unesp.bmp

Discriminante de Corpos de Números

Cátia Regina de Oliveira Quilles

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Dissertação apresentada ao Departamento de Matemática - IBILCE - UNESP, como parte dos requisitos para a obtenção do Título de Mestre em Matemática.

São José do Rio Preto - SP

Fevereiro - 2006

"É graça divina começar bem e persistir na caminhada certa. Graça maior é diante das dificuldades não desistir nunca, pois provavelmente aquele que nunca cometeu um erro nunca fez uma descoberta."

D. Hélder Câmara e Samuel Smiles

Ao meus pais,
José e Maria
Aos meus irmãos,
Maria Angélica e Lucas
Aos meus avós,
José e Teresinha
E ao meu namorado, Igor

dedico

Agradecimentos

Ao concluir este trabalho, agradeço:

A Deus, que me deu a vida e o presente de ter chegado até aqui.

Aos meus pais, que com muito esforço me possibilitaram a sonhar. Que mesmo sem perceber, ao mostrar o orgulho e confiança que depositavam em mim me davam forças pra continuar.

Aos meus avós que estiveram sempre com as mãos estendidas pra me ajudar nos momentos de dificuldade, pela confiança, amor e carinho depositados.

Aos meus irmãos que entenderam a minha ausência em momentos importantes.

Ao meu namorado Igor, pelo seu amor, confiança e incentivo, que foram fundamentais para a minha perseverança e a quem dedico toda a minha vida e minhas conquistas.

Ao Prof. Dr. Antonio Aparecido de Andrade, pela amizade tão sincera, pelo incentivo, pela paciência e dedicação.

Aos professores do Departamento de Matemática da UNESP - S.J.R.Preto, pela excelente formação e amizade.

Aos professores da banca examinadora: Prof. Dr. Trajano P. N. Neto (IBILCE - UNESP - São José do Rio Preto - SP), Prof. Dr. André Luiz Flores (Universidade Camilo Castelo Branco - Fernandópolis - SP), Prof. Dr. Edson Donizete de Carvalho (FEIS - UNESP - Ilha Solteira - SP) e Prof. Dr. Edson Agustini (Universidade Federal de Uberlândia - MG).

À minha irmã de coração Elen, com quem sempre pude contar em todos os momentos de dificuldade e de alegria.

Aos meus grandes amigos Tatiane, Giovana, Fernanda, Marcus e Franciele por compartilharem as alegrias, tristezas e dificuldades desde o início de nossa caminhada.

Aos colegas do curso de Pós-graduação, pela amizade sincera e o agradável convívio.

A todos que direta ou indiretamente contribuíram para a realização deste trabalho.

À Capes por parte do auxílio financeiro.

Resumo

O objetivo deste trabalho é mostrar duas maneiras de se calcular o discriminante de um corpo de números. Da primeira forma, utilizando a teoria algébrica dos números clássica vimos como calcular o discriminante dos corpos quadráticos e corpos ciclotômicos. Através desta teoria é possível calcular o discriminante somente desses corpos com um árduo trabalho. Da segunda maneira utilizando os caracteres de Dirichlet e seus condutores vimos o cálculo do discriminante para qualquer corpo abeliano de uma maneira não muito trabalhosa. Finalmente, utilizando esses resultados damos aplicações sobre reticulados algébricos.

Palavras-chave: discriminante, caracter de Dirichlet, condutor, empacotamento esférico, reticulados, densidade de empacotamento, densidade de centro.

Abstract

The aim of this work is to make a parallel between two forms of computing discriminants of fields of numbers. In the first form, by classic algebraic number theory we computed the discriminant of quadratics fields and ciclotomic fields. Through of this theory, is possible to computing the discriminant alone of this fields with a arduous work. In the second form using Dirichlet's character and their conductors we computed the discriminant of any abelian field of a form not very hard. Finally, using this results we give applications on algebraic lattices.

Keywords: discriminant, Dirichlet character, conductor, sphere packing, lattices, density of packing, density of center.

Índice 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

R, A: anéis

M: módulo

$\{\alpha_1, \ldots, \alpha_n\}$: n-upla

$I_R(A)$: fêcho inteiro de A em R

$A[x]$: anel dos polinômios sobre A em x

$\mathbb{K}, \mathbb{L}$: corpos

∂f: grau do polinômio f

$[\mathbb{L} : \mathbb{K}]$: grau de $\mathbb{L}$ sobre $\mathbb{K}$

$\mathbb{K}(\alpha_1, \ldots, \alpha_n)$: corpo obtido pela adjunção de $\alpha_1, \ldots, \alpha_n$ a $\mathbb{K}$

$\prod$: produtório

$\sum$: somatório

(a_{ij}): matriz

$det(a_{i,j})$: determinante de $(a_{i,j})$

$f_\alpha(x)$: polinômio característico de α

$m_\alpha(x)$: polinômio minimal de α

$Tr_{R/A}$: traço em relação à extensão R/A

$N_{R/A}$: norma em relação à extensão R/A

$I_{\mathbb{K}}(\mathbb{Z})$: anel dos inteiros de $\mathbb{K}$

$\mathcal{A}$: ideal

$\mathcal{P}, \mathcal{Q}$: ideal primo

$N(\mathcal{A})$: norma do ideal $\mathcal{A}$

$\#X$: cardinalidade do conjunto X

$\frac{A}{I}$: quociente de A por I

$D_{R/A}(\alpha_1, \ldots, \alpha_n)$: discriminante de uma n-upla de R sobre A

ζ_n: $e^{2\pi i/n} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$, raiz n-ésima primitiva da unidade

U_n: grupo das raizes n-ésimas da unidade

$mdc(m, n)$: máximo divisor comum de m e n

$\varphi(n)$: função de Euler para o inteiro n

$\phi_n(x)$: n-ésimo polinômio ciclotômico

$\mathcal{D}(R/A)$: discriminante de R sobre A

$A \times B$: produto cartesiano de A por B

$f^{'}(x)$: primeira derivada do polinômio $f(x)$

$D(f)$: discriminante do polinômio $f(x)$

log: função logaritmo

$\mathbb{K}^*$: grupo multiplicativo dos elementos inversíveis de $\mathbb{K}$

χ: caracter de Dirichlet

f_χ: condutor do caracter de Dirichlet χ

$Gal(\mathbb{L}/\mathbb{K})$: grupo de Galois de $\mathbb{L}/\mathbb{K}$

$\hat{G}$: grupo de caracteres

$X_{\mathbb{K}_i}$: grupo dos caracteres associado ao corpo $\mathbb{K}_i$

$\ker(f)$: núcleo do homomorfismo f

$o(G)$: ordem do grupo G

$\forall$: para todo

$\exists$: existe

$\bigcap$ intersecção

$\overline{x}$: conjugado complexo do elemento x

$< \alpha_1, \ldots, \alpha_n >$: ideal gerado por $\alpha_1, \ldots, \alpha_n$

$a|b$: a divide b

Λ_β: reticulado com base β

$||a||$ norma de a

$\mathcal{P}_v$: região fundamental

$vol(\Lambda_\beta)$ volume do reticulado

$\Delta(\Lambda_\beta)$: densidade de empacotamento

$\mathcal{B}(\rho)$ esfera com centro na origem e raio ρ

$\delta(\Lambda_\beta)$: densidade de centro do reticulado Λ_β

$\sigma_{\mathbb{K}}$: homomorfismo canônico ou de Minkowiski

$\overline{\sigma}$: conjugação complexa ($\overline{\sigma}(x) = \overline{x}$)

$\Re(x)$: parte real do número complexo x

$\Im(x)$:parte imaginária do número complexo x

$[z]$: o inteiro mais próximo de z

Sumário

Introdução

A teoria dos códigos corretores de erros nasceu em 1948, com o famoso trabalho de Shannon [1], onde foi demonstrado o Teorema da Capacidade de Canal. Em linhas gerais, este resultado diz que para transmissão de dados abaixo de uma taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter a probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

A prova do Teorema da Capacidade do Canal implica que no caso de valores altos da relação sinal-ruído (SNR), um código de bloco ótimo para um canal com ruído gaussiano branco (AWGN), limitado em faixa consiste em um empacotamento denso de sinais dentro de uma esfera, no espaço euclidiano n-dimensional, para n suficientemente grande. Assim, se estabeleceu o vínculo entre empacotamento esférico e Teoria da Informação.

Um empacotamento esférico é a distribuição de esferas de mesmo raio no espaço Euclidiano de modo que duas a duas toquem-se no máximo em um ponto. Um problema relacionado ao empacotamento esférico é o de distribuir esferas no espaço de modo que elas ocupem a maior parte desse espaço, ou seja, que esta distribuição tenha alta densidade. Os empacotamentos esféricos cujo conjunto dos centros das esferas formam um subgrupo discreto do $\mathbb{R}^n$ são denominados empacotamentos reticulados.

Os empacotamentos interessantes são aqueles associados a um reticulado Λ_β em que as esferas tenham raio máximo, onde possamos cobrir a maior área possível. Para a determinação deste raio, temos que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n;\ |x| \leq k\}$ com o reticulado Λ_β é um conjunto finito, de onde segue que o número $\Lambda_{\beta_m} = min\{|\lambda|;\ \lambda \in \Lambda_\beta,\ \lambda \neq 0\}$ está bem definido e $(\Lambda_{\beta_m})^2$ é a norma mínima. Temos que $\rho = \Lambda_{\beta_m}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ_β e obter um empacotamento. Dessa forma, o estudo dos empacotamentos reticulados é equivalente ao estudo dos reticulados.

A densidade de empacotamento de um reticulado Λ_β, que é definida como a proporção do espaço $\mathbb{R}^n$ coberto pela união das esferas, é dada por

$$\Delta(\Lambda_\beta) = \frac{\text{Volume de uma esfera de raio } \rho}{\text{Volume do reticulado}}.$$

Se $\mathcal{B}(\rho)$ é a esfera com centro na origem e raio ρ, temos que o seu volume é dado por

$$vol(\mathcal{B}(\rho)) = vol(\mathcal{B}(1))\rho^n,$$

onde $vol(\mathcal{B}(1))$ é o volume da esfera de raio 1. Assim, a densidade de empacotamento é dada por

$$\Delta(\Lambda_\beta) = vol(\mathcal{B}(1))\frac{\rho^n}{vol(\Lambda_\beta)}.$$

Deste modo, o problema se reduz ao estudo de um outro parâmetro, chamado de densidade de centro, que é dado por

$$\delta(\Lambda_\beta) = \frac{\rho^n}{vol(\Lambda_\beta)}.$$

Por volta de 1948, através do trabalho de Claude Shannon, podemos observar que o problema de encontrar empacotamentos esféricos densos em um dado espaço é equivalente a encontrar códigos corretores de erros eficientes. A partir de então associou o estudo dos códigos ao dos reticulados. Com isso, surgiram várias famílias de reticulados, cada uma delas visando dar uma melhor contribuição no que diz respeito à densidade de empacotamento. Dentre tais famílias, destaca-se a descrita por Minkowski, chamado método algébrico, que consiste em tomar um corpo de números de grau n e o seu anel de inteiros e obter um homomorfismo de modo que a imagem de um ideal não nulo do anel de inteiros obtido por este homomorfismo é um reticulado de posto n em $\mathbb{R}^n$.

Em outras palavras tomando $\mathbb{K}$ um corpo de números de grau n, $I_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$ e $\mathcal{A}$ um ideal não nulo de $I_\mathbb{K}$. Se $\sigma_\mathbb{K}$ é o homomorfismo canônico, ou de Minkowski, de $\mathbb{K}$, definido por

$$\sigma_\mathbb{K}(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

então $\sigma_\mathbb{K}(\mathcal{A})$ é um reticulado com volume

$$vol(\sigma_\mathbb{K}(\mathcal{A})) = 2^{-r_2}|\mathcal{D}(\mathbb{K}/\mathbb{Q})|^{1/2}N(\mathcal{A}).$$

Logo, sua densidade de centro é dada por

$$\delta(\sigma_\mathbb{K}(\mathcal{A})) = \frac{2^{r_2}\rho^n}{|\mathcal{D}(\mathbb{K}/\mathbb{Q})|^{1/2}N(\mathcal{A})},$$

onde r_2 é a metade do número de monomorfismos imaginários, $N(\mathcal{A})$ é a norma do ideal $\mathcal{A}$ e $\mathcal{D}(\mathbb{K}/\mathbb{Q})$ o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$.

Assim, se $\mathcal{A} = I_\mathbb{K}$, temos que $N(I_\mathbb{K}) = 1$ e portanto,

$$\delta(\sigma_\mathbb{K}(I_\mathbb{K}))\frac{2^{r_2}\rho^n}{|\mathcal{D}(\mathbb{K}/\mathbb{Q})|^{1/2}}.$$

Deste modo, conseguindo corpos de números com discriminante mínimo, obtemos maiores densidades de centro e consequentemente melhores reticulados.

Assim, o próximo passo é obter corpos de números $\mathbb{K}$ com discriminante mínimo. De acordo com o Teorema de Kronecker-Weber, todo corpo de números $\mathbb{K}$, abeliano de grau finito, está contido em alguma extensão ciclotômica $\mathbb{Q}(\zeta_m)$, e neste caso usamos a fórmula do Condutor-Discriminante para calcular o discriminante de $\mathbb{K}$. Temos dois caminhos na busca deste objetivo, no primeiro é trabalharmos diretamente com os subgrupos do grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$, e assim explicitar o grupo de caracteres associados a $\mathbb{K}$ e os condutores de seus elementos. No segundo, dando atenção direta ao grupo dos caracteres associados ao corpo $\mathbb{K}$, sem explicitá-los, mas calculando os possíveis valores dos condutores dos seus caracteres e a quantidade de caracteres para cada valor possível do condutor. Com o primeiro enfoque vimos resultados que dão respostas para os casos dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$ com p primo e r inteiro positivo. No segundo caso, vimos uma fórmula geral para o cálculo do discriminante dos subcorpos de $\mathbb{Q}(\zeta_m)$. A fórmula para o discriminante dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$ com p primo ímpar depende apenas do seu grau, e para o caso $p = 2$ depende do grau e do fato do subcorpo ser ou não ciclotômico. Para o caso geral, a fórmula depende dos graus das intersecções do subcorpo $\mathbb{K}$ com alguns subcorpos particulares de $\mathbb{Q}(\zeta_m)$.

A partir destes fatos, vimos alguns métodos para encontrarmos o discriminante mínimo, e deste modo utilizando os corpos de números que possuem discriminate mínimo, podemos obter melhores reticulados.

Assim, estruturamos o trabalho da seguinte maneira: No Capítulo 1, vimos conceitos básicos da teoria algébrica dos números, tais como módulos Noetherianos, elementos inteiros, norma e traço, norma de um ideal, discriminante, corpos quadráticos e corpos ciclotômicos. No Capítulo 2, vimos como calcular o discriminante de polinômios, corpos quadráticos e corpos ciclotômicos, utilizando a teoria algébrica dos números clássica. No Capítulo 3, vimos os caracteres de Dirichlet, seus condutores e algumas propriedades que são úteis para o cálculo do discriminante de corpos de números abelianos. No Capítulo 4, vimos como calcular o discriminante de corpos de números abelianos utilizando os caracteres de Dirichlet, e alguns critérios para encontrar discriminantes mínimos. Finalmente, no Capítulo 5, vimos algumas aplicações em reticulados.

Capítulo 1

Teoria algébrica dos números

1.1 Introdução

Neste capítulo apresentamos conceitos básicos da teoria algébrica dos números envolvendo módulos Noetherianos, elementos inteiros, norma e traço, norma de um ideal, discriminante, corpos quadráticos e corpos ciclotômicos. Para tal utilizamos as referências [2], [3], [4], [5], [6], [7], [8], [9] e [10].

1.2 Módulos Noetherianos

Nesta seção apresentamos a definição e algumas propriedades sobre módulos e módulos Noetherianos, necessárias para o entendimento das demais seções.

Definição 1.2.1 *Seja R um anel. Um R-módulo M é um grupo abeliano $(M, +)$, junto com a função $\alpha : R \times M \to M$ dada por $\alpha(r, m) = rm$, com $r \in R$ e $m \in M$, satisfazendo para todo $r, s \in R, m, n \in M$:*

1. $(r + s)m = rm + sm$
2. $r(m+n) = rm + rn$
3. $r(s \cdot m) = (r \cdot s)m$
4. $1 \cdot m = m$.

A função α é chamada uma R-ação sobre M. Se R é um corpo $\mathbb{K}$, então um R-módulo é o mesmo que um espaço vetorial sobre $\mathbb{K}$.

Definição 1.2.2 *Um R-submódulo de M é um subgrupo N de M tal que se $n \in N, r \in R$, então $rn \in N$.*

Definição 1.2.3 *Um módulo M é dito finitamente gerado se possuir um conjunto finito de geradores. Um R-módulo M que possui uma base (não necessariamente finita) é chamado de módulo livre, e o número de elementos da base é chamado posto de M.*

Observação 1.2.1 *Nem todo módulo finitamente gerado possui uma base, e nem todo submódulo de um módulo livre é livre.*

Definição 1.2.4 *Seja R um domínio. Dizemos que um R-módulo M é livre de torção se não existe $\alpha \in R$, $\alpha \neq 0$, tal que $\alpha m = 0$, para todo $m \in M$.*

Teorema 1.2.1 *[2, Theorem 1, p.92] Todo módulo finitamente gerado livre de torção sobre um domínio de ideais principais é um módulo livre.*

Demonstração: *Sejam R um domínio de ideais principais, M um R-módulo livre de torção e $\{\alpha_1, \ldots, \alpha_n\}$ um conjunto de geradores de M. Se $\{\beta_1, \ldots, \beta_n\}$ é um conjunto de elementos de M linearmente independentes, então $\{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n\}$ é linearmente dependente, para $1 \leq i \leq n$ e $1 \leq j \leq m$. Assim, existem $a_i, b_{i,1}, \ldots, b_{i,n} \in R$, não todos nulos, tais que*

$$a_i\alpha_i + b_{i,1}\beta_1 + \ldots + b_{i,n}\beta_n = 0. \tag{1.1}$$

Temos que a_i é não nulo, pois $b_{i,1}, \ldots, b_{i,n}$ são todos não nulos e $\{\beta_1, \ldots, \beta_n\}$ é linearmente independente. Seja então L o submódulo de M gerado por $\{\beta_1, \ldots, \beta_n\}$. Logo, L é livre, pois o conjunto de geradores é uma base. Da Equação (1.1) temos que $a_i\alpha_i = -(b_{i,1}\beta_1 + \ldots + b_{i,n}\beta_n)$, e isto implica que $a_i\alpha_i \in L$. Tomando $a = \prod_{i=1}^{n} a_i$ temos que $a\alpha_i \in L$ para todo $1 \leq i \leq n$ e como $\{\alpha_1, \ldots, \alpha_n\}$ é um conjunto de geradores de M, segue que $aM \subseteq L$, então aM é um submódulo livre. Agora, considere a função $f : M \to aM$ definida por $f(m) = am$ para todo $m \in M$. Como M é livre de torção, temos que f é um isomorfismo. Portanto, M é livre. ∎

Definição 1.2.5 *Sejam R um anel e M um R-módulo. Dizemos que M é um R-módulo Noetheriano se satisfaz uma das seguintes condições:*

1. *Toda família não vazia de R-submódulos de M tem um elemento maximal.*
2. *Toda sequência crescente de R-submódulos de M é estacionária.*
3. *Todo R-submódulo de M é finitamente gerado.*

Um anel R é Noetheriano se R considerado como um R-módulo for Noetheriano.

Proposição 1.2.1 *[3, Lemma 1, p.47] Sejam $A \subseteq R$ anéis. Se $\mathcal{P}$ é um ideal primo de R, então $\mathcal{P} \cap A$ é um ideal primo de A.*

Demonstração: *Seja a aplicação composta $\varphi : A \xrightarrow{i} R \xrightarrow{\pi} R/\mathcal{P}$, onde i e π são as aplicações inclusão e projeção, respectivamente. Como π e i são homomorfismos, segue que a função $\varphi = \pi \circ i$ é um homomorfismo. Além disso, como $\varphi(x) = (\pi \circ i)(x) = \pi(x) = x + \mathcal{P}$ e $\varphi(x) = \bar{0}$ se, e somente se, $x \in \mathcal{P} \cap A$, segue que $\ker(\varphi) = A \cap \mathcal{P}$. Assim, $A/\mathcal{P} \cap A \simeq Im(\varphi) \subset R/\mathcal{P}$. Como $R/\mathcal{P}$ é um domínio, segue que $A/\mathcal{P} \cap A$ é um domínio. Portanto, $\mathcal{P} \cap A$ é um ideal primo de A.* ∎

Proposição 1.2.2 *[3, Lemma 2, p.48] Sejam R um anel. Se $\mathcal{P}$ é um ideal primo de R que contém um produto de ideais $\mathcal{A}_1 \dots \mathcal{A}_n$ de R, então $\mathcal{P}$ contém pelo menos um dos $\mathcal{A}_i$, para algum $i = 1, 2, \dots, n$.*

Demonstração: *Suponhamos, por absurdo, que $\mathcal{A}_j \nsubseteq \mathcal{P}$, para todo $j = 1, 2, \dots, n$. Assim, para cada $j = 1, 2, \dots, n$, existe α_j tal que $\alpha_j \in \mathcal{A}_j$ e $\alpha_j \notin \mathcal{P}$. Como $\mathcal{P}$ é primo, segue que $\alpha_1 \dots \alpha_n \notin \mathcal{P}$. Mas $\alpha_1 \dots \alpha_n \in \mathcal{A}_1 \dots \mathcal{A}_n \subset \mathcal{P}$, o que é um absurdo. Portanto, $\mathcal{P}$ contém pelo menos um dos ideais $\mathcal{A}_i$, para algum $i = 1, 2, \dots, n$.* ∎

Proposição 1.2.3 *[3, Lemma 3, p.48] Se R é um anel Noetheriano, então todo ideal de R contém um produto de ideais primos.*

Demonstração: *Sejam R um anel Noetheriano e F o conjuntos dos ideais de R que não contém um produto de ideais primos. Mostraremos que $F = \emptyset$. Suponhamos, por absurdo, que $F \neq \emptyset$. Como R é Noetheriano, segue que F possui um elemento maximal M. Temos que M não é um ideal maximal, pois caso contrário, M seria primo e assim, $M \notin F$. Assim, existem $x, y \in R - M$ tal que $xy \in M$. Além disso, temos que $M \subsetneq \langle x \rangle + M$ e $M \subsetneq \langle y \rangle + M$. Portanto, $\langle x \rangle + M$ e $\langle y \rangle + M$ não pertencem a F. Assim,*

$$\mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_n \subseteq \langle x \rangle + M \text{ e } \mathcal{Q}_1\mathcal{Q}_2 \dots \mathcal{Q}_n \subseteq \langle y \rangle + M,$$

onde $\mathcal{P}_i, \mathcal{Q}_j$ são ideais primos de R. Logo,

$$(\mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_n)(\mathcal{Q}_1\mathcal{Q}_2 \dots \mathcal{Q}_n) \subseteq (\langle x \rangle + M)(\langle y \rangle + M) \subseteq M,$$

o que é um absurdo. Portanto, $F = \emptyset$, e segue que todo ideal de R contém um produto de ideais primos. ∎

Corolário 1.2.1 *[2, Lemma 2, p.199] Se R é um anel Noetheriano tal que 0 é o único elemento nilpotente, então o ideal nulo é a intersecção finita de ideais primos.*

Demonstração: *Pela Proposição 1.2.3 segue que se R é um anel Noetheriano e $\mathcal{A}$ é um ideal de R, $\mathcal{A} \neq R$, então existem ideais primos $\mathcal{P}_1, \ldots, \mathcal{P}_r$ de R tal que $\mathcal{P}_1 \ldots \mathcal{P}_r \subseteq \mathcal{A}$. Assim, sem perda de generalidade, tomando $\mathcal{A}$ como sendo o ideal nulo, temos que $0 = \prod_{i=1}^{r} \mathcal{P}_i^{e_i}$, onde os ideais primos $\mathcal{P}_i$ são distintos e $e_i \geq 1$, para $i = 1, \ldots, r$. Mostremos que $\mathcal{P}_1 \cap \ldots \cap \mathcal{P}_r = 0$. Se $\alpha \in \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_r$, então $\alpha^{e_1+\ldots+e_r} \in \mathcal{P}_1^{e_1} \ldots \mathcal{P}_r^{e_r} = 0$. Logo α é nilpotente, mas por hipótese, como 0 é o único elemento nilpotente, segue que $\alpha = 0$. Portanto, $0 = \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_r$.* ∎

Teorema 1.2.2 *[3, Theorem 1, p.21] Sejam R um anel de ideais principais e M um R-módulo livre de posto n. Se M' é um R-submódulo de M, então:*

1. *M' é livre de posto r, para $0 \leq r \leq n$.*
2. *Se $M' \neq 0$, então existe uma base $\{v_1, \ldots, v_n\}$ de M e elementos não nulos $a_1, \ldots, a_r \in R$ tais que $\{a_1 v_1, \ldots, a_r v_r\}$ é uma base de M' e que a_i divide a_{i+1}, para $1 \leq i \leq r-1$.*

Demonstração: *Para $M' = \langle 0 \rangle$ o ideal nulo, o resultado é válido. Assim, suponhamos $M' \neq \langle 0 \rangle$. Seja $L(M, R)$ o conjunto das formas lineares sobre M. Tomando $u \in L(M, R)$, temos que $u(M')$ é um submódulo de R, um ideal de R. Podemos escrever $u(M') = Ra_u$, onde $a_u \in R$, uma vez que o ideal é principal. Se $u \in L(M, R)$ é tal que Ra_u é maximal através de Ra_e, para $e \in L(M, R)$, pela definição 1.2.5. Assim, tomamos uma base $\{x_1, \ldots, x_n\}$ que identifica M com R^n. Seja $p_i : M \longrightarrow R$ a projeção sobre a i-ésima coordenada, isto é $p_i(x_j) = \delta_{ij}$. Como $M' \neq \langle 0 \rangle$, para o menor i, $1 \leq i \leq n$, $p_i(M')$ é não nulo. Assim $a_u \neq \langle 0 \rangle$. Pela nossa construção existe $v' \in M'$ tal que $u(v') = a_u$. Logo, devemos mostrar que para todo $e \in L(M, R)$, temos que $a_u | e(v')$. Assim, se $mdc(a_u, e(v')) = d$, então $d = ba_u + ce(v')$, onde $b, c \in R$, e daí $d = (bu + ce)(v')$. Agora, como $(bu + ce)$ é uma forma linear sobre M, temos que $Ra_u \subseteq Rd \subseteq u(M')$, e pela maximalidade de Ra_u, segue que $Rd = Ra_u$, e assim temos que a_u divide $e(v')$. Em particular, $a_u | p_i(v')$, então seja $p_i(v') = a_u b_i$, com $b_i \in R$. Tomando $v = \sum_{i=1}^{n} b_i x_i$, temos que $v' = a_u v$. Como, $u(v') = a_u = a_u u(v)$, segue que $u(v) = 1$, observando que $a_u \neq 0$. Assim, devemos mostrar que*

- *$M = ker(u) + Rv$, e*
- *$M' = (M' \cap ker(u)) + Rv'$, onde $v' = a_u v$.*

Para a primeira afirmação, se $x \in M$, *então* $x = u(x)v + (x - u(x)v)$, *logo* $u(x - u(x)v) = u(x) - u(x)u(v) = 0$, *uma vez que* $u(v) = 1$, *então* $x - u(x)v \in ker(u)$. *Assim, mostramos que* $Rv + ker(u) = M$, *portanto,* $Rv \cap ker(u) = \langle 0 \rangle$. *Para a segunda afirmação, seja* $y \in M'$, *logo* $u(y) = ba_u$, *onde* $b \in R$, *então* $y = ba_u v + (y - u(y)v) = bv' + (y - u(y)v)$. *Novamente, é claro que* $y - u(y)v \in ker(u)$ *e também que* $y - u(y)v = y - bv' \in M'$, *isto é,* $y - u(y)v \in M' \cap ker(u)$ *e* $bv' \in Rv' \subseteq Rv$, *e isto prova a segunda afirmação. Agora, provaremos o ítem* 1 *por indução sobre o posto* r *de* M'. *Se* $r = 0$, $M' = \langle 0 \rangle$ *e a prova é direta. Se* $r > 0$, *da segunda afirmação segue que* $M' \cap ker(u)$ *tem posto* $r - 1$, *e assim é livre de acordo com a hipótese de indução. Como, na segunda afirmação a soma é direta, obtemos uma base para* M' *adicionando* v' *a base para* $M' \cap ker(u)$. *Assim* M' *é livre e* 1 *é verdadeiro. Provaremos* 2 *por indução sobre o posto* n *de* M. *Novamente o caso* $n = 0$ *é trivial. Por* 1, *temos que* $ker(u)$ *é livre de posto* $n-1$, *uma vez que na primeira afirmação, a soma é direta. Aplicamos a hipótese de indução sobre o módulo livre* $ker(u)$ *e seu submódulo* $M' \cap ker(u)$*: se* $M' \cap ker(u) \neq \langle 0 \rangle$, *então existem* $r \leq n$, *uma base* $\{v_2, \ldots, v_n\}$ *de* $ker(u)$, *e elementos não nulos* $a_2, \ldots, a_n$ *de* R *tais que* $\{a_2v_2, \ldots, a_nv_n\}$ *é uma base para* $M' \cap ker(u)$ *e* a_i *divide* a_{i+1}, *para* $2 \leq i \leq r-1$. *Tomando a mesma notação que acima, chamamos* $a_1 = a_u$ *e* $v_1 = v$. *Então, da primeira afirmação segue que,* $\{v_1, v_2, \ldots, v_n\}$ *é uma base para* M, *da segunda e do fato que* $v' = a_1v_1$ *segue que,* $\{a_1v_1, \ldots, a_rv_r\}$ *é uma base para* M'. *Falta provar que* $a_1|a_2$. *Se* e *é a forma linear sobre* M *definida pela relação* $e(v_1) = e(v_2) = 1$ *e* $e(v_i) = 0$, *para* $i \geq 3$. *Então* $a_1 = a_u = e(a_uv_1) = e(v') \in e(M')$, *então* $Ra_u \subseteq e(M')$. *Pela maximalidade de* Ra_u *podemos concluir que* $e(M') = Ra_u = Ra_1$. *Como* $a_2 = e(a_2v_2) \in e(M')$, *vemos que* $a_2 \in Ra_1$, *isto é* $a_1|a_2$. ∎

1.3 Elementos inteiros

Nesta seção veremos o conceito de elementos inteiros sobre um anel enfocando suas principais propriedades.

Definição 1.3.1 *Sejam* $A \subseteq R$ *anéis. Um elemento* $\alpha \in R$ *é chamado inteiro sobre* A *se* α *é raiz de um polinômio mônico com coeficientes em* A, *isto é, se existem* $a_0, a_1, \ldots, a_{n-1} \in A$, *não todos nulos, tal que* $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$. *Em particular, todo elemento de* A *é inteiro sobre* A.

Exemplo 1.3.1 *O elemento* $\alpha = \frac{1}{2}(1 + \sqrt{5}) \in \mathbb{R}$ *é inteiro sobre* $\mathbb{Z}$, *pois é raiz do polinômio mônico* $x^2 - x - 1$ *com coeficientes em* $\mathbb{Z}$.

