cdots, \varphi(e_n)\}$ representa um sistema de geradores do $\mathbb{Z}_p - espaço$ $\mathrm{I_L}(\mathbb{Z})/\mathfrak{p}$ donde $\left[\mathrm{I_L}(\mathbb{Z})/\mathfrak{p} : \mathbb{Z}_p\right] \leq n = [\mathrm{L} : \mathbb{Q}]$.

■

Dado um ideal primo não nulo $\mathfrak{p}$ de $\mathrm{I_L}(\mathbb{Z})$, onde K é um corpo numérico e p o único númer primo em $\mathfrak{p}$, define-se e denota-se o grau de inércia de $\mathfrak{p}$ por:

$$f(\mathfrak{p}) = \left[\mathrm{I_L}(\mathbb{Z})/\mathfrak{p} : \mathbb{Z}_p\right]$$

Proposição 26: Seja L uma extensão de $\mathbb{Q}$ de grau $[\mathrm{L} : \mathbb{Q}] = n$. Então:

(a) Para todo ideal primo não nulo $\mathfrak{p}$ de $\mathrm{I_L}(\mathbb{Z})$ temos que $\mathcal{N}(\mathfrak{p}) = p^f$ onde f é o grau de inércia de $\mathfrak{p}$ e p o único número primo em $\mathfrak{p}$.

(b) Para quaisquer ideais não nulos $\mathfrak{a}, \mathfrak{b}$ de $\mathrm{I_L}(\mathbb{Z})$ tem-se que $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.

(c) Para todo ideal não nulo $\mathfrak{a}$ de $\mathrm{I_L}(\mathbb{Z})$ temos que $\mathcal{N}(\mathfrak{a}) \in \mathbb{N} - \{0\}$ em particular $\mathcal{N}(\mathfrak{a}) = 1$ se e somente se $\mathfrak{a} = \mathrm{I_L}(\mathbb{Z})$.

Demonstração:

(a) Sendo $\left[\mathrm{I_L}(\mathbb{Z})/\mathfrak{p} : \mathbb{Z}_p\right] = f$ segue que $\mathrm{I_L}(\mathbb{Z})/\mathfrak{p}$ é um $\mathbb{Z}_p - espaço$ de dimensão f, donde

$$\frac{\mathrm{I_L}(\mathbb{Z})}{\mathfrak{p}} \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p = {\mathbb{Z}_p}^f$$

implicando que

$$\mathcal{N}(\mathfrak{p}) = \#\left(\frac{\mathrm{I_L}(\mathbb{Z})}{\mathfrak{p}}\right) = \#\left({\mathbb{Z}_p}^f\right) = p^f$$

(b) É suficiente verificar que $\mathcal{N}(\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r)=\mathcal{N}(\mathfrak{p}_1)\mathcal{N}(\mathfrak{p}_2)\cdots\mathcal{N}(\mathfrak{p}_r)$ para r ideais primos não nulos de $\mathrm{I_L}(\mathbb{Z})$ já que $\mathrm{I_L}(\mathbb{Z})$ é um domínio de Dedekind.

A verificação segue por indução em r.

Para $r=1$ nada há para fazer. Suponha por hipótese de indução que o resultado vale para $r\geq 2$ ideais primos e que $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$, $\mathfrak{b}=\mathfrak{p}_2\mathfrak{p}_3\cdots\mathfrak{p}_r$.

Então $\mathfrak{a}=\mathfrak{p}_1\mathfrak{b}\subseteq\mathfrak{b}$ e

$$\frac{\mathrm{I_L}(\mathbb{Z})}{\mathfrak{b}}\cong\frac{\mathrm{I_L}(\mathbb{Z})/\mathfrak{a}}{\mathfrak{b}/\mathfrak{a}}$$

Por outro lado $\mathfrak{b}/\mathfrak{a}$ é um espaço $\mathrm{I_L}(\mathbb{Z})/\mathfrak{p}_1-espaço$ de dimensão 1, logo:

$$\frac{\mathfrak{b}}{\mathfrak{a}}\cong\frac{\mathrm{I_L}(\mathbb{Z})}{\mathfrak{p}_1}\Longrightarrow\frac{\#(\mathfrak{b})}{\#(\mathfrak{a})}=\#\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)=\#\left(\frac{\mathrm{I_L}(\mathbb{Z})}{\mathfrak{p}_1}\right)=\mathcal{N}(\mathfrak{p}_1)$$

Assim:

$$\mathcal{N}(\mathfrak{b})=\#\left(\frac{\mathrm{I_L}(\mathbb{Z})}{\mathfrak{b}}\right)=\#\left(\frac{\mathrm{I_L}(\mathbb{Z})/\mathfrak{a}}{\mathfrak{b}/\mathfrak{a}}\right)=\frac{\#\left(\frac{\mathrm{I_L}(\mathbb{Z})}{\mathfrak{a}}\right)}{\#\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)}=\frac{\mathcal{N}(\mathfrak{a})}{\mathcal{N}(\mathfrak{p}_1)}$$

(c) Dado um ideal não nulo $\mathfrak{m}$ de $\mathrm{I_L}(\mathbb{Z})$ temos que $\mathrm{I_L}(\mathbb{Z})/\mathfrak{m}$ possui ao menos um elemento, donde $\mathcal{N}(\mathfrak{m})\in\mathbb{N}-\{0\}$. Em particular $\mathcal{N}(\mathfrak{m})=1$ se e somente se $\mathfrak{m}=\mathrm{I_L}(\mathbb{Z})$.

■

Proposição 27: Se $\mathfrak{a}$ é ideal não nulo de $\mathrm{I_L}(\mathbb{Z})$ então:

(a) $\mathcal{N}(\mathfrak{a})\mathrm{I_L}(\mathbb{Z})=\langle\mathcal{N}(\mathfrak{a})\rangle$ é um múltiplo de $\mathfrak{a}$, ou seja $\mathcal{N}(\mathfrak{a})\in\mathfrak{a}$.

(b) Se $\mathcal{N}(\mathfrak{a})$ for um número primo então $\mathfrak{a}$ será um ideal primo.

(c) Se $\mathfrak{a}$ é um múltiplo do ideal $\mathfrak{b}$ e $\mathcal{N}(\mathfrak{a})=\mathcal{N}(\mathfrak{b})$ então $\mathfrak{a}=\mathfrak{b}$.

Demonstração:

(a) O anel "em particular o grupo aditivo" $\mathrm{I_L}(\mathbb{Z})/\mathfrak{a}$ tem ordem $r = \mathcal{N}(\mathfrak{a}) = \#(\mathrm{I_L}(\mathbb{Z})/\mathfrak{a})$, donde $\bar{r} = r\bar{1} = \bar{0}$ se e somente se $r\mathrm{I_L}(\mathbb{Z}) \subseteq \mathfrak{a}$ se e somente se $\mathfrak{a}$ divide $r\mathrm{I_L}(\mathbb{Z})$.

(b) Se $\mathfrak{a}$ não é ideal primo de $\mathrm{I_L}(\mathbb{Z})$ então $\mathfrak{a} = \mathrm{I_L}(\mathbb{Z})$ ou $\mathfrak{a} = \mathfrak{bc}$ com $\mathfrak{b}, \mathfrak{c}$ ideais não nulos distintos de $\mathrm{I_L}(\mathbb{Z})$. Então em qualquer caso segue respectivamente que $\mathcal{N}(\mathfrak{a}) = 1$ ou $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b})\mathcal{N}(\mathfrak{c}) > 1$ não sendo primo em nenhum dos casos.

(c) Segue que existe um ideal não nulo $\mathfrak{c}$ de $\mathrm{I_L}(\mathbb{Z})$ tal que $\mathfrak{a} = \mathfrak{bc}$ donde $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b})\mathcal{N}(\mathfrak{c})$ e por $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b})$ implica que $\mathcal{N}(\mathfrak{c}) = 1$ se e somente se $\mathfrak{c} = \mathrm{I_L}(\mathbb{Z})$.

Portanto $\mathfrak{a} = \mathfrak{b}\mathrm{I_L}(\mathbb{Z}) \subseteq \mathfrak{b}$, mas vale a igualdade, pois $\mathrm{I_L}(\mathbb{Z})$ é o elemento neutro no monoide dos ideais não nulos de $\mathrm{I_L}(\mathbb{Z})$.

■

Proposição 28: Para todo $r \in \mathbb{N} - \{0\}$ existe apenas um número finito de ideais não nulos $\mathfrak{a}$ de $\mathrm{I_L}(\mathbb{Z})$ tal que $\mathcal{N}(\mathfrak{a}) = r$.

Demonstração:

Isso segue segundo o fato que dado $r \in \mathbb{N} - \{0\}$ tem-se:

$$\{\mathfrak{b} \trianglelefteq \mathrm{I_L}(\mathbb{Z}) - \{0\} : \mathcal{N}(\mathfrak{b}) = r\} \subseteq \{\mathfrak{a} \trianglelefteq \mathrm{I_L}(\mathbb{Z}) - \{0\} : r\mathrm{I_L}(\mathbb{Z}) \subseteq \mathfrak{a}\}$$

uma vez que se $\mathfrak{b}$ é ideal não nulo de $\mathrm{I_L}(\mathbb{Z})$ com $\mathcal{N}(\mathfrak{b}) = r \in \mathbb{N} - \{0\}$ tem-se que $r\mathrm{I_L}(\mathbb{Z}) \subseteq \mathfrak{b}$ e da finitude de $\{\mathfrak{a} \trianglelefteq \mathrm{I_L}(\mathbb{Z}) - \{0\} : r\mathrm{I_L}(\mathbb{Z}) \subseteq \mathfrak{a}\}$.

■

Proposição 29:

(a) Todo ideal $\mathfrak{a}$ não nulo de $\mathrm{I_L}(\mathbb{Z})$ é um $\mathbb{Z} - módulo$ livre de posto n e para toda base $\alpha_1, \alpha_2, \cdots, \alpha_n$ deste $\mathbb{Z} - módulo$ temos que $disc_{(\mathrm{L}|\mathbb{Q})}(\alpha_1, \alpha_2, \cdots, \alpha_n) = \mathcal{N}(\mathfrak{a})^2 \cdot d_{\mathrm{L}}$.

(b) Para todo elemento não nulo $x \in \mathrm{I_L}(\mathbb{Z})$ temos que $\mathcal{N}\big(x\mathrm{I_L}(\mathbb{Z})\big) = \left|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(x)\right|$.

Demonstração:

(a) Segue segundo os resultados para base integral:

(i) Como $\mathrm{I_L}(\mathbb{Z})$ é um $\mathbb{Z}-módulo$ livre, L possui uma base integral $\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n\}$ e existem $a_1, a_2, \cdots, a_q \in \mathbb{Z}$ "$q \leq n$" tal que $\{a_1\varepsilon_1, a_2\varepsilon_2, \cdots, a_n\varepsilon_n\}$ é uma base do $\mathbb{Z}-módulo$ $\mathfrak{a}$.

(ii) O $\mathbb{Z}-módulo$

$$\frac{\mathrm{I_L}(\mathbb{Z})}{\mathfrak{a}} \cong \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_q} \times \mathbb{Z}^{n-q}$$

Por outro lado, se $q < n$ então seria infinita, o que é uma contradição. Portanto $n = q$ e com isso $\mathcal{N}(\mathfrak{a}) = |a_1 a_2 \cdots a_n| = |a_1||a_2| \cdots |a_n|$.

Daí segundo a propriedade do discriminante tem-se que

$$disc_{(\mathrm{L}|\mathbb{Q})}(a_1\varepsilon_1, \cdots, a_n\varepsilon_n) =$$
$$\left(det\left(a_i\delta_{ij}\right)\right)^2 disc_{(\mathrm{L}|\mathbb{Q})}(\varepsilon_1, \cdots, \varepsilon_n) =$$
$$\mathcal{N}(\mathfrak{a})^2 d_{\mathrm{L}} = |a_1 \cdots a_n|^2 d_{\mathrm{L}}$$

(iii) Toda base $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ do $\mathbb{Z}-módulo$ $\mathfrak{a}$ escreve-se como

$$\alpha_i = \sum_{j=1}^{n} c_{ij}\left(a_j\varepsilon_j\right)$$

com $c_{ij} \in \mathbb{Z}$ "$i, j = 1, 2, \cdots, n$" e $det\left(c_{ij}\right) = \pm 1$. Portanto $disc_{(\mathrm{L}|\mathbb{Q})}(\alpha_1, \alpha_2, \cdots, \alpha_n) = disc_{(\mathrm{L}|\mathbb{Q})}(a_1\varepsilon_1, \cdots, a_n\varepsilon_n)$

(b) Considere que $\{\beta_1, \beta_2, \cdots, \beta_n\}$ forma uma base integral de L. Então $\{\alpha\beta_1, \alpha\beta_2, \cdots, \alpha\beta_n\}$ forma uma base para o ideal principal $\alpha \mathrm{I}_{\mathrm{L}}(\mathbb{Z})$ como $\mathbb{Z} - m\acute{o}dulo$ onde $\alpha \in \mathrm{I}_{\mathrm{L}}(\mathbb{Z}) - \{0\}$. Logo pelo item (a)

$$disc_{(\mathrm{L}|\mathbb{Q})}(\alpha\beta_1, \cdots, \alpha\beta_n) = \mathcal{N}\big(\alpha \mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big)^2 d_{\mathrm{L}}$$

Por outro lado, existem $a_{ij} \in \mathbb{Z}$ tais que

$$\alpha\beta_i = \sum_{j=1}^{n} a_{ij}\beta_j$$

"$i, j = 1, 2, \cdots, n$".

Assim:

$$disc_{(\mathrm{L}|\mathbb{Q})}(\alpha\beta_1, \cdots, \alpha\beta_n) = \Big(det\big(a_{ij}\big)\Big)^2 d_{\mathrm{L}}$$

mas como $det\big(a_{ij}\big) = \mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\alpha)$, segue que:

$$\mathcal{N}\big(\alpha \mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big)^2 = \Big[\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\alpha)\Big]^2 \Longrightarrow \mathcal{N}\big(\alpha \mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big) = \Big|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\alpha)\Big|$$

■

Corolário 11: Seja p um número primo e a fatoração $p\mathrm{I}_{\mathrm{L}}(\mathbb{Z}) = \mathfrak{p}_1{}^{e_1}\mathfrak{p}_2{}^{e_2} \cdots \mathfrak{p}_r{}^{e_r}$ em ideais primos distintos $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ do ideal principal $p\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$com $e_{1 \le i \le r} \ge 1$. Então:

(a) $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ são os únicos ideais primos $\mathfrak{p}$ de $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$ tais que $p \in \mathfrak{p}$.

(b) $\sum_{i=1}^{r} e_i f_i = n$

onde f_i é o grau de inércia de $\mathfrak{p}_i$, $1 \le i \le r$.

Demonstração:

(a) Segue diretamente que $p \in p\mathrm{I}_{\mathrm{L}}(\mathbb{Z}) = \mathfrak{p}_1{}^{e_1}\mathfrak{p}_2{}^{e_2}\cdots\mathfrak{p}_r{}^{e_r} \subseteq \mathfrak{p}_i$ para todo $1 \leq i \leq r$, pois $\mathfrak{p}_i$ é ideal. Agora se $\mathfrak{p}$ é um ideal primo qualquer com $p \in \mathfrak{p}$, então $\mathfrak{p}$ divide $p\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$, donde $\mathfrak{p} \in \{\mathfrak{p}_i\}_{1\leq i\leq r}$, segundo a unicidade da fatoração.

(b) Agora note que $p\mathrm{I}_{\mathrm{L}}(\mathbb{Z}) = \mathfrak{p}_1{}^{e_1}\mathfrak{p}_2{}^{e_2}\cdots\mathfrak{p}_r{}^{e_r}$ implica

$$\mathcal{N}\big(p\mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big) = \mathcal{N}(\mathfrak{p}_1{}^{e_1})\mathcal{N}(\mathfrak{p}_2{}^{e_2})\cdots\mathcal{N}(\mathfrak{p}_r{}^{e_r}) = p^{e_1f_1}p^{e_2f_2}\cdots p^{e_rf_r} = p^{e_1f_1+e_2f_2+\cdots+e_rf_r}$$

de acordo com o item anterior (a) e os itens (a) e (b) da **Proposição 26**

Por outro lado, pelo item (b) da **Proposição 29** segue que

$$\mathcal{N}\big(p\mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big) = \left|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(p)\right| = p^n$$

donde resulta a igualdade esperada.

■

Seja $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$ o anel dos inteiros do corpo numérico L, com $n = [\mathrm{L} : \mathbb{Q}]$. Lembrando que para todo ideal $\mathfrak{a}$ não nulo de $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$ e $x \in \mathfrak{a} - \{0\}$, a norma $\mathcal{N}(\mathfrak{a})$ divide a norma $\mathcal{N}\big(x\mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big)$ e consequentemente

$$\frac{\mathcal{N}\big(x\mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big)}{\mathcal{N}(\mathfrak{a})} \in \mathbb{N} - \{0\}$$

em particular

$$\frac{\mathcal{N}\big(x\mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big)}{\mathcal{N}(\mathfrak{a})} = 1 \Leftrightarrow \mathfrak{a} = x\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$$

Portanto

$$n(\mathfrak{a}) = mín.\left\{\frac{\mathcal{N}\big(x\mathrm{I}_{\mathrm{L}}(\mathbb{Z})\big)}{\mathcal{N}(\mathfrak{a})} : x \in \mathfrak{a} - \{0\}\right\} \in \mathbb{N} - \{0\}$$

Em particular $n(\mathfrak{a}) = 1$ se e somente se $\mathfrak{a}$ é um ideal fracionário invertível, ou seja, principal.

Proposição 30: Para todo corpo numérico L, o conjunto $\{n(\mathfrak{a}) : \mathfrak{a} \trianglelefteq \mathrm{I_L}(\mathbb{Z}) - \{0\}\}$ é limitado ou seja existe uma cota $\rho > 0$ tal que $1 \leq n(\mathfrak{a}) \leq \rho$ para todo ideal $\mathfrak{a}$ não nulo de $\mathrm{I_L}(\mathbb{Z})$.

Demonstração:

Considere os isomorfismos $\sigma_i : \mathrm{L} \longrightarrow \mathbb{C}$ com $1 \leq i \leq n$, com L, corpo numérico e $\{e_1, e_2, \cdots, e_n\}$ uma base integral de L "$\mathrm{I_L}(\mathbb{Z})$ é um $\mathbb{Z} - m\acute{o}dulo$ livre de posto n"

Vamos verificar que:

$$\rho = \prod_{j=1}^{n} \sum_{i=1}^{n} |\sigma_j(e_i)|$$

é uma cota superior para o conjunto do enunciado.

Dado o ideal $\mathfrak{a}$ não nulo de $\mathrm{I_L}(\mathbb{Z})$ tem-se que existe um $k \in \mathbb{N} - \{0\}$ tal que

$$k^n \leq \mathcal{N}(\mathfrak{a}) \leq (k+1)^n$$

Por outro lado, defina o conjunto

$$\Gamma = \left\{ \sum_{i=1}^{n} d_i e_i : d_i \in \{0, 1, \cdots, k\}, 1 \leq i \leq n \right\}$$

então $\Gamma \subseteq \mathrm{I_L}(\mathbb{Z})$ "$\mathrm{I_L}(\mathbb{Z})$ é um $\mathbb{Z} - m\acute{o}dulo$ livre de base $\{e_1, e_2, \cdots, e_n\}$" e $\mathcal{N}(\mathfrak{a}) = \#(\mathrm{I_L}(\mathbb{Z})/\mathfrak{a}) \leq (k+1)^n = \#(\Gamma)$ segundo o **Princípio das Gavetas**, há pelo menos dois elementos distintos $\lambda, \eta \in \Gamma$ tal que $\eta + \mathfrak{a} = \lambda + \mathfrak{a}$ implicando que

$$\lambda - \eta = \sum_{i=1}^{n} a_i e_i$$

com $a_i \in \{-k, \cdots, -1, 0, 1, \cdots, k\}$.

Portanto:

$$\left|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\lambda-\eta)\right| =$$

$$\prod_{j=1}^{n}\sigma_j(\lambda-\eta) =$$

$$\prod_{j=1}^{n}\left|\sum_{i=1}^{n}a_i\sigma_j(e_i)\right| \leq$$

$$\prod_{j=1}^{n}\left[\sum_{i=1}^{n}|a_i|\left|\sigma_j(e_i)\right|\right] \leq$$

$$k^n\rho \leq \mathcal{N}(\mathfrak{a})\rho$$

donde

$$1 \leq n(\mathfrak{a}) \leq \frac{\left|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(\lambda-\eta)\right|}{\mathcal{N}(\mathfrak{a})} \leq \rho$$

Observe que:

$$|a_i| \leq k \Longrightarrow$$

$$\sum_{i=1}^{n}|a_i| \leq nk \Longrightarrow$$

$$\sum_{i=1}^{n}|a_i|\left|\sigma_j(e_i)\right| \leq n\left|\sigma_j(e_i)\right|k \Longrightarrow$$

$$\sum_{i=1}^{n}|a_i|\left|\sigma_j(e_i)\right| \leq k\sum_{i=1}^{n}\left|\sigma_j(e_i)\right| \Longrightarrow$$

$$\prod_{j=1}^{n}\left[\sum_{i=1}^{n}|a_i|\left|\sigma_j(e_i)\right|\right] \leq$$

$$k^n\prod_{j=1}^{n}\left[\sum_{i=1}^{n}\left|\sigma_j(e_i)\right|\right] = k^n\rho$$

■

Dada uma classe $[\mathfrak{u}] \in \mathrm{C}\ell_{\mathrm{L}}$ seja $m([\mathfrak{u}]) = mín.\left\{\mathcal{N}(\mathfrak{b}) : \mathfrak{b} \in [\mathfrak{u}], \mathfrak{b} \trianglelefteq \mathrm{I}_{\mathrm{L}}(\mathbb{Z}) - \{0\}\right\}$.

Proposição 31: Se $[\mathfrak{u}] \in C\ell_L$ e $\mathfrak{a}$ é um ideal não nulo de $I_L(\mathbb{Z})$ e tal que $\mathfrak{a}^{-1} \in [\mathfrak{u}]$ então $m([\mathfrak{u}]) = n(\mathfrak{a})$.

Demonstração:

Considere $\mathfrak{b}$ um ideal não nulo de $I_L(\mathbb{Z})$ e $\mathfrak{b} \in [\mathfrak{u}]$ tal que $m([\mathfrak{u}]) = \mathcal{N}(\mathfrak{b})$.

Segue de $\mathfrak{a}^{-1}, \mathfrak{b} \in [\mathfrak{u}]$ que existe $\lambda \in L - \{0\}$ tal que $\mathfrak{a}^{-1}\lambda = \mathfrak{b}$, onde $\lambda = \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$ e com isso, implica

$$n(\mathfrak{a}) \leq \frac{\mathcal{N}\left(\lambda I_L(\mathbb{Z})\right)}{\mathcal{N}(\mathfrak{a})} = \mathcal{N}(\mathfrak{b}) = m([\mathfrak{u}])$$

"$\mathfrak{a}^{-1}\lambda = \mathfrak{b} \Longrightarrow \mathfrak{a}\mathfrak{b} = \lambda I_L(\mathbb{Z})$"

Por outro lado, para $\alpha \in \mathfrak{a} - \{0\}$ tal que $\mathfrak{b} = \alpha\mathfrak{a}^{-1}$ e

$$n(\mathfrak{a}) = \frac{\mathcal{N}\left(\alpha I_L(\mathbb{Z})\right)}{\mathcal{N}(\mathfrak{a})}$$

então $\mathfrak{b} \in [\mathfrak{u}]$, $\mathfrak{a}\mathfrak{b} = \alpha I_L(\mathbb{Z})$ donde $\mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}) = \mathcal{N}\left(\alpha I_L(\mathbb{Z})\right)$ implicando que

$$m([\mathfrak{u}]) \leq \mathcal{N}(\mathfrak{b}) = \frac{\mathcal{N}\left(\alpha I_L(\mathbb{Z})\right)}{\mathcal{N}(\mathfrak{a})} = n(\mathfrak{a})$$

Portanto valendo a igualdade.

■

Proposição 32: O número de classes

$$h_L = \#(C\ell_L) = \#\left(\frac{\mathcal{F}(L)}{\mathcal{P}(L)}\right)$$

é finito. Onde $\mathcal{F}(L)$ é o grupo dos ideais fracionários e $\mathcal{P}(L)$ o subgrupo dos ideais fracionários principais.

Demonstração:

Segue da **Proposição 31** que $\{n(\mathfrak{a}) : \mathfrak{a} \trianglelefteq \mathrm{I_L}(\mathbb{Z}) - \{0\}\}$ e $\{m([\mathfrak{u}]) : [\mathfrak{u}] \in \mathrm{C}\ell_\mathrm{L}\}$ coincidem, para quando $\mathfrak{a}^{-1} \in [\mathfrak{u}]$.

Consequentemente toda classe $[\mathfrak{u}] \in \mathrm{C}\ell_\mathrm{L}$ possui um $\mathfrak{b}$ ideal não nulo de $\mathrm{I_L}(\mathbb{Z})$ tal que $\mathcal{N}(\mathfrak{b}) \leq \rho$ de acordo com a **Proposição 30**. Mas pela **Proposição 28** existe apenas um número finito de ideais não nulos $\mathfrak{b}$ de $\mathrm{I_L}(\mathbb{Z})$ tal que $\mathcal{N}(\mathfrak{b}) \leq \rho$.

Sejam $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_m$ os finitos ideais então $\mathrm{C}\ell_\mathrm{L} = \{[\mathfrak{u}_1], [\mathfrak{u}_2], \cdots, [\mathfrak{u}_m]\}$ implica $h_\mathrm{L} = \#(\mathrm{C}\ell_\mathrm{L}) \leq m$, uma vez que $[\mathfrak{u}_i]$ para $1 \leq i \leq m$ não são necessariamente distintas.

■

Para um corpo numérico L, com grau n, existem n isomorfismos distintos $\varphi_i : \mathrm{L} \longrightarrow \mathbb{C}$. Se $\psi : \mathbb{C} \longrightarrow \mathbb{C}$ dada por $\psi(z) = \overline{z}$ é a conjugação complexa, então para todo $i = 1, 2, \cdots, n$ $\psi \circ \varphi_i = \varphi_j$ para algum $j = 1, 2, \cdots, n$ e $\varphi_i = \varphi_j$ quando $\varphi_j(\mathrm{L}) \subseteq \mathbb{R}$.

Seja $r = \#\{1 \leq i \leq n : \varphi_i(\mathrm{L}) \subseteq \mathbb{R}\}$, então $s = n - r$ deve ser um número par e obtemos a igualdade $r + 2s = n$.

Podemos agora tomar uma reordenação para os isomorfismos com $1 \leq t \leq r$ de modo que $\varphi_t(\mathrm{L}) \subseteq \mathbb{R}$, $r + 1 \leq t \leq r + s$ por $\varphi_{t+s}(x) = \overline{\varphi_t(x)}$ e definir a imersão canônica $\varphi : \mathrm{K} \longrightarrow \mathbb{R}^r \times \mathbb{C}^s$ "homomorfismo injetivo" por $\varphi(x) = \big(\varphi_1(x), \cdots, \varphi_{r+s}(x)\big)$.