Observação 1.3.1 *Se R é o corpo complexo e os coeficientes do polinômio mônico são números racionais, o elemento α é chamado número algébrico. Se os coeficientes do polinômio mônico são números inteiros, o elemento α é chamado inteiro algébrico.*

Exemplo 1.3.2

1. *O elemento $\alpha = e^{\frac{2\pi i}{5}} \in \mathbb{C}$ é um inteiro algébrico, pois é raiz do polinômio mônico $x^5 - 1$ com coeficientes em $\mathbb{Z}$.*

2. *O elemento $\alpha = \frac{22}{7} \in \mathbb{C}$ é um número algébrico, pois é raiz do polinômio mônico $x - \frac{22}{7}$ com coeficientes em $\mathbb{Q}$.*

Teorema 1.3.1 *[4, Teorema 1.1] Sejam $A \subseteq R$ anéis e α um elemento de R. As seguintes afirmações são equivalentes:*

1. *α é inteiro sobre A.*

2. *O anel $A[\alpha]$ é um A-módulo finitamente gerado.*

3. *Existe um subanel B de R contendo A e α que é um A-módulo finitamente gerado.*

Demonstração: (1) $\Rightarrow$ (2) *Como α é inteiro segue que*

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

onde $a_0, a_1, \ldots, a_{n-1} \in A$ e não são todos nulos. Seja M o submódulo de R gerado por $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Temos que $M \subseteq A[\alpha]$. Por outro lado, temos que $\alpha^n = -(a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0) \in M$ e por indução segue que $\alpha^{n+j} \in M$ para todo $j \geq 0$. Assim $A[\alpha] \subseteq M$ e deste modo $A[\alpha] = M$. Portanto, $A[\alpha]$ é um A-módulo finitamente gerado.
(2) $\Rightarrow$ (3) *Neste caso, é suficiente tomar $B = A[\alpha]$.*
(3) $\Rightarrow$ (1) *Seja $\{\beta_1, \ldots, \beta_n\}$ um conjunto finito de geradores de B como um módulo sobre A, ou seja, $B = A\beta_1 + \ldots + A\beta_n$. Como $\alpha \in B$ e B é um subanel de R segue que $\alpha\beta_i \in B$ para todo $i = 1, \ldots, n$. Assim, $\alpha\beta_i = \sum_{j=1}^{n} a_{i,j}\beta_j$, com $a_{i,j} \in A$ para $1 \leq i, j \leq n$. Daí*

$$\alpha\beta_i - \sum_{j=1}^{n} a_{i,j}\beta_j = 0, \ \ e \qquad \sum_{j=1}^{n}(\alpha\frac{\beta_i}{\beta_j} - a_{i,j})\beta_j = 0.$$

Tomando $\frac{\beta_i}{\beta_j} = \delta_{i,j}$ temos que

$$\sum_{j=1}^{n}(\alpha\delta_{i,j} - a_{i,j})\beta_j = 0, \ \text{para } i = 1, \ldots, n.$$

Assim, temos um sistema de n equações lineares homogêneas em $\{\beta_1, \ldots, \beta_n\}$*, ou seja,*

$$\begin{cases} \sum_{j=1}^{n} (\alpha\delta_{1,j} - a_{1,j})\beta_j = 0 \\ \qquad\qquad \vdots \\ \sum_{j=1}^{n} (\alpha\delta_{n,j} - a_{n,j})\beta_j = 0 \end{cases}$$

Escrevendo na forma matricial obtemos que

$$\begin{pmatrix} \alpha\delta_{1,1} - a_{1,1} & \alpha\delta_{1,2} - a_{1,2} & \ldots & \alpha\delta_{1,n} - a_{1,n} \\ \alpha\delta_{2,1} - a_{2,1} & \alpha\delta_{2,2} - a_{2,2} & \ldots & \alpha\delta_{2,n} - a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha\delta_{n,1} - a_{n,1} & \alpha\delta_{n,2} - a_{n,2} & \ldots & \alpha\delta_{n,n} - a_{n,n} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Seja d o determinante $det(\delta_{i,j}\alpha - a_{i,j})$*. Pela regra de Cramer temos que* $d\beta_j = 0$ *para todo* $j = 1, 2, \ldots, n$*. Como B é gerado por* $\{\beta_1, \ldots, \beta_n\}$*, segue que* $dB = 0$*, e em particular* $d1 = d = 0$*. Deste modo, temos que d é um polinômio mônico em* α*, onde o termo com ordem máxima aparece na expansão do produto*

$$\prod_{i=1}^{n} (\delta_{i,i}\alpha - a_{i,i}) = \prod_{i=1}^{n} (\frac{\beta_i}{\beta_i}\alpha - a_{i,i}) = \prod_{i=1}^{n} (\alpha - a_{i,i})$$

das entradas da diagonal principal. Portanto, α *é raiz de um polinômio mônico com coeficientes em A, ou seja,* α *é inteiro sobre A.* ∎

Proposição 1.3.1 *[4, Corolário 1.2] Sejam* $A \subseteq R$ *anéis e* $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$*. Se* α_1 *é inteiro sobre A e* α_i *é inteiro sobre* $A[\alpha_1, \ldots, \alpha_{i-1}]$*, para* $i = 2, \ldots, n$*, então* $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *é um A-módulo finitamente gerado.*

Demonstração: *A prova será feita por indução sobre n. O caso* $n = 1$ *segue do ítem 2 do Teorema 1.3.1. Agora suponhamos que o resultado é verdadeiro para* $n - 1$*, ou seja, que* $B = A[\alpha_1, \ldots, \alpha_{n-1}]$ *é um A-módulo finitamente gerado. Logo, existe um conjunto finito* $\{\beta_1, \beta_2, \ldots, \beta_p\}$ *de geradores de B sobre A. Assim,* $B = \sum_{j=1}^{p} A\beta_j$*. Pelo ítem 2 do Teorema 1.3.1 obtemos que* $A[\alpha_1, \alpha_2, \ldots, \alpha_n] = B[\alpha_n]$ *é um B-módulo finitamente gerado, e assim possui um conjunto finito de geradores* $\{\gamma_1, \gamma_2, \ldots, \gamma_q\}$*. Deste modo, podemos escrever* $B[\alpha_n] = \sum_{k=1}^{q} B\gamma_k$*. Assim,*

$$A[\alpha_1, \alpha_2, \ldots, \alpha_n] = \sum_{k=1}^{q} B\gamma_k = \sum_{k=1}^{q} (\sum_{j=1}^{p} A\beta_j)\gamma_k = \sum_{j,k} A\beta_j\gamma_k,$$

e deste modo $(\beta_j\gamma_k)_{1\leq j\leq p, 1\leq k\leq q}$ *é um conjunto finito de geradores de* $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *como um* A*- módulo. Portanto,* $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *é um* A*-módulo finitamente gerado.* ∎

Corolário 1.3.1 *Sejam* $A \subseteq R$ *anéis. Se* $\alpha_1, \ldots, \alpha_n$ *são elementos de* R *que são inteiros sobre* A*, então* $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *é um* A*-módulo finitamente gerado.*
Demonstração: *Uma vez que se* α_i *é inteiro sobre* A *então* α_i *é inteiro sobre* $A[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}]$*, para* $i = 1, 2, \ldots, n$*, o resultado segue pela Proposição 1.3.1.* ∎

Corolário 1.3.2 *[3, Corollary 1, p.29] Sejam* $A \subseteq R$ *anéis. Se* α *e* β *são elementos de* R *que são inteiros sobre* A*, então* $\alpha + \beta$*,* $\alpha - \beta$ *e* $\alpha\beta$ *são inteiros sobre* A*.*
Demonstração: *Como* $A[\alpha, \beta]$ *é um subanel de* R *e* $\alpha, \beta \in A[\alpha, \beta]$ *segue que* $\alpha + \beta$*,* $\alpha - \beta$ *e* $\alpha\beta \in A[\alpha, \beta]$*. Pela Proposição 1.3.1, como* α *e* β *são inteiros sobre* A*, segue que* $A[\alpha, \beta]$ *é um* A*-módulo finitamente gerado. Logo existe um subanel* $B = A[\alpha, \beta]$ *de* R *contendo* $A, \alpha + \beta$*,* $\alpha - \beta$ *e* $\alpha\beta \in A[\alpha, \beta]$*. Assim, pelo ítem* 3 *do Teorema 1.3.1, segue que* $\alpha + \beta$*,* $\alpha - \beta$ *e* $\alpha\beta$ *são inteiros sobre* A*.* ∎

Definição 1.3.2 *Sejam* $A \subseteq R$ *anéis. O conjunto dos elementos de* R *que são inteiros sobre* A *é chamado fêcho inteiro de* A *em* R*, ou anel dos inteiros de* A *em* R *e denotado por* $I_R(A)$*.*

Corolário 1.3.3 *[4, Corolario 1.3] Se* $A \subseteq R$ *são anéis, então:*

1. *O conjunto* $I_R(A)$ *é um subanel de* R *que contém* A*.*

2. *Todo subanel de* R *que é um* A*-módulo finitamente gerado está contido em* $I_R(A)$*.*

Demonstração:

1. *Pelo Corolário 1.3.2 temos que* $I_R(A)$ *é um subanel de* R*. Como todo elemento de* A *é inteiro sobre* A *segue que* $I_R(A)$ *contém* A*.*

2. *Sejam* B *um subanel de* R *que é um* A*-módulo finitamente gerado e* $\{\alpha_1, \ldots, \alpha_n\}$ *um conjunto finito de geradores de* B*. Se* $\alpha \in B$*, então* $A[\alpha]$ *é finitamente gerado como* A*-módulo, pois* $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n$*, com* $a_i \in A$*. Assim pelo Teorema 1.3.1 segue que* α *é inteiro sobre* A*, ou seja,* $\alpha \in I_R(A)$*. Portanto* B *está contido em* $I_R(A)$*.* ∎

Definição 1.3.3 *Sejam* A *um domínio e* $\mathbb{K}$ *o seu corpo de frações. O fêcho inteiro de* A *em* $\mathbb{K}$ *é chamado fêcho inteiro de* A *e denotado por* $I_{\mathbb{K}}(A)$*.*

Definição 1.3.4 *Sejam* $A \subseteq R$ *anéis. Quando* $I_R(A) = R$ *dizemos que* R *é inteiro sobre* A*.*

Proposição 1.3.2 *[3, Proposition 2, p.29] (Transitividade) Sejam $A \subseteq B \subseteq R$ anéis. Assim, R é inteiro sobre B e B é inteiro sobre A, se, e somente se, R é inteiro sobre A.*

Demonstração: *Suponhamos R inteiro sobre B e B inteiro sobre A. Se $\alpha \in R$, então α é inteiro sobre B. Logo α é raiz de um polinômio mônico $f(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0$ com coeficientes em B. Tomando $B' = A[b_0, \ldots, b_{n-1}]$ temos que α é inteiro sobre B'. Como B é inteiro sobre A, segue que os $b_i's$ são inteiros sobre A. Pela Proposição 1.3.1 segue que $B'[\alpha] = A[b_0, \ldots, b_{n-1}, \alpha]$ é um A-módulo finitamente gerado, e pelo Teorema 1.3.1 segue que α é inteiro sobre A. Portanto R é inteiro sobre A. Reciprocamente, suponhamos que R é inteiro sobre A. Se $\alpha \in R$, então α é raiz de um polinômio mônico com coeficientes em A, ou seja, $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ com $a_i \in A$ para todo $i = 1, \ldots, n-1$. Como $A \subseteq B$, segue que $a_i \in B$ para todo $i = 1, \ldots, n-1$, ou seja, α é inteiro sobre B. Assim R é inteiro sobre B. Agora, se $\alpha \in B$ e como $B \subseteq R$ segue que $\alpha \in R$. Por hipótese, segue que α é inteiro sobre A. Portanto B é inteiro sobre A.* ∎

Proposição 1.3.3 *[3, Proposition 3, p.29] Sejam A um domínio e B um anel tal que $B \subseteq A$ e A é inteiro sobre B. Assim, A é um corpo se, e somente se, B é um corpo.*

Demonstração: *Suponhamos que A é um corpo e seja α um elemento não nulo de B. Logo $\alpha \in A$ e possui inverso $\alpha^{-1} \in A$. Como A é inteiro sobre B, segue que $\alpha^{-1} \in A$ é raiz de um polinômio mônico com coeficientes em B, ou seja, $\alpha^{-n} + a_{n-1}\alpha^{-n+1} + \ldots + a_1\alpha^{-1} + a_0 = 0$ com $a_i \in B$, para $i = 1, 2, \ldots, n-1$. Multiplicando por α^{n-1} obtemos que $\alpha^{-1} = -(a_{n-1} + \ldots + a_1\alpha^{n-2} + a_0\alpha^{n-1})$, o que mostra que $\alpha^{-1} \in B$. Assim B é um corpo. Reciprocamente, suponhamos que B é um corpo e seja β um elemento não nulo de A. Pelo Teorema 1.3.1, temos que $B[\beta]$ é um B-módulo finitamente gerado. Como B é um corpo, segue que $B[\beta]$ é um espaço vetorial de dimensão finita sobre B. Por outro lado, a função de $B[\beta]$ em $B[\beta]$ que leva y em βy é uma transformação linear injetiva, uma vez que $B[\beta]$ é um domínio. Como a dimensão de $B[\beta]$ sobre B é finita, segue que também é sobrejetora. Assim, existe $\beta' \in B[\beta] \subseteq A$ tal que $\beta\beta' = 1$, ou seja, β é inversível em A. Portanto, A é um corpo.* ∎

Definição 1.3.5 *Sejam $A \subseteq R$ anéis. Dizemos que A é integralmente fechado em R quando $I_R(A) = A$. Se A é um domínio e $\mathbb{K}$ é o seu corpo de frações, dizemos que A é integralmente fechado se $I_{\mathbb{K}}(A) = A$.*

Exemplo 1.3.3

1. *Sejam A um domínio e $\mathbb{K}$ o seu corpo de frações. O fêcho inteiro $I_{\mathbb{K}}(A)$ é integralmente fechado.*

2. *Todo anel de ideais principais é integralmente fechado.*

3. *Todo anel fatorial é integralmente fechado.*

De fato:

1. *Temos que $\mathbb{K}$ também é o corpo de frações de $I_{\mathbb{K}}(A)$ e que o fêcho inteiro de $I_{\mathbb{K}}(A)$, dado por $I_{\mathbb{K}}(I_{\mathbb{K}}(A))$, é inteiro sobre $I_{\mathbb{K}}(A)$. Como $A \subseteq I_{\mathbb{K}}(A)$ segue que $I_{\mathbb{K}}(A)$ é inteiro sobre A. Portanto, $I_{\mathbb{K}}(I_{\mathbb{K}}(A)) = I_{\mathbb{K}}(A)$ e assim $I_{\mathbb{K}}(A)$ é integralmente fechado.*

2. *Por definição, um anel de ideais principais é um domínio. Seja α um elemento de $\mathbb{K}$ o corpo de frações de A. Suponha que $\alpha \in I_{\mathbb{K}}(A)$, ou seja, que α é inteiro sobre A. Logo α é raiz de um polinômio mônico com coeficientes em A, ou seja, $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ com $a_i \in A$, para $i = 1, 2, \ldots, n-1$. Tomando $\alpha = \frac{b}{c}$, onde b e c são elementos de A e primos entre si, e substituindo na equação obtemos que $\frac{b^n}{c^n} + a_{n-1}\frac{b^{n-1}}{c^{n-1}} + \ldots + a_1\frac{b}{c} + a_0 = 0$. Agora, multiplicando por c^n ficamos com $b^n + a_{n-1}b^{n-1}c + \ldots + a_1bc^{n-1} + a_0c^n = b^n + c(a_{n-1}b^{n-1} + \ldots + a_1bc^{n-2} + a_0c^{n-1}) = 0$. Assim $b^n = -c(a_{n-1}b^{n-1} + \ldots + a_1bc^{n-2} + a_0c^{n-1})$, e assim c divide b^n. Como b e c são primos entre si, aplicando repetidamente o Lema de Euclides, segue que c divide b. Logo, c é um elemento inversível em A, e assim $\alpha = \frac{b}{c} \in A$. Portanto A é integralmente fechado.*

3. *O argumento é análogo ao ítem anterior.*

1.4 Extensões de corpos

Nesta seção veremos o conceito de extensões de corpos e suas principais propriedades que serão utilizados no restante do trabalho.

Definição 1.4.1 *Sejam R um anel e $\mathbb{K}$ um corpo tal que $\mathbb{K} \subseteq R$. Um elemento $\alpha \in R$ é chamado algébrico sobre $\mathbb{K}$ se for raiz de um polinômio com coeficientes em $\mathbb{K}$. Caso contrário, α é chamado transcendente sobre $\mathbb{K}$. Se α é algébrico sobre $\mathbb{K}$, então o polinômio mônico $m_\alpha(x)$ de grau mínimo tal que $m_\alpha(\alpha) = 0$ é chamado polinômio minimal de α sobre $\mathbb{K}$.*

Definição 1.4.2 *Sejam R um anel e $\mathbb{K}$ um corpo. O conjunto dos elementos de R que são algébricos sobre $\mathbb{K}$ é chamado fêcho algébrico de $\mathbb{K}$ em R e denotado por $I_R(\mathbb{K})$.*

Exemplo 1.4.1 *O elemento $\alpha = \sqrt{7} - \sqrt{3}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio $x^4 - 20x^2 + 16$ com coeficientes em $\mathbb{Q}$.*

Definição 1.4.3 *Sejam R um anel e $\mathbb{K}$ um corpo tal que $\mathbb{K} \subseteq R$. Dizemos que R é algébrico sobre $\mathbb{K}$ se todo elemento de R é algébrico sobre $\mathbb{K}$. Se R é um corpo, R é chamado uma extensão algébrica de $\mathbb{K}$.*

Observação 1.4.1 *Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos.*

1. *O fêcho algébrico de $\mathbb{K}$ em $\mathbb{L}$ é igual a $\mathbb{K}$ se, e somente se, $\mathbb{L}$ é uma extensão algébrica sobre $\mathbb{K}$.*

2. *Todo elemento algébrico sobre $\mathbb{K}$ é um elemento inteiro sobre $\mathbb{K}$. Em particular, sobre corpos, elementos algébricos e inteiros são equivalentes.*

Definição 1.4.4 *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos tal que $\mathbb{K} \subseteq \mathbb{L}$. Chamamos de dimensão de $\mathbb{L}$ sobre $\mathbb{K}$ e denotamos por $[\mathbb{L} : \mathbb{K}]$ o grau de $\mathbb{L}$ sobre $\mathbb{K}$.*

Assim podemos reescrever as equivalências do Teorema 1.3.1 para corpos da seguinte forma:

Teorema 1.4.1 *[3, p.30] Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos tal que $\mathbb{K} \subseteq \mathbb{L}$ e α um elemento de $\mathbb{L}$. As seguintes afirmações são equivalentes:*

1. *α é algébrico sobre $\mathbb{K}$.*

2. *$[\mathbb{K}[\alpha] : \mathbb{K}]$ é finito.*

Demonstração: (1) $\Rightarrow$ (2) *Suponhamos que α é algébrico sobre $\mathbb{K}$ com polinômio minimal $m_\alpha(x)$ de grau n. Temos que $\mathbb{K}(\alpha)$ é espaço vetorial sobre $\mathbb{K}$ gerado por $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Observamos que $\mathbb{K}(\alpha)$ é fechado sobre a adição, subtração e multiplicação por α. Como $\alpha^n = -m_\alpha(\alpha) + \alpha^n = g(\alpha)$, onde $\partial(g) < n$, segue que $\mathbb{K}(\alpha)$ é fechado sobre a multiplicação e assim $\mathbb{K}(\alpha)$ é um anel. Finalmente, mostramos que se $v \in \mathbb{K}(\alpha)$, $v \neq 0$, então $\frac{1}{v} \in \mathbb{K}(\alpha)$. Temos que $v = h(\alpha)$, onde $h(x) \in \mathbb{K}[x]$ e $\partial(h) < n$. Como $m_\alpha(x)$ é irredutível segue que $m_\alpha(x)$ e $h(x)$ são coprimos. Assim, existem $p(x), q(x) \in \mathbb{K}[x]$ tal que $m_\alpha p(x) + h(x)q(x) = 1$. Logo, $1 = m_\alpha(\alpha)p(\alpha) + h(\alpha)q(\alpha) = h(\alpha)q(\alpha)$. Assim $q(\alpha) = \frac{1}{v} \in \mathbb{K}(\alpha)$ e $[\mathbb{K}(\alpha) : \mathbb{K}] = n$. Portanto $[\mathbb{K}(\alpha) : \mathbb{K}]$ é finita.*
(2) $\Rightarrow$ (1) *Se $[\mathbb{K}(\alpha) : \mathbb{K}] = n$, então $\{1, \alpha, \ldots, \alpha^n\}$ é linearmente dependente. Logo existem $a_0, a_1, \ldots, a_n \in \mathbb{K}$, não todos nulos, tais que $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$ e daí temos que α é algébrico sobre $\mathbb{K}$.* ∎

Corolário 1.4.1 *[3, p.31] Toda extensão finita é algébrica.*

Demonstração: *Sejam* $\mathbb{L}$ *e* $\mathbb{K}$ *corpos tal que* $\mathbb{K} \subseteq \mathbb{L}$, $[\mathbb{L} : \mathbb{K}] = m < \infty$ *e* $\alpha \in \mathbb{L}$. *Como* $\mathbb{K}[\alpha]$ *é um subespaço de* $\mathbb{L}$ *segue que* $[\mathbb{K}(\alpha) : \mathbb{K}] = n \leq m < \infty$. *Pelo Teorema 1.4.1 segue que* α *é algébrico sobre* $\mathbb{K}$. *Assim* $\mathbb{L}$ *é uma extensão algébrica.* ∎

Definição 1.4.5 *Seja* $\mathbb{L}$ *uma extensão do corpo* $\mathbb{Q}$. *Se o grau de* $\mathbb{L}$ *sobre* $\mathbb{Q}$ *é finito, dizemos que* $\mathbb{L}$ *é um corpo de números.*

Teorema 1.4.2 *[3, Proposition 1, p.31] (Multiplicidade dos Graus) Sejam* $\mathbb{K}$, $\mathbb{L}$ *e* $\mathbb{M}$ *corpos. Se* $\mathbb{M}$ *é uma extensão algébrica finita de* $\mathbb{L}$ *e* $\mathbb{L}$ *é uma extensão algébrica finita de* $\mathbb{K}$, *então* $\mathbb{M}$ *é uma extensão algébrica finita de* $\mathbb{K}$ *e* $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Demonstração: *Sejam* $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ *uma base de* $\mathbb{M}$ *sobre* $\mathbb{L}$ *e* $\{\beta_1, \beta_2, \ldots, \beta_n\}$ *uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$. *Verifiquemos que* $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_n\}$ *é uma base de* $\mathbb{M}$ *sobre* $\mathbb{K}$. *Se* $\alpha \in \mathbb{M}$, *então* $\alpha = a_1\beta_1 + a_2\beta_2 + \ldots + a_n\beta_n$, *onde* $a_j \in \mathbb{L}$, *para* $j = 1, 2, \ldots, n$. *Agora, como cada* $a_j \in \mathbb{L}$, *segue que podemos escrevê-lo como* $a_j = b_1\alpha_1 + b_2\alpha_2 + \ldots + b_m\alpha_m$, *onde* $b_i \in \mathbb{K}$, *para* $i = 1, 2, \ldots, m$. *Assim* $\alpha = \sum_{j=1}^{n} a_j\beta_j = \sum_{i,j} b_{i,j}\alpha_i\beta_j$, *onde* $b_{i,j} \in \mathbb{K}$. *Logo* $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_n\}$ *gera* $\mathbb{M}$ *sobre* $\mathbb{K}$. *Da relação* $\sum_{i,j} b_{i,j}\alpha_i\beta_j = 0$, *temos que* $\sum_{j=1}^{n}(\sum_{i=1}^{m} b_{i,j}\alpha_i)\beta_j = 0$. *Como* $\{\beta_1, \beta_2, \ldots, \beta_n\}$ *é linearmente independente, segue que* $\sum_{i=1}^{m} b_{i,j}\alpha_i = 0$ *e novamente como* $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ *é linearmente independente segue que* $b_{i,j} = 0$ *para todo* $i = 1, 2, \ldots, m$ *e* $j = 1, 2, \ldots, n$. *Assim,* $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_n\}$ *é linearmente independente. Portanto é uma base de* $\mathbb{M}$ *sobre* $\mathbb{K}$. *Além disso, temos que* $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$. ∎

Definição 1.4.6 *Sejam* $\mathbb{L}$ *e* $\mathbb{M}$ *extensões de um corpo* $\mathbb{K}$. *Dizemos que dois elementos* $\alpha \in \mathbb{L}$ *e* $\alpha' \in \mathbb{M}$ *são conjugados sobre* $\mathbb{K}$ *se existe um* $\mathbb{K}$*-isomorfismo* φ *de* $\mathbb{K}(\alpha)$ *em* $\mathbb{K}(\alpha')$ *tal que* $\varphi(\alpha) = \alpha'$.

Definição 1.4.7 *Sejam* $\mathbb{L}$ *e* $\mathbb{M}$ *extensões de um corpo* $\mathbb{K}$. *Dizemos que* $\mathbb{L}$ *e* $\mathbb{M}$ *são conjugados sobre* $\mathbb{K}$, *ou são* $\mathbb{K}$*-isomorfos, se existe um* $\mathbb{K}$*-isomorfismo* σ *de* $\mathbb{L}$ *em* $\mathbb{M}$ *tal que* $\sigma(a) = a$, *para todo* $a \in \mathbb{K}$.

Definição 1.4.8 *Seja* $\mathbb{K}$ *um corpo. Dizemos que* $\mathbb{K}$ *tem característica* m *se* $m\alpha = 0$ *para todo elemento* $\alpha \in \mathbb{K}$, *e* m *é o menor inteiro positivo com esta propriedade. Se* $m\alpha \neq 0$ *para todo elemento não nulo* α *e inteiro positivo* m, *dizemos que* $\mathbb{K}$ *tem característica zero.*

Observação 1.4.2 *Todo corpo possui um único subcorpo minimal, chamado subcorpo primo, e este é isomorfo a $\mathbb{Q}$ ou a $\mathbb{Z}_p$, onde p é primo. Se é isomorfo a $\mathbb{Q}$ o corpo tem característica zero e se é isomorfo a $\mathbb{Z}_p$ o corpo tem característica p.*

1.5 Norma e traço

Nesta seção veremos os conceitos de norma e traço de um elemento e suas principais propriedades que serão úteis para o desenvolvimento das propriedades do anel dos inteiros de um corpo e também do cálculo do discriminante.

Sejam $A \subseteq R$ anéis tal que R é um A-módulo livre de posto finito n. Sejam $\{\alpha_1, \ldots, \alpha_n\}$ uma base de R sobre A e $\varphi : R \longrightarrow R$ um homomorfismo. Assim

$$\begin{cases} \varphi(\alpha_1) = a_{11}\alpha_1 + a_{12}\alpha_2 + \ldots + a_{1n}\alpha_n \\ \varphi(\alpha_2) = a_{21}\alpha_1 + a_{22}\alpha_2 + \ldots + a_{2n}\alpha_n \\ \vdots \\ \varphi(\alpha_n) = a_{n1}\alpha_1 + a_{n2}\alpha_2 + \ldots + a_{nn}\alpha_n, \end{cases}$$

com $a_{ij} \in A$, e $1 \leq i, j \leq n$. Na forma matricial, temos

$$\begin{pmatrix} \varphi(\alpha_1) \\ \varphi(\alpha_2) \\ \vdots \\ \varphi(\alpha_n) \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,n} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Definição 1.5.1 *Sejam $A \subseteq R$ anéis tal que R é um A-módulo livre de posto n. Seja o endomorfismo $\varphi_\alpha : R \longrightarrow R$ dado por $\varphi_\alpha(x) = \alpha x$, com $\alpha \in R$. Definimos:*

1. *O traço de $\alpha \in R$ relativo a A, como o traço do endomorfismo φ_α e denotamos por $Tr_{R/A}(\alpha) = Tr_{R/A}(\varphi_\alpha)$.*

2. *A norma de $\alpha \in R$ relativo a A, como o deteminante do endomorfismo φ_α e denotamos por $N_{R/A}(\alpha) = det(\varphi_\alpha)$.*

3. *O polinômio característico de $\alpha \in R$ relativo a A, como o polinômio característico do endomorfismo φ_α e denotamos por $f_\alpha(x) = det(xI - \varphi_\alpha)$.*

Observação 1.5.1 *Seja $A \subseteq R$ anéis tal que R é um A-módulo livre de posto finito. Se $\alpha, \beta \in R$ e $a \in A$, então*

1. $\varphi_\alpha + \varphi_\beta = \varphi_{\alpha+\beta}$,

2. $\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha\beta}$ *e*

3. $\varphi_{a\alpha} = a\varphi_\alpha$.

Além disso, a matriz de φ_a em relação a uma base de R sobre A é a matriz diagonal onde a é a entrada de todas as diagonais.

Para um endomorfismo φ, segue da Álgebra Linear que:

1. O traço de φ é definido por $Tr_{R/A}(\varphi) = \sum_{i=1}^{n} a_{ii}$,

2. A norma de φ é definida por $N_{R/A}(\varphi) = \det(a_{ij})$, e

3. O polinômio característico de φ é definido por $det(xI - \varphi) = det(x\delta_{i,j} - a_{i,j})$.

Para os endomorfismos φ e ρ temos que:

1. $Tr_{R/A}(\varphi + \rho) = Tr_{R/A}(\varphi) + Tr_{R/A}(\rho)$,

2. $det(\varphi \cdot \rho) = det(\varphi)det(\rho)$ e

3. $det(xI - \varphi) = x^n - (Tr_{R/A}(\varphi))x^{n-1} + \cdots + (-1)^n det(\varphi)$.

Agora, sejam $\mathbb{K}, \mathbb{L}$ e $\mathbb{M}$ corpos tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ e $[\mathbb{L} : \mathbb{K}] = n$. Se $\alpha, \beta \in \mathbb{L}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades:

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\beta)$

2. $Tr_{\mathbb{L}/\mathbb{K}}(a\alpha)$=$aTr_{\mathbb{L}/\mathbb{K}}(\alpha)$

3. $Tr_{\mathbb{L}/\mathbb{K}}(a) = na$

4. $N_{\mathbb{L}/\mathbb{K}}(a) = a^n$

5. $N_{\mathbb{L}/\mathbb{K}}(a\alpha) = a^n N_{\mathbb{L}/\mathbb{K}}(\alpha)$

6. $N_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}/\mathbb{K}}(\alpha)N_{\mathbb{L}/\mathbb{K}}(\beta)$

7. $N_{\mathbb{L}/\mathbb{K}}(\alpha) = N_{\mathbb{M}/\mathbb{K}}(N_{\mathbb{L}/\mathbb{M}}(\alpha))$

8. $T_{\mathbb{L}/\mathbb{K}}(\alpha) = T_{\mathbb{M}/\mathbb{K}}(T_{\mathbb{L}/\mathbb{M}}(\alpha))$.

Proposição 1.5.1 *[3, Proposition 1, p.36] Sejam $\mathbb{K}$ um corpo finito ou de característica zero, $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$ de grau n e α um elemento de $\mathbb{L}$. Se $\alpha_1, \ldots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{K}$, cada uma repetida $[\mathbb{L} : \mathbb{K}(\alpha)]$-vezes, então:*

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 + \ldots + \alpha_n$,
2. $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 \ldots \alpha_n$ *e*
3. $m_\alpha(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.

Além disso, o polinômio característico é a $[\mathbb{L} : \mathbb{K}(\alpha)]$-ésima potência do polinômio minimal de α sobre $\mathbb{K}$.

Demonstração: *Suponhamos que α é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$, ou seja, $\mathbb{L} = \mathbb{K}[\alpha]$. Se $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, com $a_i \in \mathbb{K}$ para $i = 0, 1, \ldots, n-1$, é o polinômio minimal de α sobre $\mathbb{K}$, então $\mathbb{L}$ é $\mathbb{K}$-isomorfo a $\frac{\mathbb{K}[x]}{\langle m_\alpha(x) \rangle}$ e $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Além disso, temos que a matriz do endomorfismo $\varphi_\alpha : \mathbb{L} \longrightarrow \mathbb{L}$ com relação a base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é dada por*

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

Assim, temos que $\det(xI - \varphi_\alpha)$ é o determinante da matriz

$$xI_n - M = \begin{bmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x + a_{n-1} \end{bmatrix}.$$

Logo, pelo cálculo do determinante da matriz $xI_n - M$, obtemos o polinômio característico $f_\alpha(x)$ de α, que é igual a $m_\alpha(x)$, o polinômio minimal de α. Mas por definição temos que,

$$f_\alpha(x) = \det(xI - \varphi_\alpha(x)) = \det(xI_n - M) = x^n - (Tr_{\mathbb{L}/\mathbb{K}}(\varphi_\alpha))x^{n-1} + \ldots + (-1)^n \det(\varphi_\alpha).$$

Além disso, como α é primitivo segue que

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

e daí obtemos que

$$x^n - (Tr_{\mathbb{L}/\mathbb{K}}(\varphi_\alpha))x^{n-1} + \ldots + (-1)^n \det(\varphi_\alpha) = x^n - \left(\sum_{i=1}^{n} \alpha_i\right) x^{n-1} + \cdots + (-1)^n \left(\prod_{i=1}^{n} \alpha_i\right).$$

Portanto, $Tr_{\mathbb{L}/\mathbb{K}}(\varphi_\alpha) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \alpha_i$ *e* $N_{\mathbb{L}/\mathbb{K}}(\varphi_\alpha) = N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \alpha_i$. *Consideremos, agora, o caso geral. Se* $[\mathbb{L} : \mathbb{K}[\alpha]] = m$, *é suficiente mostrarmos que o polinômio característico* $f_\alpha(x)$ *de* α, *com relação a* $\mathbb{L}$ *sobre* $\mathbb{K}$, *é igual a* m*-ésima potência do polinômio minimal de* α *sobre* $\mathbb{K}$. *Se* $\{\alpha_1, \ldots, \alpha_r\}$ *é uma base de* $\mathbb{K}[\alpha]$ *sobre* $\mathbb{K}$ *e* $\{\beta_1, \ldots, \beta_m\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}[\alpha]$, *então* $\{\alpha_1\beta_1, \ldots, \alpha_r\beta_m\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$. *Pelo Teorema 1.4.2 temos que* $n = rm$. *Seja* $M = (a_{ih})$ *a matriz do endomorfismo de* $\mathbb{K}[\alpha]$ *sobre* $\mathbb{K}$ *com relação a base* $(\alpha_i)_{1 \leq i \leq r}$. *Assim* $\alpha\alpha_i = \sum_h (a_{ih})\alpha_h$, *e deste modo* $\alpha(\alpha_i\beta_j) = \left(\sum_h a_{ih}\alpha_h\right)\beta_j = \sum_h a_{ih}(\alpha_h\beta_j)$. *Logo,*

$$\begin{cases} \alpha\alpha_1\beta_1 = a_{11}\alpha_1\beta_1 + a_{12}\alpha_2\beta_1 + \ldots + a_{1r}\alpha_r\beta_1 \\ \alpha\alpha_2\beta_1 = a_{21}\alpha_1\beta_1 + a_{22}\alpha_2\beta_1 + \ldots + a_{2r}\alpha_r\beta_1 \\ \quad \vdots \\ \alpha\alpha_r\beta_1 = a_{r1}\alpha_1\beta_1 + a_{r2}\alpha_2\beta_1 + \ldots + a_{rr}\alpha_r z_1 \end{cases}$$

Agora, ordenamos a base $\{\alpha_1\beta_1, \ldots, \alpha_r\beta_m\}$ *de* $\mathbb{L}$ *sobre* $\mathbb{K}$, *de modo que a matriz do endomorfismo seja da forma*

$$M_1 = \begin{bmatrix} M & 0 & \cdots & 0 & 0 \\ 0 & M & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & M \end{bmatrix},$$

isto é, M *se repete* m*-vezes na diagonal principal como blocos diagonais na matriz* M_1. *Assim,*

$$xI_n - M_1 = \begin{bmatrix} xI_n - M & 0 & \cdots & 0 & 0 \\ 0 & xI_n - M & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & xI_n - M \end{bmatrix},$$

e $\det(xI_n - M_1) = \det(xI_q - M)^m$. *Dessa forma,* $f_\alpha(x) = det(xI_n - M_1)$ *é o polinômio característico de* α *sobre* $\mathbb{K}$ *e* $det(xI_q - M)$ *é o polinômio minimal de* α *sobre* $\mathbb{K}$, *de acordo com a primeira parte da demonstração.* ∎

Observação 1.5.2 *Da Proposição 1.5.1, segue que:*

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = mTr_{\mathbb{K}[\alpha]/\mathbb{K}}(\alpha)$,

2. $N_{\mathbb{L}/\mathbb{K}}(\alpha) = (N_{\mathbb{K}[\alpha]/\mathbb{K}}(\alpha))^m$ *e*

3. $f_\alpha(x) = (m_\alpha(x))^m$.

Exemplo 1.5.1 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{7})$ *e* $\alpha = -1 + \sqrt{7} \in \mathbb{Q}(\sqrt{7})$. *O polinômio característico de* α *sobre* $\mathbb{Q}$ *é* $f_\alpha(x) = x^2 + 2x - 6$, $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha) = -2$ *e* $N_{\mathbb{L}/\mathbb{Q}}(\alpha) = -6$. *Se* $\mathbb{M} = \mathbb{Q}(i, \sqrt{7})$, *então temos que* $m = [\mathbb{M} : \mathbb{L}] = 2$. *Assim, pela Observação 1.5.2, segue que* $Tr_{\mathbb{M}/\mathbb{Q}}(\alpha) = 2(Tr_{\mathbb{L}/\mathbb{Q}}(\alpha)) = 2 \cdot (-2) = -4$ *e* $N_{\mathbb{M}/\mathbb{Q}}(\alpha) = (N_{\mathbb{L}/\mathbb{Q}}(\alpha))^2 = (-6)^2 = 36$.

Proposição 1.5.2 *[3, Proposition 2, p.38] Sejam* A *um domínio e* $\mathbb{K}$ *seu corpo de frações, onde* $\mathbb{K}$ *tem característica zero. Se* $\mathbb{L}$ *é uma extensão finita de* $\mathbb{K}$ *e* $\alpha \in \mathbb{L}$ *é um elemento inteiro sobre* A, *então os coeficientes do polinômio característico* f_α *são inteiros sobre* A. *Em particular,* $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ *e* $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ *são inteiros sobre* A.

Demonstração: *Pela Proposição* 1.5.1, *temos que o polinômio característico de* α *é dado por* $f_\alpha(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$, *onde* $\alpha_1, \ldots, \alpha_n$ *são as raízes do polinômio minimal de* α. *Como os coeficientes de* $f_\alpha(x)$ *são a menos de isomorfismos somas e produtos dos* α_i, *segue que é suficiente mostrar que os* α_i *são inteiros sobre* A, *uma vez que, pelo Corolário 1.3.2, temos que a soma, a diferença e o produto são inteiros sobre* A. *Pela Teoria de Galois temos que, cada* α_i *é um conjugado de* α *sobre* $\mathbb{K}$ *e assim existe um* $\mathbb{K}$*-isomomorfismo* $\sigma_i : \mathbb{K}[\alpha] \longrightarrow \mathbb{K}[\alpha_i]$ *tal que* $\sigma_i(\alpha) = \alpha_i$, *para todo* $i = 1, \ldots, n$. *Assim, como* α *é inteiro sobre* A, *segue que* $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$, *com* $a_i \in A$, *não todos nulos. Aplicando* σ_i *obtemos que* $\sigma_i(\alpha)^n + a_{n-1}\sigma_i(\alpha)^{n-1} + \ldots + a_0 = 0$, *e consequentemente* $\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \ldots + a_1\alpha_i + a_0 = 0$, *ou seja,* α_i *é inteiro sobre* A, *para cada* $i = 1, 2, \ldots, n$. *Portanto os coeficientes de* $f_\alpha(x)$ *são inteiros sobre* A. ∎

Corolário 1.5.1 *[3, Corollary, p.38] Se* A *é um anel integralmente fechado, então os coeficientes do polinômio característico* $f_\alpha(x)$ *são elementos de* A. *Em particular,* $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ *e* $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ *são elementos de* A.

Demonstração: *Os coeficientes do polinômio característico* $f_\alpha(x)$ *são elementos de* $\mathbb{K}$ *e são inteiros sobre* A. *Como* A *é integralmente fechado, os coeficientes de* $f_\alpha(x)$ *pertencem a* A. *Assim,* $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ *e* $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ *são elementos de* A. ∎

Proposição 1.5.3 *[5, Proposição 1.2.3] Sejam* A *um anel integralmente fechado,* $\mathbb{K}$ *seu corpo de frações,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $I_{\mathbb{L}}(A)$ *o anel dos inteiros de* A *em* $\mathbb{L}$. *Sejam* $\{\alpha_1, \ldots, \alpha_n\}$ *uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$, *onde* $\det(Tr_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j)) \neq 0$ *e* $\alpha \in \mathbb{L}$. *Se* $Tr_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = 0$

para todo $\beta \in \mathbb{L}$, então $\alpha = 0$.