A proposição seguinte é enunciada sem demonstração por ser necessário um desenvolvimento de uma Teoria de Análise "medida" e Métodos Geométricos.

Proposição 33: Dado um corpo numérico L de grau n tal que $n = r + 2s$, como definido anteriormente, de discriminante d_L e $\mathfrak{a}$ um ideal não nulo de L. Então $\mathfrak{a}$ contém algum elemento não nulo x tal que:

$$\left|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(x)\right| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d_\mathrm{L}|}\mathcal{N}(\mathfrak{a})$$

Demonstração:

O leitor encontrará a verificação em SAMUEL, P. **Algebraic theory of number,** Proposição 01 da Seção 4.3 do Capítulo IV, página 57.

Corolário 12: Toda classe de ideais de L contém um ideal $\mathfrak{b}$ de $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$de tal que

$$\mathcal{N}(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{s} \frac{n!}{n^{n}} \sqrt{|d_{\mathrm{L}}|}$$

Demonstração:

Seja o grupo de classe

$$\mathrm{C}\ell_{\mathrm{L}} = \frac{\mathcal{F}(\mathrm{L})}{\mathcal{P}(\mathrm{L})} = \{[\mathfrak{a}] : \mathfrak{a} \in \mathcal{F}(\mathrm{L})\}$$

Considere $\mathfrak{b}$ um ideal fracionário de alguma classe $[\mathfrak{a}]$.

Podemos multiplicar $\mathfrak{b}$ por um ideal principal de $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$ de modo a não mudar a classe. Sem perda de generalidade podemos assumir que $\mathfrak{b}^{-1}$ é ideal de $\mathrm{I}_{\mathrm{L}}(\mathbb{Z})$.

Tal candidato é $\mathfrak{m} = x\mathfrak{b}$ onde x é elemento não nulo de $\mathfrak{b}^{-1}$ que satisfaz a desigualdade da **Proposição 33**.

Logo e $\langle x \rangle = \mathfrak{m}\mathfrak{b}^{-1}$ e

$$\mathcal{N}(\langle x \rangle) = \mathcal{N}(x) = \mathcal{N}(\mathfrak{m})\mathcal{N}(\mathfrak{b}^{-1}) \Longrightarrow$$
$$\mathcal{N}(\mathfrak{m})\mathcal{N}(\mathfrak{b}^{-1}) \leq \left(\frac{4}{\pi}\right)^{s} \frac{n!}{n^{n}} \sqrt{|d_{\mathrm{L}}|}\mathcal{N}(\mathfrak{b}^{-1}) \Longrightarrow$$
$$\mathcal{N}(\mathfrak{m}) \leq \left(\frac{4}{\pi}\right)^{s} \frac{n!}{n^{n}} \sqrt{|d_{\mathrm{L}}|}$$

■

A cota abaixo é conhecida como Cota de **Hermann Minkowski** que auxilia na determinação do número de classes de corpos numéricos

$$\rho_{\mathrm{L}} = \left(\frac{4}{\pi}\right)^{s} \frac{n!}{n^{n}} \sqrt{|d_{\mathrm{L}}|}$$

Proposição 34: Para todo corpo numérico L com grau $n = [\mathrm{L} : \mathbb{Q}]$, valem as desigualdades:

$$|d_{\mathrm{L}}| \geq \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{n!} \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

Demonstração:

Segue da **Proposição 30** e do **Corolário 12** que para todo ideal não nulo $\mathfrak{a}$ de $\mathrm{I_L}(\mathbb{Z})$ tem-se $1 \leq \mathcal{N}(\mathfrak{a}) \leq \rho_{\mathrm{L}}$, donde

$$\sqrt{|d_{\mathrm{L}}|} \geq \left(\frac{\pi}{4}\right)^{s} \cdot \frac{n^n}{n!}$$

Agora defina

$$a_n = \left(\frac{\pi}{4}\right)^{s} \cdot \frac{n^{2n}}{(n!)^2}$$

para $n \geq 2$. Então $|d_{\mathrm{L}}| \geq a_n$ já que ${}^{\pi}/_{4} < 1$ e $2s = n - r < n$.

Por outro lado

$$a_2 = \frac{\pi^2}{4}$$

e

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} > \frac{3\pi}{4}$$

para todo $n \geq 2$. Assim:

$$a_n = \frac{a_n}{a_{n-1}} \cdot \frac{a_{n-1}}{a_{n-2}} \cdots \frac{a_3}{a_2} a_2 > \left(\frac{3\pi}{4}\right)^{n-2} \frac{\pi^2}{4} = \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}$$

■

Corolário 13: Para todo corpo numérico $\mathrm{L} \neq \mathbb{Q}$ tem-se que $|d_{\mathrm{L}}| > 1$.

Demonstração:

Basta notar que ${}^{\pi}/_{3} > 1$ e ${}^{3\pi}/_{4} > 1$

■

Proposição 35: Se K é um corpo de numérico, então o número de classe $h_{\mathrm{K}} = 1$, quando uma das condições for satisfeita:

(i) Todo ideal primo $\mathfrak{p}$ não nulo de $\mathrm{I_K}(\mathbb{Z})$ com norma $\mathcal{N}(\mathfrak{p}) \leq \rho_{\mathrm{L}}$ é principal.

(ii) Para qualquer número primo $p \leq \rho_{\mathrm{L}}$ o ideal $p\mathrm{I_K}(\mathbb{Z})$ é primo.

Demonstração:

(1) Todo ideal $\mathfrak{b}$ cuja $\mathcal{N}(\mathfrak{b}) \leq \rho_{\mathrm{L}}$ é um produto de ideais primos $\mathfrak{p}$. E considerando condição (i) tais ideais são principais e consequentemente $\mathfrak{b}$ também o é.

(2) Seja o ideal primo $\mathfrak{p}$ não nulo com norma $\mathcal{N}(\mathfrak{p}) \leq \rho_{\mathrm{L}}$. De acordo com a **Proposição 26** temos que $\mathcal{N}(\mathfrak{p}) = p^f$ onde $f \geq 1$ e p é número primo único em $\mathfrak{p}$, logo $p \leq \rho_{\mathrm{L}}$ e $p\mathrm{I}_{\mathrm{K}}(\mathbb{Z}) \subseteq \mathfrak{p}$. E considerando (ii) vale a igualdade $p\mathrm{I}_{\mathrm{K}}(\mathbb{Z}) = \mathfrak{p}$ haja vista que $\mathrm{I}_{\mathrm{K}}(\mathbb{Z})$ é domínio de Dedekind e assim a condição (i) é satisfeita. Usando a parte (1) resulta que $h_{\mathrm{K}} = 1$.

■

3.4.2 Exemplos

Para um domínio fatorial R a fatoração única $\alpha = \alpha_1\alpha_2 \cdots \alpha_r$ em fatores irredutíveis $\alpha_1, \alpha_2, \cdots, \alpha_r$ fornece uma fatoração para $\alpha\mathrm{R}$ já que $\alpha_1\mathrm{R}, \alpha_2\mathrm{R}, \cdots, \alpha_r\mathrm{R}$ são ideais primos não nulos de R. Mas se R não for fatorial, então existem elementos α_i irredutíveis que não são primos e portanto $\alpha_i\mathrm{R}$ será um produto de pelo menos dois ideais primos. Então a fatoração de $\alpha\mathrm{R}$ em ideais primos é obtida juntando as fatorações dos ideais $\alpha_1\mathrm{R}, \alpha_2\mathrm{R}, \cdots, \alpha_r\mathrm{R}$ seja qual for a fatoração em fatores irredutíveis.

Exemplo 11: Considere o corpo quadrático $\mathrm{L} = \mathbb{Q}\left(\sqrt{-17}\right)$, então o anel $\mathrm{R} = \mathrm{I}_{\mathrm{L}}(\mathbb{Z}) = \mathbb{Z}\left[\sqrt{-17}\right] = \left\{m + n\sqrt{-17} : m, n \in \mathbb{Z}\right\}$ não é fatorial, uma vez que admite as fatorações distintas $18 = 2 \cdot 3 \cdot 3 = \left(1 + \sqrt{-17}\right)\left(1 - \sqrt{-17}\right)$ em fatores irredutíveis.

Para isso sejam os ideais de R

$$\mathfrak{p} = 2\mathrm{R} + \left(1 + \sqrt{-17}\right)\mathrm{R}$$

$$\mathfrak{q} = 3\mathrm{R} + \left(1 + \sqrt{-17}\right)\mathrm{R}$$

$$\mathfrak{r} = 3\mathrm{R} + \left(1 - \sqrt{-17}\right)\mathrm{R}$$

Então:

(i) $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ são ideais primos de R e $f(\mathfrak{p}) = f(\mathfrak{q}) = f(\mathfrak{r}) = 1$

(ii) $18\mathrm{R} = \mathfrak{p}^2 \cdot \mathfrak{q}^2 \cdot \mathfrak{r}^2$

(iii) $2\mathrm{R} = \mathfrak{p}^2, 3\mathrm{R} = \mathfrak{q} \cdot \mathfrak{r}, \left(1+\sqrt{-17}\right)\mathrm{R} = \mathfrak{p} \cdot \mathfrak{q}^2, \left(1-\sqrt{-17}\right)\mathrm{R} = \mathfrak{p} \cdot \mathfrak{r}^2$

Solução:

(i) De fato, tem-se que $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ são ideais de R e

$$\frac{\mathrm{R}}{\mathfrak{p}} = \{\mathfrak{p}, 1+\mathfrak{p}\}$$
$$\frac{\mathrm{R}}{\mathfrak{q}} = \{\mathfrak{q}, 1+\mathfrak{q}, 2+\mathfrak{q}\}$$
$$\frac{\mathrm{R}}{\mathfrak{r}} = \{\mathfrak{r}, 1+\mathfrak{r}, 2+\mathfrak{r}\}$$

Daí segundo a definição $\mathcal{N}(\mathfrak{p}) = 2, \mathcal{N}(\mathfrak{q}) = 3, \mathcal{N}(\mathfrak{r}) = 3$.

Segundo a o item (a) da **Proposição 26** $f(\mathfrak{p}) = f(\mathfrak{q}) = f(\mathfrak{r}) = 1$.

(ii) Note que $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ são ideais dois a dois comaximais, donde $\mathfrak{p}^2 \cap \mathfrak{q}^2 \cap \mathfrak{r}^2 = \mathfrak{p}^2 \cdot \mathfrak{q}^2 \cdot \mathfrak{r}^2$. Por outro lado:

$$3 \in \mathfrak{q} \cap \mathfrak{r} = \mathfrak{q} \cdot \mathfrak{r} \Longrightarrow 18\mathrm{R} \in \mathfrak{q}^2 \cdot \mathfrak{r}^2$$
$$18 = \left(1+\sqrt{-17}\right)\left(1-\sqrt{-17}\right) \in \mathfrak{p}^2$$

donde $18^2 \in \mathfrak{p}^2 \cap \mathfrak{q}^2 \cap \mathfrak{r}^2 = \mathfrak{p}^2 \cdot \mathfrak{q}^2 \cdot \mathfrak{r}^2$.

Logo $\mathcal{N}(18\mathrm{R}) = \left|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(18)\right| = 18^2 = 2^2 \cdot 3^2 \cdot 3^2 = \mathcal{N}(\mathfrak{p}^2 \cdot \mathfrak{q}^2 \cdot \mathfrak{r}^2)$ e $18\mathrm{R}$ é múltiplo de $\mathfrak{p}^2 \cdot \mathfrak{q}^2 \cdot \mathfrak{r}^2$, pelo item (a) da **Proposição 27** e (b) da **Proposição 29**.

Portanto pelo item (c) da **Proposição 29**, tem-se que $18\mathrm{R} = \mathfrak{p}^2 \cdot \mathfrak{q}^2 \cdot \mathfrak{r}^2$.

(iii) Segue que $2\mathrm{R}$, $3\mathrm{R}$, $\left(1+\sqrt{-17}\right)\mathrm{R}$ e $\left(1-\sqrt{-17}\right)\mathrm{R}$ são múltiplos de $18\mathrm{R} = \mathfrak{p}^2 \cdot \mathfrak{q}^2 \cdot \mathfrak{r}^2$. Mas $2 \notin \mathfrak{q}$ e $2 \notin \mathfrak{r}$ logo $2\mathrm{R}$ divide $\mathfrak{p}^2$ e como $\mathcal{N}(2\mathrm{R}) = \left|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}(2)\right| = 4 = \mathcal{N}(\mathfrak{p}^2)$ resulta que $\mathfrak{p}^2 = 2\mathrm{R}$.

Também $3 \in \mathfrak{q} \cap \mathfrak{r} = \mathfrak{q} \cdot \mathfrak{r}$ donde 3R é múltiplo de $\mathfrak{q} \cdot \mathfrak{r}$ e por $\mathcal{N}(3\mathrm{R}) = 9 = \mathcal{N}(\mathfrak{q} \cdot \mathfrak{r})$ segue que $\mathfrak{q} \cdot \mathfrak{r} = 3\mathrm{R}$.

Como $\left(1 + \sqrt{-17}\right) \in \mathfrak{p} \cap \mathfrak{q} = \mathfrak{p} \cdot \mathfrak{q}$, mas $\left(1 - \sqrt{-17}\right) \notin \mathfrak{r}$ tem-se que $\left(1 + \sqrt{-17}\right)\mathrm{R}$ é múltiplo de $\mathfrak{p} \cdot \mathfrak{q}$. Daí $\left(1 + \sqrt{-17}\right)$ é um dos ideais $\mathfrak{p} \cdot \mathfrak{q}$, $\mathfrak{p}^2 \cdot \mathfrak{q}$, $\mathfrak{p} \cdot \mathfrak{q}^2$, $\mathfrak{p}^2 \cdot \mathfrak{q}^2$, mas somente $\mathcal{N}(\mathfrak{p} \cdot \mathfrak{q}^2) = 18 = \left|\mathcal{N}_{(\mathrm{L}|\mathbb{Q})}\left(1 + \sqrt{-17}\right)\right| = \mathcal{N}\left(1 + \sqrt{-17}\right)$ resultando $\left(1 + \sqrt{-17}\right)\mathrm{R} = \mathfrak{p} \cdot \mathfrak{q}^2$.

De modo análogo verifica-se que $\left(1 - \sqrt{-17}\right) = \mathfrak{p} \cdot \mathfrak{r}^2$.

Exemplo 12: Para um corpo quadrático $\mathrm{L} = \mathbb{Q}\left(\sqrt{d}\right)$ com d livre de quadrados tem-se que:

$$\rho_{\mathrm{L}} = \begin{cases} \frac{1}{2}\sqrt{|d_{\mathrm{L}}|}, d > 0 \\ \frac{2}{\pi}\sqrt{|d_{\mathrm{L}}|}, d < 0 \end{cases}$$

Solução:

Segue direto da cota de Minkowski, com $r + 2s = n = 2$ e como $\mathrm{A}ut(\mathrm{L}) = \{id, \varphi\}$ com $\varphi\left(a + b\sqrt{d}\right) = a - b\sqrt{d}$, resulta que $s = 0$, quando $d > 0$ e $s = 1$ quando $d < 0$.

Também

$$d_{\mathrm{L}} = \begin{cases} 4d, \text{quando } d \equiv 2, 3 \; mod(4) \\ d, \text{quando } d \equiv 1 \; mod(4) \end{cases}$$

4 A CONJECTURA DE GAUSS E OS CORPOS DE CLASSES DE HILBERT

Em Disquisitiones Arithmeticae de **Carl F. Gauss**, há evidências de uma conjectura que fala sobre a existência de uma enumeração segundo o aumento do valor absoluto do discriminante de corpos numéricos com número de classe igual a 1. Mais precisamente:

"Existem infinitos corpos quadráticos com número de classe igual a 1 e que exatamente 9 deles são complexos"

Esse enunciado é a versão adaptada de Disquisitiones Arithmeticae, Conjecturado por Gauss para os objetivos do capítulo.

Heegner e Stark verificaram a existência desses 9 corpos quadráticos complexos independentemente da veracidade do primeiro enunciado da conjectura e Baker exibiu esses 9 corpos.

O primeiro enunciado continua ainda um problema em aberto e mais ainda não sabe se existem infinitos corpos numéricos com número de classe igual a 1. Para tratar de problemas como esse, é natural recorrer aos corpos de classes de Hilbert.

O objetivo dos resultados é sugerir uma família de corpos numéricos "corpos de classes de Hilbert de corpos quadráticos complexos" que pode abrigar uma infinidade de corpos com número de classe igual a 1 e relacionar isso com a Conjectura de Gauss.

4.1 $\ell(\mathrm{K}) = 0$ e Corpos de Classes de Hilbert

Dado um corpo numérico K, adotamos a seguinte notação $\mathrm{C}\ell_{\mathrm{K}}$, $h_{\mathrm{K}} = \#(\mathrm{C}\ell_{\mathrm{K}})$ e $d_{\mathrm{K}} = disc(\mathrm{K})$ para ser o seu grupo de classes, seu número de classes e seu discriminante respectivamente.

Seja K um corpo numérico com número de classes $h_{\mathrm{K}} = \#(\mathrm{C}\ell_{\mathrm{K}})$. O corpo de classes de Hilbert de K "denotado por H(K)" é uma extensão abeliana maximal não ramificada sobre K, com grau $[\mathrm{H}(\mathrm{K}):\mathrm{K}] = h_{\mathrm{K}}$.

Defina por $\mathrm{H}_0(\mathrm{K}) = \mathrm{K}$, $\mathrm{H}_{i+1}(\mathrm{K}) = \mathrm{H}\big(\mathrm{H}_i(\mathrm{K})\big)$ para $i \in \mathbb{N}$ e $\mathbb{H} = \bigcup_{i\in\mathbb{N}} \mathrm{H}_i(\mathrm{K})$. Considere também o invariante $\ell(\mathrm{K})$ chamado comprimento da cadeia de corpos de

classes de Hilbert de K como segue $\ell(\mathrm{K}) = mín.\{i \in \mathbb{N} : \mathrm{H}_{i+1}(\mathrm{K}) = \mathrm{H}_i(\mathrm{K})\}$ quando tal $i \in \mathbb{N}$ existe e $\ell(\mathrm{K}) = +\infty$ caso contrário.

Dizer que o comprimento $\ell(\mathrm{K}) = +\infty$ é equivalente a dizer que cada extensão finita de K, tem número de classes $h_{\mathrm{K}} > 1$ ou então que a cadeia dos corpos

$$\mathrm{K} = \mathrm{H}_0(\mathrm{K}) \subseteq \mathrm{H}_1(\mathrm{K}) \subseteq \cdots \subseteq \mathrm{H}_n(\mathrm{K}) \subseteq \cdots \subseteq \mathbb{H}$$

não é estacionária. O resultado de **Heegner**-**Stark**-**Baker** agora pode ser enunciado por:

"Existem somente 9 corpos quadráticos complexos K *tal que* $\ell(\mathrm{K}) = 0$*"*

E os tais corpos com essa propriedade são:

$\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$

Os discriminantes dos corpos acima "denominados discriminantes fundamentais negativos" são respectivamente:

$$d_{\mathrm{K}} = disc(\mathrm{K}) = -4, -8, -3, -7, -11, -19, -43, -67, -163$$

Para um corpo numérico K, com $h_{\mathrm{K}} = |\mathrm{C}\ell_{\mathrm{K}}| = p^n m$ tal que p é primo que não divide m, a $p - parte$ de $\mathrm{C}\ell_{\mathrm{K}}$ é o $p - Sylow$ S "Sylow $p - subgrupo$ de ordem p^n", ou seja:

$$\{id\} \leq \cdots \leq \mathrm{S} \leq \mathrm{Gal}(\mathrm{H}(\mathrm{K})|\mathrm{K})$$

Uma $p - extensão$ L de um corpo K é uma extensão galoisiana tal que o grupo Gal(L|K) é um $p - grupo$, ou seja $[\mathrm{L} : \mathrm{K}] = p^a$.

Para um número primo fixo p, o corpo $p - classe$ de Hilbert de K denotado por $\mathrm{H}^p(\mathrm{K})$ é uma $p - extensão$ maximal não ramificada contida em H(K), ou seja:

$$\mathrm{K} = \mathrm{H}_0(\mathrm{K}) \subseteq \cdots \subset \mathrm{H}^p(\mathrm{K}) \subseteq \mathrm{H}(\mathrm{K})$$

As seguintes propriedades do corpo $\mathrm{H}(\mathrm{K})$ são consequências do Teorema de Hilbert da Teoria dos Corpos de Classes:

(1) Existe o corpo de classe de Hilbert de um corpo numérico e é unicamente determinado.

(2) Todo ideal $\mathfrak{a}$ de $\mathrm{I}_{\mathrm{K}}(\mathbb{Z})$ é principal em $\mathrm{I}_{\mathrm{H(K)}}(\mathbb{Z})$, ou seja $\mathfrak{a} = \langle\alpha\rangle = \alpha\mathrm{I}_{\mathrm{H(K)}}(\mathbb{Z})$ para algum $\alpha \in \mathrm{I}_{\mathrm{H(K)}}(\mathbb{Z})$.

(3) $\mathrm{H}(\mathrm{K}) = \mathrm{K}$ se e somente se $h_{\mathrm{K}} = 1$.

(4) $\mathrm{K} \subseteq \mathrm{L}$ implica $\mathrm{H}(\mathrm{K}) \cdot \mathrm{L} \subseteq \mathrm{H}(\mathrm{L})$.

(5) $\mathrm{Gal}(\mathrm{H}(\mathrm{K})|\mathrm{K}) \cong \mathrm{C}\ell_{\mathrm{K}}$.

Exemplo 01: As extensões:

$$\mathbb{Q}\left(\sqrt{6}, \sqrt{-2}\right), \mathbb{Q}\left(\sqrt{-23}, \alpha\right), \mathbb{Q}\left(\sqrt{-31}, \beta\right), \mathbb{Q}\left(\sqrt{-14}, \sqrt{2\sqrt{2}-1}\right)$$

dos respectivos corpos

$$\mathbb{Q}\left(\sqrt{6}\right), \mathbb{Q}\left(\sqrt{-23}\right), \mathbb{Q}\left(\sqrt{-31}\right), \mathbb{Q}\left(\sqrt{-14}\right)$$

são exemplos de corpos de classes de Hilbert sobre a base do corpo, onde $\alpha^3 - \alpha - 1 = 0$ e $\beta^2 + \beta + 1 = 0$. Veja maiores detalhes na referência CONRAD, K. **History of Class Field Theroy.**

Proposição 01: Para todo corpo numérico K, as condições são equivalentes:

(a) $[\mathbb{H} : \mathrm{K}]$ é finito.

(b) A cadeia $\mathrm{K} = \mathrm{H}_0(\mathrm{K}) \subseteq \mathrm{H}_1(\mathrm{K}) \subseteq \cdots \subseteq \mathrm{H}_n(\mathrm{K}) \subseteq \cdots \subseteq \mathbb{H}$ é estacionária.

(c) Existe uma extensão finita L de K tal que $h_{\mathrm{L}} = 1$.

Demonstração:

$(a) \Longrightarrow (b)$ Segue que para todo $i \in \mathbb{N}$ tem-se $\mathrm{H}_i(\mathrm{K}) \subseteq \bigcup_{i\in\mathbb{N}} \mathrm{H}_i(\mathrm{K}) = \mathbb{H}$. Considere então a cadeia $\mathrm{K} = \mathrm{H}_0(\mathrm{K}) \subseteq \mathrm{H}_1(\mathrm{K}) \subseteq \cdots \subseteq \mathrm{H}_n(\mathrm{K}) \subseteq \cdots$

Logo $[\mathrm{H}_i(\mathrm{K}) : \mathrm{K}] \leq [\mathbb{H} : \mathrm{H}_i(\mathrm{K})] \cdot [\mathrm{H}_i(\mathrm{K}) : \mathrm{K}] = [\mathbb{H} : \mathrm{K}]$ para todo $i \in \mathbb{N}$, e com isso com por hipótese $[\mathbb{H}: \mathrm{K}]$ é finito, existe um $n_0 \in \mathbb{N}$ tal que $\mathrm{H}_n(\mathrm{K}) = \mathrm{H}_{n_0}(\mathrm{K})$ para $n \geq n_0$ significando que $\big(\mathrm{H}_i(\mathrm{K})\big)_{i\in\mathbb{N}}$ é estacionária.

$(b) \Longrightarrow (c)$ Se existir um $m \in \mathbb{N}$ tal que $\mathrm{H}_m(\mathrm{K}) = \mathrm{H}_{m+1}(\mathrm{K}) = \cdots = \mathbb{H}$, então para a extensão $\mathrm{L} = \mathbb{H}$ tem-se que $\mathrm{H}(\mathrm{L}) = \mathrm{H}(\mathbb{H}) = \mathbb{H} = \mathrm{L}$ donde $h_{\mathrm{L}} = 1$.

$(c) \Longrightarrow (a)$ É suficiente verificar que $[\mathrm{H}_n(\mathrm{K}) : \mathrm{K}]$ é finito para todo $n \in \mathbb{N}$. Vamos usar indução matemática. Para $n = 0$ tem-se $\mathrm{H}_0(\mathrm{K}) = \mathrm{K}$ donde $[\mathrm{H}_0(\mathrm{K}) : \mathrm{K}] = 1$. Admita por hipótese que para $i > 0$ exista uma extensão $\mathrm{L}|\mathrm{K}$ em que $\mathrm{H}_i(\mathrm{K}) \subseteq \mathrm{L}$.

Como por hipótese $h_{\mathrm{L}} = 1$, tem-se que $\mathrm{H}(\mathrm{L}) = \mathrm{L}$, donde $\mathrm{H}_i(\mathrm{K}) \subseteq \mathrm{L}$ implica $\mathrm{H}_{i+1}(\mathrm{K}) = \mathrm{H}\big(\mathrm{H}_i(\mathrm{K})\big) \subseteq \mathrm{H}\big(\mathrm{H}_i(\mathrm{K})\big) \cdot \mathrm{L} \subseteq \mathrm{H}(\mathrm{L}) = \mathrm{L}$

Portanto $\mathrm{H}_{i+1}(\mathrm{K}) \subseteq \mathrm{L}$ e consequentemente $\mathbb{H} \subseteq \mathrm{L}$. Logo $[\mathbb{H} : \mathrm{K}] \leq [\mathrm{L} : \mathrm{K}] < \infty$ e consequentemente $\mathbb{H}$ é a menor extensão de K com número de classe $h_{\mathrm{K}} = 1$.

■

Um problema em aberto que tratava em saber se todo corpo numérico K estava contido em outro corpo numérico L, tal que o número de classe $h_{\mathrm{L}} = 1$, foi resolvido em 1964 por **Golod-Shafarevich**.

Segundo a **Proposição 01**, a pergunta ao problema seria equivalente a perguntar se para todo corpo numérico K, a torre de corpos $\mathrm{K} = \mathrm{H}_0(\mathrm{K}) \subseteq \mathrm{H}_1(\mathrm{K}) \subseteq \cdots \subseteq \mathrm{H}_n(\mathrm{K}) \subseteq \cdots$ é estacionária e para o caso afirmativo, existiria uma menor extensão $\mathbb{H}$ de K com o número de classe $h_{\mathbb{H}} = 1$.