Demonstração: *Se $\alpha \in \mathbb{L}$, então $\alpha = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n$, onde $a_i \in \mathbb{K}$, para $i = 1, \ldots, n$. Assim, é suficiente mostrarmos que se $Tr(\alpha\alpha_j) = 0$, para cada $j = 1, \ldots, n$, então $\alpha = 0$. Deste modo, temos que*

$$0 = Tr_{\mathbb{L}/\mathbb{K}}(\alpha\alpha_j) = a_1 Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1\alpha_j) + a_2 Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2\alpha_j) + \ldots + a_n Tr_{\mathbb{L}/\mathbb{K}}(\alpha_n\alpha_j),$$

para cada $j = 1, \ldots, n$, e na forma matricial temos que

$$\begin{bmatrix} Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1\alpha_1) & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2\alpha_1) & \ldots & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_n\alpha_1) \\ Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1\alpha_2) & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2\alpha_2) & \ldots & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_n\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1\alpha_n) & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2\alpha_n) & \ldots & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_n\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Como $\det(Tr_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j)) \neq 0$ segue que $a_1 = a_2 = \ldots = a_n = 0$. Portanto, $\alpha = 0$. ∎

Corolário 1.5.2 *[5, Corolário 1.2.2] Com as mesmas hipóteses da Proposição 1.5.3, temos que a aplicação $\rho : \mathbb{L} \longrightarrow Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K})$ dada por $\rho(\alpha) = S_\alpha$, onde $S_\alpha(\beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha\beta)$, com $\beta \in \mathbb{L}$ é um isomorfismo.*

Demonstração: *Se $\alpha_1, \alpha_2 \in \mathbb{L}$, então*

$$\begin{cases} \rho(\alpha_1 + \alpha_2)(\beta) = S_{\alpha_1+\alpha_2}(\beta) = Tr_{\mathbb{L}/\mathbb{K}}((\alpha_1 + \alpha_2)\beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1\beta) + Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2\beta) \\ \qquad\qquad = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) = (\rho(\alpha_1) + \rho(\alpha_2))(\beta), \ e \\ \rho(a\alpha)(\beta) = S_{a\alpha}(\beta) = Tr_{\mathbb{L}/\mathbb{K}}(a\alpha\beta) = aTr_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = aS_\alpha(\beta) = a\rho(\alpha)(\beta), \end{cases}$$

para todo $\beta \in \mathbb{L}$. Assim, ρ é um homomorfismo. Agora, se $\alpha \in \mathbb{L}$ é tal que $\rho(\alpha) = 0$, então $\rho(\alpha)(\beta) = S_\alpha(\beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = 0$, para todo $\beta \in \mathbb{L}$. Pela Proposição 1.5.3, segue que $\alpha = 0$. Assim ρ é injetora. Além disso, como $dim_{\mathbb{K}}\mathbb{L} = dim_{\mathbb{K}}(Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K}))$, segue que ρ é sobrejetora. Portanto, ρ é um isomorfismo. ∎

Teorema 1.5.1 *[5, Teorema 1.2.1] Se A é um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $I_{\mathbb{L}}(A)$ o anel dos inteiros de A em $\mathbb{L}$, então $I_{\mathbb{L}}(A)$ é um A-submódulo de um A-módulo livre.*

Demonstração: *Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Corolário 1.4.1 temos que toda extensão finita é algébrica, logo todos os $\alpha_i's$ são algébricos sobre $\mathbb{K}$, ou seja, existem $a_i \in A$, para $i = 0, 1, \ldots, n$, não todos nulos, tal que $a_n\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \ldots + a_0 = 0$. Supondo, sem perda de generalidade, que $a_n \neq 0$ e multiplicando esta equação por a_n^{n-1}, obtemos que*

$$a_n^{n-1}(a_n\alpha_i^n + \ldots + a_0) = (a_n\alpha_i)^n + a_{n-1}(a_n\alpha_i)^{n-1} + \ldots + a_n^{n-1}a_0 = 0,$$

ou seja, $a_n\alpha_i$ é inteiro sobre A, para $i = 1, 2, \ldots, n$. Agora, seja $a_n\alpha_i = \beta_i \in I_{\mathbb{L}}(A)$, para $i = 1, 2, \ldots, n$. Mostremos que $\{\beta_1, \ldots, \beta_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Para isso, suponhamos que $b_1\beta_1 + b_2\beta_2 + \ldots + b_n\beta_n = 0$, onde $b_i \in A$, para $i = 1, \ldots, n$. Logo $b_1a_n\alpha_1 + b_2a_n\alpha_2 + \ldots + b_na_n\alpha_n = 0$, e como $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ segue que $b_ia_n = 0$ e portanto $b_i = 0$ para $i = 1, \ldots, n$. Assim, $\{\beta_1, \ldots, \beta_n\}$ é linearmente independente e como possui n elementos segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Corolário 1.5.2, segue que para $i, j = 1, \ldots, n$, existe uma base dual $\{\gamma_1, \ldots, \gamma_n\}$ tal que $\rho(\beta_i)(\gamma_j) = S_{\beta_i}(\gamma_j) = Tr_{\mathbb{L}/\mathbb{K}}(\beta_i\gamma_j) = \delta_{ij}$. Agora, se $\alpha \in I_{\mathbb{L}}(A)$ então $\alpha\beta_i \in I_{\mathbb{L}}(A)$, para $i = 1, \ldots, n$. Pelo Corolário 1.5.1, segue que $Tr_{\mathbb{L}/\mathbb{K}}(\alpha\beta_i) \in A$, para $i = 1, \ldots, n$. Assim, como $\alpha = c_1\gamma_1 + \ldots + c_n\gamma_n$, com $c_i \in \mathbb{K}$, para $i = 1, \ldots, n$, segue que $Tr_{\mathbb{L}/\mathbb{K}}(\alpha\beta_i) = c_i \in A$, para $i = 1, \ldots, n$. Portanto, $I_{\mathbb{L}}(A)$ é um submódulo de um A-módulo livre gerado por $\{\gamma_1, \ldots, \gamma_n\}$. ■

Corolário 1.5.3 *[5, Corolário 1.2.3, 1.2.4] Com as mesmas hipóteses do Teorema* 1.5.1*, se A é um anel principal, então:*

1. *$I_{\mathbb{L}}(A)$ é um A-módulo livre de posto n.*
2. *Se $\mathcal{A} \subseteq I_{\mathbb{L}}(A)$ é um ideal, então $\mathcal{A}$ é um A-módulo livre de posto n.*

Demonstração:

1. *Se A é um anel principal, então temos que um submódulo de um A-módulo livre é livre de posto menor ou igual a n. Logo, pelo Teorema* 1.5.1*, segue que $I_{\mathbb{L}}(A)$ contém uma base de $\mathbb{L}$ sobre $\mathbb{K}$ que possui n elementos. Portanto, $I_{\mathbb{L}}(A)$ tem posto n.*
2. *Sejam α um elemento não nulo de $\mathcal{A}$ e $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $I_{\mathbb{L}}(A)$. Se $a_1\alpha\alpha_1 + \ldots + a_n\alpha\alpha_n = 0$, com $a_i \in A$, para $i = 1, \ldots, n$, então $a_i\alpha = 0$ para $i = 1, \ldots, n$. Como A é um domínio segue que $a_i = 0$, para $i = 1, \ldots, n$. Assim $\{\alpha\alpha_1, \ldots, \alpha\alpha_n\} \in \mathcal{A}$ é linearmente independente sobre A. Portanto $\mathcal{A}$ é um A-módulo livre de posto n.* ■

1.6 Norma de um ideal

Nesta seção apresentamos o conceito de norma de um ideal do anel dos inteiros de um corpo de números e suas principais propriedades que serão úteis para o cálculo da densidade de centro de reticulados obtidos via corpos de números através do homomorfismo de Minkowski.

Definição 1.6.1 *Sejam $\mathbb{K}$ um corpo de números, $I_{\mathbb{K}}(\mathbb{Z})$ o anel dos inteiros e $\mathcal{A}$ um ideal de $I_{\mathbb{K}}(\mathbb{Z})$. A norma do ideal $\mathcal{A}$ é definida como sendo o número de elementos do anel quociente $\frac{I_{\mathbb{K}}(\mathbb{Z})}{\mathcal{A}}$, ou seja,*

$$N(\mathcal{A}) = \#\frac{I_{\mathbb{K}}(\mathbb{Z})}{\mathcal{A}}.$$

Exemplo 1.6.1 *Seja $\mathcal{A}$ um ideal principal de $\mathbb{Z}[i]$, onde $i^2 = -1$, gerado por $2 - i$. Assim, $\frac{\mathbb{Z}[i]}{\mathcal{A}} = \{x + \mathcal{A};\, x \in \mathbb{Z}[i]\}$. A norma de $\mathcal{A}$ é o número das classes laterais de $\mathcal{A}$. Uma vez que $2 - i \equiv 0 (mod\, \mathcal{A})$, segue que $2 \equiv i (mod\, \mathcal{A})$. Assim para $x = a + bi$, com a, $b \in \mathbb{Z}$, temos que $x = a + bi \equiv a + 2b (mod\, \mathcal{A})$. Como $(2 + i)(2 - i) = 5 \in \mathcal{A}$, segue que as classes laterais de $\mathcal{A}$ em $\mathbb{Z}[i]$ são $\{0, 1, 2, -1, -2\}$, ou seja, $N(\mathcal{A}) = 5$.*

Observação 1.6.1 *Se α é um elemento não nulo de $I_{\mathbb{K}}(\mathbb{Z})$, então pelo Corolário* 1.5.1*, temos que $N(\alpha) \in \mathbb{Z}$.*

Proposição 1.6.1 *[3, Proposition 1, p.52] Se $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$, então*

$$|N(\alpha)| = \#\frac{I_{\mathbb{K}}(\mathbb{Z})}{I_{\mathbb{K}}(\mathbb{Z})\alpha},$$

onde $I_{\mathbb{K}}(\mathbb{Z})\alpha =< \alpha >$ é o ideal de $I_{\mathbb{K}}(\mathbb{Z})$ gerado por α.

Demonstração: *Pelo Corolário* 1.5.3*, temos que $I_{\mathbb{K}}(\mathbb{Z})$ é um $\mathbb{Z}$-módulo livre de posto n. Como $\varphi : I_{\mathbb{K}}(\mathbb{Z}) \longrightarrow I_{\mathbb{K}}(\mathbb{Z})\alpha$ definida por $\varphi(a) = a\alpha$, para $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$, é um isomorfismo, segue que $I_{\mathbb{K}}(\mathbb{Z})\alpha$ é um $\mathbb{Z}$-módulo livre de posto n. Como $\mathbb{Z}$ é um anel principal e $I_{\mathbb{K}}(\mathbb{Z})$ é um $\mathbb{Z}$-módulo livre segue que existe uma base $\{e_1, \ldots, e_n\}$ de $I_{\mathbb{K}}(\mathbb{Z})$ e $c_1, \ldots, c_n \in \mathbb{Z}$ tal que $\{c_1e_1, \ldots, c_ne_n\}$ é uma base de $I_{\mathbb{K}}(\mathbb{Z})\alpha$. A aplicação $\psi : I_{\mathbb{K}}(\mathbb{Z}) \longrightarrow \mathbb{Z}/c_1\mathbb{Z} \times \ldots \times \mathbb{Z}/c_n\mathbb{Z}$ definida por $\psi(\sum_{i=1}^{n} a_ie_i) = (\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n})$ é um homomorfismo sobrejetor, e $\ker(\psi) = I_{\mathbb{K}}(\mathbb{Z})\alpha$, pois $a = \sum_{i=1}^{n} a_ie_i \in \ker(\psi)$ se, e somente se, $\psi(a) = \bar{0}$ se, e somente se, $\bar{a_i} = \bar{0}$, para $i = 1, \ldots, n$, se, e somente se, $a_i \in c_i\mathbb{Z}$, para $i = 1, \ldots, n$, se, e somente se, c_i divide a_i, para $i = 1, \ldots, n$, se, e somente se, $a = \sum_{i=1}^{n} a_ie_i = \sum_{i=1}^{n} b_ic_ie_i$. Como $b_i \in \mathbb{Z}$, para $i = 1, 2, \ldots, n$, segue que $a \in I_{\mathbb{K}}(\mathbb{Z})\alpha$. Portanto $\ker(\psi) = \langle\alpha\rangle$, e deste modo*

$$I_{\mathbb{K}}(\mathbb{Z})/I_{\mathbb{K}}(\mathbb{Z})\alpha \simeq \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_n\mathbb{Z}.$$

Assim, $\#\frac{A}{A\alpha} = c_1c_2 \ldots c_n$. Seja a aplicação $\mathbb{Z}$-linear $\mu : I_{\mathbb{K}}(\mathbb{Z}) \longrightarrow I_{\mathbb{K}}(\mathbb{Z})\alpha$ definida por $\mu(e_i) = c_ie_i$, para $i = 1, \ldots, n$. Logo, $\mu(e_1) = c_1e_1 + 0e_2 + \ldots + 0e_n, \ldots, \mu(e_n) = 0e_1 + \ldots + c_ne_n$ e $\det(\mu) = c_1c_2 \ldots c_n$. Por outro lado, temos que $B = \{c_1e_1, \ldots, c_ne_n\}$ e $C = \{\alpha e_1, \ldots, \alpha e_n\}$ são bases de

$I_{\mathbb{K}}(\mathbb{Z})\alpha$, e portanto existe um automorfismo $v : I_{\mathbb{K}}(\mathbb{Z})\alpha \longrightarrow I_{\mathbb{K}}(\mathbb{Z})\alpha$ tal que $v(c_i e_i) = \alpha e_i$, para $i = 1, \ldots, n$. Como a matriz mudança de base é inversível, segue que $\det(v)$ é inversível em $\mathbb{Z}$, isto é, $\det(v) = \pm 1$. Também, $(v \circ \mu)(e_i) = v(\mu(e_i)) = v(c_i e_i) = \alpha e_i$, para $i = 1, \ldots, n$. Assim, $(v \circ \mu)(a) = \alpha a$. Finalmente, $N(\alpha) = \det(v \circ \mu) = \det(v)\det(\mu) = \pm 1 c_1 c_2 \ldots c_n = \pm \#\frac{I_{\mathbb{K}}(\mathbb{Z})}{I_{\mathbb{K}}(\mathbb{Z})\alpha}$. Portanto, $|N(\alpha)| = \#\frac{I_{\mathbb{K}}(\mathbb{Z})}{I_{\mathbb{K}}(\mathbb{Z})\alpha}$. ∎

Proposição 1.6.2 *[5, Proposição 1.7.2] A $N(\mathcal{A})$ é finita.*

Demonstração: *Se $\alpha \in \mathcal{A}$ é um elemento não nulo, então $I_{\mathbb{K}}(\mathbb{Z})\alpha \subset \mathcal{A}$. Além disso, podemos escrever $I_{\mathbb{K}}(\mathbb{Z})/\mathcal{A}$ como um quociente de $I_{\mathbb{K}}(\mathbb{Z})/I_{\mathbb{K}}(\mathbb{Z})\alpha$. Assim,*

$$\#\frac{I_{\mathbb{K}}(\mathbb{Z})}{I_{\mathbb{K}}(\mathbb{Z})\alpha} = \#\frac{I_{\mathbb{K}}(\mathbb{Z})}{\mathcal{A}}\#\frac{\mathcal{A}}{I_{\mathbb{K}}(\mathbb{Z})\alpha}$$

Mas pela Proposição 1.6.1 *temos que $\#\frac{I_{\mathbb{K}}(\mathbb{Z})}{I_{\mathbb{K}}(\mathbb{Z})\alpha}$ é finito. Portanto $\#\frac{I_{\mathbb{K}}(\mathbb{Z})}{\mathcal{A}}$ é finito.* ∎

1.7 Discriminante de uma n-upla

Nesta seção veremos o conceito do discriminante de uma n-upla enfocando suas principais propriedades.

Definição 1.7.1 *Sejam $A \subseteq R$ anéis tal que R é um A-módulo livre de posto finito n. Seja $\{\alpha_1, \ldots, \alpha_n\}$ um conjunto de elementos de R. Definimos o discriminante de $\{\alpha_1, \ldots, \alpha_n\}$ por*

$$D_{R/A}(\alpha_1, \ldots, \alpha_n) = det(Tr_{R|A}(\alpha_i \alpha_j)),$$

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

Exemplo 1.7.1 *Se $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ é um corpo de números e $\{1, \sqrt{7}\}$ é um conjunto de elementos de $\mathbb{K}$, então*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{7}) = \begin{vmatrix} Tr_{\mathbb{K}/\mathbb{Q}}(1) & Tr_{\mathbb{K}/\mathbb{Q}}(\sqrt{7}) \\ Tr_{\mathbb{K}/\mathbb{Q}}(\sqrt{7}) & Tr_{\mathbb{K}/\mathbb{Q}}(\sqrt{7})^2 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 14 \end{vmatrix} = 28.$$

Proposição 1.7.1 *[3, Proposition 1, p.38] Sejam $A \subseteq R$ anéis tal que R é um A-módulo livre de posto finito n. Se $\{\beta_1, \ldots, \beta_n\}$ é um conjunto de elementos de R tal que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, com $a_{ij} \in A$ para $i = 1, \ldots, n$, então $D_{R/A}(\beta_1, \ldots, \beta_n) = (det(a_{ij}))^2 D_{R/A}(\alpha_1, \ldots, \alpha_n)$.*

Demonstração: *Por definição temos que*

$$D_{R/A}(\beta_1, \ldots, \beta_n) = det(Tr_{R|A}(\beta_r \beta_s)),$$

onde $\beta_r = \sum_{i=1}^{n} a_{ri}\alpha_i$, $\beta_s = \sum_{j=1}^{n} a_{sj}\alpha_j$, *e* $\beta_r\beta_s = \sum_{i=1}^{n} a_{ri}a_{sj}\alpha_i\alpha_j$. *Assim,*

$$Tr_{R|A}(\beta_r\beta_s) = \sum_{i=1}^{n} a_{ri}a_{sj}Tr_{R|A}(\alpha_i\alpha_j),$$

e na forma matricial obtemos que

$$(Tr_{R|A}(\beta_r\beta_s)) = (a_{ri})(Tr_{R|A}(\alpha_i\alpha_j))(a_{sj})^t.$$

Logo,

$$\begin{aligned} D_{R/A}(\beta_1,\ldots,\beta_n) &= det(Tr_{R|A}(\beta_r\beta_s)) = det((a_{ri})(Tr_{R|A}(\alpha_i\alpha_j))(a_{sj})^t) \\ &= det(a_{ri})det(Tr_{R|A}(\alpha_i\alpha_j))det((a_{sj})^t) = (det(a_{i,j}))^2 D_{R/A}(\alpha_1,\ldots,\alpha_n). \end{aligned}$$

■

Corolário 1.7.1 *[3, p.39] Sejam $A \subseteq R$ anéis tais que R é um A-módulo livre de posto finito n e A um domínio. Se $\{\alpha_1,\ldots,\alpha_n\}$ e $\{\beta_1,\ldots,\beta_n\}$ são bases de R, então $D_{R/A}(\alpha_1,\ldots,\alpha_n)$ e $D_{R/A}(\beta_1,\ldots,\beta_n)$ são associados ou ambos possuem determinantes nulos.*

Demonstração: *Como $\{\alpha_1,\ldots,\alpha_n\}$ e $\{\beta_1,\ldots,\beta_n\}$ são bases de R, segue que existem elementos $a_{ij} \in A$ tais que $\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i$, para todo $j = 1,\ldots,n$. Assim, pela Proposição 1.7.1, temos que*

$$D_{R|A}(\beta_1,\ldots,\beta_n) = (\det(a_{ij}))^2 D_{R|A}(\alpha_1,\ldots,\alpha_n).$$

Como (a_{ij}) é uma matriz inversível, segue que $\det(a_{ij})$ é uma unidade do anel A. Assim $D_{R/A}(\alpha_1,\ldots,\alpha_n)$ e $D_{R/A}(\beta_1,\ldots,\beta_n)$ são elementos associados ou ambos determinantes são nulos. ■

Exemplo 1.7.2 *No Exemplo* 1.7.1*, vimos que o discriminante da base $\{1,\sqrt{7}\}$ de $\mathbb{Q}(\sqrt{7})$ é 28. Tomando $\{1+\sqrt{7},-4-\sqrt{7}\}$ como outra base de $\mathbb{K}$, pela Proposição* 1.7.1*, temos que*

$$D_{\mathbb{K}/\mathbb{Q}}(1+\sqrt{7},-4-\sqrt{7}) = \begin{vmatrix} 1 & 1 \\ -4 & -1 \end{vmatrix}^2 D_{\mathbb{K}/\mathbb{Q}}(1,\sqrt{7}) = (3)^2 28 = 756.$$

Proposição 1.7.2 *[2, p.97] Sejam A um domínio, R anel tal que $A \subseteq R$ e R é um A-módulo livre de posto finito n. Se o conjunto $\{\alpha_1,\ldots,\alpha_n\}$ de elementos de R é linearmente dependente sobre A, então*

$$D_{R/A}(\alpha_1,\ldots,\alpha_n) = 0.$$

Demonstração: *Como* $\{\alpha_1, \ldots, \alpha_n\}$ *é linearmente dependente sobre* A*, segue que existem* $a_1, \ldots, a_n \in A$*, não todos nulos, tal que* $a_1\alpha_1 + \ldots + a_n\alpha_n = 0$*. Reordenando e tomando* $a_1 \neq 0$*, consideremos o conjunto* $\{\alpha_1', \ldots, \alpha_n'\}$ *de elementos de* R*, onde* $\alpha_1' = 0$ *e* $\alpha_i' = \alpha_i$ *para* $i = 2, \ldots, n$*. Assim,* $\alpha_i' = a_{1,i}\alpha_1 + \ldots + a_{n,i}\alpha_n$ *para* $i = 1, 2, \ldots, n$*, onde* $a_{j,1} = a_j$*, e se* $i > 1$ *temos que* $a_{j,i} = 1$ *para* $j = i$ *e* $a_{j,i} = 0$ *para* $j \neq i$*. Temos que* $D_{R/A}(\alpha_1', \ldots, \alpha_n') = D_{R/A}(0, \alpha_2, \ldots, \alpha_n) = 0$*, pois a matriz da aplicação traço possui a primeira linha nula. Assim, pela Proposição 1.7.1, segue que*

$$0 = D_{R/A}(0, \alpha_2, \ldots, \alpha_n) = D_{R/A}(\alpha_1', \ldots, \alpha_n') = (det(a_{i,j}))^2 D_{R/A}(\alpha_1, \ldots, \alpha_n).$$

Mas

$$(a_{i,j}) = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

logo $det(a_{i,j}) = a_1 \neq 0$*. Portanto, como* A *é um domínio segue que* $D_{R/A}(\alpha_1, \ldots, \alpha_n) = 0$*.* ∎

Lema 1.7.1 *(Lema de Dedekind)[3, p.39] Se* G *é um grupo,* $\mathbb{K}$ *um corpo, e* $\sigma_1, \ldots, \sigma_n$ *são homomorfismos distintos de* G *no grupo multiplicativo* $\mathbb{K}^*$*, então os* $\sigma_i's$ *são linearmente independentes sobre* $\mathbb{K}$*.*

Demonstração: *Suponhamos, por absurdo, que os* $\sigma_i's$ *são linearmente dependentes. Assim, existem* $a_1, \ldots, a_n \in \mathbb{K}$*, não todos nulos, tal que* $\sum_{i=1}^{n} a_i\sigma_i = 0$*, com o número* r *dos* $a_i's$ *não nulos o menor possível. Temos que* $r \geq 2$*, pois os* $\sigma_i's$ *são não nulos. Se* $g \in G$*, então*

$$a_1\sigma_1(g) + a_2\sigma_2(g) + \ldots + a_r\sigma_r(g) = 0. \tag{1.2}$$

Como os $\sigma_i's$ *são homomorfismos, segue que a Equação (1.2) é válida para todo* $g \in G$*. Assim, para* gh*, com* $h \in G$*, temos que*

$$a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_2(h) + \ldots + a_r\sigma_r(g)\sigma_r(h) = 0. \tag{1.3}$$

Multiplicando a Equação (1.2) *por* $\sigma_1(h)$ *obtemos que*

$$a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_1(h) + \ldots + a_r\sigma_r(g)\sigma_1(h) = 0,$$

e subtraindo da Equação (1.3) segue que

$$a_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + \cdots + a_r(\sigma_1(h) - \sigma_r(h))\sigma_r(g) = 0.$$

Como isso vale para todo $g \in G$ e como tomamos r o menor possível, segue que $a_2(\sigma_1(h) - \sigma_2(h)) = 0$. Assim $\sigma_1(h) = \sigma_2(h)$, para todo $h \in G$, pois $a_2 \neq 0$. Mas isto contradiz a hipótese de que os $\sigma_i's$ são distintos. Portanto os $\sigma_i's$ são linearmente independentes. ∎

Proposição 1.7.3 *[3, Proposition 3, p.39] Sejam $\mathbb{L}$ uma extensão finita de grau n de um corpo $\mathbb{K}$, onde $\mathbb{K}$ é finito ou tem característica zero, e $\sigma_1, \ldots, \sigma_n$, os distintos $\mathbb{K}$-isomorfismo de $\mathbb{L}$. Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então*

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(\sigma_i(\alpha_j))^2 \neq 0.$$

Demonstração: *Por definição $D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = \det(Tr_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j))$. Como o traço de $\alpha_i\alpha_j$ é a soma de seus conjugados, segue que*

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = \det(Tr_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j)) = \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right).$$

Mas, temos que

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j).$$

Assim, $\det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) = \det\left(\sigma_i(\alpha_j)\right)^2$. *Portanto, $D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(\sigma_i(\alpha_j))^2$. Agora, se $\det(\sigma_i(\alpha_j)) = 0$, então existem $a_1, \ldots, a_n \in \mathbb{C}$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$, para $j = 1, \ldots, n$. Pela linearidade concluímos que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$, para todo $\alpha \in \mathbb{L}$, o que é um absurdo, pois pelo Lema 1.7.1 os σ_i são linearmente independentes. Logo $\det(\sigma_i(\alpha_j))^2 \neq 0$. Portanto, $D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 \neq 0$.* ∎

Exemplo 1.7.3 *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ e $\alpha = a + b\sqrt{7} \in \mathbb{K}$. Como $[\mathbb{K} : \mathbb{Q}] = 2$, segue que existem dois $\mathbb{Q}-$isomorfismos, σ_1, σ_2, onde $\sigma_1(a + b\sqrt{7}) = a + b\sqrt{7}$ e $\sigma_2(a + b\sqrt{7}) = a - b\sqrt{7}$. Como $\{1, \sqrt{7}\}$ é uma base de $\mathbb{Q}(\sqrt{7})$ sobre $\mathbb{Q}$ segue que*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{7}) = \begin{vmatrix} 1 & 1 \\ \sqrt{7} & -\sqrt{7} \end{vmatrix}^2 = (-2\sqrt{7})^2 = 28.$$

Proposição 1.7.4 *[6, Proposition 2.17] Se $\mathbb{K}$ é um corpo finito ou de característica zero, $\mathbb{L} = \mathbb{K}[\alpha]$ uma extensão finita de $\mathbb{K}$ de grau n e $m_\alpha(x)$ o polinômio minimal de α sobre $\mathbb{K}$, então*

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(m_\alpha^{'}(\alpha)),$$

onde $m_\alpha^{'}(x)$ é a derivada de $m_\alpha(x)$.

Demonstração: *Sejam $\alpha, \alpha^2, \ldots, \alpha^n$ as raízes de $m_\alpha(x)$ em uma extensão de $\mathbb{K}$, que são conjugados de α. Pela Proposição* 1.7.3*, segue que $D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1}) = \det(\sigma_i(\alpha^j))^2$, onde σ_i, $1 \leq i \leq n$, são $\mathbb{K}$-isomorfismos de $\mathbb{K}[\alpha]$. Além disso, temos que*

$$\det(\sigma_i(\alpha^j)) = \begin{bmatrix} \sigma_1(\alpha) & \sigma_2(\alpha) & \cdots & \sigma_n(\alpha) \\ \sigma_1(\alpha^2) & \sigma_2(\alpha^2) & \cdots & \sigma_n(\alpha^2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha^n) & \sigma_2(\alpha^n) & \cdots & \sigma_n(\alpha^n) \end{bmatrix} = \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha)^1 & \cdots & \sigma_n(\alpha)^1 \\ \sigma_1(\alpha)^2 & \sigma_2(\alpha)^2 & \cdots & \sigma_n(\alpha)^2 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha)^n & \sigma_2(\alpha)^n & \cdots & \sigma_n(\alpha)^n \end{bmatrix},$$

que é um determinante de Vandermonde. Logo, $\det(\sigma_i(\alpha^j)) = \prod_{1 \leq i < j \leq n} (\alpha^i - \alpha^j)$*, e assim,*

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha^i - \alpha^j)^2.$$

Por outro lado, como o polinômio minimal de α é dado por $m_\alpha(x) = \prod_{i=1}^{n}(x - \alpha^i)$ segue que

$$m_\alpha^{'}(x) = \sum_{j=1}^{n} \prod_{i=1, i \neq j}^{n} (x - \alpha^i) \text{ e } \quad m_\alpha^{'}(\alpha^j) = \prod_{i=1, i \neq j}^{n} (\alpha^j - \alpha^i).$$

Assim

$$\prod_{j=1}^{n} m_\alpha^{'}(\alpha_j) = \prod_{i,j=1, i \neq j}^{n} (\alpha^j - \alpha^i),$$

e como $\prod_{j=1}^{n} m_\alpha^{'}(\alpha_j) = N_{\mathbb{L}/\mathbb{K}}(m_\alpha^{'}(\alpha))$, segue que

$$N_{\mathbb{L}/\mathbb{K}}(m_\alpha^{'}(\alpha)) = \prod_{i,j=1, i \neq j}^{n} (\alpha^j - \alpha^i) \tag{1.4}$$

Agora, em $\prod_{i,j=1, i \neq j}^{n} (\alpha^j - \alpha^i)$ cada fator $(\alpha^i - \alpha^j)$ para $i < j$ aparece duas vezes, uma como $(\alpha^i - \alpha^j)$ e outra como $(\alpha^j - \alpha^i)$, e o produto das duas é $-(\alpha^i - \alpha^j)^2$. Assim, no produto da Equação (1.4) aparece o termo $(-1)^s$, onde s é o número de pares (i, j), com $1 \leq i < j \leq n$,

ou seja, $N_{\mathbb{L}/\mathbb{K}}(m'_\alpha(\alpha)) = \prod_{1\leq i<j\leq n}(-1)^s(\alpha^i-\alpha^j)^2$. *Mas, para*

$$\begin{cases} i=1, & \text{temos} \quad j=2,3,\ldots,n \quad e \quad s=1 \\ i=2, & \text{temos} \quad j=3,4,\ldots,n \quad e \quad s=2 \\ \vdots & \\ i=n-1, & \text{temos} \quad j=n \ e \ s=1. \end{cases}$$

Assim $(n-1)+(n-2)+\ldots+1 = \frac{((n-1)+1)n-1}{2} = \frac{1}{2}n(n-1) = s$. *Logo* $N_{\mathbb{L}/\mathbb{K}}(m'_\alpha(\alpha)) = (-1)^{\frac{1}{2}n(n-1)}\prod_{1\leq i<j\leq n}(\alpha^i-\alpha^j)^2$. *Portanto* $N_{\mathbb{L}/\mathbb{K}}(m'_\alpha(\alpha)) = (-1)^{\frac{1}{2}n(n-1)}D_{\mathbb{L}/\mathbb{K}}(1,\alpha,\ldots,\alpha^{n-1})$ *e deste modo*

$$D_{\mathbb{L}/\mathbb{K}}(1,\alpha,\ldots,\alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)}N_{\mathbb{L}/\mathbb{K}}(m'_\alpha(\alpha)).$$

■

Exemplo 1.7.4 *Sejam* $\mathbb{L}=\mathbb{Q}(\sqrt{7})$ *e* $m_\alpha(x)=x^2-7$ *o polinômio minimal de* $\alpha=\sqrt{7}$ *sobre* $\mathbb{Q}$. *Temos que* $m'_\alpha(\sqrt{7})=2\sqrt{7}$, *e* $N_{\mathbb{L}/\mathbb{K}}(2\sqrt{7})=-28$. *Assim, pela Proposição 1.7.4, segue que* $D_{\mathbb{L}/\mathbb{K}}(1,\sqrt{7}) = (-1)^{\frac{1}{2}2}N_{\mathbb{L}/\mathbb{K}}(m'_\alpha(\sqrt{7})) = 28$.

1.8 Corpos quadráticos

Nesta seção apresentamos os corpos quadráticos e suas principais propriedades enfocando o anel dos inteiros desses corpos.