A resposta a essa pergunta é negativa, **Igor Shafarevich** e **Evgeny Golod** provaram que existem corpos numéricos K com $\ell(\mathrm{K}) = +\infty$, por exemplo, encontraram os corpos quadráticos real e complexo $\mathrm{M} = \mathbb{Q}\big(\sqrt{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19}\big)$ e $\mathrm{N} = \mathbb{Q}\big(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13}\big)$ cuja cadeia de corpos de classes de Hilbert são infinitas e não estão contidos em nenhum outro corpo numérico L com número de classe $h_{\mathrm{L}} = 1$.

Então no intuito de encontrar respostas para a Conjectura de Gauss, podemos investigar o fato sobre a existência de infinitos corpos quadráticos K com $\ell(\mathrm{K}) = 1$.

4.2 $\ell(\mathrm{K}) = 1$ e Principais Resultados

Nessa seção $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ será um corpo quadrático complexo e δ_{K} é considerado para representar o número de divisores primos do discriminante $d_{\mathrm{K}} = disc(\mathrm{K})$.

4.2.1 $\ell(\mathrm{K}) = 1$

Lema 01: Se $\ell(\mathrm{K}) = 1$, então cada subcorpo quadrático complexo F de $\mathrm{H}(\mathrm{K})$ exceto K tem número de classe $h_{\mathrm{F}} = 1$.

Demonstração:

Se $\delta_{\mathrm{K}} = 1$ então não há nada para fazer, uma vez que o único subcorpo quadrático de $\mathrm{H}(\mathrm{K})$ é o próprio K.

Se $\delta_{\mathrm{K}} > 1$ e M é um subcorpo quadrático de $\mathrm{H}(\mathrm{K})$ distinto de K, então $\mathrm{L} = \mathrm{KM}$ é uma extensão intermediária de $\mathrm{H}(\mathrm{K})|\mathrm{K}$, portanto quadrática não ramificada sobre K, com $[\mathrm{L} : \mathrm{K}] = 2$.

Por outro lado, L também é uma $(2,2) - extensão$ de $\mathbb{Q}$, significando que $\mathrm{Gal}(\mathrm{L}|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ no que resulta em $\#\big(\mathrm{Gal}(\mathrm{L}|\mathbb{Q})\big) = \#(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2^2$ e segundo os Teoremas de Sylow e da Correspondência de Galois, existe um subgrupo de ordem 2 correspondente a um terceiro subcorpo quadrático N de L.

Então $\mathrm{K} \subset \mathrm{M}, \mathrm{N}, \mathrm{L} \subset \mathrm{H}(\mathrm{K})$ e denotando o número de classes de M e N respectivamente por h_{M} e h_{N}, segue que segundo a fórmula de **Herglotz "**G. HERGLOTZ. **Uber Einen Dirichletschen Satz"**, que o número de classes de L é dado por:

$$h_{\mathrm{L}} = \frac{h_{\mathrm{K}} h_{\mathrm{M}} h_{\mathrm{N}}}{\rho}$$

onde $\rho = 1$ ou $\rho = 2$.

Mas H(L) é uma extensão abeliana não ramificada de H(K) e é consequentemente igual a H(K) uma vez que pela hipótese $\ell(\mathrm{K}) = 1$ equivalentemente a $h_{\mathrm{H(K)}} = 1$. Portanto:

$$[\mathrm{H(K)} : \mathrm{K}] = [\mathrm{H(L)} : \mathrm{K}] = [\mathrm{H(L)} : \mathrm{L}] \cdot [\mathrm{L} : \mathrm{K}] \Leftrightarrow h_{\mathrm{K}} = 2h_{\mathrm{L}} \Leftrightarrow h_{\mathrm{L}} = \frac{h_{\mathrm{K}}}{2}$$

e pela fórmula de Herglotz resulta

$$\frac{h_{\mathrm{K}}}{2} = h_{\mathrm{L}} = \frac{h_{\mathrm{K}} h_{\mathrm{M}} h_{\mathrm{N}}}{\rho} \Longrightarrow h_{\mathrm{M}} h_{\mathrm{N}} = \frac{\rho}{2}$$

Por outro lado, o número de classes é um inteiro, resultando $\rho = 2$ e $h_{\mathrm{M}} h_{\mathrm{N}} = 1$, donde $h_{\mathrm{M}} = 1$, ficando provado.

■

Lema 02: Suponha que $\ell(\mathrm{K}) = 1$. Então:

(a) A $p - parte$ de $\mathrm{C}\ell_{\mathrm{K}}$ com p ímpar é cíclica.

(b) Se a $2 - parte$ de $\mathrm{C}\ell_{\mathrm{K}}$ não é cíclica, então $d_{\mathrm{K}} = disc(\mathrm{K}) = d_0 d_1 d_2$ com $d_i = d_{\mathrm{L}_i} = disc(\mathrm{L}_i), i = 0, 1, 2$ distintos e L_i corpo quadrático complexo com número de classes $h_{\mathrm{L}_i} = 1$.

Demonstração:

(a) **Afirmação 01:** Se o grupo de classe de um corpo quadrático complexo K tem $p - parte$ não cíclica para algum primo ímpar p, então p divide o número de classes do corpo $p - classe$ de Hilbert de K.

Essa afirmação nem sempre é válida para $p = 2$.

Suponhamos por absurdo que a ímpar $- parte$ S de $\mathrm{C}\ell_{\mathrm{K}}$ seja não cíclica, logo $|\mathrm{S}| = p^a$, onde $h_{\mathrm{K}} = p^a m$ com p não dividindo m.

Então de acordo com a **Afirmação 01**, p divide $h_{\mathrm{H}^p(\mathrm{K})}$ "$h_{\mathrm{H}^p(\mathrm{K})} = pm_0$" e pelos Teoremas de Sylow e da Correspondência de Galois existe um subcorpo intermediário F

de H(K)|K tal que $[\mathrm{H}(\mathrm{K}) : \mathrm{F}] = p^a$. Por outro lado $\mathrm{Gal}(\mathrm{H}^p(\mathrm{K})|\mathrm{K})$ é isomorfo ao $p - Sylow$, donde:

$$h_{\mathrm{K}} = [\mathrm{H}(\mathrm{K}) : \mathrm{K}] = [\mathrm{H}(\mathrm{K}) : \mathrm{F}] \cdot [\mathrm{F} : \mathrm{H}^p(\mathrm{K})] \cdot [\mathrm{H}^p(\mathrm{K}) : \mathrm{K}] \Leftrightarrow$$
$$h_{\mathrm{K}} = p^a \cdot [\mathrm{F} : \mathrm{H}^p(\mathrm{K})] \cdot h_{\mathrm{H}^p(\mathrm{K})} \Leftrightarrow$$
$$h_{\mathrm{K}} = p^a \cdot [\mathrm{F} : \mathrm{H}^p(\mathrm{K})] \cdot pm_0 \Leftrightarrow$$
$$h_{\mathrm{K}} = p^{a+1} m_0 \cdot [\mathrm{F} : \mathrm{H}^p(\mathrm{K})]$$

o que é uma contradição com a maximalidade do $p - Sylow$. Veja maiores detalhes na referência R. BOND. **Unramified Abelian Extensions of Number Fields** ou A. NOMURA. **On the Existence of Unramified p-Extensions**.

(b) Agora suponha que o grupo de classe de K tem $2 - parte$ não cíclica e que o corpo de classes de Hilbert de K tem número de classes $h_{\mathrm{H(K)}} = 1 \Leftrightarrow \ell(\mathrm{K}) = 1$.

Pela **Teoria de Gênero** "teoria desenvolvida por Gauss que envolve caracteres e formas quadráticas", o discriminante $d_{\mathrm{K}} = disc(\mathrm{K})$ de K é divisível por pelo menos 3 números primos. Seja então $d_{\mathrm{K}} = disc(\mathrm{K}) = d_1 d_2 d_3$ onde d_i para $i = 1, 2, 3$, são discriminantes de corpos quadráticos. Então $\mathrm{L}_i = \mathrm{K}\left(\sqrt{d_i}\right)$ é uma extensão quadrática de K não ramificada para $i = 1, 2, 3$. Segundo o **Lema 01**, esses 6 corpos quadráticos $\mathbb{Q}\left(\sqrt{d_r}\right)$, $\mathbb{Q}\left(\sqrt{d_s d_t}\right)$ $r, s, t \in \{1, 2, 3\}$ com $s \neq t$, tem número de classe igual a 1.

Portanto $\mathbb{Q}\left(\sqrt{d_s d_t}\right)$ deve ser um corpo quadrático real para $s \neq t$, pois do contrário, o número de classes desse corpo seria par.

Então os discriminantes d_i para $i = 1, 2, 3$, devem ser todos de mesmo sinal, mais precisamente todos negativos, uma vez que $d_{\mathrm{K}} = disc(\mathrm{K})$ é negativo.

Portanto os discriminantes d_i para $i = 1, 2, 3$ estão entre os 9 discriminantes fundamentais negativos de **Heegner**-**Stark**-**Baker**.

■

4.2.2 Principais Resultados

Proposição 02: Se $\ell(\mathrm{K}) = 1$, então o corpo quadrático complexo K é uma das seguintes classificações:

(i) $\delta_{\mathrm{K}} = 1$ e $\mathrm{C}\ell_{\mathrm{K}}$ é cíclico de ordem ímpar.

(ii) $\delta_{\mathrm{K}} = 2$ e $\mathrm{C}\ell_{\mathrm{K}}$ é cíclico de ordem par com $d_{\mathrm{K}} = disc(\mathrm{K}) = d_0 d_1$ onde d_0 é o discriminante de um corpo quadrático complexo M com número de classe $h_{\mathrm{M}} = 1$ e d_1 é o discriminante de um corpo quadrático real N com número de classe $h_{\mathrm{N}} = 1$, sendo $d_1 = 8$ ou $d_1 = p$ com p primo.

(iii) $\delta_{\mathrm{K}} = 3$ e $d_{\mathrm{K}} = d_0 d_1 d_2$ com $d_i = d_{\mathrm{L}_i} = disc(\mathrm{L}_i)$, $i = 0, 1, 2$ distintos e L_i corpo quadrático complexo com número de classe $h_{\mathrm{L}_i} = 1$.

Demonstração:

(i) Se $\delta_{\mathrm{K}} = 1$, então pela Teoria de Gênero, e o **Lema 02**, $\mathrm{C}\ell_{\mathrm{K}}$ é cíclico de ordem ímpar.

(ii) Se $\delta_{\mathrm{K}} = 2$, então pelo mesmo raciocínio do item (i), $\mathrm{C}\ell_{\mathrm{K}}$ é cíclico de ordem par, donde $d_{\mathrm{K}} = d_0 d_1$, onde d_0 é algum discriminante primo negativo e d_1 é algum discriminante primo positivo. Por outro lado, pelo **Lema 01**, os corpos quadráticos com discriminante d_0 e d_1 tem número de classe igual a 1.

(iii) Se $\delta_{\mathrm{K}} \geq 3$, então a $2 - parte$ de $\mathrm{C}\ell_{\mathrm{K}}$ não é cíclica e assim pelo item (b) do **Lema 02**, K será um entre os 6 finitos corpos cujo o discriminante é o produto de 3 inteiros distintos, cada um dos quais é o discriminante de um corpo quadrático complexo com número de classe igual a 1, ou seja $d_{\mathrm{K}} = disc(\mathrm{K}) = d_0 d_1 d_2$ com $d_i = d_{\mathrm{L}_i} = disc(\mathrm{L}_i)$, $i = 0, 1, 2$ distintos e L_i corpo quadrático complexo com número de classe $h_{\mathrm{L}_i} = 1$.

■

Diz-se que K é do tipo (i), (ii) ou (iii), se ele satisfaz as correspondentes condições da **Proposição 02.**

Exemplo 02: Como os corpos de discriminantes fundamentais de **Heegner-Baker-Stark**, estão em número finito, também existe apenas um número finito de corpos do tipo (iii). E os tais corpos com os respectivos discriminantes são:

$$\mathrm{K}=\mathbb{Q}\left(\sqrt{-21}\right)\Longrightarrow d_{\mathrm{K}}=disc(\mathrm{K})=-84=-2^2\cdot 3\cdot 7$$

$$\mathrm{K}=\mathbb{Q}\left(\sqrt{-33}\right)\Longrightarrow d_{\mathrm{K}}=disc(\mathrm{K})=-132=-2^2\cdot 3\cdot 11$$

$$\mathrm{K}=\mathbb{Q}\left(\sqrt{-42}\right)\Longrightarrow d_{\mathrm{K}}=disc(\mathrm{K})=-168=-2^3\cdot 3\cdot 7$$

$$\mathrm{K}=\mathbb{Q}\left(\sqrt{-57}\right)\Longrightarrow d_{\mathrm{K}}=disc(\mathrm{K})=-228=-2^2\cdot 3\cdot 19$$

$$\mathrm{K}=\mathbb{Q}\left(\sqrt{-133}\right)\Longrightarrow d_{\mathrm{K}}=disc(\mathrm{K})=-532=-2^2\cdot 7\cdot 19$$

$$\mathrm{K}=\mathbb{Q}\left(\sqrt{-627}\right)\Longrightarrow d_{\mathrm{K}}=disc(\mathrm{K})=-627=-3\cdot 11\cdot 19$$

Todos eles têm grupo de classes do tipo $(2,2)$, ou seja $\mathrm{C}\ell_{\mathrm{K}}\cong\mathbb{Z}_2\times\mathbb{Z}_2$.

Veja maiores detalhes também na tabela da referência K. YAMAMURA. **The Determination of The Imaginary Abelian Number Fields with Class Number One**.

O próximo exemplo é um resultado extra também relacionado quanto ao uso da fórmula de Herglotz.

Exemplo 03: Se $\ell(\mathrm{K})=1$ e o corpo $2-classe$ de Hilbert de K tem número de classes ímpar, então $\delta_{\mathrm{K}}\leq 3$.

Solução:

Suponha por absurdo que $\delta_{\mathrm{K}}>3$. Escrevendo $d_{\mathrm{K}}=disc(\mathrm{K})=d_0d_1d_2d_3$ onde d_i "$i=0,1,2,3$" estão entre os discriminantes fundamentais.

Como por hipótese o corpo $2-classe$ de Hilbert de K tem número de classes $h_{\mathrm{H}^2(\mathrm{K})}$ ímpar e ele também é o corpo $2-classe$ de Hilbert da extensão quadrática não ramificada $\mathrm{L}=\mathrm{K}\left(\sqrt{d_0}\right)$, logo:

$$[\mathrm{H}^2(\mathrm{K}):\mathrm{K}]=[\mathrm{H}^2(\mathrm{L}):\mathrm{K}]=[\mathrm{H}^2(\mathrm{L}):\mathrm{L}]\cdot[\mathrm{L}:\mathrm{K}]\Leftrightarrow$$

$$h_{\mathrm{H}^2(\mathrm{L})}=2h_{\mathrm{H}^2(\mathrm{L})}\Leftrightarrow h_{\mathrm{H}^2(\mathrm{L})}=\frac{1}{2}h_{\mathrm{H}^2(\mathrm{K})}$$

Então denotando por h'_{F} a ordem de $2-parte$ de $\mathrm{C}\ell_{\mathrm{F}}$ para o corpo numérico F, segue segundo a fórmula de Herglotz que:

$$h'_{\mathrm{L}}=\frac{h'_{\mathrm{K}}\cdot h'_{\mathbb{Q}\left(\sqrt{d_0}\right)}\cdot h'_{\mathbb{Q}\left(\sqrt{d_1d_2d_3}\right)}}{\rho}=\frac{h'_{\mathrm{K}}}{2}\Longrightarrow h'_{\mathbb{Q}\left(\sqrt{d_0}\right)}\cdot h'_{\mathbb{Q}\left(\sqrt{d_1d_2d_3}\right)}=\frac{\rho}{2}$$

com $\rho = 2$ e assim $h'_{\mathbb{Q}(\sqrt{d_0})} \cdot h'_{\mathbb{Q}(\sqrt{d_1 d_2 d_3})} = 1$ implicando que $h'_{\mathbb{Q}(\sqrt{d_1 d_2 d_3})} = 1$ e portanto $\mathbb{Q}\left(\sqrt{d_1 d_2 d_3}\right)$ tem número de classe ímpar, sendo uma contradição pois $h'_{\mathbb{Q}(\sqrt{d_1 d_2 d_3})}$ é par.

Veja maiores detalhes na referência R. BOND. **Unramified Abelian Extensions of Number Fields**.

As considerações finais enunciadas pelos corolários abaixo são consequências da **Proposição 02** e da conjectura:

Conjectura 01 "Hajir": Existem infinitos corpos quadráticos complexos K, com $\delta_{\mathrm{K}} = 1$ e bem como infinitos corpos quadráticos complexos K, com $\delta_{\mathrm{K}} > 1$, ambos os casos para $\ell(\mathrm{K}) = 1$.

Corolário 01:

(a) Se existem infinitos corpos quadráticos complexos K satisfazendo $\ell(\mathrm{K}) = 1$ então existem infinitos corpos quadráticos complexos K com grupo de classe cíclico.

(b) Se existem infinitos corpos quadráticos complexos K, com $\ell(\mathrm{K}) = 1$ e $\delta_{\mathrm{K}} > 1$ então existem infinitos corpos quadráticos reais com discriminante primo e número de classe igual a 1.

Demonstração:

(a) Como os corpos do tipo (iii) estão em número finito, "segundo **Heegner-Stark-Baker**" esses infinitos corpos são do tipo (i) e do tipo (ii) segundo a veracidade da **Conjectura 01**. Portanto com grupo de classe cíclico.

(b) Novamente como os corpos do tipo (iii) estão em número finito, então existindo infinitos corpos quadráticos complexos $\{\mathrm{K}_i\}_{i\in\Gamma}$ com $\ell(\mathrm{K}_i) = 1$ e $\delta_{\mathrm{K}_i} > 1$ os mesmos serão do tipo (ii).

Por outro lado cada $\mathrm{K}_i = \mathbb{Q}\left(\sqrt{d_i}\right)$ tem $d_{\mathrm{K}_i} = disc(\mathrm{K}_i) = d_0 d_1$ onde d_0 está entre os 9 discriminantes fundamentais negativos e d_1 é o discriminante de um corpo quadrático real N com número de classe $h_{\mathrm{N}} = 1$, sendo $d_1 = 8$ ou $d_1 = p$ com p primo.

Note também que $d_{\mathrm{K}_i} = 4d_i$ ou $d_{\mathrm{K}_i} = d_i$ donde $d_0 d_1 = 4d_i$ ou $d_0 d_1 = d_i$. Portanto $d_1 \neq 8$ resultando $d_1 = p$ em número infinito.

■

Corolário 02:

(a) Com exceção de 6, os corpos quadráticos complexos K com $\ell(\mathrm{K}) = 1$ tem grupo de classe cíclico.

(b) Se existir uma infinidade de corpos quadráticos complexos K com $\ell(\mathrm{K}) = 1$ e número de classes h_{K} par, então a Conjectura de Gauss é verdadeira.

Demonstração:

(a) Isso decorre da veracidade da **Conjectura 01** e do fato dos 6 corpos do **Exemplo 02,** cada um ter grupo de classe do tipo $\mathbb{Z}_2 \times \mathbb{Z}_2$ que não é cíclico.

(b) Segue do item (a) do **Corolário 01** que os corpos serão do tipo (ii) de acordo com a **Proposição 02**. Portanto do item (b) do **Corolário 01** existem infinitos corpos quadráticos reais com discriminante primo e número de classe igual a 1.

■

4.3. $\ell(\mathrm{K}) > 1$, Evidências e Outras Considerações

Essa seção é destinada a uma discussão informal de algumas evidências, fatos ou dados relacionados ao número de classes que fornece algumas justificativas para a introdução de algumas conjecturas levantadas.

4.3.1 $\ell(\mathrm{K}) > 1$

Observe que $\ell(\mathrm{K}) > 1$ é equivalente a $h_{\mathrm{H(K)}} > 1$. Na demonstração do item (a) do **Corolário 01** da Seção 2.2, espera-se que os corpos do tipo (i) e tipo (ii) estejam em número infinito, apesar de ser desconhecida a veracidade do seguinte enunciado:

Conjectura 02: Há infinitos corpos quadráticos complexos com grupo de classes cíclico.

Poderíamos então perguntar se existem infinitos corpos quadráticos complexos K do tipo (i) respectivamente do tipo (ii) com $\ell(\mathrm{K}) > 1$?

Na tabela de K. YAMAMURA. **Maximal Unramified Extensions of Imaginary Quadratic Number Fields of Small Conductors**, há exemplos quanto a existência de corpos K do tipo (i), (ii) e (iii) com $\ell(\mathrm{K}) > 1$.

O **Resultado 01** abaixo mostra um caso interessante relacionado a essa questão, por exemplo, na condição de que os corpos K do tipo (i), com o número de classes h_{K} múltiplo de 3, a de $h_{\mathrm{H(K)}}$ para esses corpos é influenciada pela existência de corpos quárticos particulares.

Primeiramente vejamos a afirmação seguinte:

Afirmação 02: Seja L uma extensão galoisiana de K de grau primo $[\mathrm{L} : \mathrm{K}] = p$ e q um primo que não divide ph_{K}. Se q divide h_{L}, então q^f divide h_{L}, onde f é a ordem de q em $\mathcal{U}(\mathbb{Z}_p)$. Em outras palavras, o $q - posto$ de $\mathrm{C}\ell_{\mathrm{L}}$ é divisível por f.

Demonstração:

Isso segue pelo estudo da $q - parte$ de $\mathrm{C}\ell_{\mathrm{L}}$ como $\mathrm{Gal(L|K)} - módulo$.

Veja maiores detalhes na referência K. IWASAWA. **A Note on Ideal Class Groups**.

■

Resultado 01: Se $\mathrm{K} = \mathbb{Q}(\sqrt{-p})$ onde $p \equiv 3\ mod(4)$ é um primo, então existe um corpo quártico F de discriminante $disc(\mathrm{F}) = -p$ se e somente se existe uma extensão cúbica cíclica não ramificada N de K, cujo número de classes h_{N} é par.

Demonstração:

Seja F um corpo quártico de $disc(\mathrm{F}) = -p$.

Afirmação 03: O corpo de divisão E de F é uma $\mathrm{S}_4 - extensão$ de $\mathbb{Q}$ "$\mathrm{Gal(E|\mathbb{Q})} \cong \mathrm{S}_4$" não ramificada sobre K.

Por outro lado como E|K tem grupo de Galois A_4, segue que $\#\big(\mathrm{Gal(E|K)}\big) = |A_4| = {|S_4|}/{2} = 2^2 \cdot 3$, donde pelos Teoremas de Sylow e da Correspondência de Galois existe um corpo intermediário N tal que N|K é cúbica cíclica, logo

$$[H(K) : K] = [H(K) : N] \cdot [N : K] \Leftrightarrow h_K = 3 \cdot [H(K) : N]$$

donde 3 divide h_K e como E|N é $(2,2) - extensão$ "$\mathrm{Gal(E|N)} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$" segue que

$$[H(N) : N] = [H(N) : E] \cdot [E : N] \Leftrightarrow h_N = 4 \cdot [H(N) : E]$$

Portanto h_N é par.

Reciprocamente suponha que exista uma extensão cúbica cíclica não ramificada N de K tal que o número de classes h_N é par. De acordo com a **Afirmação 02**, o grupo de classes de N tem posto pelo menos 2, com isso existe uma extensão não ramificada E de K com o grupo de Galois S_4, ou seja:

$$\mathrm{Gal(E|K)} \cong S_4 \Longrightarrow \#\big(\mathrm{Gal(E|K)}\big) = |S_4| = 2^3 \cdot 3$$

Portanto pelos Teoremas de Sylow e da Correspondência de Galois, E|K admite um corpo intermediário F que é quártico.

Veja maiores detalhes na referência J. P. SERRE. **Modular Forms of Weight 1 and Galois Representations, in 'Algebraic Number Fields'** e T. KONDO. **Algebraic Number Fields with Discriminant Equal to That of a Quadratic Number Field**.

■

Exemplo 04: Existem 6 corpos $K = \mathbb{Q}\big(\sqrt{-p}\big)$ com $0 < p < 1000$, nas condições do **Resultado 01**, todos com h_K múltiplo de 3, mais precisamente $h_K = 3$ e N é a única extensão cúbica cíclica de K não ramificada com número de classes h_N múltiplo de 4, logo par. A saber esses corpos são:

$$\mathbb{Q}\big(\sqrt{-283}\big), \mathbb{Q}\big(\sqrt{-331}\big), \mathbb{Q}\big(\sqrt{-491}\big), \mathbb{Q}\big(\sqrt{-563}\big), \mathbb{Q}\big(\sqrt{-643}\big), \mathbb{Q}\big(\sqrt{-751}\big)$$

Veja maiores detalhes também na tabela da referência K. YAMAMURA. **The Determination of The Imaginary Abelian Number Fields with Class Number One**.

A questão natural que podemos levantar agora é quanto a quantidade de corpos quárticos, em outras palavras:

Conjectura 03: Existem infinitos corpos quárticos com discriminante $-p$, onde p é primo.

Essa conjectura é provável ser verdadeira, mas difícil verificar sua veracidade. Uma consequência dela é o seguinte corolário:

Corolário 03: Se para uma quantidade infinita dos primos p_i o grupo de classes de $\mathrm{K}_i = \mathbb{Q}\left(\sqrt{-p_i}\right)$ é cíclico, então existirão infinitos corpos do tipo (i) cuja cadeia de corpos de classes de Hilbert tem comprimento $\ell(\mathrm{K}_i) > 1$.

Demonstração:

Segue direto da **Conjectura 03** e do **Resultado 01**, uma vez que $\delta_{\mathrm{K}_i} = 1$, h_{N_i} é par e consequentemente $h_{\mathrm{H}(\mathrm{K}_i)} \geq h_{\mathrm{N}_i} = h_{\mathrm{H}^3(\mathrm{K}_i)} \geq 2 > 1$ se e somente se $\ell(\mathrm{K}_i) > 1$.

■

Quanto aos corpos do tipo (ii) também é esperado que existam infinitos corpos quadráticos reais com discriminante primo e número de classe igual a 1 que admitem extensões não ramificadas não solúveis e assim infinitos corpos K do tipo (ii) com $\ell(\mathrm{K}) > 1$. Veja maiores detalhes na referência K. YAMAMURA. **Maximal Unramified Extensions of Imaginary Quadratic Number Fields of Small Conductors** e suas referências.

4.3.2 Evidências e Outras Considerações

Há pelo menos 3 fatos responsáveis pela existência de corpos numéricos com número de classe grande.

Comentamos brevemente sobre a explicação do fato responsável em cada um deles.

Teoria de Gêneros

Afirmação 04: Se K|F é uma extensão galoisiana de grau $p = [\mathrm{K}: \mathrm{F}]$ em que muitos primos são ramificados, então a $p - parte$ de $\mathrm{C}\ell_{\mathrm{K}}$ tem $p - posto$ grande e consequentemente K tem número de classes h_{K} também grande.

Veja maiores detalhes na referência J. MARTINET. **Tours de Corps de Classes et Estimations de Discriminants**.