Definição 1.8.1 *Um corpo quadrático é uma extensão de grau* 2 *sobre o corpo* $\mathbb{Q}$ *dos números racionais.*

Proposição 1.8.1 *[6, Proposition 3.1] Todo corpo quadrático é da forma* $\mathbb{Q}(\sqrt{d})$, *onde* d *é um inteiro livre de quadrados.*

Demonstração: *Se* $\mathbb{K}$ *é um corpo quadrático, então todo elemento* $\alpha\in\mathbb{K}$ *tal que* $\alpha\notin\mathbb{Q}$ *é de grau* 2 *sobre* $\mathbb{Q}$. *Pelo Teorema do Elemento Primitivo temos que* $\mathbb{K}=\mathbb{Q}(\alpha)$. *Tomando o polinômio minimal de* α *sobre* $\mathbb{K}$, $m_\alpha(x)=x^2+bx+c$, *e resolvendo a equação quadrática* $\alpha^2+b\alpha+c=0$, *obtemos que* $2\alpha=-b\pm\sqrt{b^2-4c}$. *Portanto,* $\mathbb{K}=\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{b^2-4c})$. *Observando que* b^2-4c *é um número racional da forma* $\frac{u}{v}=\frac{uv}{v^2}$, *com* $u,v\in\mathbb{Z}$, *temos que* $\mathbb{Q}(\sqrt{b^2-4c})=\mathbb{Q}(\sqrt{uv})$. *Assim, como* $uv\in\mathbb{Z}$, *segue que* uv *é fatorado em produtos de primos. Portanto,* $\mathbb{Q}(\sqrt{uv})=\mathbb{Q}(\sqrt{d})$, *onde* d *é inteiro livre de quadrados.* ■

Observação 1.8.1

1. *Pela Proposição 1.8.1, temos que todo corpo quadrático é da forma* $\mathbb{Q}(\sqrt{d})$*, onde* d *é um inteiro livre de quadrados. Portanto,* $\{1, \sqrt{d}\}$ *é uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$*.*

2. *O elemento* $\sqrt{d} \in \mathbb{K}$ *é uma raiz do polinômio irredutível* $x^2 - d$*, e seu conjugado é* $-\sqrt{d}$*. Assim, existe um automorfismo* σ *tal que* $\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$ *é dado por* $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$*.*

Lema 1.8.1 *[3, p.35] Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *um corpo quadrático, onde* d *é um inteiro livre de quadrados. Se* $\alpha = a + b\sqrt{d}$ *é um inteiro algébrico, então* $2a$ *e* $2b$ *são números inteiros.*
Demonstração: *Pelo ítem* 2 *da Observação* 1.8.1*, temos que existe um automorfismo* σ *tal que* $\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$ *é dado por* $\sigma(\alpha) = \sigma(a + b\sqrt{d}) = a - b\sqrt{d}$*. Como* $\sigma(\alpha)$ *também é raiz da mesma equação de* α*, segue que* $\sigma(\alpha) \in I_{\mathbb{K}}(\mathbb{Z})$*. Como* α *e* $\sigma(\alpha) \in I_{\mathbb{K}}(\mathbb{Z})$*, pelo Corolário* 1.3.2*, segue que* $\alpha + \sigma(\alpha) \in I_{\mathbb{K}}(\mathbb{Z})$ *e* $\alpha\sigma(\alpha) \in I_{\mathbb{K}}(\mathbb{Z})$*. Além disso,* $\alpha + \sigma(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in \mathbb{Q}$ *e* $\alpha\sigma(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}$*. Como* $\mathbb{Z}$ *é um anel de ideais principais, pelo Exemplo* 1.3.3*, segue que* $\mathbb{Z}$ *é integralmente fechado e portanto* $2a \in \mathbb{Z}$ *e* $a^2 - db^2 \in \mathbb{Z}$*. Assim, temos que* $(2a)^2 - d(2b)^2 \in \mathbb{Z}$*, e como* $2a \in \mathbb{Z}$*, segue que* $(2a)^2 \in \mathbb{Z}$*. Por outro lado, se* $2b \notin \mathbb{Z}$*, o seu denominador teria um fator primo* p *e este fator apareceria como* p^2 *no denominador de* $d(2b)^2$*. Sendo* d *livre de quadrados, segue que* $d(2b)^2 \notin \mathbb{Z}$*, o que é um absurdo. Portanto,* $2b \in \mathbb{Z}$*.* ∎

Teorema 1.8.1 *[6, Theorem 3.2] Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *um corpo quadrático, onde* $d \in \mathbb{Z}$ *é livre de quadrados, ou seja,* $d \not\equiv 0(modulo\ 4)$*. Se* $d \not\equiv 1(modulo\ 4)$*, então o anel dos inteiros* $I_{\mathbb{K}}(\mathbb{Z})$ *é* $\mathbb{Z}[\sqrt{d}]$ *e* $\{1, \sqrt{d}\}$ *é uma base de* $\mathbb{Z}[\sqrt{d}]$ *como um* $\mathbb{Z}$*-módulo.*
Demonstração: *Seja* $\alpha = a + b\sqrt{d}$ *com* $a, b \in \mathbb{Q}$ *um inteiro algébrico sobre* $\mathbb{Z}$*. Pelo Lema 1.8.1 temos que* $a = \frac{u}{2}, b = \frac{v}{2}$*, com* $u, v \in \mathbb{Z}$*, e* $a^2 - db^2 \in \mathbb{Z}$*. Substituindo* a *e* b *por* $\frac{u}{2}$ *e* $\frac{v}{2}$*, respectivamente, temos que* $u^2 - dv^2 \in 4\mathbb{Z}$*. Se* $d \not\equiv 1(modulo\ 4)$*, então* $d \equiv 2$ *ou* $d \equiv 3(modulo\ 4)$*. Assim,* u *e* v *são pares. Se por absurdo,* v *fosse ímpar, então* $v^2 \equiv 1(modulo\ 4)$*. Como* $u^2 - dv^2 \in 4\mathbb{Z}$ *segue que* $u^2 - d(4k + 1) \in 4\mathbb{Z}$ *o que implica que* $u^2 - d \in 4\mathbb{Z}$*. Assim,* $u^2 \equiv d(modulo\ 4)$*. Portanto,* $d \equiv 1(modulo\ 4)$ *ou* $d \equiv 0(modulo\ 4)$*, o que é um absurdo por hipótese. Assim, sendo* v *par, temos que* $v^2 \equiv 0(modulo\ 4)$ *e deste modo* $u^2 \in 4\mathbb{Z}$*. Portanto,* u *também é par. Assim,* u *e* v *são pares. Logo,* $a, b \in \mathbb{Z}$ *e* $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$*. Portanto,* $I_{\mathbb{K}}(\mathbb{Z}) \subset \mathbb{Z}[\sqrt{d}]$*. Por outro lado, tomando* $\alpha \in \mathbb{Z}[\sqrt{d}]$*, temos que* α *é raiz do polinômio* $x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$*. Assim,* $\mathbb{Z}[\sqrt{d}] \subset I_{\mathbb{K}}(\mathbb{Z})$*, e portanto,* $\mathbb{Z}[\sqrt{d}] = I_{\mathbb{K}}(\mathbb{Z})$*.* ∎

Teorema 1.8.2 *[6, Theorem 3.2] Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *um corpo quadrático, onde* $d \in \mathbb{Z}$ *é livre de quadrados, ou seja,* $d \not\equiv 0(modulo\ 4)$. *Se* $d \equiv 1(modulo\ 4)$, *então o anel dos inteiros* $I_{\mathbb{K}}(\mathbb{Z})$ *é* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *e* $\{1, \frac{1+\sqrt{d}}{2}\}$ *é uma base de* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *como um* $\mathbb{Z}$*-módulo.*

Demonstração: *Se* $d \equiv 1(modulo\ 4)$, *então* u, v *tem a mesma paridade. Assim, se* u *e* v *são pares temos que* $a, b \in \mathbb{Z}$, *e que* $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. *Se* u *e* v *são ímpares, então* $\alpha = \frac{u}{2} + \frac{v\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. *Portanto, temos que* $I_{\mathbb{K}}(\mathbb{Z}) \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. *Por outro lado, se* $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *com* $a, b \in \mathbb{Z}$, *então temos que* α *é raiz do polinômio* $x^2 - (2a+b)x + \left(a^2 + ab - \frac{(1-d)b^2}{4}\right) \in \mathbb{Z}[x]$, *pois* $d \equiv 1(modulo\ 4)$. *Assim, segue que* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset I_{\mathbb{K}}(\mathbb{Z})$. *Portanto,* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = I_{\mathbb{K}}(\mathbb{Z})$. ∎

1.9 Corpos ciclotômicos

Nesta seção apresentamos o conceito dos corpos ciclotômicos, seu subcorpo maximal real e algumas de suas propriedades, que serão úteis para o cálculo do discriminante destes corpos. Também veremos o anel dos inteiros desses corpos.

Definição 1.9.1 *Seja* $\mathbb{K}$ *um corpo. Um elemento* $\zeta \in \mathbb{K}$ *tal que* $\zeta^n = 1$ *é chamado raiz n-ésima da unidade, onde* n *é um inteiro positivo. Dizemos que* ζ *é uma raiz n-ésima primitiva da unidade se* $\zeta^n = 1$ *e* $\zeta^m \neq 1$ *para* $1 \leq m < n$.

Proposição 1.9.1 *[7, p.205] Sejam* $m, n \in \mathbb{Z}$ *tal que* $mdc(m, n) = 1$. *Temos que* $\zeta_m^k \zeta_n^l$, *para* $0 \leq k \leq m-1$ *e* $0 \leq l \leq n-1$, *é uma raiz* mn*-ésima primitiva da unidade se, e somente se,* ζ_m^k *é uma raiz* m*-ésima primitiva da unidade e* ζ_n^l *é uma raiz* n*-ésima primitiva da unidade.

Demonstração: *Se* ζ_m^k *não é uma raiz* m*-ésima primitiva da unidade, então temos que* $mdc(k, m) = d > 1$. *Assim,* $(\zeta_m^k \zeta_n^l)^{\frac{mn}{d}} = ((\zeta_m^k \zeta_n^l)^{mn})^{\frac{1}{d}} = 1^{\frac{1}{d}} = 1$, *o que é absurdo, pois* $\frac{mn}{d} < mn$. *Reciprocamente, se* ζ_m^k *é uma raiz* m*-ésima primitiva da unidade e* ζ_n^l *é uma raiz* n*-ésima primitiva da unidade, então* $mdc(k, m) = mdc(l, n) = 1$. *Assim,*

$$(\zeta_m^k \zeta_n^l)^a = 1 \iff \zeta_m^{ka} \zeta_n^{la} = 1 \iff \zeta_m^{ka} = \zeta_n^{-la} \iff \zeta_m^{kan} = \zeta_n^{-lan} \iff (\zeta_m^k)^{na} = (\zeta_n^n)^{-la} \iff$$
$$(\zeta_m^k)^{na} = 1^{-la} \iff (\zeta_m^k)^{na} = 1 \iff m | na.$$

Como $mdc(m, n) = 1$ *segue que* $m|a$. *De modo análogo,* $n|a$. *Ainda, usando o fato de que* $mdc(m, n) = 1$ *segue que* $mn|a$. *Assim temos que,* $(\zeta_m^k \zeta_n^l)^{mn} = (\zeta_m^m)^{kn} (\zeta_n^n)^{lm} = 1$. *Logo* mn

é a menor potência tal que $(\zeta_m^k\zeta_n^l)^{mn} = 1$. *Portanto* $\zeta_m^k\zeta_n^l$ *é uma raiz mn-ésima primitiva da unidade.* ■

Observação 1.9.1

1. *Pela Definição 1.9.1, temos que as raízes n-ésimas da unidade são as raízes do polinômio* $x^n - 1$.

2. *O número de raízes n-ésimas primitivas da unidade é dado por*

$$\varphi(n) = \#\{0 < m < n : mdc(m, n) = 1; m, n \in \mathbb{Z}\},$$

onde φ *é a função de Euler.*

Seja $U_n = \{\zeta_n^{r_1}, \ldots, \zeta_n^{r_n}\}$ o conjunto de todas as raízes distintas de $x^n - 1$ em $\mathbb{K}$, ou seja, de todas as raízes n-ésimas da unidade. Como $(\zeta_n^i\zeta_n^j)^n = (\zeta_n^i)^n(\zeta_n^j)^n = (\zeta_n^n)^i(\zeta_n^n)^j = 1$ e $\left(\frac{\zeta_n^i}{\zeta_n^j}\right)^n = \frac{(\zeta_n^i)^n}{(\zeta_n^j)^n} = \frac{(\zeta_n^n)^i}{(\zeta_n^n)^j} = 1$, segue que o conjunto U_n é um grupo multiplicativo. Agora, como todo grupo multiplicativo finito num corpo é cíclico, temos que U_n é um grupo cíclico. Assim, podemos representar as n raízes n-ésimas da unidade por $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1$, onde ζ_n é um gerador do grupo U_n. As raízes n-ésimas primitivas da unidade são os geradores do grupo U_n, isto é, os elementos ζ_n^k com $mdc(k, n) = 1$, para $k = 1, 2, \ldots, n$.

Lema 1.9.1 *[7, p.204] Sejam* $m, n \in \mathbb{Z}$. *Se* $mdc(m, n) = 1$, *então* $U_{mn} \cong U_m \times U_n$, *onde* U_n *denota o grupo de todas as n-ésimas raízes da unidade.*

Demonstração: *Seja a seguinte função:*

$$\begin{aligned} \phi : U_m \times U_n &\longrightarrow U_{mn} \\ (a,\ b) &\longmapsto\ ab \end{aligned}$$

i) ϕ *esta bem definida, pois* $(ab)^{mn} = (a^m)^n(b^n)^m = 1$

ii) ϕ *é homomorfismo, pois* $\forall\,(a,\ b), (c, d) \in U_m \times U_n$ *temos que* $\phi((a,\ b)(c,\ d)) = \phi(ac,\ bd) = (acbd) = (ab)(cd) = \phi(a,\ b)\phi(c,\ d)$.

iii) ϕ *é injetora: Temos que provar que* $Ker(\phi) = \{(a,\ b) \in U_m \times U_n : \phi(a,\ b) = 1\} = \{1\}$. *Deste modo, temos que mostrar que para* $\forall\,(a,\ b) \in U_m \times U_n$ *tal que* $\phi(a,\ b) = ab = 1 \Longrightarrow a = b = 1$. *Para isto, sejam* $a = \zeta_m^k$ *e* $b = \zeta_n^l$, *onde* $0 \leq k \leq m - 1$ *e* $0 \leq l \leq n - 1$. *Assim,* $ab = 1 \iff \zeta_m^k\zeta_n^l = 1 \iff \zeta_m^k = \zeta_n^{-l} \iff \zeta_m^{nk} = \zeta_n^{-nl} \iff \zeta_m^{nk} = 1$. *Logo, como* ζ_m *é uma raiz m-ésima primitiva da unidade, segue que* $m|nk$. *Como* $mdc(m,\ n) = 1$ *segue que* $m|k$, *e isto implica que* $k = mx$. *Analogamente* $n|l$, *e isto implica que* $l = ny$. *Deste*

modo, $\zeta_m^k = \zeta_m^{mx} = 1 = \zeta_n^{-ny} = \zeta_n^{-l}$*, ou seja,* $\zeta_m^k = \zeta_n^{-l} = 1$*. Isto implica que* $k = l = 0$*, pois* ζ_m *e* ζ_n *são raízes m-ésima e n-ésima primitivas da unidade, respectivamente. Portanto* $ab = 1 \Longleftrightarrow a = b = 1$*. Portanto* $Ker(\phi) = \{1\}$ *e assim* ϕ *é injetora.*
iv) ϕ *é sobrejetora: Como* $o(U_m \times U_n) = o(U_{mn})$ *e* ϕ *é injetora, segue que* ϕ *é sobrejetora. Por iii) e iv),* ϕ *é bijetora. Portanto* ϕ *é isomorfismo.* ∎

Definição 1.9.2 *O polinômio* $\phi_n(x) = \prod_{j=1, mdc(j,n)=1}^{n} (x - \zeta_n^j)$ *é chamado de n-ésimo polinômio ciclotômico.*

Proposição 1.9.2 *[7, p.206] Se n é um inteiro positivo, então* $x^n - 1 = \prod_{d|n} \phi_d(x)$.

Demonstração: *Seja* $f(x) = x^n - 1$*. As raízes de* $f(x)$ *são* $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$*. Assim,*

$$x^n - 1 = (x-1)(x-\zeta_n)(x-\zeta_n^2)\ldots(x-\zeta_n^{n-1}).$$

Analisando os períodos de cada raiz de $f(x)$*, e escrevendo todas as raízes de mesmo período como um polinômio da forma*

$$\phi_d(x) = \prod_{d=periodo\ \zeta} (x - \zeta_n),$$

segue que $x^n - 1 = \prod_{d|n} \phi_d(x)$. ∎

Exemplo 1.9.1 *Seja* $f(x) = x^4 - 1$*. As raízes de* $f(x)$ *são* $1, \zeta_4, \zeta_4^2$ *e* ζ_4^3 *que possuem períodos* $1, 4, 2$ *e* 4*, respectivamente. Assim,* $\phi_1(x) = x - 1$*,* $\phi_2(x) = (x - \zeta_4^2)$ *e* $\phi_4(x) = (x - \zeta_4)(x - \zeta_4^3)$*. Como os divisores de* 4 *são* $1, 2$ *e* 4*, temos que*

$$x^4 - 1 = \prod_{d|n} \phi_d(x) = \phi_1(x)\phi_2(x)\phi_4(x) = (x-1)(x-\zeta_4^2)(x-\zeta_4)(x-\zeta_4^3).$$

Corolário 1.9.1 *Se n é um inteiro positivo, então*

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} \phi_d(x)}.$$

Demonstração: *É uma consequência direta da Proposição 1.9.2.* ∎

Exemplo 1.9.2 *Pelo Corolário 1.9.1 temos que*

$$\phi_1(x) = x - 1 \qquad \phi_2(x) = \tfrac{x^2-1}{x-1} = x + 1$$
$$\phi_3(x) = \tfrac{x^3-1}{x-1} = x^2 + x + 1 \quad \phi_4(x) = \tfrac{x^4-1}{(x+1)(x-1)} = x^2 + 1.$$

Observação 1.9.2 *Quando $n = p$, onde p é um número primo, o p-ésimo polinômio ciclotômico é dado por*

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Definição 1.9.3 *Um corpo ciclotômico é um corpo gerado por uma raiz n-ésima da unidade sobre o corpo $\mathbb{Q}$ dos números racionais.*

Definição 1.9.4 *Dado n um inteiro positivo, definimos a raiz n-ésima da unidade ζ_n como $e^{\frac{2\pi i}{n}}$ e o corpo $\mathbb{Q}(\zeta_n)$ é chamado o n-ésimo corpo ciclotômico.*

Teorema 1.9.1 *[7, Theorem 6, p.204] Se ζ_n é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, onde φ é a função de Euler.*

Demonstração: *Seja $f(x)$ um polinômio mônico, irredutível e de menor grau de ζ_n sobre $\mathbb{Q}$. Logo $x^n - 1 = f(x)g(x)$, com $g(x) \in \mathbb{Q}[x]$. Pelo Lema de Gauss segue que $f(x), g(x) \in \mathbb{Z}(x)$. Se p é um primo tal que $p \nmid n$, então ζ_n^p é uma raiz n-ésima primitiva da unidade. Assim, $(\zeta_n^p)^n - 1 = f(\zeta_n^p)g(\zeta_n^p)$, ou seja, $f(\zeta_n^p)g(\zeta_n^p) = 0$. Logo, se ζ_n^p não é raiz de $f(x)$, então ζ_n^p é raiz de $g(x)$, e ζ_n é raiz de $g(x^p)$. Portanto, temos que $f(x) \mid g(x^p)$, ou seja, $g(x^p) = f(x)h(x)$, com $h(x) \in \mathbb{Z}[x]$, pelo Lema de Gauss. Mas, pelo Teorema de Fermat, temos que $a^p \equiv a(mod\ p)$, e daí segue que $g(x^p) \equiv g(x)^p(mod\ p)$. Assim, $f(x)h(x) \equiv g(x)^p(mod\ p)$, ou seja, $g(x)^p \equiv f(x)h(x)(mod\ p)$. Portanto, $g(\bar{\zeta_n})^p = \bar{0}$, pois, ζ_n é raiz de $f(x)$. Recursivamente chegamos que $\bar{g}(\zeta_n) = 0$, ou seja, $\bar{f}$ e $\bar{g}$ tem uma raiz em comum. Assim, $x^n - \bar{1} = \bar{f}\bar{g}$, e deste modo $x^n - \bar{1}$ tem raízes múltiplas. Logo, $nx^{n-1} = \bar{0}$ e daí, para qualquer $\alpha \in \mathbb{Z}_p$, temos que $n\alpha^{n-1} = \bar{0}$. Como a característica de $\mathbb{Z}_p$ é p segue que $p \mid n$, o que contradiz o fato de termos suposto que $p \nmid n$. Portanto ζ_n^p é raiz de $f(x)$ para todo p tal que $p \nmid n$ e $mdc(p, n) = 1$. Portanto $\partial(f(x)) \geq \partial(g(x))$, pois toda raiz de $\phi_n(x)$ é raiz de $f(x)$, e como $f(x) \mid \phi_n(x)$, segue que $\partial(\phi_n(x)) \geq \partial(f(x))$. Assim, $\partial(f(x)) = \partial(\phi_n(x)) = \varphi(n)$.* ∎

Corolário 1.9.2 *Se ζ_n é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \frac{\varphi(n)}{2}$, onde φ é a função de Euler.*

Demonstração: *Temos que $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{Q}(\zeta_n)$. Agora, pelo Teorema 1.9.1 temos que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Assim, pelo Teorema 1.4.2 basta mostrar que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. Mas isso segue do fato que o polinômio $f(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1$ tem ζ_n como raiz e é irredutível sobre $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Portanto, $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \frac{\varphi(n)}{2}$.* ∎

Proposição 1.9.3 *O n-ésimo polinômio ciclotômico $\phi_n(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração: *Temos que existe um único polinômio minimal $m_\alpha(x)$ tal que $m_\alpha(\zeta_n) = 0$.*

Pelo Teorema 1.9.1 segue que $\partial(m_\alpha(x)) = \partial(\phi_n(x))$ *e* $\phi_n(\zeta_n) = 0$. *Portanto* $m_\alpha \equiv \phi_n$, *e assim* $\phi_n(x)$ *é irredutível sobre* $\mathbb{Q}$. ∎

Corolário 1.9.3 *[7, p.205] Se* m *e* n *são primos entre si, então* $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.
Demonstração: *Segue da Proposição 1.9.1.* ∎

Lema 1.9.2 *[8, p.24] Se* ζ_p *é uma raiz p-ésima primitiva da unidade e* $\mathbb{K} = \mathbb{Q}(\zeta_p)$, *onde p é um número primo, então:*

1. $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j) = -1$, *para* $j = 1, \ldots, p-1$.
2. $Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p^j) = p$, *para* $j = 1, \ldots, p-1$.
3. $N_{\mathbb{K}/\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p$ *e* $N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p) = p$.
4. $p = (1 - \zeta_p)(1 - \zeta_p^2)\ldots(1 - \zeta_p^{p-1})$.

Demonstração:

1. *Pela Observação 1.9.2 temos que o p-ésimo polinômio ciclotômico de* ζ_p *é dado por* $\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$. *As raízes de* $\phi_p(x)$ *são* $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$. *Assim,* $0 = \phi_p(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j + 1$, *e daí segue que* $\zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j = -1$. *Portanto,* $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j = -1$, *para* $j = 1, \ldots, p-1$.
2. *Temos que* $Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p^j) = Tr_{\mathbb{K}/\mathbb{Q}}(1) - Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j)$. *Mas como* $[\mathbb{Q}[\zeta_p] : \mathbb{Q}] = p - 1$ *segue que* $Tr_{\mathbb{K}/\mathbb{Q}}(1) = 1 + 1 + \ldots + 1 = p - 1$, *e do ítem 1 temos que* $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^j) = -1$. *Assim, obtemos que* $Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p^j) = p - 1 + 1 = p$.
3. *Como* $\zeta_p - 1$ *é uma raiz do polinômio* $f(x)$ *dado por* $f(x) = x^{p-1} + \sum_{j=p-1}^{1} \binom{p}{j} x^{j-1}$ *segue que,* $N(\zeta_p - 1) = (-1)^{p-1}p$, *e* $N(1 - \zeta_p) = N((-1)(\zeta_p - 1)) = N(-1)N(\zeta_p - 1) = (-1)^{p-1}(-1)^{p-1}p = (-1)^{2(p-1)}p = p$.
4. *Como* $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ *são raízes do polinômio mônico* $\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$, *segue que* $x^{p-1} + x^{p-2} + \ldots + x + 1 = (x - \zeta_p)(x - \zeta_p^2)\ldots(x - \zeta_p^{p-1})$. *Assim, tomando* $x = 1$, *obtemos que* $(1 - \zeta_p)(1 - \zeta_p^2)\ldots(1 - \zeta_p^{p-1}) = p$. ∎

Lema 1.9.3 *[8, Lema 2.3.3] Se* $\mathbb{K} = \mathbb{Q}(\zeta_p)$, *onde p é um número primo,* $I_{\mathbb{K}}(\mathbb{Z})$ *é o anel dos inteiros de* $\mathbb{K}$, *e* $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$, *então:*

1. $(1 - \zeta_p)I_{\mathbb{K}}(\mathbb{Z}) \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$.

2. $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in p\mathbb{Z}$, *para todo* $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$.

Demonstração:

1. *Pelo ítem 4 do Lema 1.9.2 temos que* $p = (1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$. *Assim,* $p \in (1-\zeta_p)I_{\mathbb{K}}(\mathbb{Z})$, *e portanto,* $\langle p\rangle \subset (1-\zeta_p)\cap\mathbb{Z}$. *Por outro lado, suponhamos que o ideal* $p\mathbb{Z} \nsubseteq (1-\zeta_p)I_{\mathbb{K}}(\mathbb{Z})\cap\mathbb{Z} \subset \mathbb{Z}$. *Como* $p\mathbb{Z}$ *é maximal, segue que* $(1-\zeta_p)I_{\mathbb{K}}(\mathbb{Z})\cap\mathbb{Z} = \mathbb{Z}$. *Daí,* $1 \in \mathbb{Z}$, *e então* $1 = (1-\zeta_p)a$, *com* $a \in I_{\mathbb{K}}(\mathbb{Z})$. *Assim,* $1-\zeta_p$ *é inversível, e portanto* $1-\zeta_p^j$ *são inversíveis em* $I_{\mathbb{K}}(\mathbb{Z})$. *Deste modo,* $(1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1}) = p$ *é inversível em* $\mathbb{Z}$, *o que é um absurdo. Portanto,* $p\mathbb{Z} = (1-\zeta_p)I_{\mathbb{K}}(\mathbb{Z})\cap\mathbb{Z}$.

2. *Cada conjugado* $\alpha_i(1-\zeta_p^i)$ *de* $\alpha(1-\zeta_p)$ *é um múltiplo de* $(1-\zeta_p^i)$ *em* $I_{\mathbb{K}}(\mathbb{Z})$, *onde* $i = 1, 2, \ldots, p-1$. *Como*

$$1-\zeta_p^i = (1-\zeta_p)(\zeta_p^{i-1}+\zeta_p^{i-2}+\ldots+\zeta_p+1),$$

segue que $1-\zeta_p^i$ *é um múltiplo de* $1-\zeta_p$ *em* $I_{\mathbb{K}}(\mathbb{Z})$. *Como o traço é a soma dos conjugados, segue que*

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) = \alpha_1(1-\zeta_p)+\alpha_2(1-\zeta_p^2)+\ldots+\alpha_p(1-\zeta_p^p) = \beta(1-\zeta_p),$$

onde $\beta \in I_{\mathbb{K}}(\mathbb{Z})$. *Portanto,* $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in I_{\mathbb{K}}(\mathbb{Z})$. *Como* $\mathbb{Z}$ *é integralmente fechado, segue que* $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in \mathbb{Z}$. *Assim,*

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) \in (1-\zeta_p)I_{\mathbb{K}}(\mathbb{Z})\cap\mathbb{Z}{=}p\mathbb{Z}.$$

■

Teorema 1.9.2 *[3, Theorem 2, p.43] O anel dos inteiros de* $\mathbb{K} = \mathbb{Q}(\zeta_p)$, *onde* p *é um número primo, é* $\mathbb{Z}[\zeta_p]$ *e* $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ *é uma base de* $\mathbb{Z}[\zeta_p]$ *como um* $\mathbb{Z}$*-módulo.*
Demonstração: *Seja* $I_{\mathbb{K}}(\mathbb{Z})$ *o anel dos inteiros de* $\mathbb{Q}(\zeta_p)$. *Temos que* $\mathbb{Z}[\zeta_p] \subset I_{\mathbb{K}}(\mathbb{Z})$. *Agora, vamos provar que* $I_{\mathbb{K}}(\mathbb{Z}) \subset \mathbb{Z}[\zeta_p]$. *Se* $\alpha \in I_{\mathbb{K}}(\mathbb{Z}) \subset \mathbb{Q}(\zeta_p)$, *então*

$$\alpha = a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2}, \text{ com } a_i \in \mathbb{Q}, \text{ para } i = 0, 1, \ldots, p-2.$$

Multiplicando por $1-\zeta_p$ *em ambos os lados obtemos que*

$$\alpha(1-\zeta_p) = a_0(1-\zeta_p) + a_1(\zeta_p-\zeta_p^2) + \ldots + a_{p-2}(\zeta_p^{p-2}-\zeta_p^{p-1}).$$

Pelo Lema 1.9.3 segue que

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1-\zeta_p)) = a_0Tr_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p) + a_1Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p-\zeta_p^2) + \ldots + a_{p-2}Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^{p-2}-\zeta_p^{p-1}) \in p\mathbb{Z}.$$

Assim, como $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^i - \zeta_p^{i+1}) = 0$, *para* $i = 1, 2, \ldots, p-2$, *segue que* $a_0 Tr_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p) = a_0 p \in p\mathbb{Z}$, *onde* $a_0 \in \mathbb{Z}$. *Analogamente, como* $\zeta_p^{-1} = \zeta_p^{p-1} \in I_{\mathbb{K}}(\mathbb{Z})$, *segue que*

$$(\alpha - a_0)\zeta_p^{-1} = a_1 + a_2\zeta_p + \ldots + a_{p-2}\zeta_p^{p-3}.$$

Multiplicando ambos os lados por $1 - \zeta_p$ *obtemos que*

$$(\alpha - a_0)\zeta_p^{-1}(1 - \zeta_p) = a_1(1 - \zeta_p) + a_2\zeta_p(1 - \zeta_p) + \ldots + a_{p-2}\zeta_p^{p-3}(1 - \zeta_p),$$

e assim, pelo Lema 1.9.3, segue que

$$Tr_{\mathbb{K}/\mathbb{Q}}((\alpha-a_0)\zeta_p^{-1}(1-\zeta_p)) = a_1 Tr_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p)+a_2 Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p-\zeta_p^2)+\ldots+a_{p-2}Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^{p-3}-\zeta_p^{p-2}) \in p\mathbb{Z}.$$

Logo, $a_1 Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p) = a_1 p \in p\mathbb{Z}$, *onde* $a_1 \in \mathbb{Z}$. *Prosseguindo, desta forma, temos que* $a_i \in \mathbb{Z}$, *para cada* $i = 1, \cdots, n$. *Assim,* $\alpha \in \mathbb{Z}[\zeta_p]$. *Portanto,* $\mathbb{Z}[\zeta_p] = I_{\mathbb{K}}(\mathbb{Z})$. ∎

Proposição 1.9.4 *O anel dos inteiros de* $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, *onde* p *é um número primo é* $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ *e* $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ *é uma base de* $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ *como um* $\mathbb{Z}$*-módulo.*

Demonstração: *Temos que o anel dos inteiros de* $\mathbb{Q}(\zeta_p)$ *é* $\mathbb{Z}[\zeta_p]$. *Como* ζ_p *é inteiro, segue que é uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *e como* ζ_p^{-1} *é inteiro e pelo Corolário 1.3.2, segue que* $\zeta_p + \zeta_p^{-1}$ *também. Portanto* $\mathbb{Z}[\zeta_p + \zeta_p^{-1}] \subseteq I_{\mathbb{K}}(\mathbb{Z})$. *Mostremos, agora, que* $I_{\mathbb{K}}(\mathbb{Z}) \subseteq \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. *Se* $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$ *um inteiro algébrico, então*

$$\alpha = a_1(\zeta_p + \zeta_p^{-1}) + a_2(\zeta_p^2 + \zeta_p^{-2}) + \ldots + a_{\frac{p-1}{2}}(\zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}), \text{ onde } a_i \in \mathbb{Q}, \text{ para } i = 1, 2, \ldots \frac{p-1}{2}.$$

Temos que mostrar que $a_i \in \mathbb{Z}$. *Multiplicando* α *por* $\zeta_p^{\frac{p-1}{2}}$, *obtemos que*

$$\zeta_p^{\frac{p-1}{2}}\alpha = a_1\zeta_p^{\frac{p+1}{2}} + a_1\zeta_p^{\frac{p-3}{2}} + a_2\zeta_p^{\frac{p+3}{2}} + a_2\zeta_p^{\frac{p-5}{2}} + \ldots + a_{\frac{p-1}{2}}\zeta_p^{p-1} + a_{\frac{p-1}{2}},$$

que é um inteiro algébrico de $\mathbb{Q}(\zeta_p)$, *logo pertence a* $\mathbb{Z}[\zeta_p]$. *Assim segue que* $a_i \in \mathbb{Z}$, *para* $i = 1, 2, \ldots, \frac{p-1}{2}$. *Portanto* $I_{\mathbb{K}}(\mathbb{Z}) = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, *ou seja, o anel dos inteiros de* $\mathbb{K}$ *é* $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. *Como* $\{\zeta_p+\zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}}+\zeta_p^{\frac{1-p}{2}}\}$ *é uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *e como* $\{\zeta_p+\zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}}+\zeta_p^{\frac{1-p}{2}}\} \subseteq \mathbb{Z}[\zeta_p+\zeta_p^{-1}] \subseteq I_{\mathbb{K}}(\mathbb{Z})$, *segue que é suficiente mostrar que* $\{\zeta_p+\zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}}+\zeta_p^{\frac{1-p}{2}}\}$ *é linearmente independente, para isso, sejam* $a_1, a_2, \ldots, a_{\frac{p-1}{2}} \in \mathbb{Z}$ *tal que*

$$a_1(\zeta_p + \zeta_p^{-1}) + a_2(\zeta_p^2 + \zeta_p^{-2}) + \ldots + a_{\frac{p-1}{2}}(\zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}) = 0.$$

Logo

$$a_1\zeta_p + a_1\zeta_p^{p-1} + a_2\zeta_p^2 + a_2\zeta_p^{p-2} + \ldots + a_{\frac{p-1}{2}}\zeta_p^{\frac{p-1}{2}} + a_{\frac{p-1}{2}}\zeta_p^{\frac{p-1}{2}} = 0.$$

Como $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ *é uma base de* $\mathbb{Z}[\zeta_p]$ *sobre* $\mathbb{Z}$*, segue que estes elementos são linearmente independentes, e deste modo temos que* $a_1 = a_2 = \ldots = a_{\frac{p-1}{2}} = 0$*. Assim* $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ *é linearmente independente. Portanto,* $\{\zeta_p+\zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}}+\zeta_p^{\frac{1-p}{2}}\}$ *é uma base de* $\mathbb{Z}[\zeta_p+\zeta_p^{-1}]$ *sobre* $\mathbb{Z}$*.* ∎

Observação 1.9.3 *Quando* $n = p^r$*, onde* p *é um número primo e* r *é um inteiro maior que* 1*, o* p^r*-ésimo polinômio ciclotômico é dado por*

$$\phi_{p^r}(x) = \frac{x^{p^r} - 1}{\phi_1(x)\phi_2(x)\ldots\phi_{p^{r-1}}(x)} = \frac{x^{p^r-1}}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \ldots + x^{p^{r-1}} + 1.$$

Lema 1.9.4 *[8, p.26] Seja* $\mathbb{K} = \mathbb{Q}(\zeta_p^r)$*, onde* p *é um número primo e* r *é um inteiro maior que* 1*. Se* $I_{\mathbb{K}}(\mathbb{Z})$ *é o anel dos inteiros de* $\mathbb{K}$*, e* $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$*, então:*

1. $(1 - \zeta_p^r)I_{\mathbb{K}}(\mathbb{Z}) \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$.

2. $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha(1 - \zeta_p^r)) \in p\mathbb{Z}$*, para todo* $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$.

Demonstração: *A demonstração é análoga a feita no Lema 1.9.3.* ∎

Lema 1.9.5 *[9, Lemma 1, p.30] Temos que* $\mathbb{Z}[1 - \zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$.
Demonstração: *Por definição temos que* $\mathbb{Z}[\alpha] = \{\sum a_i\alpha^i;\ a_i \in \mathbb{Z}\}$*. Assim, para todo* $\alpha \in \mathbb{Z}[1 - \zeta_{p^r}]$ *temos que*

$$\begin{aligned} \alpha &= a_0 + a_1(1 - \zeta_{p^r}) + a_2(1 - \zeta_{p^r})^2 + \ldots + a_{(p-1)p^{r-1}}(1 - \zeta_{p^r})^{(p-1)p^{r-1}} \\ &= (a_0 + a_1 + \ldots + a_{(p-1)p^{r-1}}) + (-a_1 - 2a_2)\zeta_{p^r} + \ldots. \end{aligned}$$

Assim, $\alpha = b_0 + b_1\zeta_{p^r} + b_2\zeta_{p^r}^2 + \ldots + b_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}$*, e portanto* $\alpha \in \mathbb{Z}[\zeta_{p^r}]$*. Agora, se* $\alpha \in \mathbb{Z}[\zeta_{p^r}]$*, então* $\alpha = a_0 + a_1\zeta_{p^r} + a_2\zeta_{p^r}^2 + \ldots + a_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}$*. Como* $\zeta_{p^r} = 1 - (1 - \zeta_{p^r})$*, então podemos escrever* α *da forma*

$$\begin{aligned} \alpha &= a_0 + a_1(1 - (1 - \zeta_{p^r})) + a_2(1 - (1 - \zeta_{p^r}))^2 + \ldots + a_{(p-1)p^{r-1}}(1 - (1 - \zeta_{p^r}))^{(p-1)p^{r-1}} \\ &= a_0 + a_1 - a_1(1 - \zeta_{p^r}) + a_2(1 - 2(1 - \zeta_{p^r} + (1 - \zeta_{p^r}))^2)) + \ldots \\ &= a_0 + a_1 - a_1(1 - \zeta_{p^r}) + a_2 - 2a_2(1 - \zeta_{p^r}) + a_2(1 - \zeta_{p^r})^2 + \ldots \\ &= (a_0 + a_1 + a_2 + \ldots + a_{(p-1)p^{r-1}-1}) + (-a_1 - 2a_2 - \ldots - ((p-1)p^{r-1} - 1)a_{(p-1)p^{r-1}-1}) \\ &\quad (1 - \zeta_{p^r}) + (a_2 - 3a_3 + \ldots)(1 - \zeta_{p^r})^2 + \ldots, \end{aligned}$$

ou seja, $\alpha = b_0+b_1(1-\zeta_{p^r})+b_2(1-\zeta_{p^r})^2+\ldots+b_{(p-1)p^{r-1}}(1-\zeta_{p^r})^{(p-1)p^{r-1}} \in \mathbb{Z}[1-\zeta_{p^r}]$*. Portanto,* $\mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[1 - \zeta_{p^r}]$. ∎

Proposição 1.9.5 *[9, Lemma 2, p.31] Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um inteiro maior que 1, então:*

1. $N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = (-1)^{(p-1)p^{r-1}}$,
2. $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = -1$,
3. $Tr_{\mathbb{K}/\mathbb{Q}}(\mathcal{A}) = (p-1)p^{r-1}\mathcal{A}$, *onde* $\mathcal{A}$ *é um ideal,*
4. $N_{\mathbb{K}/\mathbb{Q}}(\mathcal{A}) = \mathcal{A}^{(p-1)p^{r-1}}$,
5. $\prod_k (1-\zeta_{p^r}^k) = p$, *com* $1 \leq k \leq p^r$, *e tal que* $p \not| k$. *Em particular,* $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = p$,
6. $Tr_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = (p-1)p^{r-1}+1$.

Demonstração:

1. *Temos que* $N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = \zeta_{p^r}^j \zeta_{p^r}^{j+1} \ldots \zeta_{p^r}^{j+(p-1)p^{r-1}}$. *Como* $\zeta_{p^r}^j$ *e* $\zeta_{p^r}^{j+p^{r-1}}$ *são conjugados segue que* $\zeta_{p^r}\zeta_{p^r}^{j+1} \ldots \zeta_{p^r}^{j+(p-1)p^{r-1}} = (-1)^{(p-1)p^{r-1}}$. *Portanto,* $N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = (-1)^{(p-1)p^{r-1}}$, *para* $j = 0, \ldots, p^{r-1}$ *e* $mdc(j, p^r) = 1$.

2. *Temos que* $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = \zeta_{p^r}^j + \zeta_{p^r}^{j+1} + \ldots + \zeta_{p^r}^{j+(p-1)p^{r-1}}$. *Como* $\phi_{p^r}(\zeta_{p^r}^j) = \zeta_{p^r}^j + \zeta_{p^r}^{j+1} + \ldots + \zeta_{p^r}^{j+(p-1)p^{r-1}} + 1 = 0$, *segue que* $\zeta_{p^r}^j + \zeta_{p^r}^{j+1} + \ldots + \zeta_{p^r}^{j+(p-1)p^{r-1}} = -1$. *Portanto,* $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = -1$.

3. $Tr_{\mathbb{K}/\mathbb{Q}}(\mathcal{A}) = \mathcal{A} + \mathcal{A} + \ldots + \mathcal{A} = (p-1)p^{r-1}\mathcal{A}$

4. $N_{\mathbb{K}/\mathbb{Q}}(\mathcal{A}) = \mathcal{A}.\mathcal{A} \ldots \mathcal{A} = \mathcal{A}^{(p-1)p^{r-1}}$.

5. *Como* $\phi_{p^r}(x) = \dfrac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \ldots + x^{(p-1)p^{r-1}}$, *segue que todos os* $\zeta_{p^r}^k$, *onde* $1 \leq k \leq p^r$ *e tal que* $p \nmid k$ *são raízes de* $\phi_{p^r}(x)$ *uma vez que são raízes de* $x^{p^r}-1$ *mas não de* $x^{p^{r-1}}-1$. *Deste modo,* $\phi_{p^r}(x) = \prod_k (x-\zeta_{p^r}^k)$ *e existem exatamente* $\varphi(p^r) = (p-1)p^{r-1}$ *valores de* k *pois* $\partial(\phi_{p^r}(x)) = (p-1)p^{r-1}$. *Tomando* $x = 1$, *obtemos que* $\phi_{p^r}(1) = \prod_{k=1, p\nmid k}^{p^r} (1-\zeta_{p^r}^k) = 1 + 1^{p^{r-1}} + \ldots + 1^{(p-1)p^{r-1}} = p$. *Portanto,* $\prod_{k=1, p\nmid k}^{p^r} (1-\zeta_{p^r}^k) = p$.

   Agora, como $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = \prod_{j=1, p\nmid j}^{p^r} (1-\zeta_{p^r}^j)$, *segue que* $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = p$.

6. *Como* $Tr_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = Tr_{\mathbb{K}/\mathbb{Q}}(1) - T_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r})$, *segue, pelo ítem 3, que* $Tr_{\mathbb{K}/\mathbb{Q}}(1) = (p-1)p^{r-1}$ *e pelo ítem 2, que* $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}) = -1$. *Portanto,* $Tr_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) = (p-1)p^{r-1}+1$.■

Teorema 1.9.3 *[9, Theorem 9, p.29] Sejam $\mathbb{K}$ uma extensão finita de grau n de $\mathbb{Q}$, $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, onde $\alpha_i \in I_{\mathbb{K}}(\mathbb{Z})$ e $D_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = d$. Se $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$, então α pode ser escrito na forma*

$$\frac{m_1\alpha_1 + \ldots + m_n\alpha_n}{d},$$

com $m_j \in \mathbb{Z}$ e m_j^2 divisível por d, para $j = 1, 2, \ldots, n$.

Demonstração: *Seja $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$. Como $I_{\mathbb{K}}(\mathbb{Z}) \subseteq \mathbb{K}$ segue que $\alpha \in \mathbb{K}$. Sendo $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, temos que α pode ser escrito na forma*

$$\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n,$$

com $a_j \in \mathbb{Q}$, para $j = 1, \ldots, n$. Sejam $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Aplicando cada σ_i, para $i = 1, \ldots, n$, em α, obtemos um sistema de n equações dado por

$$\sigma_i(\alpha) = a_1\sigma_i(\alpha_1) + \ldots + a_n\sigma_i(\alpha_n),$$

para $i = 1, \ldots, n$. Resolvendo esse sistema pela regra de Cramer, obtemos que as n raízes são dadas por $a_j = \frac{\gamma_j}{\delta}$, onde $\delta = \det(\sigma_i(\alpha_j))$ e γ_j é obtido de δ trocando a j-ésima coluna por $\sigma_i(\alpha)$. Temos que os γ_j, para $j = 1, 2, \ldots, n$, e δ são inteiros algébricos uma vez que são obtidos a partir dos $\alpha_i's$, que são, por hipótese, inteiros algébricos. Pela Proposição 1.7.3, temos que $\delta^2 = d$ e portanto $da_j = d\frac{\gamma_j}{\delta} = \delta^2\frac{\gamma_j}{\delta} = \delta\gamma_j$ é um inteiro algébrico. Como $\mathbb{Z}$ é integralmente fechado segue que $da_j \in \mathbb{Z}$, para $j = 1, 2, \ldots, n$. Seja $m_j = da_j$, para $j = 1, 2, \ldots n$. Se mostrarmos que $\frac{m_j^2}{d} \in \mathbb{Z}$, teremos que m_j^2 é divisível por d. Mas, como $\frac{m_j^2}{d} \in \mathbb{Q}$ e como $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$ então é suficiente mostrarmos que $\frac{m_j^2}{d}$ é um inteiro algébrico. Como $m_j = da_j = \delta\gamma_j$ segue que $m_j^2 = d^2a_j^2 = \delta^2\gamma_j^2 = d\gamma_j^2$. Logo $\frac{m_j^2}{d} = \gamma_j^2$ é um inteiro algébrico pois γ_j é um inteiro algébrico. Portanto $\frac{m_j^2}{d} \in \mathbb{Z}$ e assim m_j^2 é divisível por d. Assim, $\alpha = \frac{m_1\alpha_1 + \ldots + m_n\alpha_n}{d}$, com $m_j \in \mathbb{Z}$ e m_j^2 divisível por d, para $j = 1, 2, \ldots, n$. ∎

Lema 1.9.6 *[9, p.31] Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um inteiro maior que 1. Se $D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = d$, então $d = p^s$ para algum $s \in \mathbb{N}$.*

Demonstração: *Pela Observação 1.9.3 temos que o p^r-ésimo polinômio ciclotômico é dado por*

$$\phi_{p^r}(x) = \frac{x^{p^r-1}}{x^{p^{r-1}} - 1}.$$

Logo

$$x^{p^r} - 1 = \phi_{p^r}(x)g(x), \tag{1.5}$$

onde $g(x) = x^{p^{r-1}} - 1$. *Derivando ambos os lados da Equação (1.5) obtemos que*

$$p^r x^{p^r-1} = \phi'_{p^r}(x)g(x) + \phi_{p^r}(x)g'(x),$$

e substituindo x *por* ζ_{p^r} *obtemos que*

$$p^r \zeta_{p^r}^{p^r-1} = \phi'_{p^r}(\zeta_{p^r})g(\xi_{p^r}) + \phi_{p^r}(\zeta_{p^r})g'(\zeta_{p^r}).$$

Como $\phi_{p^r}(\zeta_{p^r}) = 0$ *segue que* $p^r \xi_{p^r}^{p^r-1} = \phi'_{p^r}(\xi_{p^r})g(\xi_{p^r})$, *ou seja,*

$$p^r \zeta_{p^r}^{p^r} \xi_{p^r}^{-1} = \phi'_{p^r}(\xi_{p^r})g(\xi_{p^r}).$$

Logo,

$$p^r = \zeta_{p^r}\phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}),$$

e aplicando a função norma em ambos os lados da última igualdade ficamos com

$$p^{(p-1)p^{r-1}r} = N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r}))N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Assim, pela Proposição 1.7.4, temos que

$$p^{(p-1)p^{r-1}r} = \pm D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1})N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Portanto, $d | p^{r(p-1)p^{r-1}}$, *ou seja,* $d = p^s$, *para algum inteiro* s. ∎

Teorema 1.9.4 *[9, Theorem 10, p.30] O anel dos inteiros de* $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, *onde* p *é um número primo e* r *é um inteiro maior que* 1, *é* $\mathbb{Z}[\zeta_{p^r}]$ *e* $\{1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ *é uma base de* $\mathbb{Z}[\zeta_{p^r}]$ *como um* $\mathbb{Z}$*-módulo.*

Demonstração: *Mostraremos que* $I_{\mathbb{K}}(\mathbb{Z}) = \mathbb{Z}[1 - \zeta_{p^r}]$. *Suponhamos, por absurdo, que* $I_{\mathbb{K}}(\mathbb{Z}) \neq \mathbb{Z}[1 - \zeta_{p^r}]$. *Se* $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$, *então pelo Teorema 1.9.3 temos que*

$$\alpha = \frac{m_0 + m_1(1 - \zeta_{p^r}) + \ldots + m_{(p-1)p^{r-1}-1}(1 - \zeta_{p^r})^{(p-1)p^{r-1}-1}}{p^s},$$

onde $m_i \in \mathbb{Z}$, *para* $i = 1, 2, \ldots, (p-1)p^{r-1}$. *Pelo Lema 1.9.6, temos que* $d = p^s$, *onde* $s \in \mathbb{N}$. *Logo, existe* $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$ *tal que nem todos os* $m'_i s$ *são divisíveis por* p^s. *Suponhamos que* m_j, *com* $j \leq (p-1)p^{r-1}$, *não seja divisível por* p^s. *Deste modo, temos que existem* $q, r \in \mathbb{Z}$ *tal que* $m_j = p^s q + r$, *onde* $0 < r < p^s$. *Assim, substituindo* m_j *na equação de* α *obtemos que*

$$\alpha = \frac{m_0 + m_1(1 - \xi_{p^r}) + \ldots + (p^s q + r)(1 - \zeta_{p^r})^j + \ldots + m_{(p-1)p^{r-1}-1}(1 - \zeta_{p^r})^{(p-1)p^{r-1}-1}}{p^s}.$$

Logo, $I_{\mathbb{K}}(\mathbb{Z})$ possui um elemento da forma

$$\beta = \frac{r(1-\zeta_{p^r})^{j-1} + m_j(1-\zeta_{p^r})^j + \ldots + m_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}}{p^s}.$$

Multiplicando ambos os lados por p^{s-1}, ficamos com

$$\beta p^{s-1} = \frac{r(1-\zeta_{p^r})^{j-1} + m_j(1-\zeta_{p^r})^j + \ldots + m_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}}{p},$$

que pode ser escrito como

$$\gamma = \frac{a_{j-1}(1-\zeta_{p^r})^{j-1} + a_j(1-\zeta_{p^r})^j + \ldots + a_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}}{p},$$

onde $a_i \in \mathbb{Z}$ e a_j não é divisível por p. Agora, pelo ítem 5, da Proposição 1.9.5, temos que $\prod^{p^r}(1-\zeta_{p^r}) = p$. Logo $\frac{p}{(1-\zeta_{p^r})^n} \in \mathbb{Z}[1-\zeta_{p^r}]$ uma vez que $1-\zeta_{p^r}^k$ é divisível, em $\mathbb{Z}[1-\zeta_{p^r}]$, por $(1-\zeta_{p^r})$. Assim, $\frac{p}{(1-\zeta_{p^r})^j} \in \mathbb{Z}[1-\zeta_{p^r}]$ e daí $\frac{\gamma p}{(1-\zeta_{p^r})^j} \in I_{\mathbb{K}}(\mathbb{Z})$. Subtraindo termos que estão em $I_{\mathbb{K}}(\mathbb{Z})$, obtemos que $\frac{a_j}{(1-\zeta_{p^r})} \in I_{\mathbb{K}}(\mathbb{Z})$. Daí $N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_{p^r}) | N_{\mathbb{K}/\mathbb{Q}}(a_j)$. Mas, como $N_{\mathbb{K}/\mathbb{Q}}(a_j) = a_j^n$, segue do ítem 5 da Proposição 1.9.5, que $p \mid a_j^n$, o que é um absurdo pois $p \nmid a_j$. Assim, $I_{\mathbb{K}}(\mathbb{Z}) = \mathbb{Z}[1-\zeta_{p^r}]$. Agora, pelo Lema 1.9.5, temos que $\mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$. Portanto, $I_{\mathbb{K}}(\mathbb{Z}) = \mathbb{Z}[\zeta_{p^r}]$. ■

Proposição 1.9.6 *O anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, onde p é um número primo e r é um inteiro maior que 1 é $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ e $\{\zeta_{p^r} + \zeta_{p^r}^{-1}, \ldots, \zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ como um $\mathbb{Z}$-módulo.*

Demonstração: *Temos que o anel dos inteiros de $\mathbb{Q}(\zeta_{p^r})$ é $\mathbb{Z}[\zeta_{p^r}]$. Como ζ_{p^r} é inteiro, segue que $\zeta_{p^r}^{-1}$ é inteiro e pelo Corolário 1.3.2, segue que $\zeta_{p^r} + \zeta_{p^r}^{-1}$ também é inteiro. Portanto $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}] \subseteq I_{\mathbb{K}}(\mathbb{Z})$. Mostremos agora que $I_{\mathbb{K}}(\mathbb{Z}) \subseteq \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$. Se $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$ é um inteiro algébrico, então*

$$\alpha = a_1(\zeta_{p^r} + \zeta_{p^r}^{-1}) + a_2(\zeta_{p^r}^2 + \zeta_{p^r}^{-2}) + \ldots + a_{\frac{(p-1)p^{r-1}}{2}}(\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}),$$

onde $a_i \in \mathbb{Q}$, para $i = 1, 2, \ldots, \frac{(p-1)p^{r-1}}{2}$. Temos que mostrar que $a_i \in \mathbb{Z}$. Multiplicando α por $\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}$, obtemos que

$$\begin{aligned}\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}\alpha &= a_1\zeta_p^{\frac{(p-1)p^{r-1}+2}{2}} + a_1\zeta_{p^r}^{\frac{(p-1)p^{r-1}-2}{2}} + a_2\zeta_{p^r}^{\frac{(p-1)p^{r-1}+4}{2}} + a_2\zeta_{p^r}^{\frac{(p-1)p^{r-1}-4}{2}} + \ldots \\ &+ a_{\frac{(p-1)p^{r-1}}{2}}\zeta_{p^r}^{(p-1)p^{r-1}} + a_{\frac{(p-1)p^{r-1}}{2}},\end{aligned}$$

que é um inteiro algébrico em $\mathbb{Q}(\zeta_{p^r})$, logo pertence a $\mathbb{Z}[\zeta_{p^r}]$. Assim segue que $a_i \in \mathbb{Z}$, para $i = 1, 2, \ldots, \frac{(p-1)p^{r-1}}{2}$. Portanto $I_{\mathbb{K}}(\mathbb{Z}) = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$, ou seja, o anel dos inteiros de $\mathbb{K}$ é

$\mathbb{Z}[\zeta_{p^r}+\zeta_{p^r}^{-1}]$. *Como* $\{\zeta_{p^r}+\zeta_{p^r}^{-1},\ldots,\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}+\zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\}$ *é uma* $\mathbb{Z}$*-base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *e como* $\{\zeta_{p^r}+\zeta_{p^r}^{-1},\ldots,\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}+\zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\}\subseteq\mathbb{Z}[\zeta_{p^r}+\zeta_{p^r}^{-1}]\subseteq I_{\mathbb{K}}(\mathbb{Z})$, *segue que é suficiente mostrar que é linearmente independente. Para isso, sejam* $a_1,a_2,\ldots,a_{\frac{(p-1)p^{r-1}}{2}}\in\mathbb{Z}$ *e suponhamos que*

$$a_1(\zeta_{p^r}+\zeta_{p^r}^{-1})+a_2(\zeta_{p^r}^2+\zeta_{p^r}^{-2})+\ldots+a_{\frac{(p-1)p^{r-1}}{2}}(\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}+\zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}})=0.$$

Logo

$$a_1\zeta_{p^r}+a_1\zeta_{p^r}^{(p-1)p^{r-1}-1}+a_2\zeta_{p^r}^2+a_2\zeta_{p^r}^{(p-1)p^{r-1}-2}+\ldots+a_{\frac{(p-1)p^{r-1}}{2}}\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}+a_{\frac{(p-1)p^{r-1}}{2}}\zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}=0.$$

Como $\{1,\zeta_{p^r},\ldots,\zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ *é uma base de* $\mathbb{Z}[\zeta_{p^r}]$ *sobre* $\mathbb{Z}$, *segue que estes elementos são linearmente independentes, e daí segue que* $a_1=a_2=\ldots=a_{\frac{(p-1)p^{r-1}}{2}}=0$. *Assim* $\{\zeta_{p^r}+\zeta_{p^r}^{-1},\ldots,\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}+\zeta^{\frac{(1-p)p^{r-1}}{2}}\}$ *é linearmente independente. Portanto,* $\{\zeta_{p^r}+\zeta_{p^r}^{-1},\ldots,\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}+\zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\}$ *é uma base de* $\mathbb{Z}[\zeta_{p^r}+\zeta_{p^r}^{-1}]$ *sobre* $\mathbb{Z}$. ∎

Agora, nosso objetivo é determinar o anel dos inteiros para qualquer corpo ciclotômico $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. Esta generalização seguirá de um resultado mais geral considerando os inteiros algébricos de um corpo composto $\mathbb{KL}$, onde $\mathbb{K}$ e $\mathbb{L}$ são corpos de números. Para isso, se $\mathbb{K}$ e $\mathbb{L}$ são corpos de números, então o corpo composto $\mathbb{KL}$, que é definido como o menor subcorpo de $\mathbb{C}$ que contém $\mathbb{K}$ e $\mathbb{L}$, consiste de todas as somas finitas

$$\alpha_1\beta_1+\cdots+\alpha_r\beta_r,\ \text{onde}\ \alpha_i\in\mathbb{K},\ \text{e}\ \beta_i\in\mathbb{L},\ \text{para}\ i=1,\,2,\ldots,r.$$

Se $I_{\mathbb{K}}(\mathbb{Z})$, $I_{\mathbb{L}}(\mathbb{Z})$ e $I_{\mathbb{KL}}(\mathbb{Z})$ são os anéis dos inteiros algébricos de $\mathbb{K}$, $\mathbb{L}$ e $\mathbb{KL}$, respectivamente, então $I_{\mathbb{KL}}(\mathbb{Z})$ contém o anel

$$I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})=\{\alpha_1\beta_1+\ldots+\alpha_r\beta_r:\ \alpha_i\in I_{\mathbb{K}},\ \beta_i\in I_{\mathbb{L}},\ \text{para}\ i=1,\,2,\ldots,r\}.$$

Em geral, não temos uma igualdade. Entretanto, podemos mostrar que $I_{\mathbb{KL}}(\mathbb{Z})=I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$ sob certas condições sobre os corpos ciclotômicos. Sejam m e n os graus de $\mathbb{K}$ e $\mathbb{L}$, respectivamente, sobre $\mathbb{Q}$, e seja $d=mdc(d_1,\,d_2)$, onde d_1 e d_2 são os discriminantes de $I_{\mathbb{K}}(\mathbb{Z})$ e $I_{\mathbb{L}}(\mathbb{Z})$, respectivamente.

Teorema 1.9.5 *[9, Theorem 12, p.33] Se* $[\mathbb{KL}:\mathbb{Q}]=mn$, *então* $I_{\mathbb{KL}}(\mathbb{Z})\subset\frac{1}{d}I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$.
Demonstração: *Sejam* $\{\alpha_1,\ldots,\alpha_m\}$ *uma base de* $I_{\mathbb{K}}(\mathbb{Z})$ *sobre* $\mathbb{Z}$ *e* $\{\beta_1,\ldots,\beta_n\}$ *uma base de* $I_{\mathbb{L}}(\mathbb{Z})$ *sobre* $\mathbb{Z}$. *Assim, temos que* $B=\{\alpha_i\beta_j,\ i=1,\ldots,m;\ j=1,\ldots,n\}$ *é uma base de*

$I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$ *sobre* $\mathbb{Z}$ *e também uma base de* $\mathbb{KL}$ *sobre* $\mathbb{Q}$. *Se* $\alpha \in I_{\mathbb{KL}}(\mathbb{Z})$, *então pelo Teorema 1.9.3 temos que* α *pode ser escrito na forma*

$$\alpha = \sum_{i,\,j} \frac{m_{ij}}{r}\alpha_i\beta_j, \tag{1.6}$$

onde r *e todos os* m_{ij} *estão em* $\mathbb{Z}$, *e que estes* $mn+1$ *inteiros não tem fatores comuns maiores que* 1, *ou seja,* $mdc(r, mdc(m_{ij})) = 1$. *Para mostrarmos o teorema, temos que mostrar que* $r|d$ *para qualquer* α. *Para isto, devemos mostrar que* $r|d_1$ *e* $r|d_2$ *pois assim, pela definição de máximo divisor comum, teremos que* $r \mid d$. *Temos que todo monomorfismo* σ *de* $\mathbb{K}$ *em* $\mathbb{C}$ *extende a um monomorfismo (que também denotamos por* σ*) de* $\mathbb{KL}$ *em* $\mathbb{C}$, *fixando* $\mathbb{L}$. *Portanto, para cada* σ *temos que*

$$\sigma(\alpha) = \sum_{i,\,j} \frac{m_{ij}}{r}\sigma(\alpha_i)\beta_j.$$

Tomando $x_i = \displaystyle\sum_{j=1}^{n} \frac{m_{ij}}{r}\beta_j$, *para cada* $i = 1, \ldots, m$, *obtemos* m *equações* $\displaystyle\sum_{i=1}^{m} \sigma(\alpha_i)x_i = \sigma(\alpha)$ *para cada* σ, *e resolvendo este sistema pela regra de Cramer, obtemos que* $x_i = \dfrac{\gamma_i}{\delta}$, *onde* δ *é o determinante da matriz formado pelos coeficientes* $\sigma(\alpha_i)$ *e* γ_i *é obtido de* δ *trocando a* i*-ésima coluna por* $\sigma(\alpha)$, *para* $i = 1, 2, \ldots, m$. *Temos que* δ *e todos os* γ_i *são inteiros algébricos, pois todos os* $\sigma(\alpha_i)$ *e* $\sigma(\alpha)$ *são, e além disso* $\delta^2 = d_1$. *Se* $e = d_1$, *temos que* $ex_i = \delta\gamma_i \in I_{\mathbb{C}}(\mathbb{Z})$, *onde* $I_{\mathbb{C}}(\mathbb{Z})$ *é o anel dos inteiros algébricos de* $\mathbb{C}$, *e portanto* $ex_i = \displaystyle\sum_{j=1}^{n} \frac{em_{ij}}{r}\beta_j \in I_{\mathbb{C}}(\mathbb{Z}) \cap \mathbb{L} = I_{\mathbb{L}}(\mathbb{Z})$. *Como* $\{\beta_1, \ldots, \beta_n\}$ *forma uma base integral para* $I_{\mathbb{L}}(\mathbb{Z})$, *concluímos que os números racionais* $\dfrac{em_{ij}}{r}$ *devem ser inteiros, e deste modo* r *divide* em_{ij}, *para todo* i *e* j. *Como assumimos que* r *é relativamente primo com* $mdc(m_{ij})$, *segue que* $r|e = d_1$. *Da mesma forma mostramos que,* $r|d_2$. *Assim,* $r|d_1$ *e* $r|d_2$. *Portanto,* $r \mid d$ *e daí* $d = kr$, *com* $k \in \mathbb{Z}$, *ou seja,* $r = \dfrac{d}{k}$. *Substituindo na Equação (1.6) temos que*

$$\alpha = \sum_{i,\,j} \frac{km_{ij}}{d}\alpha_i\beta_j = \frac{1}{d}\sum_{i,j} km_{ij}\alpha_i\beta_j.$$

Logo $\alpha \in \dfrac{1}{d}I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$. *Portanto* $I_{\mathbb{KL}}(\mathbb{Z}) \subset \dfrac{1}{d}I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$. ∎

Corolário 1.9.4 *[9, Corollary 1, p.34] Se* $[\mathbb{KL} : \mathbb{Q}] = mn$ *e* $d = 1$, *então* $I_{\mathbb{KL}}(\mathbb{Z}) = I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$.
Demonstração: *Temos que* $I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z}) \subseteq I_{\mathbb{KL}}(\mathbb{Z})$, *e pelo Teorema 1.9.5, temos que* $I_{\mathbb{KL}}(\mathbb{Z}) \subseteq \frac{1}{d}I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$. *Como por hipótese* $d = 1$, *segue que* $I_{\mathbb{KL}}(\mathbb{Z}) \subseteq I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$. *Portanto,* $I_{\mathbb{KL}}(\mathbb{Z}) = I_{\mathbb{K}}(\mathbb{Z})I_{\mathbb{L}}(\mathbb{Z})$. ∎

Teorema 1.9.6 *[9, Corollary 2, p.34] O anel dos inteiros de* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *é* $\mathbb{Z}[\zeta_n]$ *e* $\{1, \zeta_n, \ldots, \zeta_n^{\frac{\varphi(n)}{2}-1}\}$ *é uma base de* $\mathbb{Z}[\zeta_n]$ *como um* $\mathbb{Z}$*-módulo.*

Demonstração: *O teorema já foi provado se n é primo ou se é uma potência de um primo. Agora, se n não é primo ou não é uma potência de um primo, então podemos escrever* $n = n_1 n_2$*, para inteiros relativamente primos* n_1*,* n_2 *maiores que 1. Vamos mostrar por indução que se o resultado também é válido para* n_1 *e* n_2*, então o resultado é válido para n. Para aplicar o Corolário 1.9.4, temos que mostrar que*

1. $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$ *e como consequência* $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}]$.
2. $\varphi(n) = \varphi(n_1)\varphi(n_2)$.
3. $d = 1$.

De fato:

1. *Do Corolário 1.9.3 temos que* $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$.
2. *Como* n_1 *e* n_2 *são relativamente primos segue que* $\varphi(n) = \varphi(n_1)\varphi(n_2)$.
3. *Pela Proposição 1.7.4 temos que* $D(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(m'_\alpha(\alpha))$*. Seja* d_{n_1} *e* d_{n_2} *os discriminantes de* $\mathbb{Z}[\zeta_{n_1}]$ *e* $\mathbb{Z}[\zeta_{n_2}]$*, respectivamente. Como* $m_\alpha(x) = x^{n_1} - 1$*, segue que* $m'_\alpha(x) = n_1 x^{n_1-1}$*, e substituindo x por* ζ_{n_1} *temos que* $m'_\alpha(\zeta_{n_1}) = n_1 \zeta_{n_1}^{n_1-1} = \frac{n_1}{\zeta_{n_1}}$*. Assim aplicando a função norma em ambos os lados e usando a sua linearidade temos que*

$$N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(m'_\alpha(\zeta_{n_1})) = \frac{N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(n_1)}{N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(\zeta_{n_1})} = \frac{n_1^{\varphi(n_1)}}{\pm 1}.$$

Portanto $d_{n_1} = \pm n_1^{\varphi(n_1)}$*, e isto implica que* $d_{n_1} | n_1^{\varphi(n_1)}$*. Analogamente,* $d_{n_2} | n_2^{\varphi(n_2)}$*. Sendo* $d = mdc(d_{n_1}, d_{n_2})$*, temos que*

$$\begin{cases} d | d_{n_1} \, e \, d_{n_1} | n_1^{\varphi(n_1)} \Longrightarrow d | n_1^{\varphi(n_1)} \\ d | d_{n_2} \, e \, d_{n_2} | n_2^{\varphi(n_2)} \Longrightarrow d | n_2^{\varphi(n_2)}. \end{cases}$$

Como $mdc(n_1^{\varphi(n_1)}, n_2^{\varphi(n_2)}) = 1$ *segue que* $d|1$*, e portanto* $d = 1$.

Assim, pelo Corolário 1.9.4 temos que $\mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}] = \mathbb{Z}[\zeta_n]$*. Portanto* $I_{\mathbb{K}}(\mathbb{Z}) = \mathbb{Z}[\zeta_n]$. ∎

Proposição 1.9.7 *[10, Proposition 2.16] O anel dos inteiros de* $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$*, para qualquer n, é* $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$*, e* $\{\zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}\}$ *é uma base de* $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ *como um* $\mathbb{Z}$*-módulo.*

Demonstração: *Temos que o anel dos inteiros de* $\mathbb{Q}(\zeta_n)$ *é* $\mathbb{Z}(\zeta_n)$*. Como* ζ_n *é inteiro temos*

que ζ_n^{-1} *é inteiro e pelo Corolário 1.3.2, temos que* $\zeta_n + \zeta_n^{-1}$ *também é inteiro. Portanto* $\mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subseteq I_{\mathbb{K}}(\mathbb{Z})$ *o anel dos inteiros de* $\mathbb{K}$*. Agora, mostremos que* $I_{\mathbb{K}}(\mathbb{Z}) \subseteq \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$*. Se* $\alpha \in I_{\mathbb{K}}(\mathbb{Z})$ *é um inteiro algébrico, então*

$$\alpha = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \ldots + a_{\frac{\varphi(n)}{2}}(\zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}),$$

onde $a_i \in \mathbb{Q}$*, para* $i = 1, 2, \ldots, \frac{\varphi(n)}{2}$*. Temos que mostrar que* $a_i \in \mathbb{Z}$*. Multiplicando* α *por* $\zeta_n^{\frac{\varphi(n)}{2}}$*, obtemos que*

$$\zeta_n^{\frac{\varphi(n)}{2}}\alpha = a_1\zeta_n^{\frac{p+1}{2}} + a_1\zeta_n^{\frac{p-3}{2}} + a_2\zeta_n^{\frac{p+3}{2}} + a_2\zeta_n^{\frac{p-5}{2}} + \ldots + a_{\frac{\varphi(n)}{2}}\zeta_n^{\varphi(n)} + a_{\frac{\varphi(n)}{2}},$$

que é um inteiro algébrico em $\mathbb{Q}(\zeta_n)$*, logo pertence a* $\mathbb{Z}(\zeta_n)$*. Assim segue que* $a_i \in \mathbb{Z}$*, para* $i = 1, 2, \ldots, \frac{\varphi(n)}{2}$*. Portanto* $I_{\mathbb{K}}(\mathbb{Z}) = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$*, ou seja, o anel dos inteiros de* $\mathbb{K}$ *é* $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$*. Como* $\{\zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}\}$ *é uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *e como* $\{\zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}\} \subseteq \mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subseteq I_{\mathbb{K}}(\mathbb{Z})$*, segue que é suficiente mostrar que é linearmente independente. Para isso, sejam* $a_1, a_2, \ldots, a_{\frac{\varphi(n)}{2}} \in \mathbb{Z}$ *e suponhamos que*

$$a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \ldots + a_{\frac{\varphi(n)}{2}}(\zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}) = 0.$$

Logo

$$a_1\zeta_n + a_1\zeta_n^{\varphi(n)} + a_2\zeta_n^2 + a_2\zeta_n^{p-2} + \ldots + a_{\frac{\varphi(n)}{2}}\zeta_n^{\frac{\varphi(n)}{2}} + a_{\frac{\varphi(n)}{2}}\zeta_n^{\frac{\varphi(n)}{2}} = 0.$$

Como $\{1, \zeta_n, \ldots, \zeta_n^{p-2}\}$ *é uma base de* $\mathbb{Z}[\zeta_n]$ *sobre* $\mathbb{Z}$*, temos que estes elementos são linearmente independentes, e daí segue que* $a_1 = a_2 = \ldots = a_{\frac{\varphi(n)}{2}} = 0$*. Assim, segue que* $\{\zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}\}$ *é linearmente independente, e portanto é uma base de* $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ *sobre* $\mathbb{Z}$*.* ∎

Capítulo 2

Discriminante via teoria algébrica dos números

2.1 Introdução

Neste capítulo veremos como calcular o discriminante de uma extensão de anéis utilizando a teoria algébrica dos números. Deste modo, na Seção 2.2 veremos que o discriminante de uma extensão de anéis é um ideal. Na Seção 2.3 veremos o cálculo do discriminante de polinômios. Na Seção 2.4 veremos o cálculo do discriminante dos corpos quadráticos. Na Seção 2.5 veremos o cálculo do discriminante dos corpos ciclotômicos. Neste capítulo foram utilizadas as referências [2], [3], [5], [6], [8], [9] e [10].