Extensões CM

Um corpo numérico K é denominado totalmente real, se para cada imersão canônica $\sigma : \mathrm{K} \longrightarrow \mathbb{C}$ a imagem encontra-se contida no conjunto dos números reais e é denominado totalmente complexo ou totalmente imaginário se a imagem da imersão canônica $\sigma : \mathrm{K} \longrightarrow \mathbb{C}$ não está contida em $\mathbb{R}$.

Um corpo numérico K é dito CM quando é uma extensão quadrática totalmente complexa de um corpo totalmente real. São denominados assim por serem corpos numéricos particulares e estarem ligados a Teoria da Multiplicação Complexa "CM".

Qualquer corpo numérico que é uma extensão galoisiana sobre o conjunto dos racionais deve ser totalmente real ou totalmente complexo.

O corpo quadrático K de grau 2 sobre $\mathbb{Q}$ por exemplo é real ou é complexo e no caso real é então totalmente real.

Extensões abelianas de $\mathbb{Q}$ ou são totalmente reais, ou contém um subcorpo totalmente real sobre o qual tem grau 2.

Harold Stark conjecturou em 1974 que há um número finito de corpos CM com número de classe igual a 1 e mostrou que há um número finito com grau fixo. Também tem mostrado que os corpos CM tendem a ter número de classes grande.

Princípio de Stark: Se K é variado sobre as extensões quadráticas totalmente complexas de um corpo fixo F totalmente real, então "o menor número de classe" $h_{\mathrm{K}}/h_{\mathrm{F}}$ tende para infinito.

Algum tempo depois, **Andrew Odlyzko** mostrou que há somente um número finito de extensões CM galoisianas com número de classe igual a 1.

V. Kumar Murty mostrou em 2001, que de todos os corpos CM cujo fecho de Galois tem grupo de Galois solúvel, somente um número finito tem número de classe igual a 1.

A completa lista dos 172 corpos CM abelianos com número de classe igual a 1 foi determinada no início de 1990 por **Ken Yamamura**. Esta mesma lista com a obra de **Stéphane Louboutin** e **Ryotaro Okazaki** fornece uma lista também completa de corpos CM's quárticos com número de classe igual a 1.

Veja maiores detalhes nas referências LOUBOUTIN, S.; OKAZAKI, R. **Determination of all Non-Normal Quartic CM-Fields and of all Non-Abelian Normal Octic CM-Fields with Class Number One**, MURRTY, V. KUMAR. **Class Numbers of CM-Fields with Solvable Normal Closure**, A. M. ODLYZKO. **Some Analytic Estimates of Class Numbers and Discriminants**, H. M. STARK. **Some Effective Cases of The Brauer-Siegel Theorem** e K. YAMAMURA. **The Determination of The Imaginary Abelian Number Fields with Class Number One.**

Grupo de Classe não Cíclico

Afirmação 05: Se F é um corpo numérico que satisfaz o critério de **Golod-Shafarevich** em p, então o $p-posto$ de $C\ell_K$ tende para o infinito quando K é variado ao longo das $p-extensões$ de F não ramificadas.

Em outras palavras, nos dois primeiros fatos anteriores, a ramificação é o mecanismo por trás do número de classes grande, mas algumas vezes, o número de classes é grande, como resultado de extensões não cíclicas que não se ramificam.

O critério de **Golod-Shafarevich** "o $p-posto$ de $C\ell_F$ é grande com relação ao grau de F" foi provado em 1964 pelos dois matemáticos russos, Evgeny Golod e Igor Shafarevich e é um resultado em Álgebra não Comutativa Homológica que tem consequências em vários ramos da Álgebra.

Veja maiores detalhes na referência F. HAJIR. **On the Growth of p-Class Groups in p-Class Field Towers.**

Diante dos dados numéricos sugestivos que o número de classe igual a 1 é uma ocorrência comum, falta um entendimento dos mecanismos por trás disso, pode-se reunir

fatos conhecidos e responsáveis pelo número de classes grande e supor que na sua ausência, o número de classes tende a ser pequeno.

Em uma tentativa de formalizar uma afirmação mais precisa, notamos que algumas vezes, um corpo numérico tem número de classes grande porque um de seus subcorpos está sob a influência de um dos fatos discutidos: Teoria de Gêneros, Extensões CM ou Grupo de Classes não Cíclico.

Para levar isso em conta, defina e denote o novo corpo de classes de Hilbert do corpo numérico K, por:

$$\widetilde{\mathrm{H}}(\mathrm{K}) = \bigcup_{\substack{\mathrm{K}|\mathrm{N} \\ \mathrm{N}\subsetneq\mathrm{K}}} \mathrm{H}(\mathrm{N})$$

De fato $\widetilde{\mathrm{H}}(\mathrm{K}) \subseteq \mathrm{H}(\mathrm{K})$ e definindo o novo número de classes de K por $\left[\mathrm{H}(\mathrm{K}) : \widetilde{\mathrm{H}}(\mathrm{K})\right] = \tilde{h}_{\mathrm{K}}$, podemos formular de acordo com os resultados de **Stark** a seguinte pergunta:

Em uma família genérica de corpos numéricos não CM's enumerados segundo o aumento absoluto do valor do discriminante, uma proporção positiva, tem $\tilde{h}_K = 1$*?*

O termo genérico deve ser tomado com cuidado de modo a evitar número de classes proveniente da contribuição da **Afirmação 04** da Teoria de Gêneros, por exemplo, para os corpos não CM's, subextensões normais de primos indexados, devem ter alguns primos ramificados.

Sugerimos agora a família dos corpos de classes de Hilbert de corpos numéricos com grupo de classe cíclica. Em outras palavras:

Conjectura 04: Uma enumeração de acordo com o aumento do valor absoluto do discriminante de corpos numéricos K com grupo de classes cíclico tem $\ell(\mathrm{K}) = 1$

Conjectura 05: O corpo H(K) de um corpo numérico K com $\mathrm{C}\ell_{\mathrm{K}}$ cíclico tem $h_{\mathrm{H(K)}} = 1$.

Algumas evidências para a **Conjectura 04** são provenientes do próximo resultado.

Resultado 02: Se a $p-parte$ de $C\ell_K$ é cíclico, então p não divide o número de classes do corpo $p-classe$ de Hilbert de K.

Demonstração:

Se G é o grupo de Galois sobre K de uma $p-extensão$ não ramificada L de K, ou seja $G = Gal(L|K)$, então G é um $p-grupo$, ou seja $[L : K] = p^a$ e por base do **Teorema de Burside**, G é cíclico "logo abeliano" porque seu quociente abeliano maximal é isomorfo a $C\ell_K$ pela Teoria dos Corpos de Classes.

Como G é abeliano, os corpos $p-classe$ de Hilbert de K são extensões maximais não ramificadas de K, assim devem ter número de classes p primo.

■

Os próximos exemplos são evidências e indicações quanto a veracidade da **Conjectura 04** e da **Conjectura 01**.

Exemplo 05: Considere a família $\{K_i\}_{i\in\Gamma}$ dos corpos quadráticos reais tal que o discriminante $d_{K_i} = disc(K_i) = 5p_i$ onde p_i é um primo e $p_i \equiv 13\ mod(20)$ ou $p_i \equiv 17\ mod(20)$.

Então veja que $2-parte$ de $C\ell_{K_i}$ tem ordem prima 2 "desde que p_i não é resíduo $mod(5)$" e por H. COHEN and H. W. LENSTRA. **Heuristics on Class Groups of Number Fields** espera-se infinitos desses K_i tenham a ímpar $-parte$, o grupo trivial.

Para a família de corpos $\{K_i\}_{i\in\Gamma}$ temos $H(K_i) = \mathbb{Q}(\sqrt{5}, \sqrt{p_i})$ e pelo **Resultado 02**, 2 não divide $h_{H^2(K_i)}$ e assim $H(K_i)$ tem número de classe $h_{H(K_i)}$ ímpar, daí pela fórmula de **Herglotz**

$$h_{H(K_i)} = h_{\mathbb{Q}(\sqrt{5})} \cdot h_{\mathbb{Q}(\sqrt{p_i})}$$

e $\ell(K_i) = 1$ se e somente se $h_{H(K_i)} = 1$ se somente se $h_{\mathbb{Q}(\sqrt{p_i})} = 1$ e segundo H. COHEN and H. W. LENSTRA. **Heuristics on Class Groups of Number Fields** é esperado ou provável que $h_{\mathbb{Q}(\sqrt{p_i})} = 1$ em quantidade infinita de p_i's.

De modo mais geral, as evidências da referência H. COHEN and H. W. LENSTRA. **Heuristics on Class Groups of Number Fields** prevê o fato conjecturado:

Conjectura 06: Uma grande densidade positiva de corpos quadráticos reais com número de classes igual a 2, tem cadeia de corpos de classes de Hilbert de comprimento igual a 1.

Exemplo 06: Suponha que K seja um corpo quadrático complexo e L é uma extensão de K não ramificada de grau primo ímpar p. Então:

$$h_{\mathrm{L}} = \frac{(h_{\mathrm{F}})^2 \cdot h_{\mathrm{K}}}{p} a$$

onde $a = 1$ ou $a = p$.

Se a $p - parte$ de $\mathrm{C}\ell_{\mathrm{K}}$ é cíclica, então $a = 1$. Em particular se K é corpo quadrático complexo com número de classes $h_{\mathrm{K}} = p$ primo então $h_{\mathrm{H(K)}} = (h_{\mathrm{F}})^2$ onde F é um subcorpo real maximal de H(K), além disso, p não divide $h_{\mathrm{H(K)}}$ e nem h_{F}.

A primeira afirmação segue pelo **Teorema IV.1** na referência N. MOSER. **Unités et Nombre de Classes d'une Extension Galoisienne Diédrale de Q**.

Agora se a $p - parte$ de $\mathrm{C}\ell_{\mathrm{K}}$ é cíclica, então pelo **Resultado 02** o número de classes da $p - parte$ de L é ${}^{h_{\mathrm{K}}}/_{p}$. Logo:

$$\frac{h_{\mathrm{K}}}{p} = h_{\mathrm{L}} = \frac{(h_{\mathrm{F}})^2 \cdot h_{\mathrm{K}}}{p} a \Longrightarrow (h_{\mathrm{F}})^2 a = 1 \Longrightarrow a = 1$$

Para o caso particular em que K é quadrático complexo com número de classe $h_{\mathrm{K}} = p$ prima tem-se que H(K) é uma extensão de K não ramificada, portanto $a = 1$ resultando $h_{\mathrm{H(K)}} = (h_{\mathrm{F}})^2$.

Por outro lado, como $\mathrm{C}\ell_{\mathrm{K}}$ é cíclico segue do **Resultado 02** que p não divide $h_{\mathrm{H(K)}} = (h_{\mathrm{F}})^2$ e consequentemente não divide h_{F}.

Então o **Princípio de Stark** sugere que h_{F} e $h_{\mathrm{H(K)}}$ sejam frequentemente igual a 1 e que corpos quadráticos complexos K com $\ell(\mathrm{K}) = 1$ não tem subcorpos CM de grau grande, que pela Teoria de Gêneros, traduz-se na condição de que a $2 - parte$ deve ser cíclico, o que foi confirmado na **Proposição 02**.

O entendimento e estudo da **Conjectura 04** será mais fácil, quando o grupo $C\ell_K$ tem ordem prima. Para isso considere então que K é um corpo numérico com número de classes $h_K = p$ primo. Então de acordo com o **Resultado 02** p não divide $h_{H(K)}$, algum outro primo q de fato pode dividir $h_{H(K)}$. Logo tem-se que $h_{H(K)} \neq 1$ e consequentemente por outro lado $h_{H(K)} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ é um produto de potências de primos $p_i's$ tal que $p_i \equiv 1\ mod(p)$, portanto tende a ser um pouco maior que p, especialmente para p muito grande.

Mais precisamente se q divide $h_{H(K)}$ e $q \not\equiv 1\ mod(p)$, então $C\ell_{H(K)}$ não é cíclico. Isso é bastante significativo, porque o princípio de H. COHEN and H. W. LENSTRA. **Heuristics on Class Groups of Number Fields** afirma que ao prever a proporção dos corpos numéricos que tem grupo abeliano G_2 como seu grupo de classes, deve ponderar o grupo com fator $1/|Aut(G)|$.

Em particular, as partes do grupo de classes de corpos numéricos não se encontrando sob a influência da Teoria de Gêneros tendem a ser cíclicas. Por exemplo, primos q que são raízes primitivas $mod(p)$ são prováveis não dividir $h_{H(K)}$.

Essas restrições sobre a forma de grupo de classes H(K) sugerem que este corpo deve ter uma afinidade com o número de classe igual a 1. Quando H(K) tem um fator primo não trivial q, então a classe residual de $q\ mod(p)$ é provável ser 1, uma vez que este mantenha a possibilidade que $C\ell_{H(K)}$ ser cíclico. Nesse caso, temos a seguinte afirmação:

Afirmação 06: Suponha que $h_K = p$ seja primo e H(K) tem grupo de classes cíclico. Se $h_{H_2(K)} > 1$, então $C\ell_{H_2(K)}$ é a soma direta de p cópias de um grupo abeliano.

Veja maiores detalhes na referência T. HONDA. **On Absolute Class Fields of Certain Algebraic Number Fields**.

Resumindo, uma grande densidade positiva de corpos numéricos K com número de classe primo deve satisfazer $\ell(K) = 1$, com a maior parte deles satisfazendo $\ell(K) = 2$.

Agora voltando a **Conjectura 04** para os corpos numéricos com grupo de classe, cíclica e cardinalidade composta, ainda esperasse que o número de classes do corpo de classes de Hilbert é muitas vezes igual a 1. Por exemplo, para todo primo p dividindo h_K considere a extensão abeliana não ramificada $H(K)|H^p(K)$. Como p não

divide o número de classe de $\mathrm{H}^{p}(\mathrm{K})$, da **Afirmação 02** e resultados de **Cohen-Lenstra** [**CL**] implicam que $h_{\mathrm{H(K)}}$ tende a ser o primo p.