2.2 Discriminante

Nesta seção apresentamos o conceito de discriminante de uma extensão de anéis. Para isso, sejam A e R anéis tais que $A \subseteq R$ e R é um A-módulo livre de posto finito n. A Proposição 1.7.1 mostra que o discriminante de bases de R sobre A são associados em A, isto é, a matriz (a_{ij}) que expressa uma base em termos da outra tem uma inversa com entradas em A. Assim $det(a_{ij})$ e $det((a_{ij})^{-1})$ são inversíveis em A. Podemos então formular a seguinte definição:

Definição 2.2.1 *Sejam $A \subseteq R$ anéis tal que R é um A-módulo livre de posto finito n. Definimos o discriminante de R sobre A como o ideal de A, gerado por $D_{R/A}(\alpha_1, \ldots, \alpha_n)$, onde $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de R sobre A, e denotamos $\mathcal{D}(R/A)$.*

Proposição 2.2.1 *[3, Proposition 2, p.39] Sejam $A \subseteq R$ anéis tal que R é um A-módulo livre de posto finito n. Se $\mathcal{D}(R/A)$ possui um elemento que não é um divisor de zero, então o conjunto $\{\alpha_1, \ldots, \alpha_n\}$ de elementos de R é uma base de R sobre A se, e somente se, $D_{R/A}(\alpha_1, \ldots, \alpha_n)$ gera $\mathcal{D}(R/A)$.*

Demonstração: *Se o conjunto $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de R sobre A, por definição temos que $D_{R/A}(\alpha_1, \ldots, \alpha_n)$ gera $\mathcal{D}(R/A)$. Reciprocamente, suponhamos que $D_{R/A}(\alpha_1, \ldots, \alpha_n)$ gera $\mathcal{D}(R/A)$. Se $\{\beta_1, \ldots, \beta_n\}$ é uma outra base de R sobre A, então $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$, com $a_{ij} \in A$ para $1 \leq i, j \leq n$. Pela Proposição 1.7.1 segue que $D_{R/A}(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2 D_{R/A}(\beta_1, \ldots, \beta_n)$. Mas por hipótese temos que,*

$$AD_{R/A}(\alpha_1, \ldots, \alpha_n) = \mathcal{D}(R/A) = AD_{R/A}(\beta_1, \ldots, \beta_n).$$

Assim, existe $a \in A$ tal que $D_{R/A}(\beta_1, \ldots, \beta_n) = aD_{R/A}(\alpha_1, \ldots, \alpha_n)$, e deste modo

$$D_{R/A}(\alpha_1, \ldots, \alpha_n)(1 - a\det(a_{ij})^2) = 0.$$

Temos que $D_{R/A}(\alpha_1, \ldots, \alpha_n)$ não é um divisor de zero, pois caso contrário, como $D_{R/A}(\alpha_1, \ldots, \alpha_n)$ gera $\mathcal{D}(R/A)$ teríamos que todo elemento de $\mathcal{D}(R/A)$ seria um divisor de zero, o que não ocorre. Assim, $1 - a\det(a_{ij})^2 = 0$ e daí, $a\det(a_{ij})\det(a_{ij}) = 1$. Logo $\det(a_{ij})$ é inversível e portanto a matriz (a_{ij}) é inversível. Consequentemente $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de R sobre A. ∎

Proposição 2.2.2 *[2, p.198] Sejam $R_1, \ldots, R_r$ anéis comutativos contendo um domínio A. Se cada anel R_i, para $i = 1, 2, \ldots, r$, é um A-módulo livre de posto finito, então*

$$\mathcal{D}(R_1 \times \ldots \times R_r/A) = \prod_{i=1}^{n} \mathcal{D}(R_i/A).$$

Demonstração: *Por indução, é suficiente provarmos a afirmação para $n = 2$. Assim, se $\{\alpha_1, \ldots, \alpha_r\}$ é uma base de R_1 sobre A e se $\{\beta_1, \ldots, \beta_s\}$ é uma base de R_2 sobre A, então $\{(\alpha_1, 0), \ldots, (\alpha_r, 0), (0, \beta_1), \ldots, (0, \beta_s)\}$ é uma base de $R_1 \times R_2$ sobre A. Tomando $\gamma_i = (\alpha_i, 0)$ para $i = 1, \ldots, r$ e $\gamma_{r+i} = (0, \beta i)$ para $i = 1, \ldots, s$, temos que $\mathcal{D}(R_1 \times R_2/A)$ é o ideal principal de A gerado por $det(Tr_{R_1\times R_2/A}(\gamma_i\gamma_j)) = D_{R_1\times R_2/A}(\gamma_1, \ldots, \gamma_{r+s})$. Agora, se $\theta \in R_1$, então $Tr_{R_1\times R_2/A}(\theta, 0) = Tr_{R_1/A}(\theta)$, que podem ser deduzidos considerando as matrizes do endomorfismo $\varphi_{(\theta,0)}$ de $R_1 \times R_2$ e φ_θ de R_1, relativos as bases $\{\beta_1, \ldots, \beta_{r+s}\}$ e $\{\alpha_1, \ldots, \alpha_r\}$, respectivamente. Analogamente, temos que $Tr_{R_1\times R_2/A}(0, \theta) = Tr_{R_2/A}(\theta)$. Assim*

$$\begin{aligned} det(Tr_{R_1\times R_2/A}(\gamma_i\gamma_j)) &= \det \begin{pmatrix} Tr_{R_1/A}(\alpha_i\alpha_j) & 0 \\ 0 & Tr_{R_2/A}(\beta_i\beta_j) \end{pmatrix} \\ &= \det(Tr_{R_1/A}(\alpha_i\alpha_j))\det(Tr_{R_2/A}(\beta_i\beta_j)), \end{aligned}$$

e este elemento gera o ideal $\mathcal{D}(R_1/A)\mathcal{D}(R_2/A)$. ∎

Definição 2.2.2 *Sejam* $A \subseteq R$ *anéis. Dizemos que o traço em* R *é degenerado se existe um elemento* $\alpha \in R$, $\alpha \neq 0$, *tal que* $Tr_{R/A}(\alpha\beta) = 0$ *para todo* $\beta \in R$.

Definição 2.2.3 *Seja* V *um espaço vetorial sobre um corpo* $\mathbb{K}$. *Dizemos que* V *é uma* $\mathbb{K}$*-álgebra se existe uma multiplicação de* $V \times V$ *em* V *dada por* $(a, b) \longmapsto ab$ *satisfazendo para todo* $a, b, c \in V$ *e* $\alpha \in \mathbb{K}$*:*

1. $a(b + c) = ab + ac$.
2. $a(\alpha b) = (a\alpha)b = \alpha(ab)$
3. $a(bc) = (ab)c$
4. *Existe* $1_V \in V$ *tal que* $a1_V = a = 1_V a$.

Se além disso $ab = ba$, *dizemos que* V *é uma* $\mathbb{K}$*-álgebra comutativa.*

Proposição 2.2.3 *[2, p.198] Sejam* $\mathbb{K}$ *um corpo e* R *uma álgebra comutativa de dimensão* n *sobre* $\mathbb{K}$. *Então* $\mathcal{D}(R/\mathbb{K}) = 0$, *se e somente se, o traço em* R *sobre* $\mathbb{K}$ *é degenerado.*
Demonstração: *Suponhamos que* $\mathcal{D}(R/\mathbb{K}) = 0$ *e tomemos uma base* $\{\alpha_1, \ldots, \alpha_n\}$ *de* R *sobre* $\mathbb{K}$. *Assim, temos que* $D_{R/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(Tr_{R/\mathbb{K}}(\alpha_i\alpha_j)) = 0$. *Logo o conjunto* $(Tr_{R/\mathbb{K}}(\alpha_i\alpha_j))$ *é linearmente dependente, ou seja, existem elementos* $a_1, \ldots, a_n$ *de* $\mathbb{K}$ *não todos nulos tal que*

$$\sum_{i=1}^{n} a_i Tr_{R/\mathbb{K}}(\alpha_i\alpha_j) = 0, \text{ para todo } j = 1, \ldots, n.$$

Tomando $\alpha = \sum_{i=1}^{n} a_i\alpha_i$ *temos que* $\alpha \neq 0$ *e para todo* $\beta = \sum_{j=1}^{n} b_j\alpha_j$, *com* $b_j \in \mathbb{K}$ *temos que*

$$Tr_{R/\mathbb{K}}(\alpha\beta) = \sum_{i,j=1}^{n} a_i b_j Tr_{R/\mathbb{K}}(\alpha_i\alpha_j) = 0.$$

Portanto, o traço em R *é degenerado. Reciprocamente, suponhamos que o traço em* R *seja degenerado. Tomemos* $\alpha \in R$, $\alpha \neq 0$, *tal que* $Tr_{R/\mathbb{K}}(\alpha\beta) = 0$ *para todo* $\beta \in R$ *e consideremos uma base* $\{\alpha_1, \ldots, \alpha_n\}$ *de* R *sobre* $\mathbb{K}$ *tal que* $\alpha_1 = \alpha$. *Assim,* $\mathcal{D}(R/\mathbb{K})$ *é o ideal de* $\mathbb{K}$ *gerado por* $D_{R/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(Tr_{R/\mathbb{K}}(\alpha_i\alpha_j)) = 0$. *Portanto* $\mathcal{D}(R/\mathbb{K}) = 0$. ∎

Definição 2.2.4 *Seja* $\mathbb{K}$ *um corpo.*

1. *Um polinômio mônico $f(x) \in \mathbb{K}[x]$ é chamado separável se $f(x)$ e sua derivada $f'(x)$ são primos entre si.*

2. *Um elemento $\alpha \in \mathbb{C}$ algébrico sobre $\mathbb{K}$ é chamado separável se é raiz de um polinômio separável $f(x) \in \mathbb{K}[x]$.*

3. *Uma extensão $\mathbb{L}$ de $\mathbb{K}$ é chamada separável se todo $\alpha \in \mathbb{L}$ for separável sobre $\mathbb{K}$.*

Definição 2.2.5 *Um corpo $\mathbb{K}$ é chamado perfeito se toda extensão $\mathbb{L}$ de $\mathbb{K}$ é separável.*

Proposição 2.2.4 *[2, p.199] Sejam $\mathbb{K}$ um corpo perfeito e R uma $\mathbb{K}$-álgebra comutativa de dimensão finita. Então $\mathcal{D}(R/\mathbb{K}) \neq 0$ se, e somente se, 0 é o único elemento nilpotente de R.*
Demonstração: *Suponhamos, por absurdo, que R contém um elemento $\alpha \neq 0$ nilpotente. Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de R sobre $\mathbb{K}$, tal que $\alpha_1 = \alpha$. Como R é comutativa, segue que $\alpha\alpha_j$ também é nilpotente, para todo $j = 1, \ldots, n$. O polinômio minimal do endomorfismo $\varphi_{\alpha\alpha_j}$ é x^r, para algum $r > 0$. Pela Proposição 1.5.1 temos que o polinômio característico é um múltiplo do polinômio minimal, tendo o mesmo fator irredutível e grau n. Logo o polinômio característico de $\varphi_{\alpha\alpha_j}$ é x^n, e daí $Tr_{R/\mathbb{K}}(\alpha\alpha_j) = 0$ para todo $j = 1, \ldots, n$. Portanto $D_{R/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(Tr_{R/\mathbb{K}}(\alpha\alpha_j) = 0$, pois a matriz do traço tem a primeira linha nula. Assim $\mathcal{D}(R/\mathbb{K}) = 0$, o que é um absurdo por hipótese. Portanto, 0 é o único elemento nilpotente de R. Reciprocamente, suponhamos que 0 é o único elemento nilpotente de R. Como todo ideal de R é um subespaço vetorial de R, e como R tem dimensão n sobre $\mathbb{K}$, segue que toda cadeia de subespaços, também de ideais, de R deve ser finita. Assim R é um anel Noetheriano. Pelo Corolário 1.2.1 podemos escrever $0 = \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_r$, onde cada $\mathcal{P}_i$ é um ideal primo de R. Como $\mathcal{P}_i \cap \mathbb{K}$ é um ideal de $\mathbb{K}$, segue que $\mathcal{P}_i \cap \mathbb{K} = 0$, para $i = 1, \ldots, r$. Assim $\mathbb{K} \subseteq R/\mathcal{P}_i$ (a menos de isomorfismo) e $R/\mathcal{P}_i$ é um $\mathbb{K}$-espaço de dimensão finita que é também um domínio. Pelo Teorema 1.3.1, temos que todo elemento de $R/\mathcal{P}_i$ é inteiro sobre $\mathbb{K}$ e pela Proposição 1.3.3 segue que $R/\mathcal{P}_i$ é um corpo, logo $\mathcal{P}_i$ é um ideal maximal de R. Agora, como os ideais são maximais, segue que $\mathcal{P}_i + \bigcap_{j \neq i} \mathcal{P}_j = R$, pois caso contrário, teríamos $\bigcap_{j \neq i} \mathcal{P}_j \subseteq \mathcal{P}_i$ e assim $\mathcal{P}_j \subseteq \mathcal{P}_i$ para algum $j \neq i$. Logo $\mathcal{P}_j = \mathcal{P}_i$ pelo fato dos ideais serem distintos, o que não acorre. Assim $R = R/0 \cong \prod_{i=1}^{r} R/\mathcal{P}_i = \prod_{i=1}^{r} \mathbb{L}_i$, onde $\mathbb{L}_i$, para $i = 1, \ldots, r$, é uma extensão de $\mathbb{K}$. Pela Proposição 2.2.2 segue que $\mathcal{D}(R/\mathbb{K}) = \prod_{i=1}^{r} \mathcal{D}(\mathbb{L}_i/\mathbb{K})$. Como o corpo $\mathbb{L}_i$ é uma extensão finita, segue pelo Corolário 1.4.1, que $\mathbb{L}_i$ é uma extensão algébrica de $\mathbb{K}$, para todo $i = 1, \ldots, r$. Por hipótese, temos que $\mathbb{K}$ é um corpo perfeito, logo*

$\mathbb{L}_i$ *é separável sobre* $\mathbb{K}$*, para todo* $i = 1, \ldots, r$*. Assim, existe um elemento* $\alpha_i \in \mathbb{L}$ *tal que* $Tr_{\mathbb{L}_i/\mathbb{K}}(\alpha_i) \neq 0$*. Logo, o traço não é degenerado, pois se existir* $\alpha' \neq 0$ *tal que* $Tr_{\mathbb{L}_i/\mathbb{K}}(\alpha'\beta) = 0$ *para todo* $\beta \in \mathbb{L}$*, temos para* $\alpha_i = \alpha'(\alpha'^{-1}\alpha_i)$ *que* $Tr_{\mathbb{L}_i/\mathbb{K}}(\alpha_i) = 0$*, o que não ocorre. Pela Proposição 2.2.3, segue que* $\mathcal{D}(\mathbb{L}_i/\mathbb{K}) \neq 0$*. Assim,* $\mathcal{D}(\mathbb{L}_i/\mathbb{K}) = \mathbb{K}$ *e daí* $\mathcal{D}(R/\mathbb{K}) = \mathbb{K} \neq 0$*.* ∎

Proposição 2.2.5 *Sejam* A *um anel de Dedekind,* $\mathbb{K}$ *seu corpo de frações e* $\mathbb{L}$ *uma extensão separável finita de* $\mathbb{K}$*. Se* $M_1 \subseteq M_2$ *são dois módulos livres de posto finito* n *sobre* A*, contidos em* $\mathbb{L}$*, então* $\mathcal{D}(M_1/A)$ *divide* $\mathcal{D}(M_2/A)$ *(como ideais principais). Em particular, se* $\mathcal{D}(M_1/A) = \mathcal{D}(M_2/A).u$ *para alguma unidade de* A*, então* $M_1 = M_2$*.*

Demonstração: *Sejam* $\{\alpha_1, \ldots, \alpha_n\}$ *uma base de* M_1 *sobre* A*, e* $\{\beta_1, \ldots, \beta_n\}$ *uma base de* M_2 *sobre* A*. Como* $M_1 \subseteq M_2$*, segue que* $\beta_i = \sum_{i=1}^{n} a_{i,j}\alpha_j$*. Pela Proposição 1.7.1 temos que* $D_{\mathbb{L}/\mathbb{K}}(\beta_1, \ldots, \beta_n) = (det(a_{i,j})^2) D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n)$*. Portanto* $\mathcal{D}(M_1/A)$ *divide* $\mathcal{D}(M_2/A)$*.* ∎

2.3 Discriminante de polinômios

Nesta seção apresentamos o conceito de discriminante de polinômios.

Definição 2.3.1 *Sejam* $\mathbb{K}$ *um corpo e* $f(x) \in \mathbb{K}[x]$ *um polinômio mônico de grau* n *com raízes* $\alpha_1, \ldots, \alpha_n$*. O discriminante de* $f(x)$ *é definido por*

$$D(f) = \prod_{i<j}(\alpha_j - \alpha_i)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_j - \alpha_i) = \prod_{i=1}^{n} \prod_{j=i+1}^{n} (\alpha_j - \alpha_i)^2.$$

Exemplo 2.3.1 *Seja* $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$*. As raízes de* $f(x)$ *são*

$$\alpha_1 = \frac{-a + \sqrt{a^2 - 4b}}{2} \text{ e } \alpha_2 = \frac{-a - \sqrt{a^2 - 4b}}{2}.$$

Assim $D(x^2 + ax + b) = (\alpha_2 - \alpha_1)^2 = a^2 - 4b$*.*

Exemplo 2.3.2 *Seja* $f(x) = x^3 + a_0x^2 + b_0x + c_0 \in \mathbb{K}[x]$*, onde* $\mathbb{K}$ *é um corpo de característica diferente de* 2 *ou* 3*. Vamos reduzir este polinômio a* $f_1(x) = x^3 + bx + c$*. Temos que*

$$(x+l)^3 + a_0(x+l)^2 + b_0(x+l) + c_0 = x^3 + 3x^2l + 3xl^2 + l^3 + a_0x^2 + 2a_0xl + a_0l^2 + b_0x + b_0l + c_0.$$

Fazendo $l = \frac{-a_0}{3}$ *e substituindo apenas no primeiro termo contendo* x^2 *ficamos com* $x^3 - a_0x^2 + l^3 + a_0x^2 + 2a_0xl + a_0l^2 + b_0x + b_0l + c_0 = x^3 + (3l^2 + 2a_0l + b_0)x + (l^3 + a_0l^2 + b_0l + c_0) = x^3 + bx + c$*.*

Sejam α_1, α_2 *e* α_3 *as raízes distintas de* $f(x)$ *e* $\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \prod_{i<j}(\alpha_i - \alpha_j)$.

Por definição temos que $D(f) = \Delta^2$, *e*

$$\Delta = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix} = \prod_{i<j}(\alpha_i - \alpha_j).$$

Assim,

$$D(f) = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix} \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{vmatrix} = \begin{vmatrix} 3 & \alpha_1+\alpha_2+\alpha_3 & \alpha_1^2+\alpha_2^2+\alpha_3^2 \\ \alpha_1+\alpha_2+\alpha_3 & \alpha_1^2+\alpha_2^2+\alpha_3^2 & \alpha_1^3+\alpha_2^3+\alpha_3^3 \\ \alpha_1^2+\alpha_2^2+\alpha_3^2 & \alpha_1^3+\alpha_2^3+\alpha_3^3 & \alpha_1^4+\alpha_2^4+\alpha_3^4 \end{vmatrix}.$$

Por outro lado, temos que $x^3 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, *e dividindo ambos os lados por* x^3 *ficamos com*

$$1 + b\frac{1}{x^2} + c\frac{1}{x^3} = (1 - \alpha_1\frac{1}{x})(1 - \alpha_2\frac{1}{x})(1 - \alpha_3\frac{1}{x}).$$

Logo

$$1 + b(\frac{1}{x})^2 + c(\frac{1}{x})^3 = (1 - \alpha_1\frac{1}{x})(1 - \alpha_2\frac{1}{x})(1 - \alpha_3\frac{1}{x}).$$

Substituindo $\frac{1}{x}$ *por* y *obtemos que* $1 + by^2 + cy^3 = (1 - \alpha_1 y)(1 - \alpha_2 y)(1 - \alpha_3 y)$, *e usando que* $\frac{d}{dx}(log(f(x))) = \frac{f'(x)}{f(x)}$ *obtemos que*

$$\frac{2by + 3cy^2}{1 + by^2 + cy^3} = -(\frac{\alpha_1}{1 - \alpha_1 y} + \frac{\alpha_2}{1 - \alpha_2 y} + \frac{\alpha_3}{1 - \alpha_3 y}),$$

ou seja,

$$2by + 3cy^2\frac{1}{1 + (by^2 + cy^3)} = -(\alpha_1\frac{1}{1 - \alpha_1 y} + \alpha_2\frac{1}{1 - \alpha_2 y} + \alpha_3\frac{1}{1 - \alpha_3 y}).$$

Agora, usando o fato que $\frac{1}{1+v} = 1 - v + v^2 - v^3 + \cdots$ *e* $\frac{1}{1-v} = 1 + v + v^2 + v^3 + \cdots$, *temos que o lado esquerdo desta última equação fica como*

$$(2by + 3cy^2)(1 - (by^2 + cy^3) + (by^2 + cy^3)^2 - \ldots) = 2by + 3cy^2 - 2b^2y^3 - \ldots$$

e o lado direito fica como

$-(\alpha_1(1 + \alpha_1 y + (\alpha_1 y)^2 + \ldots) + \alpha^2(1 + \alpha_2 y + (\alpha_2 y)^2 + \ldots) + \alpha_3(1 + \alpha_3 y + (\alpha_3 y)^2 + \ldots) + \ldots)$
$= -(\alpha_1 + \alpha_2 + \alpha_3 + (\alpha_1^2 + \alpha_2^2 + \alpha_3^2)y + (\alpha_1^3 + \alpha_2^3 + \alpha_3^3)y^2 + (\alpha_1^4 + \alpha_2^4 + \alpha_3^4)y^3 + \ldots).$

Da igualdade segue que

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = -2b \\ \alpha_1^3 + \alpha_2^3 + \alpha_3^3 = -3c \\ \alpha_1^4 + \alpha_2^4 + \alpha_3^4 = 2b^2, \end{cases}$$

e substituindo na matriz do discriminante temos que

$$D(f) = \begin{vmatrix} 3 & 0 & -2b \\ 0 & -2b & -3c \\ -2b & -3c & -2b^2 \end{vmatrix} = -4b^3 - 27c^2.$$

Exemplo 2.3.3 *Sejam $f(x) = x^n + bx + c \in \mathbb{K}[x]$ e α uma raiz de $f(x)$. Logo $f'(\alpha) = n\alpha^{n-1} + b$. Mas temos que $f(\alpha) = \alpha^n + b\alpha + c = 0$ implica que $\alpha^n = -b\alpha - c$ e daí $n\alpha^{n-1} = -nb - nc\alpha^{-1}$. Assim podemos escrever $f'(\alpha) = n\alpha^{n-1} + b = (-nb - nc\alpha^{-1}) + b = -(n-1)b - nc\alpha^{-1}$. Logo, obtemos que $\alpha^{-1} = (-nc)^{-1}(f'(\alpha) + (n-1)b)$ e $\alpha = -nc(f'(\alpha) + (n-1)b)^{-1}$. O polinômio minimal de $f'(\alpha)$ sobre $\mathbb{K}$ é o numerador de $c^{-1}f(-nc(f'(\alpha)+(n-1)b)^{-1})$, e calculando obtemos que*

$$(f'(\alpha) + (n-1)b)^n - nb(f'(\alpha) + (n-1)b)^{n-1} + (-1)^n c^{n-1} n^n.$$

A norma de $f'(\alpha)$ é $(-1)^n$ vezes o termo constante deste polinômio, isto é,

$$n^n c^{n-1} + (-1)^{n-1}(n-1)^{n-1} b^n.$$

Assim pela Proposição 1.7.4 temos que

$$D_{\mathbb{K}/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)}(n^n c^{n-1} + (-1)^{n-1}(n-1)^{n-1} b^n).$$

Observação 2.3.1 *No Exemplo 2.3.3, para $n = 2$ obtemos $D(f) = b^2 - 4c$, como no Exemplo 2.3.1, e para $n = 3$, obtemos que $D(f) = -27c^2 - 4b^3$ como no Exemplo 2.3.2.*

2.4 Discriminante de corpos quadráticos

Nesta seção apresentamos o cálculo do discriminante de corpos quadráticos, ou seja, dos corpos da forma $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.

Proposição 2.4.1 *[6, Theorem 3.3] Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados e $I_{\mathbb{K}}(\mathbb{Z})$ é o anel dos inteiros de $\mathbb{K}$. Se $d \not\equiv 1 (modulo\ 4)$, então o discriminante de $I_{\mathbb{K}}(\mathbb{Z})$ é dado*

por $4d$.

Demonstração: *Pelo Teorema 1.8.1, temos que se* $d \not\equiv 1(\text{modulo } 4)$, *então* $\{1, \sqrt{d}\}$ *é uma base do anel dos inteiros de* $\mathbb{K}$. *Assim, por definição, temos que*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{d}) = \begin{vmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(\sqrt{d})^2 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d.$$

■

Proposição 2.4.2 *[6, Theorem 3.3] Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, *onde* $d \in \mathbb{Z}$ *é livre de quadrados e* $I_{\mathbb{K}}(\mathbb{Z})$ *é o anel dos inteiros de* $\mathbb{K}$. *Se* $d \equiv 1(\text{modulo } 4)$, *então o discriminante de* $I_{\mathbb{K}}(\mathbb{Z})$ *é dado por* d.

Demonstração: *Pelo Teorema 1.8.2, temos que se* $d \equiv 1(\text{modulo } 4)$, *então* $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ *é uma base do anel dos inteiros de* $\mathbb{K}$. *Assim,*

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

■

Exemplo 2.4.1 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *um corpo de números. Como* $5 \equiv 1(\text{modulo } 4)$, *segue pelo Teorema 1.8.2, que* $\left\{1, \frac{1}{2} + \frac{\sqrt{5}}{2}\right\}$ *é uma base de* $\mathbb{K}$. *Assim, pela Proposição 2.4.2, temos que*

$$D_{\mathbb{K}/\mathbb{Q}}\left(1, \frac{1+\sqrt{5}}{2}\right) = \begin{vmatrix} Tr(1) & Tr\left(\frac{1+\sqrt{5}}{2}\right) \\ Tr\left(\frac{1+\sqrt{5}}{2}\right) & Tr\left(\frac{1+\sqrt{5}}{2}\right)^2 \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \frac{1+5}{2} \end{vmatrix} = 1 + 5 - 1 = 5.$$

2.5 Discriminante de corpos ciclotômicos

Nesta seção apresentamos o cálculo do discriminante de corpos ciclotômicos, ou seja, corpos da forma $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima da unidade.

Proposição 2.5.1 *[6, Theorem 3.6] Se* $\mathbb{K} = \mathbb{Q}(\zeta_p)$, *onde* p *é um número primo ímpar, então o discriminante de* $\mathbb{Q}(\zeta_p)$ *sobre* $\mathbb{Q}$ *é dado por*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Demonstração: *Pelo Teorema* 1.9.2*, temos que* $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ *é uma base integral. Pela Proposição 1.7.4, temos que*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{\mathbb{K}/\mathbb{Q}}(\phi_p^{'}(\zeta_p)),$$

onde $\phi_p^{'}(x)$ *é a derivada do p-ésimo polinômio ciclotômico* $\phi_p(x)$ *que é dado por*

$$\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1}.$$

Derivando-o de ambos os lados obtemos que

$$\phi_p^{'}(\zeta_p) = \frac{(\zeta_p - 1)p\zeta_p^{p-1} - (\zeta_p^p - 1)}{(\zeta_p - 1)^2} = \frac{-p\zeta_p^{p-1}}{1 - \zeta_p}.$$

Assim, aplicando a norma, usando sua linearidade e o Lema 1.9.2 temos que

$$N_{\mathbb{K}/\mathbb{Q}}(\phi_p^{'}(\zeta_p)) = \frac{N_{\mathbb{K}/\mathbb{Q}}(-p)N_{\mathbb{K}/\mathbb{Q}}(\zeta_p)^{p-1}}{N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p)} = \frac{(-p)^{p-1}1^{p-1}}{p} = p^{p-2}.$$

Além disso, como p é ímpar, segue que $(-1)^{p-2} = -1$*, e assim* $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{(p-1)}{2}}$*. Portanto,*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

■

Proposição 2.5.2 *[10, Proposition 2.1] Se* $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$*, onde* $r > 1 \in \mathbb{Z}$ *e p é um número primo ímpar, então o discriminante de* $\mathbb{Q}(\zeta_{p^r})$ *sobre* $\mathbb{Q}$ *é dado por*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = \pm p^{p^{r-1}(r(p-1)-1)}.$$

Demonstração: *Pelo Teorema 1.9.4 temos que* $\{1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ *é uma base integral. Pela Proposição 1.7.4, temos que*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = \pm N_{\mathbb{K}/\mathbb{Q}}(\phi_{p^r}^{'}(\zeta_{p^r})),$$

onde $\phi_{p^r}^{'}(x)$ *é a derivada do* p^r*-ésimo polinômio ciclotômico que é dado por*

$$\phi_{p^r}(x) = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \ldots + x^{p^{r-1}} + 1 = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}.$$

Derivando ambos os lados obtemos que

$$\phi_{p^r}^{'}(x) = \frac{p^r x^{p^r-1}(x^{p^{r-1}} - 1) - (x^{p^r} - 1)p^{r-1}x^{p^{r-1}-1}}{(x^{p^{r-1}} - 1)^2},$$

ou seja,

$$\phi'_{p^r}(\zeta_{p^r}) = \frac{p^r\zeta_{p^r}^{p^r-1}(\zeta_{p^r}^{p^{r-1}}-1) - (\zeta_{p^r}^{p^r}-1)p^{r-1}\zeta_{p^r}^{p^{r-1}-1}}{(\zeta_{p^r}^{p^{r-1}}-1)^2}.$$

Mas como $\zeta_{p^r}^{p^r} = 1$ *segue que* $\zeta_{p^r}^{p^{r-1}} = (e^{\frac{2\pi i}{p^r}})^{p^{r-1}} = e^{\frac{2\pi i}{p}} = \zeta_p$. *Assim,*

$$\phi'_{p^r}(\zeta_{p^r}) = \frac{p^r\zeta_{p^r}^{-1}}{\zeta_{p^r}^{p^{r-1}}-1} = \frac{-p^r}{(1-\zeta_{p^r}^{p^{r-1}})\zeta_{p^r}}.$$

Agora, aplicando a função norma em ambos os membros e usando sua linearidade temos que

$$N_{\mathbb{K}/\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r})) = \frac{N_{\mathbb{K}/\mathbb{Q}}(-p^r)}{N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p)N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r})}.$$

Mas, pela Proposição 1.9.5, temos que
$N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}) = \pm 1$,
$N_{\mathbb{K}/\mathbb{Q}}(-p^r) = (-p^r)^{(p-1)p^{r-1}}$, *e*
$N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p) = N_{\mathbb{K}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{Q}(\zeta_p)}(1-\zeta_p)) = N_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p)^{p^{r-1}} = p^{p^{r-1}}$.
Assim, $N_{\mathbb{K}/\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r})) = \dfrac{\pm p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}} = \pm p^{p^{r-1}(r(p-1)-1)}$. *Portanto*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = \pm p^{p^{r-1}(r(p-1)-1)}.$$

■

Proposição 2.5.3 *[9, Exercise 23, p.43] Sejam* $\mathbb{K}, \mathbb{L}$ *e* $\mathbb{M}$ *corpos de números tais que* $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$. *Se* $[\mathbb{L}:\mathbb{K}] = n$ *e* $[\mathbb{M}:\mathbb{L}] = m$, *então* $D(\mathbb{M}/\mathbb{K}) = D(\mathbb{L}/\mathbb{K})^m N_{\mathbb{L}/\mathbb{K}}(D(\mathbb{M}/\mathbb{L}))$.

Demonstração: *Sejam* $\{\alpha_1, \ldots, \alpha_n\}$ *e* $\{\beta_1, \ldots, \beta_m\}$ *bases de* $\mathbb{L}$ *sobre* $\mathbb{K}$ *e* $\mathbb{M}$ *sobre* $\mathbb{L}$, *respectivamente. Sejam* $\sigma_1, \ldots, \sigma_n$ *os* $\mathbb{K}$*-homomorfismos de* $\mathbb{L}$ *em* $\mathbb{C}$ *e* $\tau_1, \ldots, \tau_m$ *os* $\mathbb{L}$*-homomorfismos de* $\mathbb{M}$ *em* $\mathbb{C}$. *Fixemos uma extensão normal* $\mathbb{N}$ *de* $\mathbb{Q}$ *tal que* $\mathbb{M} \subseteq \mathbb{N}$. *Deste modo, todos os* $\sigma_i's$ *e* $\tau_j's$ *podem ser extendidos aos automorfismos de* $\mathbb{N}$. *Assim fixamos uma extensão de cada e novamente denotamos estas extensões por* σ_i *e* τ_j. *Sejam* A *e* B *matrizes* $(mn)\times(mn)$ *tais que*

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & A_n \end{pmatrix}_{mn\times mn}, \text{ onde } A_i = \begin{pmatrix} \sigma_i\tau_1(\beta_1) & \sigma_i\tau_1(\beta_2) & \cdots & \sigma_i\tau_1(\beta_m) \\ \sigma_i\tau_2(\beta_1) & \sigma_i\tau_2(\beta_2) & \cdots & \sigma_i\tau_2(\beta_m) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_i\tau_m(\beta_1) & \sigma_i\tau_m(\beta_2) & \cdots & \sigma_i\tau_m(\beta_m) \end{pmatrix}_{m\times m},$$

ou seja A *tem* $\sigma_i\tau_h(\beta_k)$ *na linha* $m(i-1)+h$ *e na coluna* $m(i-1)+k$, *onde* $1 \leq i \leq n$, $1 \leq h \leq m$, $1 \leq k \leq m$, $1 \leq j \leq n$ *e zeros em todo o resto. Desta forma,* A *consiste de* n *blocos* $m \times m$ *arranjados diagonalmente do topo esquerdo ao inferior direito. Temos, ainda, que*

$$B = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1n} \\ B_{21} & B_{22} & \cdots & B_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ B_{n1} & B_{n2} & \cdots & B_{nn} \end{pmatrix}_{mn\times mn}, \text{ onde } B_{ij} = \begin{pmatrix} \sigma_i(\alpha_j) & 0 & \cdots & 0 \\ 0 & \sigma_i(\alpha_j) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_i(\alpha_j) \end{pmatrix}_{m\times m},$$

ou seja, B tem $\sigma_i(\alpha_j)$ na linha $m(i-1)+t$ e na coluna $m(j-1)+t$, para cada $1 \leq t \leq m$, onde $1 \leq i \leq n$, $1 \leq j \leq m$ e zero em todo o resto. Desta forma, B é obtido por um múltiplo correspondente da matriz identidade $m \times m$. Assim, temos que

$$\det A = \prod_{i=1}^{n} \det A_i = \prod_{i=1}^{n} \det(\sigma_i\tau_j(\beta_k)),$$

e deste modo

$$(\det A)^2 = \prod_{i=1}^{n} \sigma_i \det(\tau_j(\beta_k))^2 = N_{\mathbb{L}/\mathbb{K}}(\det(\tau_j(\beta_k))^2) = N_{\mathbb{L}/\mathbb{K}}(D(\mathbb{M}/\mathbb{L})).$$

Portanto, $(\det A)^2 = N_{\mathbb{L}/\mathbb{K}}(D(\mathbb{M}/\mathbb{L}))$.
Temos ainda que $\det B = \det(\sigma_i(\alpha_j))^m$, *e assim*

$$(\det B)^2 = \det(\sigma_i(\alpha_j))^{2m}.$$

Mas, como temos que

$$D(\mathbb{L}/\mathbb{K}) = D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2,$$

segue que

$$(\det B)^2 = D(\mathbb{L}/\mathbb{K})^m.$$

Assim $(\det B)^2(\det A)^2 = D(\mathbb{L}/\mathbb{K})^m N_{\mathbb{L}/\mathbb{K}}(D(\mathbb{M}/\mathbb{L}))$. *Por outro lado, temos que*

$$AB = \begin{pmatrix} A_1B_{11} & A_1B_{12} & \cdots & A_1B_{1n} \\ A_2B_{21} & A_2B_{22} & \cdots & A_2B_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_nB_{n1} & A_nB_{n1} & \cdots & A_nB_{nn} \end{pmatrix},$$

onde

$$A_iB_{ij} = \begin{pmatrix} \sigma_i\tau_1(\beta_1)\sigma_i(\alpha_j) & \sigma_i\tau_1(\beta_2)\sigma_i(\alpha_j) & \cdots & \sigma_i\tau_1(\beta_m)\sigma_i(\alpha_j) \\ \sigma_i\tau_2(\beta_1)\sigma_i(\alpha_j) & \sigma_i\tau_2(\beta_2)\sigma_i(\alpha_j) & \cdots & \sigma_i\tau_2(\beta_m)\sigma_i(\alpha_j) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_i\tau_m(\beta_1)\sigma_i(\alpha_j) & \sigma_i\tau_m(\beta_2)\sigma_i(\alpha_j) & \cdots & \sigma_i\tau_m(\beta_m)\sigma_i(\alpha_j) \end{pmatrix},$$

ou seja, AB tem $\sigma_i\tau_h(\beta_k)\sigma_i(\alpha_j)$ *na linha* $m(i-1)+h$ *e na coluna* $m(i-1)+k$*, onde* $1 \leq i \leq n$, $1 \leq h \leq m$, $1 \leq k \leq m$, $1 \leq j \leq n$ *e zeros em todo o resto. Mas, temos que*

$$\sigma_i\tau_h(\beta_k)\sigma_i(\alpha_j) = \sigma_i\tau_h(\beta_k\alpha_j),$$

pois τ_h *fixa os* α_j*, ou seja* $\tau_h(\alpha_j) = \alpha_j$*, e assim* $\sigma_i\tau_h(\beta_k\alpha_j) = \sigma_i\tau_h(\beta_k)\sigma_i\tau_h(\alpha_j) = \sigma_i\tau_h(\beta_k)\sigma_i(\alpha_j)$*. Dessa forma,*

$$\det(AB) = \det(\sigma_i\tau_h(\beta_k)\sigma_i(\alpha_j)) = \det(\sigma_i\tau_h(\beta_k\alpha_j)),$$

e assim

$$(\det(AB))^2 = (\det(\sigma_i\tau_h(\beta_k\alpha_j)))^2 = D_{\mathbb{M}/\mathbb{K}}(\alpha_k\beta_j) = D(\mathbb{M}/\mathbb{K}).$$

Portanto $(\det(AB))^2 = D(\mathbb{M}/\mathbb{K})$*. Agora, como* $(\det(AB))^2 = (\det A)^2(\det B)^2$*, segue que*

$$D(\mathbb{M}/\mathbb{K}) = D(\mathbb{L}/\mathbb{K})^m N_{\mathbb{L}/\mathbb{K}}(D(\mathbb{M}/\mathbb{L})).$$

■

Na próxima proposição omitiremos a demonstração, visto que utiliza a teoria de diferente, que não faz parte do enfoque do nosso trabalho.

Proposição 2.5.4 *[2, p.217] Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos de números tais que* $\mathbb{K} \subseteq \mathbb{L}$*. Se* $[\mathbb{KL} : \mathbb{L}] = n$ *e* $[\mathbb{KL} : \mathbb{K}] = m$*, então* $N_{\mathbb{L}/\mathbb{Q}}(D(\mathbb{KL}/\mathbb{L}))$ *divide* $D(\mathbb{K}/\mathbb{Q})^m$ *e* $N_{\mathbb{K}/\mathbb{Q}}(D(\mathbb{KL}/\mathbb{K}))$ *divide* $D(\mathbb{L}/\mathbb{Q})^n$*.*

Definição 2.5.1 *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos de números,* $\{\alpha_1, \ldots, \alpha_n\}$ *e* $\{\beta_1, \ldots, \beta_m\}$ *bases de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *e* $\mathbb{L}$ *sobre* $\mathbb{Q}$*, respectivamente. Dizemos que* $\mathbb{K}$ *e* $\mathbb{L}$ *são linearmente disjuntos se* $\{\alpha_1\beta_1, \ldots, \alpha_n\beta_m\}$ *é uma base de* $\mathbb{KL}$ *sobre* $\mathbb{Q}$*.*

Proposição 2.5.5 *[2, p.218] Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos de números de grau* n *e* m*, respectivamente. Se os discriminantes* $D(\mathbb{K}/\mathbb{Q})$ *e* $D(\mathbb{L}/\mathbb{Q})$ *são relativamente primos e os corpos são linearmente disjuntos, então*

$$D(\mathbb{KL}/\mathbb{Q}) = D(\mathbb{K}/\mathbb{Q})^m D(\mathbb{L}/\mathbb{Q})^n.$$

Demonstração: *Pela Proposição 2.5.3 temos que*

$$D(\mathbb{KL}/\mathbb{Q}) = D(\mathbb{K}/\mathbb{Q})^m N_{\mathbb{K}/\mathbb{Q}}(D(\mathbb{KL}/\mathbb{K})) = D(\mathbb{L}/\mathbb{Q})^n N_{\mathbb{L}/\mathbb{Q}}(D(\mathbb{KL}/\mathbb{L})).$$

Daí $D(\mathbb{K}/\mathbb{Q})^m$ *e* $D(\mathbb{L}/\mathbb{Q})^n$ *dividem* $D(\mathbb{KL}/\mathbb{Q})$ *e como, por hipótese, são relativamente primos segue que* $D(\mathbb{K}/\mathbb{Q})^m D(\mathbb{L}/\mathbb{Q})^n$ *divide* $D(\mathbb{KL}/\mathbb{Q})$*. Por outro lado, pela Proposição 2.5.4, temos*

que $N_{\mathbb{L}/\mathbb{Q}}(D(\mathbb{KL}/\mathbb{L}))$ *divide* $D(\mathbb{K}/\mathbb{Q})^m$*, e assim* $D(\mathbb{KL}/\mathbb{Q}) = D(\mathbb{L}/\mathbb{Q})^n N_{\mathbb{L}/\mathbb{Q}}(D(\mathbb{KL}/\mathbb{L}))$ *divide* $D(\mathbb{L}/\mathbb{Q})^n D(\mathbb{K}/\mathbb{Q})^m$*. Portanto*

$$D(\mathbb{KL}/\mathbb{Q}) = D(\mathbb{K}/\mathbb{Q})^m D(\mathbb{L}/\mathbb{Q})^n.$$

■

Teorema 2.5.1 *[10, Proposition 2.7] Se* $\mathbb{K} = \mathbb{Q}(\zeta_n)$*, onde* n *é um inteiro maior que* 1*, então o discriminante de* $\mathbb{Q}(\zeta_n)$ *sobre* $\mathbb{Q}$ *é dado por*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}) = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Demonstração: *Pela Proposição 2.5.5, se* $n = p^{\alpha_1} p^{\alpha_2}$*,* $\mathbb{K} = \mathbb{Q}(\zeta_{p^{\alpha_1}})$ *e* $\mathbb{L} = \mathbb{Q}(\zeta_{p^{\alpha_2}})$ *segue que*

$$D(\mathbb{KL}/\mathbb{Q}) = D(\mathbb{K}/\mathbb{Q})^{[\mathbb{L}:\mathbb{Q}]} D(\mathbb{L}/\mathbb{Q})^{[\mathbb{K}:\mathbb{Q}]}.$$

Aplicando a função logaritmo em ambos os lados e usando suas propriedades segue que

$$\log|D(\mathbb{KL}/\mathbb{Q})| = [\mathbb{L}:\mathbb{Q}] \log|D(\mathbb{K}/\mathbb{Q})| + [\mathbb{K}:\mathbb{Q}] \log|D(\mathbb{L}/\mathbb{Q})|.$$

Como toda extensão ciclotômica é Galoisiana, temos que $[\mathbb{KL}:\mathbb{Q}] = [\mathbb{K}:\mathbb{Q}][\mathbb{L}:\mathbb{Q}]$*, e assim*

$$\frac{\log|D(\mathbb{KL}/\mathbb{Q})|}{[\mathbb{KL}:\mathbb{Q}]} = \frac{\log|D(\mathbb{K}/\mathbb{Q})|}{[\mathbb{K}:\mathbb{Q}]} + \frac{\log|D(\mathbb{L}/\mathbb{Q})|}{[\mathbb{L}:\mathbb{Q}]}.$$

De modo geral, tomando $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ *temos que*

$$\frac{\log|D(\mathbb{K}/\mathbb{Q})|}{[\mathbb{Q}(\zeta_n):\mathbb{Q}]} = \frac{\log|D(\mathbb{K}_1/\mathbb{Q})|}{[\mathbb{Q}(\zeta_{p_1^{\alpha_1}}):\mathbb{Q}]} + \ldots + \frac{\log|D(\mathbb{K}_r/\mathbb{Q})|}{[\mathbb{Q}(\zeta_{p_r^{\alpha_r}}):\mathbb{Q}]} = \sum_{i=1}^{n} \frac{\log|D(\mathbb{K}_r/\mathbb{Q})|}{\varphi(p_i^{\alpha_i})},$$

onde $\mathbb{K}_i = \mathbb{Q}(\zeta_{p_i^{\alpha_i}})$*,* $i = 1, 2, \ldots, r$*. Assim, pelo Teorema 1.9.1 e pela Proposição 2.5.2, temos que*

$$\begin{aligned}
\frac{\log|D(\mathbb{K}/\mathbb{Q})|}{\varphi(n)} &= \sum_{i=1}^{r} \frac{\log p_i^{p_i^{\alpha_i-1}(\alpha_i(p_i-1)-1)}}{p_i^{\alpha_i-1}(p_i-1)} = \sum_{i=1}^{r} \frac{p_i^{\alpha_i-1}(\alpha_i(p_i-1)-1)}{p_i^{\alpha_i-1}(p_i-1)} \log p_i \\
&= \sum_{i=1}^{r} \left(\alpha_i - \frac{1}{p_i-1}\right) \log p_i = \sum_{i=1}^{r} \alpha_i \log p_i - \sum_{i=1}^{r} \frac{\log p_i}{p_i-1} \\
&= \sum_{i=1}^{r} \log p_i^{\alpha_i} - \sum_{i=1}^{r} \log p_i^{\frac{1}{p_i-1}} = \log\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) - \log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right) \\
&= \log(n) - \log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right),
\end{aligned}$$

e consequentemente,

$$\log|D(\mathbb{K}/\mathbb{Q})| = \varphi(n)\left(\log(n) - \log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right)\right) = \log\left(\frac{n}{\prod_{i=1}^{r} p_i^{p_i-1}}\right)^{\varphi(n)}.$$

Assim, $|D(\mathbb{K}/\mathbb{Q})| = \left(\frac{n}{\prod_{i=1}^{r} p_i^{p_i-1}}\right)^{\varphi(n)}$, *e portanto,*

$$D_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}) = (-1)^{\varphi(n)/2}\frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

■

Capítulo 3

Caracteres de Dirichlet

3.1 Introdução

Neste capítulo apresentamos os caracteres de Dirichlet, seus condutores e algumas propriedades que serão úteis para o cálculo do discriminante de corpos de números abelianos. Esses caracteres descrevem parte da aritmética de um corpo abeliano e mostram que qualquer grupo abeliano finito pode ser analisado como um subgrupo de um grupo de Galois de um corpo ciclotômico $\mathbb{Q}(\zeta_n)$. Deste modo, na Seção 3.2, veremos conceitos dos caracteres de Diririchlet juntamente com suas principais propriedades. Na Seção 3.3, veremos os caracteres de Dirichlet definidos módulo p^r, onde p é um primo ímpar e r um inteiro positivo. Na Seção 3.4, veremos os caracteres de Dirichlet definidos módulo 2^r, onde r é um número inteiro positivo. Neste capítulo utilizamos as referências [10], [11], [12], [13] e [14].

3.2 Caracteres de Dirichlet

Nesta seção apresentamos os caracteres de Dirichlet juntamente com suas principais propriedades, com o intuito de usá-las no cálculo do discriminante dos corpos de números abeliano.

Definição 3.2.1 *Sejam G um grupo, $\mathbb{K}$ um corpo e $\mathbb{K}^*$ o grupo multiplicativo dos elementos inversíveis de $\mathbb{K}$. Um homomorfismo de grupos $\sigma : G \longrightarrow \mathbb{K}^*$ é chamado de caracter de G em $\mathbb{K}$.*

Observação 3.2.1

1. *Pelo Lema de Dedekind 1.7.1 temos que se $\{\sigma_1, \ldots, \sigma_n\}$ são caracteres distintos de G em $\mathbb{K}^*$, então $\{\sigma_1, \ldots, \sigma_n\}$ é linearmente independente.*

2. O conjunto dos caracteres forma um grupo.

Definição 3.2.2 *Um homomorfismo multiplicativo $\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ é chamado de caracter de Dirichlet definido módulo n.*

Observação 3.2.2 *Um caracter de Dirichlet χ definido módulo n satisfaz as seguintes propriedades:*

1. $\chi(1) = 1$,
2. $\chi(a) = \chi(a+n)$, *para todo a inteiro positivo,*
3. $\chi(ma) = \chi(m)\chi(a)$, *para quaisquer m e a inteiros positivos,*
4. $\chi(a) = 0$, *para todo a tal que $mdc(a,n) \neq 1$.*

Exemplo 3.2.1 *Uma função χ dada por $\chi(a) = (-1)^{\frac{a-1}{2}}$, para todo a ímpar e $\chi(a) = 0$, para todo a par, é um caracter de Dirichlet módulo 4, uma vez que satisfaz as condições da Observação 3.2.2, para $n = 4$.*

Observação 3.2.3 *Sejam n e m inteiros positivos. Se n divide m, então o caracter $\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ induz um homomorfismo $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathbb{C}^*$, via a composição com o homomorfismo canônico sobrejetor $\theta : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.*

Definição 3.2.3 *Seja χ um caracter de Dirichlet. Definimos o condutor de χ e denotamos por f_χ, o menor valor de n que satisfaz a condição 2 da Observação 3.2.2.*

Observação 3.2.4 *Podemos extender o homomorfismo χ a uma função $\chi' : \mathbb{Z} \longrightarrow \mathbb{C}$ tomando $\chi(a) = 0$ se $mdc(a, f_\chi) \neq 1$.*

Exemplo 3.2.2 *Seja $G = (\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\}$. O grupo de caracteres de Dirichlet de G é $\{\chi_0, \chi_1\}$ e podemos descrevê-los através da seguinte tabela:*

	χ_0	χ_1
1	*1*	*1*
3	*1*	*-1*
f_χ	*1*	*4*

Exemplo 3.2.3 *Seja $G = (\mathbb{Z}/10\mathbb{Z})^* = \{1, 3, 7, 9\}$. O grupo de caracteres de Dirichlet de G é $\{\chi_0, \chi_1, \chi_2, \chi_3\}$ e podemos descrevê-los através da seguinte tabela:*

	χ_0	χ_1	χ_2	χ_3
1	*1*	*1*	*1*	*1*
3	*1*	*1*	*-1*	*-1*
7	*1*	*-1*	*1*	*-1*
9	*1*	*-1*	*-1*	*1*
f_χ	*1*	*5*	*5*	*5*

Os caracteres χ_1, χ_2 e χ_3 podem ser definidos módulo 5, pois $\chi_i(a+5) = \chi_i(a)$, para todo a e $i = 1, 2, 3$. Assim, como 5 é o mínimo que isso ocorre, segue que o condutor de χ_i é $f_{\chi_i} = 5$, para $i = 1, 2, 3$.

Teorema 3.2.1 *[12, Lemma 3.2] Seja χ um caracter de Dirichlet definido módulo m. Se n divide m, então o condutor de χ é n se, e somente se, $\chi(a) = 1$ quando $mdc(a, m) = 1$ e $a \equiv 1(mod\ n)$.*

Demonstração: *Suponhamos que n divide m e que o condutor de χ é n. Se χ' é um caracter induzido por um caracter χ, então para qualquer a tal que $mdc(a, m) = 1$ temos que $\chi'(a) = \chi\theta(a) = \chi(a)$, onde θ é o homomorfismo dado na Observação 3.2.3. Assim, se $a \equiv 1(mod\ n)$, então $\chi'(a) = \chi(a) = \chi(1) = 1$. Reciprocamente, suponhamos que n divide m e que $\chi'(a) = 1$ para qualquer a tal que $mdc(a, m) = 1$ e $a \equiv 1(mod\ n)$. Para qualquer b tal que $mdc(b, n) = 1$, podemos determinar a_0 tal que $mdc(a_0, m) = 1$ e $a_0 \equiv b(mod\ m)$. Seja $\chi(b) = \chi'(a)$. O valor de $\chi(b)$ não depende da escolha de a_0, pois se $a_0 \equiv b_0(mod\ n)$, com $mdc(b_0, m) = 1$, então $b_0 = pa_0(mod\ m)$, para algum p primo, tal que p não divide m. Como $a \equiv 1(mod\ n)$ segue por hipótese que $\chi'(a) = 1$, e daí $\chi'(b_0) = \chi'(p)\chi'(a_0) = \chi'(a_0)$. Tomando $\chi(c) = 0$ quando $mdc(c, n) \neq 1$ obtemos χ. Visto que $\chi'(a) = \chi(a)$ quando $mdc(a, m) = 1$, concluímos que χ' é induzido por χ.* ■

Teorema 3.2.2 *[11, Teorema 4.1.3] Seja χ um caracter de Dirichlet. Se χ é induzido por um caracter χ' módulo n e também por um caracter χ'' módulo m, então χ é induzido por um caracter χ''' módulo t, onde $t = mdc(m, n)$.*

Demonstração: *Suponhamos que χ seja definido módulo q, onde $m|q$, $n|q$ e seja $t = mdc(m, n)$. Pelo Teorema 3.2.1 basta mostrarmos que se $mdc(a, q) = 1$ e $a \equiv 1(mod\ t)$, então $\chi(a) = 1$, para termos que o caracter χ módulo q é induzido pelo caracter χ''' módulo t. Assim, vamos supor que $mdc(a, q) = 1$ e $a \equiv 1(mod\ t)$. Pelo Teorema Chinês dos Restos, existe um inteiro k satisfazendo $k \equiv 1(mod\ m)$ e $k \equiv a(mod\ n)$, e deste modo podemos assumir que $mdc(k, q) = 1$. Tomando $r \equiv ak^{-1}(mod\ q)$, temos que $r \equiv 1(mod\ n)$ e $r \equiv a(mod\ m)$. Além*

disso, $r \equiv ak^{-1}(mod\ q)$ *implica que* $a \equiv kr(mod\ q)$*, e o fato de* $k \equiv r \equiv 1(mod\ n)$ *implica que* $\chi(k) = \chi(r) = 1$*. Portanto, temos que* $\chi(a) = \chi(k)\chi(r) = 1$*, como queríamos demonstrar. Portanto* χ *é induzido por* χ''' *módulo* t*.* ■

Exemplo 3.2.4 *Seja* $G = (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$*. O grupo de caracteres de Dirichlet de* G *é* $\{\chi_0, \chi_1, \chi_2, \chi_3\}$ *e podemos descrevê-los através da seguinte tabela:*

	χ_0	χ_1	χ_2	χ_3
1	*1*	*1*	*1*	*1*
3	*1*	*1*	*-1*	*-1*
5	*1*	*-1*	*1*	*-1*
7	*1*	*-1*	*-1*	*1*
f_χ	*1*	*8*	*4*	*8*

Pelo Teorema 3.2.1 o condutor do caracter χ_2 *é* $f_{\chi_2} = 4$*, pois temos que* $4|8$*,* $mdc(5, 8) = 1$*,* $5 \equiv 1(mod\ 4)$ *e* $\chi_2(5) = 1$*.*

Definição 3.2.4 *Um caracter de Dirichlet* χ *é chamado par se* $\chi(-1) = 1$ *e ímpar se* $\chi(-1) = -1$*.*

Exemplo 3.2.5 *No Exemplo 3.2.2 o caracter* χ_1 *é ímpar, pois* $3 \equiv -1(mod\ 4)$ *e* $\chi_1(3) = -1$*. No Exemplo 3.2.3 o caracter* χ_3 *é par, pois* $9 \equiv -1(mod\ 10)$ *e* $\chi_3(9) = 1$*.*

Definição 3.2.5 *Um caracter de Dirichlet definido módulo o seu condutor é chamado caracter primitivo.*

Exemplo 3.2.6 *No Exemplo 3.2.4 os caracteres* χ_1 *e* χ_3 *definidos módulo* 8 *são primitivos. O caracter* χ_2 *não é primitivo, pois seu condutor é* $f_{\chi_2} = 4$*.*

Definição 3.2.6 *Sejam* χ *e* ψ *dois caracteres de Dirichlet primitivos com condutores* f_χ *e* f_ψ*, respectivamente. Definimos o homomorfismo* $\chi\psi : (\mathbb{Z}/mmc(f_\chi, f_\psi)\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ *dado por* $\chi\psi(a) = \chi(a)\psi(a)$*.*

Observação 3.2.5 *O caracter* $\chi\psi$ *é primitivo.*

Exemplo 3.2.7 *Sejam χ um caracter definido módulo 8 por $\chi(1) = 1$, $\chi(3) = -1$, $\chi(5) = -1$, $\chi(7) = 1$ e ψ um caracter definido módulo 4 por $\psi(1) = 1$, $\psi(3) = -1$. Assim o caracter $\chi\psi : (\mathbb{Z}/8\mathbb{Z})^* \longrightarrow \mathbb{C}^*$, onde $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$, tem os valores*

$$\begin{aligned} \chi\psi(1) &= 1 \\ \chi\psi(3) &= \chi(3)\psi(3) = 1 \\ \chi\psi(5) &= \chi(5)\psi(1) = -1 \\ \chi\psi(7) &= \chi(7)\psi(3) = -1. \end{aligned}$$

Portanto, $\chi\psi$ tem condutor 8, e deste modo é primitivo.

Observação 3.2.6 *Seja χ um caracter e $\psi = \bar{\chi}$ o seu conjugado complexo. Se $mdc(a, f_\chi) = 1$, então $\psi(a) = \chi(a)^{-1}$. Logo $\chi\psi(a) = \chi(a)\psi(a) = 1$, para todo a.*

Proposição 3.2.1 *[11, Exemplo 4.5] Sejam χ e ψ dois caracteres de Dirichlet primitivos com condutores f_χ e f_ψ, respectivamente. Se $mdc(f_\chi, f_\psi) = 1$, então $f_{\chi\psi} = f_\chi f_\psi$.*
Demonstração: *Sejam $\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ e $\psi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathbb{C}^*$. Por definição $\chi\psi : (\mathbb{Z}/mmc(f_\chi, f_\psi)\mathbb{Z})^* \longrightarrow \mathbb{C}^*$. Por hipótese temos que $mdc(f_\chi, f_\psi) = 1$, e assim segue que f_χ e f_ψ são relativamente primos, logo $mmc(f_\chi, f_\psi) = f_\chi f_\psi$ e pela minimalidade de $f_\chi f_\psi$, concluímos que o condutor de $\chi\psi$ é $f_\chi f_\psi$, ou seja, $f_{\chi\psi} = f_\chi f_\psi$.* ∎

Exemplo 3.2.8 *Sejam χ um caracter módulo 4 definido por $\chi(1) = 1$, $\chi(3) = -1$ e ψ um caracter módulo 5 definido por $\psi(1) = 1$, $\psi(2) = -1$, $\psi(3) = -1$, $\psi(4) = 1$. Os caracteres χ e ψ são primitivos com condutores $f_\chi = 4$ e $f_\psi = 5$, e deste modo $mdc(f_\chi, f_\psi) = 1$. Portanto, pela Proposição 3.2.1, temos que o condutor de $\chi\psi$ é $f_{\chi\psi} = 20$.*

Observação 3.2.7

1. *A vantagem de usarmos caracteres de Dirichlet primitivos é evidente quando tomamos um produto de vários caracteres com vários condutores, pois o módulo de definição cresce rapidamente.*

2. *Algumas vezes é vantajoso pensar nos caracteres de Dirichlet como os caracteres dos grupos de Galois de corpos ciclotômicos. Se identificarmos $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ com $(\mathbb{Z}/n\mathbb{Z})^*$, então o caracter de Dirichlet módulo n é chamado um caracter de Galois.*

Exemplo 3.2.9 *No Exemplo 3.2.3, temos que $(\mathbb{Z}/10\mathbb{Z})^* \simeq Gal(\mathbb{Q}(\zeta_{10})/\mathbb{Q})$. Mas como $\mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(\zeta_{10})$ e $[\mathbb{Q}(\zeta_{10}) : \mathbb{Q}] = 2 = [\mathbb{Q}(\zeta_5) : \mathbb{Q}]$, segue que $\mathbb{Q}(\zeta_{10}) = \mathbb{Q}(\zeta_5)$. Assim, um caracter módulo 10 e um caracter módulo 5 são caracteres do mesmo grupo de Galois.*

Exemplo 3.2.10 *No Exemplo 3.2.4, temos que* $(\mathbb{Z}/8\mathbb{Z})^* \simeq Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})$. *O núcleo do carac ter* χ_2 *é* $\{1, 5(mod\ 8)\}$. *Assim, seja* $\mathbb{K}$ *o corpo fixo por* $\{\sigma_1, \sigma_5\}$. *Como* $\zeta_8^8 = 1$ *e* $\zeta_8^4 = -1$ *segue que* $\sigma_5(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3) = a_0 + a_1\zeta_8^2 + a_2\zeta_8^{10} + a_3\zeta_8^{15} = a_0 - a_1\zeta_8 + a_2\zeta_8^2 - a_3\zeta_8^3$. *Temos que* $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(\zeta_8)$ *e que* $[\mathbb{Q}(\zeta_4) : \mathbb{Q}] = 2$. *Sendo* ζ_8^2 *uma raíz* 4*-ésima da unidade e como* $\{1, \zeta_8^2\}$ *gera* $\mathbb{Q}(\zeta_4)$, *segue que* $\mathbb{K} = \mathbb{Q}(\zeta_4)$. *Assim,* $Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)) \simeq \{\sigma_1, \sigma_5\}$, *e temos que* $\chi_2 : \frac{(\mathbb{Z}/8\mathbb{Z})^*}{\{1,5\}} \longrightarrow \mathbb{C}^*$, *onde*

$$\frac{(\mathbb{Z}/8\mathbb{Z})^*}{\{1,5\}} \simeq \frac{Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})}{Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4))} \simeq Gal(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq (\mathbb{Z}/4\mathbb{Z})^*.$$

Portanto, χ_2 *é um caracter de* $(\mathbb{Z}/4\mathbb{Z})^*$.

Definição 3.2.7 *Sejam* χ *um caracter de Dirichlet do grupo de Galois* $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *e* $\mathbb{K}$ *o corpo fixo do núcleo de* χ. *O corpo* $\mathbb{K}$ *é chamado corpo associado a* χ.

Observação 3.2.8

1. *O corpo* $\mathbb{K}$ *associado a* χ *é um subcorpo de* $\mathbb{Q}(\zeta_n)$, *e se* n *é o menor valor, então* n *é o condutor de* χ.

2. *O corpo* $\mathbb{K}$ *depende somente de* χ.

3. *Se* X *é um grupo finito de caracteres de Dirichlet e* $mmc(f_{\chi_i}) = n$, *onde* $\chi_i \in X$, *então* X *é um subgrupo do grupo dos caracteres de Dirichlet* $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Definição 3.2.8 *Seja* X *um grupo finito de caracteres de Dirichlet,* H *a intersecção dos núcleos destes caracteres e* $\mathbb{K}$ *o corpo fixo de* H. *O corpo* $\mathbb{K}$ *é chamado corpo associado a* X.

Observação 3.2.9

1. *Como* X *é isomorfo a* $Gal(\mathbb{K}/\mathbb{Q})$, *segue que o grau de* $\mathbb{K}/\mathbb{Q}$ *é igual a ordem de* X.

2. *Se* X *é cíclico, gerado por* χ, *então* $\mathbb{K}$ *é precisamente o mesmo corpo associado a* χ *mencionado acima.*

Observação 3.2.10 *Observemos que*

$$Gal(\mathbb{K}/\mathbb{Q}) = \frac{Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})}{Gal(\mathbb{Q}(\zeta_n)/\mathbb{K})} \simeq \frac{(\mathbb{Z}/n\mathbb{Z})^*}{H}.$$

$$\begin{array}{c} \mathbb{Q}(\zeta_n) \\ | \\ \mathbb{K} \\ | \\ \mathbb{Q} \end{array}$$

Temos que X é o conjunto dos automorfismos de $Gal(\mathbb{K}/\mathbb{Q})$ em $\mathbb{C}^*$, ou ainda equivalentemente, é o conjunto dos automorfismos de $\frac{(\mathbb{Z}/n\mathbb{Z})^*}{H}$ em $\mathbb{C}^*$. Se $\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$, então podemos definir $\bar{\chi} : \frac{(\mathbb{Z}/n\mathbb{Z})^*}{H} \longrightarrow \mathbb{C}^*$ dado por $\bar{\chi}(\bar{a}) = \chi(a)$. Temos que $\bar{\chi}$ é um caracter de Dirichlet, pois $\bar{a} = \bar{b} \Longleftrightarrow ab^{-1} \in H \Longleftrightarrow \chi(ab^{-1}) = 1 \Longleftrightarrow \chi(a)\chi(b^{-1}) = 1 \Longleftrightarrow \chi(a) = \chi(b)$. Mais ainda, χ é um homomorfismo. Assim, definindo

$$\begin{array}{rccc} \tau : & X & \longrightarrow & \{\psi : \frac{(\mathbb{Z}/n\mathbb{Z})^*}{H} \longrightarrow \mathbb{C}^*\}, \\ & \chi & \longrightarrow & \bar{\chi} \end{array}$$

temos que τ está bem definido, e $\tau_1 \neq \tau_2 \Longleftrightarrow$ existe $x \in (\mathbb{Z}/n\mathbb{Z})^*$, tal que $\tau_1(x) \neq \tau_2(x)$. Assim, $\tau_1(\bar{x}) = \tau_2(\bar{x})$ e portanto τ é injetiva e deste modo

$$o(X) < o\{ \text{ conjunto dos homomorfismos de} \frac{(\mathbb{Z}/n\mathbb{Z})^*}{H} \longrightarrow \mathbb{C}^*\}.$$

Por outro lado, se $\chi : \frac{(\mathbb{Z}/n\mathbb{Z})^*}{H} \longrightarrow \mathbb{C}^*$ é um homomorfismo, definimos $\chi' : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ por $\chi'(a) = \chi(\bar{a})$. Temos que χ' está bem definida e χ' é um homomorfismo, pois $\chi'(ab) = \chi(\bar{ab}) = \chi(\bar{a})\chi(\bar{b}) = \chi'(a)\chi'(b)$. Além disso, se $\chi_1 \neq \chi_2$, então $\chi_1' \neq \chi_2'$. Assim,

$$o\{\tau : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^* : \tau \text{ é um homomorfismo}\} \leq o(X),$$

isto é,

$$o(X) = o\{\tau : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^* : \tau \text{ é um homomorfismo}\}.$$

Deste modo, X é o conjunto dos homomorfismos de $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$.

Exemplo 3.2.11 *Se X é o grupo de caracteres de $(\mathbb{Z}/n\mathbb{Z})^*$ satisfazendo $\chi(-1) = 1$, então a conjugação complexa ($\zeta_n \mapsto \zeta_n^{-1}$) está no núcleo de cada $\chi_i \in X$. O corpo $\mathbb{K}$ associado a X é $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, que é o subcorpo maximal real de $\mathbb{Q}(\zeta_n)$, ou seja, $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{Q}(\zeta_n)$. Considerando a correspondência $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, temos que 1 é a identidade e -1 é a conjugação complexa. Assim, a conjugação complexa está no núcleo de qualquer $\chi \in X$. Em geral, se χ é um caracter e $\mathbb{K}$ é o corpo fixo por χ, então $\mathbb{K} \subseteq \mathbb{R}$ se, e somente se, $\chi(-1) = 1$. De fato, se $\chi(-1) = 1$, então $\mathbb{K} \subseteq \mathbb{R}$, pois $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Agora, se $\mathbb{K} \subseteq \mathbb{R}$, então os automorfismos estão no núcleo de χ (só os reais). Portanto, $\chi(-1) = 1$.*

Exemplo 3.2.12 *Consideremos o grupo $G = (\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$. O grupo de caracteres de Dirichlet associado a G é $\{\chi_0, \chi_1, \chi_2, \chi_3\}$ e podemos descrevê-los pela tabela abaixo:*

	χ_0	χ_1	χ_2	χ_3	
1	*1*	*1*	*1*	*1*	σ_1
5	*1*	*1*	*-1*	*-1*	σ_5
7=-5	*1*	*-1*	*-1*	*1*	σ_7
11=-1	*1*	*-1*	*1*	*-1*	σ_{11}
f_χ	*1*	*4*	*12*	*3*	

Os subgrupos multiplicativos do grupo de Galois são:

$$H_0 = \{\sigma_1\} \qquad H_1 = \{\sigma_1, \sigma_5\}$$
$$H_2 = \{\sigma_1, \sigma_{11}\} \quad H_3 = \{\sigma_1, \sigma_7\}$$
$$H_4 = G.$$

Assim, temos que $\mathbb{K}_0 = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{-3})\mathbb{Q}(\sqrt{-1})$ *é fixado por* H_0, $\mathbb{K}_1$ *é fixado por* H_1 *e os caracteres associados são* $\{\chi_0, \chi_1\}$. *Assim* $\mathbb{K}_1$ *tem condutor 4, e deste modo* $\mathbb{K}_1 = \mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$. *O corpo* $\mathbb{K}_2$ *é fixado por* H_2, *e os caracteres associados são* $\{\chi_0, \chi_2\}$. *Assim* $\mathbb{K}_2$ *tem condutor 12, e deste modo* $\mathbb{K}_2 = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{3})$. *O fato que* $\chi_2(-1) = 1$ *informa que* $\mathbb{K}_2$ *é um subcorpo real. O corpo* $\mathbb{K}_3$ *é fixado por* H_3 *e os caracteres associados são* $\{\chi_0, \chi_3\}$. *Assim* $\mathbb{K}_3$ *tem condutor* 3 *e deste modo* $\mathbb{K}_3 = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. *O corpo* $\mathbb{Q}$ *é fixado por* G.

Estas noções preliminares podem ser usadas no conjunto dos caracteres dos grupos abelianos finitos, o que faremos agora.

Definição 3.2.9 *Seja* G *um grupo abeliano finito. Definimos o grupo* $\hat{G}$ *como o grupo dos caracteres de* G *em* $\mathbb{C}^*$.

Lema 3.2.1 *Se* G_1 *e* G_2 *são grupos abelianos finitos, então*

$$\widehat{G_1 \times G_2} \simeq \hat{G}_1 \times \hat{G}_2.$$

Demonstração: *Seja*

$$\begin{array}{rccc} \theta: & \hat{G}_1 \times \hat{G}_2 & \longrightarrow & \widehat{G_1 \times G_2} \\ & (\chi_1, \chi_2) & \longmapsto & \chi_1\chi_2. \end{array}$$

Assim

1. $\theta((\chi_1, \chi_2)(\varphi_1, \varphi_2)) = \theta(\chi_1\varphi_1, \chi_2\varphi_2) = \chi_1\varphi_1\chi_2\varphi_2 = \chi_1\chi_2\varphi_1\varphi_2 = \theta(\chi_1\chi_2)\theta(\varphi_1\varphi_2)$.

2. $\chi_1\chi_2(a, 1) = \chi_1(a)\chi_2(1) = \chi_1(a) = 1$ *e* $\chi_1\chi_2(1, a) = \chi_1(1)\chi_2(a) = \chi_2(a) = 1$.

3. *Se* $\varphi \in \widehat{G_1 \times G_2}$, *então existe* $(\varphi_{|G_1}, \varphi_{|G_2}) \in \hat{G}_1 \times \hat{G}_2$ *tal que* $\theta(\varphi_{|G_1}, \varphi_{|G_2})$.

Portanto θ *é um isomorfismo, ou seja,* $\widehat{G_1 \times G_2} \simeq \hat{G}_1 \times \hat{G}_2$. ∎

Proposição 3.2.2 *[10, Lemma 3.1, Corollary 3.2] Se* G *é um grupo abeliano finito e* $\hat{G}$ *é o grupo dos homomorfismos multiplicativos de* G *em* $\mathbb{C}^*$, *ou seja, dos caracteres de* G *em* $\mathbb{C}^*$, *então*

1. G *é isomorfo a* $\hat{G}$,
2. G *é isomorfo a* $\hat{\hat{G}}$.

Demonstração:

1. *Pelo Teorema fundamental dos grupos abelianos temos que qualquer grupo abeliano finito pode ser escrito como um produto direto de subgrupos cíclicos, isto é,*

$$G \simeq \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}.$$

Pelo Lema 3.2.1 temos que $\hat{G} \simeq \widehat{\mathbb{Z}_{n_1}} \times \ldots \times \widehat{\mathbb{Z}_{n_r}}$. *Assim, é suficiente provarmos quando* G *é cíclico. Seja* G *um grupo cíclico de ordem* n, *ou seja,* $G = \langle g \rangle$. *Se* $\zeta_n = e^{\frac{2\pi i}{n}}$ *e* $\chi \in \hat{G}$, *então* $\chi(g) = \zeta_n^k$, *para* $0 \leq k < n$ ($k \neq n$, *pois caso contrário* $\chi = \chi_0$). *Como* $\chi(g^m) = \chi(g)^m$, *temos que* χ *é determinado pelo seu valor em* g. *Reciprocamente, se* $0 \leq k < n$ *definimos* $\chi(g^m) = \zeta_n^{km}$, *temos que* χ *está bem definida e é um caracter de Dirichlet. Assim, existem exatamente* n *caracteres em* G. *Agora, seja* $\chi_1 \in \hat{G}$ *tal que* $\chi_1(g) = \zeta_n$. *Se* $\chi \in \hat{G}$ *e* $\chi(g) = \zeta_n^k$, *então* $\chi(g) = \chi_1(g)^k$, *isto é,* $\chi_1^k = \chi$. *Isto prova que* $\hat{G}$ *é cíclico e gerado por* χ_1. *Portanto,* G *e* $\hat{G}$ *são grupos cíclicos de mesma ordem, logo* $G \simeq \hat{G}$.