Existe a possibilidade de que para um diferente primo q dividindo h_{K}, a potência de q no número de classes cresce de K para $\mathrm{H}^{p}(\mathrm{K})$, mas isso também figura a ser uma ocorrência relativamente rara porque transfere a extensão $\mathrm{H(K)}|\mathrm{H}^{q}(\mathrm{K})$, onde o número de classe do corpo de base e grau da extensão é o primo q, se aplicando assim a **Afirmação 02**.

Dados computados a respeito de extensões maximais não ramificadas de corpos quadráticos complexos cujo discriminante é d com $-1000 < d < 0$ estão computados na tabela da referência K. YAMAMURA. **Maximal Unramified Extensions of Imaginary Quadratic Number Fields of Small Conductors**.

Nessa faixa existem 239 corpos com grupo de classe cíclica, sendo 89 do tipo (i) e exatamente 6 com $\ell(\mathrm{K}) > 1$, 109 do tipo (ii) têm $\ell(\mathrm{K}) = 1$, exceto para $d = 731 = 17 \cdot 43$ e 41 de nenhum tipo têm $\ell(\mathrm{K}) > 1$.

5 CONSIDERAÇÕES FINAIS

A presente dissertação destinou a comentar o problema do número de classes de Gauss, resumido em duas conjecturas, onde os matemáticos como: Hans **Heilbronn**, Kurt **Heegner**, Harold **Stark**, Alan **Baker**, Kenneth **Ireland**, Michael **Rosen**, Mark **Watkins** apresentaram primeiras contribuições relevantes ao problema entre 1952 a 2004 onde uma das conjecturas foi provada e a outra permanecendo sem solução e com evidências de veracidade.

O principal objetivo do trabalho está na proposta do artigo publicado pelo autor **Farshid Hajir** em 1997, onde o mesmo, elabora uma nova conjectura cuja veracidade implicará na veracidade da segunda conjectura. O texto evidencia sobre a ideia conectada através dos Corpos de Classes de Hilbert, como a ferramenta matemática alternativa mais indicada para obter avanços significativos sobre conclusões para a Segunda Conjectura de Gauss. E segundo autor Hajir, as convicções que levam a conjectura ser verdadeira, estão em evidências, como dados computados na tabela da referência de **Yamamura** dentre outros artigos referências do próprio artigo.

Além disso, esse material teve por outro objetivo, apresentar uma introdução inicial da Teoria dos Números Algébricos com capítulo preliminar, destinado aos leitores que tem noções básicas da Teoria Elementar dos Números e Álgebra Abstrata, bem como aqueles que tenham interesse em aprofundar-se sobre o estudo.

A diversidade dos conceitos, propriedades, teoremas, fatorações, estruturas gerais como: módulos, corpos de números algébricos, anéis de inteiros, domínio de Dedekind, que foram apresentados, enriquecem e organizam o trabalho como um todo, proporcionado criação de bases teóricas consistentes, possibilitando aprofundamento e servindo de referência para leitura ou consulta aos que se fazem interessado e despertam curiosidade por esse ramo da Matemática.

REFERÊNCIAS

ALBUQUERQUE, J. V. M. **Finitude do grupo das classes de um corpo de números via empacotamentos reticulados.** 2013. 51 f. Dissertação (Mestrado em Matemática) - Centro de Ciências, Universidade Federal do Ceará, Fortaleza-CE, 2013.

ARNO, S.; ROBINSON, M. L.; Wheeler, F.S. **Imaginary quadratic fields with small odd class number.** Acta Arith., v. 83, p. 295-330, 1998.

ARTIN, E. **Bewweis dês allgemeinein reciprocitätsgesetzes**. Abh. Math. Sem. Univ. Hamburg, v. 5, p. 353-363, 1927.

ATIYAH, M. F.; MACDONALD, I. G. **Introduction to commutative algebra**. London: Addison-Wesley, 1969.

BAKER, A. Linear Forms in the logarithms of algebraic numbers. **Mathematika**, v. 13, p. 204-216, 1966.

BASILLA, J. M.; WADA, H. On efficient computation of the 2-parts od ideal class groups of quadratic fields. **Proc. Japan Acad**., n. 10, p. 191-193, 2004.

BOREVICH, Z. I.; SHAFAREVICH, I. R. **Number theory**. New York: Academic Press, 1966.

BHATTACHARYA, P. B.; JAIN, S. K.; NAGPAUL, S. R. **Basic abstract algebra.** 2nd ed. New York: Cambridge University, c1995.

BOND, R. Unramified abelian extensions of number fields. **J. Number Theory**, v. 30, p.1-10, 1988.

CHILDRESS, N. **Class field theory**. New York: Springer, 2009. (Universitext)

CONRAD, K. **History of class field theory**. Note

CONRAD, K. **Class group calculations**. Notes.

COHEN, H.; LENSTRA, H. W. Heuristics on class groups of number fields. (Lecture notes in Mathematics, v.1068, p.33-62, 1984.

CORIOLANO, M. W. L. **Reticulados de Craig transladados.** 2011. 111 f.; Dissertação (Mestrado em Matemática) - Centro de Ciências, Universidade Federal do Ceará, Fortaleza-CE, 2011.

CRAVEN, D. A. **The theory of p-groups**. Hilary Term, 2008.

ENDLER, O. **Teoria dos corpos**. Rio de Janeiro: IMPA, 1987. (Publicações Matemáticas)

ENDLER, O. **Teoria dos números algébricos**. 2.ed. Rio de Janeiro: IMPA, 2006. (Projeto Euclides)

FERREIRA, L. A. **Teoria de corpos de classes e aplicações**. São Carlos: USP, 2012.

GAUSS, C. F. **Disquisitiones arithmeticae**. New York: Yale Univ. Press, 1966.

GOLDFELD, D. **The Gauss class number problem for imaginary quadratic fields**. Heegner points and Rankin L-series. Edited by H. Darmon, S-W. Zhang. Cambridge: Cambridge Univ. Press, 2004.

GOLDFELD, D. Gauss class number problem for imaginary quadratic fields. **Bulletin (New Series) of the American Mathematical Society**, v. 13, n. 1, 1985.

GOLDFELD, D. **Gauss class number problem for imaginary quadratic fields**. Cambridge: Cambridge University Press, 2004.

GOUVÊA, Q. F. Uma maravilhosa demonstração. **Matemática Universitária**, n. 19, p. 16-43, 1995.

HAJIR, F. On the class number of Hilbert class fields. **Pacific Journal of Mathematics**, v. 181, n.3, p. 177-187, 1997.

HAJIR, F. On the Growth of p-class groups in p-class field towers. **J. Algebra**, v. 188, p. 256-271, 1997.

HAJIR, F. Unramified elliptic units. (Thesis) - Massachusetts Institute of Technology, Dept. of Mathematics, 1993.

HARALD, N.; CHAOPING, X. Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places. **Acta Arithemetica**, LXXIX.1, 1997.

HEEGNER, K. Diophantische analysis und modulfunktionen. **Math. Z.**, v. 56, p. 227-253, 1952.

HERGLOTZ, G. Uber einen dirichletschen Satz. **Math. Z.**, v. 12, p. 255-261, 1992.

HEILBRONN, H. On the class number in imaginary quadratic fields. **Quartely J. of Math.**, v. 5, p. 150-160, 1934.

HONDA, T. On absolute class fields of certain algebraic number fields. **J. Reine Angew. Math**., v. 203, p. 80-89, 1960.

IRELAND, K.; ROSEN, M. **A Classical introduction to modern number theory**. New York: Springer-Verlag, p. 358-361, 1993.

IWASAWA, K. A Note on ideal class groups. **Nagoya Math. J**., v. 27, p. 239-247, 1966.

KONDO, T. Algebraic number fields with discriminant equal to that of a quadratic number field. **J. Math. Soc. Japan**, v. 47, n. 1, p. 31-36, 1995.

LEMMERMEYER, F. **Class field theory**. Ankara, Turkey: Bilkent University, Dept. Mathematics, 2007. Notes

LEMMERMEYER, F. **Class field towers**. Ankara, Turkey: Bilkent University, Dept. Mathematics, 2010. Notes

LEMMERMEYER, F. **Construction of Hilbert 2-class fields**. Ankara, Turkey: Bilkent University.

LINMAN, J. **Burnside's theorem**. Oregon State University, 2010.

LOUBOUTIN, S.; OKAZARI, R. Determination of all non-normal quartic CM-fields with class number one. **Acta Arithmetica**, v. 67, p. 47–62, 1994.

MARTINET, J. Tours de corps de classes et estimations de discriminants. **Inv. Math**., v. 44, p. 65-73, 1978.

MARCUS, D. A. **Number fields**. New York: Springer, 1977.

MILLER, N. **The Structure of the class group of imaginary quadratic fields**. Master of Science. Blacksburg, Virginia, 2005.

MONTEIRO, L. H. J. **Teoria de Galois.** Poços de Caldas: IMPA, 1969. (7º Colóquio Brasileiro de Matemática)

MOSER, N. Unités et Nombre de classes d'une extension Galoisienne Diédrale de Q. **Abh. Math. Sem. Univ. Hamburg**, v. 1, v. 48, p. 54-75, 1979.

MOLLIN, R. A. **Algebraic number theory**. New York : Chapman and Hall/CRC, 1999.

MURRTY, V. KUMAR. Class numbers of CM-Fields with solvable normal closure. **Compositio Mathematica**, v. 127, n. 3, p. 273-287, 2001.

MURTY, M. RAM. **Artin's conjecture for primitive roots**. Montreal, Canadá : McGill University, Department of Mathematics.

NOMURA, A. On the existence of unramified p-extensions. **Osaka J. Math**., v. 28, p. 55-62, 1991.

ODLYZKO, A. M. Some analytic estimates of class numbers and discriminants. **Invent. Math**., v. 29, p. 275-286, 1975.

PIERCE, L. B. **The 3-Part of class numbers of quadratic fields**. Trinity: Oxford University Master of Science, 2004.

RIBENBOIM, P. **Classical theory of algebraic numbers**. New York: Springer, 2001.

RIBENBOIM, P. **Algebraic numbers**. New York: Wiley-Interscience, 1972.

RIBENBOIM, P. Os recordes dos números primos. **Matemática Universitária,** nº 14, p. 29-46, 1992.

SAMUEL, P. **Algebraic theory of number**. Hermman, Paris: Dover Publications, 1970.

SERRE**,** J. P. **Modular forms of weight 1 and Galois representations, in ' Algebraic number fields'**. London: Academic Press, p. 193-268, 1977.

SHEMANSKE, T. R. **An overview of Class Field Theory**. New Hampshire :Department of Mathematics, Dartmouth College, Hanover, 2001. Notes.

SILVA, A. B. **Famílias infinitas de corpos quadráticos imaginários**.2010. 64 f. Dissertação (Mestrado em Matemática). Centro de Ciências, Universidade Federal do Ceará, Fortaleza-CE, 2010.

SILVA, J. C.; COSTA, F. S. **Grupo de classes de ideais em reticulados quadráticos**. Águas de Lindóias, SP, UEMA, 2012. Dept. de Matemática e Informática. Congresso Nacional de Matemática Aplicada e Computacional.

SILVA, J. P. **Discriminante da potência de um número algébrico**. 2010. 98 f. Dissertação (Mestrado em Matemática). Centro de Ciências, Universidade Federal do Ceará, Fortaleza-CE ,2010.

SILVA FILHO, J. C. **Corpos quadráticos e reticulados**. 2001. Dissertação (Mestrado em Matemática) – Centro de Ciências Exatas e da Natureza, Universidade Federal da Paraíba, João Pessoa-Pb, 2001.

SILVEIRA, S. D. **Teorema $p^a p^b$ de Burnside**. DMAT, UFMG, 2011.

SILVEIRA, T. **Elementos da teoria dos números algébricos**. Monografia de Graduação. Joinville, UDESC, 2013.

SIME, PATRICK J. On the ideal class group of real biquadratic fields. **Transactions of the American Mathematical Society,** v. 347, nº 12, 1995.

STARK, H. M. A Complete determination of the complex quadratic fields of class number one. **Mich. Math. J**., v. 14, p. 1-27, 1967.

STARK, H. M. **Some effective cases of the Brauer-Siegel theorem**, Invent. Math., v. 23, p. 135-152, 1974.

SUMIDA-TAKAHASHI, Hiroki. Computation of the p-part of the ideal class group of certain real Abelian fields**. Mathematics of Computation**, v. 76, p. 1059-1071, 2007.

TAVARES, M. F. C. **Reticulados Obtidos por Colagens**. Dissertação (Mestrado em Matemática) – Centro de Ciências, Universidade Federal do Ceará, 2011.

TATEYAMA, K. On the ideal class groups of some cyclotomic fields. **Proc. Japan Acad.** Ser. A, v. 58, nº 7, p. 333-335 1982.

VOLOCH, J. F. Raízes primitivas e a conjectura de Artin. **Matemática Universitária**, nº9/10, 1989.

WASHINGTON, L. C. **Introduction to cyclotomic**. New York: Ed. Springer, 1982.

WATKINS, M. Class numbers of imaginary quadratic fields**. Mathematics of Computation**, v. 73, nº 246, p. 907-938, 2003.

YAMAMURA, K. The Determination of the imaginary Abelian number fields with class number one. **Math Comp**., v. 62, nº 206, p. 899-921, 1994.

YAMAMURA, K. **Maximal unramified extensions of imaginary quadratic number fields of small conductors**. Preprint, 1997.

ZARISKI, O.; SAMUEL, P. **Commutative Algebra**. I. New York: Van Nostrand, 1958.