2. *Seja*

$$\begin{array}{rccc} \theta: & G & \longrightarrow & \hat{\hat{G}} \\ & g & \longmapsto & \theta_g \end{array} \quad , \quad \text{onde } \theta_g(\chi) = \chi(g).$$

Temos que θ *é um homomorfismo. Suponhamos que o núcleo de* θ *é dado por* H *que é um subgrupo de* G. *Assim, para qualquer caracter* χ *de* G *temos que* $\chi(b) = 1$, *para todo* $b \in H$. *Isto significa que* χ *pode ser visto como um caracter de* G/H. *Assim,*

$$o(G) = o(\hat{G}) \leq o(G/H) = \frac{o(G)}{o(H)},$$

e deste modo $o(H) = 1$ *e* $H = \{Id\}$. *Portanto,* θ *é injetiva e* $\hat{\hat{G}} \simeq G$. ∎

Observação 3.2.11 *As vezes é conveniente identificarmos* $\hat{\hat{G}} = G$*, e assim temos uma função bilinear natural*

$$\begin{array}{rccc} b: & G \times \hat{G} & \longrightarrow & \mathbb{C}^* \\ & (g, \chi) & \longmapsto & \chi(g). \end{array}$$

Esta função é não degenerada, pois se $\chi(g) = 1$ *para todo* $\chi \in \hat{G}$*, então* $g = 1$ *pelo ítem* 2 *da Proposição 3.2.2; e se* $\chi(g) = 1$ *para todo* $g \in G$*, então* $\chi = 1$*. Além disso, se* $\chi(g) = 1$ *para todo* $\chi \in \hat{G}$*, temos que* $\langle g \rangle \subseteq G$*, e* $G/\langle g \rangle$ *têm a mesma quantidade de caracteres distintos que* G*. Mas,* $o(G) \leq \frac{o(G)}{o(\langle g \rangle)}$*, e isto só é possível se* $o(\langle g \rangle) = 1$*, isto é,* $g = 1$*.*

Proposição 3.2.3 *[10, Proposition 3.3, 3.4] Se* H *é um subgrupo de* G *e* $H^\perp = \{\chi \in \hat{G} : \chi(h) = 1,\ \forall h \in H\}$*, então*

1. $H^\perp$ *é isomorfo a* $\widehat{G/H}$*,*
2. $\hat{H}$ *é isomorfo a* $\hat{G}/H^\perp$*,*
3. $(H^\perp)^\perp = H$*.*

Demonstração:

1. *Seja*

$$\begin{array}{rccc} \theta: & H^\perp & \longrightarrow & \widehat{G/H}, \quad \textit{onde } \bar{\chi}(\bar{g}) = \chi(g). \\ & \chi & \longmapsto & \bar{\chi} \end{array}$$

   Tomando a composição

$$\begin{array}{ccc} G/H & \longrightarrow^{\varphi} & \mathbb{C}^* \\ \uparrow_{\pi} & \nearrow_{\varphi \circ \pi} & \\ G & & \end{array}$$

   temos que $\varphi \circ \pi = \chi, \theta(\chi) = \bar{\chi} = \varphi$ *e* $\varphi(\bar{g}) = \varphi(\pi(g)) = \chi(g)$*. Assim,* $(\varphi \circ \pi)(h) = 1$*. Portanto,* θ *é um isomorfismo.*

2. *Seja a função* $b : G \times \hat{G} \longrightarrow \mathbb{C}^*$ *dada por* $b(g, \chi) = \chi(g)$*. Tomando a restrição de* G *por* H *obtemos* $b' : H \times \hat{G} \longrightarrow \hat{H}$ *dada por* $b'(h, \chi) = \chi(h)$*. Se* $(h_0, \chi_0) \in H \times \hat{G}$*, pertence ao núcleo de* b'*, então* $b'(h_0, \chi_0) = \chi_0(h_0) = 1$*, e deste modo* $\chi_0 \in H^\perp$*. Portanto* $H \times H^\perp$ *é o núcleo de* b'*. Resta mostrar que* b' *é sobrejetiva. Pelo ítem* 1*, segue que*

$$o(H^\perp) = o(\frac{\hat{G}}{H}) = o(\frac{G}{H}) = \frac{o(G)}{o(H)}.$$

   Assim

$$o(\hat{H}) = o(H) = \frac{o(G)}{o(H^\perp)} = \frac{o(\hat{G})}{o(H^\perp)}.$$

Agora, pelo Teorema do Isomorfismo, temos que $Im(b') \simeq \frac{H\times\hat{G}}{Ker(b')}$, *ou seja,*

$$\hat{H} \simeq \frac{H \times \hat{G}}{H \times H^{\perp}} \simeq \frac{H}{H} \times \frac{\hat{G}}{H^{\perp}} \simeq \frac{\hat{G}}{H^{\perp}}.$$

Portanto $\hat{H} \simeq \frac{\hat{G}}{H^{\perp}}$.

3. *Se* $h \in H$, *então* h *é dado por* $h : \chi \longrightarrow \chi(h)$ *que leva* $H^{\perp}$ *em* 1, *e assim* $H \subseteq (H^{\perp})^{\perp}$. *Para a outra inclusão, pela demonstração do ítem* 2, *temos que* $o(H) = \frac{o(G)}{o(H^{\perp})}$ *e* $o(H^{\perp}) = \frac{o(G)}{o(H)}$. *Assim obtemos que* $o((H^{\perp})^{\perp}) = \frac{o(G)}{o(H^{\perp})} = o(H)$, *e deste modo, ambos tem a mesma ordem. Portanto são iguais, ou seja,* $H = (H^{\perp})^{\perp}$. ∎

Proposição 3.2.4 *[10, p.23] Se* X *é o grupo dos caracteres de Dirichlet associados a um corpo de números* $\mathbb{L}$, *então existe uma função bilinear* $b : Gal(\mathbb{L}/\mathbb{Q}) \times X \longrightarrow \mathbb{C}^*$.

Demonstração: *Se* $\mathbb{K}$ *é um subcorpo de* $\mathbb{L}$ *e* $Y = \{\chi \in X : \chi(g) = 1$, *para todo* $g \in Gal(\mathbb{L}/\mathbb{K})\}$, *então*

$$Y = Gal(\mathbb{L}/\mathbb{K})^{\perp} = \frac{\widehat{Gal(\mathbb{L}/\mathbb{Q})}}{Gal(\mathbb{L}/\mathbb{K})} = \widehat{Gal(\mathbb{K}/\mathbb{Q})}.$$

Por outro lado, tomando um subgrupo $Y \subseteq X$ *e* $\mathbb{K}$ *como o corpo fixo de* $Y^{\perp} = \{g \in Gal(\mathbb{L}/\mathbb{Q}) : \chi(g) = 1$, *para todo* $\chi \in Y\}$, *pela teoria de Galois, temos que* $Y^{\perp} = Gal(\mathbb{L}/\mathbb{K})$, *pois* $Gal(\mathbb{K}/\mathbb{Q}) \simeq Gal(\mathbb{L}/\mathbb{Q})/Gal(\mathbb{L}/\mathbb{K})$. *Assim* $Y = (Y^{\perp})^{\perp} = Gal(\mathbb{L}/\mathbb{K})^{\perp} = \widehat{Gal(\mathbb{K}/\mathbb{Q})}$, *e deste modo temos uma correspondência biunívoca entre os subgrupos de* X *e os subcorpos de* $\mathbb{L}$ *dada por*

$$\begin{array}{rccc} \varphi: & \mathcal{G} & \longleftrightarrow & \mathcal{C} \\ & Y & \longmapsto & \{\text{corpo fixo de } Y^{\perp}\}, \end{array}$$

onde $\mathcal{G} = \{H \subseteq X : H$ *é subgrupo*$\}$ *e* $\mathcal{C} = \{\mathbb{K} \subseteq \mathbb{L} : \mathbb{K}$ *é subcorpo*$\}$. *Se* $Y = Z$, *então* $Y^{\perp} = Z^{\perp}$, *e deste modo temos que o corpo fixo de* $Y^{\perp}$ *é o mesmo corpo fixo de* $Z^{\perp}$. *Seja ainda,*

$$\begin{array}{rccc} \psi: & \mathcal{C} & \longrightarrow & \mathcal{G} \\ & \mathbb{K} & \longmapsto & Y = \widehat{Gal(\mathbb{L}/\mathbb{K})}. \end{array}$$

Temos que $(\psi \circ \varphi)(Y) = \psi(\text{corpo fixo de } Y^{\perp}) = Y$ *e* $(\varphi \circ \psi)(1) = 1$. *Assim,* φ *e* ψ *são bijetoras, e deste modo existe uma correspondência biunívoca entre os subgrupos de* X *e os subcorpos de* $\mathbb{L}$ *dada por*

$$\begin{array}{rcl} \mathbb{K} & \longrightarrow & Gal(\mathbb{L}/\mathbb{K})^{\perp} \\ Y & \longleftrightarrow & \{\text{corpo fixo de } Y^{\perp}\}. \end{array}$$

Portanto, temos uma correspondência biunívoca entre todos os grupos de caracteres de Dirichlet e os subcorpos dos corpos ciclotômicos, pois quaisquer dois grupos podem ser vistos

como subgrupos de um grupo maior. Como $Gal(\mathbb{K}/\mathbb{Q})$ *é um grupo abeliano finito, segue que* $Y = Gal(\widehat{\mathbb{K}/\mathbb{Q}}) = Gal(\mathbb{K}/\mathbb{Q})$. *Este isomorfismo é não canônico e deste modo existe a forma bilinear natural não degenerada dada por*

$$\begin{array}{rccc} b: & Gal(\mathbb{K}/\mathbb{Q}) \times Y & \longrightarrow & \mathbb{C}^* \\ & (g, \chi) & \longmapsto & \chi(g). \end{array}$$

■

Proposição 3.2.5 *[14, Lema 3.7] Se* $X_{\mathbb{K}_i}$ *é o grupo dos caracteres associados ao corpo* $\mathbb{K}_i$, *para* $i = 1, 2$, *então:*

1. $X_{\mathbb{K}_1} \subseteq X_{\mathbb{K}_2}$ *se, e somente se,* $\mathbb{K}_1 \subseteq \mathbb{K}_2$.

2. *O grupo gerado por* $X_{\mathbb{K}_1}$ *e* $X_{\mathbb{K}_2}$ *é associado ao corpo composto* $\mathbb{K}_1\mathbb{K}_2$.

Demonstração:

1. *Suponhamos* $X_{\mathbb{K}_1} \subseteq X_{\mathbb{K}_2}$. *Sejam* $H_1 = \bigcap_{\chi \in X_{\mathbb{K}_1}} Ker(\chi)$ *e* $H_2 = \bigcap_{\chi \in X_{\mathbb{K}_2}} Ker(\chi)$. *Como* $X_{\mathbb{K}_1} \subseteq X_{\mathbb{K}_2}$ *segue que* $H_2 \subseteq H_1$. *Agora, por definição, temos que* $\mathbb{K}_i$ *é o corpo fixo por* H_i, *para* $i = 1, 2$. *Assim,* $\mathbb{K}_1 \subseteq \mathbb{K}_2$. *Por outro lado, se* $\mathbb{K}_1 \subseteq \mathbb{K}_2$, *temos que* $\mathbb{Q} \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \mathbb{Q}(\zeta_n)$ *para algum* n *inteiro positivo,* $X_{\mathbb{K}_1} = Gal(\mathbb{Q}(\zeta_n/\mathbb{K}_1))^\perp$ *e* $X_{\mathbb{K}_2} = Gal(\mathbb{Q}(\zeta_n/\mathbb{K}_2))^\perp$. *Como* $Gal(\mathbb{Q}(\zeta_n/\mathbb{K}_2)) \subseteq Gal(\mathbb{Q}(\zeta_n/\mathbb{K}_1))$, *segue que* $Gal(\mathbb{Q}(\zeta_n/\mathbb{K}_1))^\perp \subseteq Gal(\mathbb{Q}(\zeta_n/\mathbb{K}_2))^\perp$. *Portanto,* $X_{\mathbb{K}_1} \subseteq X_{\mathbb{K}_2}$.

2. *Seja* X *o grupo associado a* $\mathbb{K}_1\mathbb{K}_2$. *Pelo ítem* 1, *temos que o grupo gerado por* $X_{\mathbb{K}_1}$ *e* $X_{\mathbb{K}_2}$ *está contido em* X, *ou seja,* $\langle X_{\mathbb{K}_1}, X_{\mathbb{K}_2} \rangle \subseteq X$. *Agora, como* $\mathbb{K}_i \subseteq \mathbb{K}_1\mathbb{K}_2$, *segue que* $X_{\mathbb{K}_i} \subseteq X_{\mathbb{K}_1}X_{\mathbb{K}_2}$, *para* $i = 1, 2$. *Assim,* $\langle X_{\mathbb{K}_1}, X_{\mathbb{K}_2} \rangle \subseteq X$. *Agora, se* $\langle X_{\mathbb{K}_1}, X_{\mathbb{K}_2} \rangle \subsetneq X$, *então existe um corpo* $\mathbb{L} \subseteq \mathbb{K}_1\mathbb{K}_2$ *associado a* $\langle X_{\mathbb{K}_1}, X_{\mathbb{K}_2} \rangle \subseteq X$. *Mas, novamente pelo ítem* 1, *temos que*

$$\begin{cases} \mathbb{K}_1 \subseteq \mathbb{L} \subseteq \mathbb{K}_1\mathbb{K}_2 \\ \mathbb{K}_2 \subseteq \mathbb{L} \subseteq \mathbb{K}_1\mathbb{K}_2, \end{cases}$$

o que é um absurdo. Assim, $X = \langle X_{\mathbb{K}_1}, X_{\mathbb{K}_2} \rangle$ *e* $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$. ■

Corolário 3.2.1 *[14, Lema 3.8] Se* $\mathbb{K}$ *é um subcorpo de* $\mathbb{Q}(\zeta_n)$ *e se* s, d *são divisores de* n, *então*

$$X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)} \cap X_{\mathbb{K}\cap\mathbb{Q}(\zeta_s)} = X_{\mathbb{K}\cap\mathbb{Q}(\zeta_t)},$$

onde $t = mdc(d, s)$.

Demonstração: *Pela Proposição 3.2.5 temos que* $X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)} \cap X_{\mathbb{K}\cap\mathbb{Q}(\zeta_s)} = X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)\cap\mathbb{Q}(\zeta_s)}$. *Mas*

$\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_s) = \mathbb{Q}(\zeta_t)$, *onde* $t = mdc(d, s)$. *Portanto,* $X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)} \cap X_{\mathbb{K}\cap\mathbb{Q}(\zeta_s)} = X_{\mathbb{K}\cap\mathbb{Q}(\zeta_t)}$, *onde* $t = mdc(d, s)$. ∎

3.3 Caracteres de Dirichlet módulo p^r

Nesta seção apresentamos algumas propriedades particulares dos caracteres de Dirichlet com condutores sendo potência de um número primo ímpar.

Lema 3.3.1 *[12, Lemma 3.1] Se* g *é um inteiro tal que* $\bar{g} \equiv g(mod\ p^r)$ *é um gerador do grupo multiplicativo* $(\mathbb{Z}/p^r\mathbb{Z})^*$, *onde* p *é um número primo ímpar e* r *um inteiro positivo, então para todo* $0 < j \leq r$, *temos que* $g^k \equiv 1(mod\ p^j)$ *se, e somente se,* $k \equiv 0(mod\ (p-1)p^{j-1})$.
Demonstração: *Suponhamos que para todo* j *tal que* $0 < j \leq r$ *temos que* $g^k \equiv 1(mod\ p^j)$, *ou seja,* $g^k = 1 + p^j t$, *para algum* $t \in \mathbb{Z}$. *Elevando ambos os lados a* p*-ésima potência obtemos que* $g^{kp} = 1 + p^{j+1}t_1$, *onde* $t_1 \in \mathbb{Z}$. *Seguindo este raciocínio obtemos que* $g^{kp^{r-j}} = 1 + p^r t_{r-j}$, *onde* $t_{r-j} \in \mathbb{Z}$. *Assim,* $g^{kp^{r-j}} \equiv 1(mod\ p^r)$, *e deste modo temos que* $(p-1)p^{r-1}$ *divide* kp^{r-j}. *Logo,* $kp^{r-j} = (p-1)p^{r-1}q$, *onde* $q \in \mathbb{Z}$, *e assim* $k = (p-1)p^{j-1}q$. *Portanto* $k \equiv 0(mod\ (p-1)p^{j-1})$. *Por outro lado, suponhamos que* $k \equiv 0(mod\ (p-1)p^{j-1})$. *Como o grupo multiplicativo* $(\mathbb{Z}/p^j\mathbb{Z})^*$ *tem ordem* $(p-1)p^{j-1}$ *e* $mdc(p, g) = 1$, *pelo Teorema de Fermat, segue que* $g^k \equiv 1(mod\ p^j)$. ∎

Se g é um inteiro tal que $\bar{g} \equiv g(\text{mod } p^r)$ é um gerador do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$ e se χ é um caracter de Dirichlet, então existem $(p-1)p^{r-1}$ caracteres de Dirichlet definidos sobre $(\mathbb{Z}/p^r\mathbb{Z})^*$, uma vez que $(\mathbb{Z}/p^r\mathbb{Z})^*$ tem ordem $(p-1)p^{r-1}$, e tais caracteres são completamente determinados pela imagem de $\bar{g}$. Por outro lado, pelo Teorema 3.2.1, temos que

$$1 = \chi(\bar{1}) = \chi((\bar{g})^{(p-1)p^{r-1}}) = \chi(\bar{g})^{(p-1)p^{r-1}}.$$

Logo $\chi(g)$ é uma raíz $(p-1)p^{r-1}$-ésima da unidade. Assim, dado um caracter de Dirichlet módulo p^r, temos que existe um inteiro i, onde $0 \leq i \leq (p-1)p^{r-1}$, tal que $\chi(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$. Como existem $(p-1)p^{r-1}$ caracteres e $(p-1)p^{r-1}$ possibilidades para i, concluimos que todos os caracteres definidos módulo p^r são da forma

$$\chi_i(\bar{g}) = \zeta^i_{(p-1)p^{r-1}},$$

para $i = 0, 1, \ldots, (p-1)p^{r-1}$.

Teorema 3.3.1 *[12, Lemma 3.3] Se* i *é um inteiro tal que* $0 \leq i \leq (p-1)p^{r-1}$, *então o condutor* f_{χ_i} *de* χ_i *é* p^{r-j} *se, e somente se,* $p^j = mdc(i, p^r)$.

Demonstração: *Suponhamos que o condutor de* χ_i *é* $f_{\chi_i} = p^{r-j}$, *para* $i = 0, 1, \ldots, (p-1)p^{r-1}$. *Se* $H = \{\bar{g}^a \in (\mathbb{Z}/p^r\mathbb{Z}) : g^a \equiv 1(mod\ p^{r-j})\}$, *então* $\chi_i(x) = 1$, *para todo* $x \in H$, *e em particular* $\chi_i(g^{(p-1)p^{r-j-1}}) = 1$. *Por outro lado, temos que*

$$\chi_i(g^{(p-1)p^{r-j-1}}) = \zeta_{(p-1)p^{r-1}}^{i(p-1)p^{r-j-1}},$$

e deste modo, existe $t \in \mathbb{Z}$ *tal que* $i(p-1)p^{r-j-1} = (p-1)p^{r-1}t$. *Logo* $i = p^j t$ *e assim* $mdc(i, p^r) = p^j$. *Reciprocamente, suponhamos que* $mdc(i, p^r) = p^j$ *e mostremos que* $f_{\chi_i} = p^{r-j}$. *Para* $i = 0$ *o resultado é imediato. Assim, se* $i \neq 0$, *então* $i = p^j t$, *para algum* $t \in \mathbb{Z}$. *Deste modo,* χ *pode ser definido módulo* p^{r-j} *se, e somente se,* $\chi_i(x) = 1$, *para todo* $x \in H$. *Como* $H \subseteq (\mathbb{Z}/p^r\mathbb{Z})^*$, *segue que* $o(H)|(p-1)p^{r-1}$. *Como* $g^a \equiv 1(mod\ p^{r-j})$, *pelo Lema 3.3.1, segue que* $a \equiv 0(mod\ (p-1)p^{r-j-1})$ *e assim* $o(g) = (p-1)p^{r-j-1} = o(H)$. *Portanto* $H = \langle g^{(p-1)p^{r-j-1}} \rangle$. *Finalmente, temos que*

$$\chi_i(g^{(p-1)p^{r-j-1}}) = \zeta_{(p-1)p^{r-1}}^{i(p-1)p^{r-j-1}} = \zeta_{(p-1)p^{r-1}}^{(p-1)p^{r-1}ip^{-j}} = 1^{ip^{-j}} = 1$$

e assim χ_i *pode ser definido módulo* p^{r-j}. *Portanto o condutor* f_{χ_i} *de* χ_i *é* p^{r-j}. ∎

Exemplo 3.3.1 *Se* $n = 5^2$, *então o grupo* G *tem ordem* $(p-1)p^{r-1} = 5.4 = 20$ *e é dado por* $G = (\mathbb{Z}/25\mathbb{Z})^* = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$. *O grupo de Galois de* $\mathbb{Q}(\zeta_{25})$ *sobre* $\mathbb{Q}$ *é dado por* $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{16}, \sigma_{17}, \sigma_{18}, \sigma_{19}, \sigma_{21}, \sigma_{22}, \sigma_{23}, \sigma_{24}\}$. *Caracterizamos o grupo* $\hat{G}$ *pela Tabela abaixo.*

	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5	χ_6	χ_7	χ_8	χ_9	χ_{10}	χ_{11}	χ_{12}	χ_{13}	χ_{14}	χ_{15}	χ_{16}	χ_{17}	χ_{18}	χ_{19}
2^0=1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$2^1 = 2$	1	ζ_{20}	ζ_{20}^2	ζ_{20}^3	ζ_{20}^4	ζ_{20}^5	ζ_{20}^6	ζ_{20}^7	ζ_{20}^8	ζ_{20}^9	-1	ζ_{20}^{11}	ζ_{20}^{12}	ζ_{20}^{13}	ζ_{20}^{14}	ζ_{20}^{15}	ζ_{20}^{16}	ζ_{20}^{17}	ζ_{20}^{18}	ζ_{20}^{19}
$2^2 = 4$	1	ζ_{20}^2	ζ_{20}^4	ζ_{20}^6	ζ_{20}^8	-1	ζ_{20}^{12}	ζ_{20}^{14}	ζ_{20}^{16}	ζ_{20}^{18}	1	ζ_{20}^2	ζ_{20}^4	ζ_{20}^6	ζ_{20}^8	-1	ζ_{20}^{12}	ζ_{20}^{14}	ζ_{20}^{16}	ζ_{20}^{18}
$2^3 = 8$	1	ζ_{20}^3	ζ_{20}^6	ζ_{20}^9	ζ_{20}^{12}	ζ_{20}^{15}	ζ_{20}^{18}	ζ_{20}^1	ζ_{20}^4	ζ_{20}^7	-1	ζ_{20}^{13}	ζ_{20}^{16}	ζ_{20}^{19}	ζ_{20}^2	ζ_{20}^5	ζ_{20}^8	ζ_{20}^{11}	ζ_{20}^{14}	ζ_{20}^{17}
$2^4 = 16$	1	ζ_{20}^4	ζ_{20}^8	ζ_{20}^{12}	ζ_{20}^{16}	1	ζ_{20}^4	ζ_{20}^8	ζ_{20}^{12}	ζ_{20}^{16}	1	ζ_{20}^4	ζ_{20}^8	ζ_{20}^{12}	ζ_{20}^{16}	1	ζ_{20}^4	ζ_{20}^8	ζ_{20}^{12}	ζ_{20}^{16}
$2^5 = 7$	1	ζ_{20}^5	-1	ζ_{20}^{15}	1	ζ_{20}^5	-1	ζ_{20}^{15}	1	ζ_{20}^5	-1	ζ_{20}^{15}	1	ζ_{20}^5	-1	ζ_{20}^{15}	1	ζ_{20}^5	1	ζ_{20}^{15}
$2^6 = 14$	1	ζ_{20}^6	ζ_{20}^{12}	ζ_{20}^{18}	ζ_{20}^4	-1	ζ_{20}^{16}	ζ_{20}^2	ζ_{20}^8	ζ_{20}^{14}	1	ζ_{20}^6	ζ_{20}^{12}	ζ_{20}^{18}	ζ_{20}^4	-1	ζ_{20}^{16}	ζ_{20}^2	ζ_{20}^8	ζ_{20}^{14}
$2^7 = 3$	1	ζ_{20}^7	ζ_{20}^{14}	ζ_{20}	ζ_{20}^8	ζ_{20}^{15}	ζ_{20}^2	ζ_{20}^9	ζ_{20}^{16}	ζ_{20}^3	-1	ζ_{20}^{17}	ζ_{20}^4	ζ_{20}^{11}	ζ_{20}^{18}	ζ_{20}^5	ζ_{20}^{12}	ζ_{20}^{19}	ζ_{20}^6	ζ_{20}^{13}
$2^8 = 6$	1	ζ_{20}^8	ζ_{20}^{16}	ζ_{20}^4	ζ_{20}^{12}	1	ζ_{20}^8	ζ_{20}^{16}	ζ_{20}^4	ζ_{20}^{12}	1	ζ_{20}^8	ζ_{20}^{16}	ζ_{20}^4	ζ_{20}^{12}	1	ζ_{20}^8	ζ_{20}^{16}	ζ_{20}^4	ζ_{20}^{12}
$2^9 = 12$	1	ζ_{20}^9	ζ_{20}^{18}	ζ_{20}^7	ζ_{20}^{16}	ζ_{20}^5	ζ_{20}^{14}	ζ_{20}^3	ζ_{20}^{12}	ζ_{20}	-1	ζ_{20}^{19}	ζ_{20}^8	ζ_{20}^{17}	ζ_{20}^6	ζ_{20}^{15}	ζ_{20}^4	ζ_{20}^{13}	ζ_{20}^2	ζ_{20}^{11}
$2^{10} = 24$	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1
$2^{11} = 23$	1	ζ_{20}^{11}	ζ_{20}^2	ζ_{20}^{13}	ζ_{20}^4	ζ_{20}^{15}	ζ_{20}^6	ζ_{20}^{17}	ζ_{20}^8	ζ_{20}^{19}	-1	ζ_{20}	ζ_{20}^{12}	ζ_{20}^3	ζ_{20}^{14}	ζ_{20}^5	ζ_{20}^{16}	ζ_{20}^7	ζ_{20}^{18}	ζ_{20}^9
$2^{12} = 21$	1	ζ_{20}^{12}	ζ_{20}^4	ζ_{20}^{16}	ζ_{20}^8	1	ζ_{20}^{12}	ζ_{20}^4	ζ_{20}^{16}	ζ_{20}^8	1	ζ_{20}^{12}	ζ_{20}^4	ζ_{20}^{16}	ζ_{20}^8	1	ζ_{20}^{12}	ζ_{20}^4	ζ_{20}^{16}	ζ_{20}^8
$2^{13} = 17$	1	ζ_{20}^{13}	ζ_{20}^6	ζ_{20}^{19}	ζ_{20}^{12}	ζ_{20}^5	ζ_{20}^{18}	ζ_{20}^{11}	ζ_{20}^4	ζ_{20}^{17}	-1	ζ_{20}^3	ζ_{20}^{16}	ζ_{20}^9	ζ_{20}^2	ζ_{20}^{15}	ζ_{20}^8	ζ_{20}	ζ_{20}^{14}	ζ_{20}^7
$2^{14} = 9$	1	ζ_{20}^{14}	ζ_{20}^8	ζ_{20}^2	ζ_{20}^{16}	-1	ζ_{20}^4	ζ_{20}^{18}	ζ_{20}^{12}	ζ_{20}^6	1	ζ_{20}^{14}	ζ_{20}^8	ζ_{20}^2	ζ_{20}^{16}	-1	ζ_{20}^4	ζ_{20}^{18}	ζ_{20}^{12}	ζ_{20}^6
$2^{15} = 18$	1	ζ_{20}^{15}	-1	ζ_{20}^5	1	ζ_{20}^{15}	-1	ζ_{20}^5	1	ζ_{20}^{15}	-1	ζ_{20}^5	1	ζ_{20}^{15}	-1	ζ_{20}^5	1	ζ_{20}^{15}	-1	ζ_{20}^5
$2^{16} = 11$	1	ζ_{20}^{16}	ζ_{20}^{12}	ζ_{20}^8	ζ_{20}^4	1	ζ_{20}^{16}	ζ_{20}^{12}	ζ_{20}^8	ζ_{20}^4	1	ζ_{20}^{16}	ζ_{20}^{12}	ζ_{20}^8	ζ_{20}^4	1	ζ_{20}^{16}	ζ_{20}^{12}	ζ_{20}^8	ζ_{20}^4
$2^{17} = 22$	1	ζ_{20}^{17}	ζ_{20}^{14}	ζ_{20}^{11}	ζ_{20}^8	ζ_{20}^5	ζ_{20}^2	ζ_{20}^{19}	ζ_{20}^{16}	ζ_{20}^{13}	-1	ζ_{20}^7	ζ_{20}^4	ζ_{20}	ζ_{20}^{18}	ζ_{20}^5	ζ_{20}^2	ζ_{20}^{19}	ζ_{20}^{16}	ζ_{20}^3
$2^{18} = 19$	1	ζ_{20}^{18}	ζ_{20}^{16}	ζ_{20}^{14}	ζ_{20}^{12}	-1	ζ_{20}^8	ζ_{20}^6	ζ_{20}^4	ζ_{20}^2	1	ζ_{20}^{18}	ζ_{20}^{16}	ζ_{20}^{14}	ζ_{20}^{12}	-1	ζ_{20}^8	ζ_{20}^6	ζ_{20}^4	ζ_{20}^2
$2^{19} = 13$	1	ζ_{20}^{19}	ζ_{20}^{18}	ζ_{20}^{17}	ζ_{20}^{16}	ζ_{20}^{15}	ζ_{20}^{14}	ζ_{20}^{13}	ζ_{20}^{12}	ζ_{20}^{11}	-1	ζ_{20}^9	ζ_{20}^8	ζ_{20}^7	ζ_{20}^6	ζ_{20}^5	ζ_{20}^4	ζ_{20}^3	ζ_{20}^2	ζ_{20}^8
f_{χ_i}	1	5^2	5^2	5^2	5^2	5	5^2	5^2	5^2	5^2	5	5^2	5^2	5^2	5^2	5	5^2	5^2	5^2	5^2

O condutor f_{χ_i} *de* χ_i *é* 5^2, *para* $i = 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18$, *uma vez que* $mdc(i, 5^2) = 1 = 5^0$, *e assim pelo Teorema 3.3.1, temos que* $f_{\chi_i} = 5^{2-0} = 5^2$. *Para* $j = 5, 10, 15$,

o condutor f_{χ_j} de χ_j é 5, uma vez que $mdc(j, 5^2) = 5$, e assim novamente pelo Teorema 3.3.1 temos que $f_{\chi_j} = 5^{2-1} = 5$. Os subgrupos multiplicativos do grupo de Galois são:

$$\begin{aligned} H_0 &= \{\sigma_1\} & H_2 &= \{\sigma_1, \sigma_7, \sigma_{24}, \sigma_{18}\} \\ H_1 &= \{\sigma_1, \sigma_{24}\} & H_3 &= \{\sigma_1\sigma_{16}, \sigma_6, \sigma_{21}, \sigma_{11}\} \\ H_5 &= G & H_4 &= \{\sigma_1, \sigma_4, \sigma_{16}, \sigma_{14}, \sigma_6, \sigma_4, \sigma_{21}, \sigma_9, \sigma_{11}, \sigma_{19}\}. \end{aligned}$$

Assim, temos que $\mathbb{K}_0 = \mathbb{Q}(\zeta_{27})$ é fixado por H_0, $\mathbb{K}_1$ é fixado por H_1, $\mathbb{K}_2$ é fixado por H_2, $\mathbb{K}_3$ é fixado por H_3, $\mathbb{K}_4$ é fixado por H_4 e $\mathbb{Q}$ é fixado por G. Dessa forma os caracteres associados a $\mathbb{K}_0$ são $H_0^{\perp} = \hat{G}$, a $\mathbb{K}_1$ são $H_1^{\perp} = \{\chi_0, \chi_2, \chi_4, \chi_6, \chi_8, \chi_{10}, \chi_{12}, \chi_{14}, \chi_{16}, \chi_{18}\}$, a $\mathbb{K}_2$ são $H_2^{\perp} = \{\chi_0, \chi_4, \chi_8, \chi_{12}, \chi_{16}\}$, a $\mathbb{K}_3$ são $H_3^{\perp} = \{\chi_0, \chi_5, \chi_{10}, \chi_{15}\}$, a $\mathbb{K}_4$ são $H_4^{\perp} = \{\chi_0, \chi_{10}\}$ e a $\mathbb{Q}$ são $H_5^{\perp} = \{\chi_0\}$.

3.4 Caracteres de Dirichlet módulo 2^r

Nesta seção veremos algumas propriedades dos caracteres de Dirichlet com condutores sendo uma potência do número primo dois.

Proposição 3.4.1 *[13, Lemma 1.1] Se $t \in \mathbb{Z}$ é tal que, $t \geq 3$, então $5^{2^{t-3}} \equiv 1(mod\ 2^{t-1})$ e $5^{2^{t-3}} \not\equiv 1(mod\ 2^t)$.*

Demonstração: *Temos que*

$$\frac{5^{2^{t-3}} - 1}{5 - 1} = (5^{2^{t-4}} + 1)(5^{2^{t-5}} + 1) \ldots (5^2 + 1)(5 + 1).$$

Logo,

$$(5^{2^{t-3}} - 1) = (5^{2^{t-4}} + 1)(5^{2^{t-5}} + 1) \ldots (5^2 + 1)(5 + 1)(5 - 1).$$

Como

$$(5^{2^{t-4}} + 1) \equiv (5^{2^{t-5}} + 1) \equiv \ldots \equiv (5^2 + 1) \equiv (5 + 1) \equiv 2(mod\ 4)\ e\ (5 - 1) \equiv 0(mod\ 4),$$

segue que $5^{2^{t-3}} - 1 = k2^{t-1}$, onde k é ímpar. Assim, $5^{2^{t-3}} \equiv 1(mod\ 2^{t-1})$ e $5^{2^{t-3}} \not\equiv 1(mod\ 2^t)$. ■

Corolário 3.4.1 *[13, p.464] A ordem de $5(mod\ 2^t)$ é 2^{t-2}.*

Demonstração: *Pela Proposição 3.4.1 temos que $5^{2^{t-3}} \equiv 1(mod\ 2^{t-1})$, para todo $t \geq 3$. Mas, isto implica que $5^{2^{t-2}} \equiv 1(mod\ 2^t)$, para todo $t \geq 2$. Assim, para todo inteiro $t \geq 2$, temos que $5^{2^{t-2}} \equiv 1(mod\ 2^t)$ e $5^{2^{t-3}} \not\equiv 1(mod\ 2^t)$, o que mostra que a ordem de 5 módulo 2^t é 2^{t-2}.* ■

Proposição 3.4.2 *[13, Lemma 1.2] Se $t \in \mathbb{Z}$ é tal que, $t \geq 3$, então $(-1)^a 5^b \equiv 1(mod\ 2^t)$ se, e somente se, a é par e $b \equiv 0(mod\ 2^{t-2})$.*

Demonstração: *Suponhamos que $(-1)^a 5^b \equiv 1(mod\ 2^t)$. Se, por absurdo, a for ímpar, então $-5^b \equiv 1(mod\ 2^t)$, isto é, $5^b \equiv -1(mod\ 2^t)$. Mas, isto não pode ocorrer pois temos que $5^b + 1 \equiv 2(mod\ 4)$. Assim, $4 \nmid 5^b + 1$ e consequentemente nenhuma potência de 2 com expoente maior que 1 divide $5^b + 1$, ou seja, $5^b \not\equiv -1(mod\ 2^t)$. Portanto a é par. Assim, como $5^b \equiv 1(mod\ 2^t)$, pelo Corolário 3.4.1, segue que a ordem de $5(mod\ 2^t)$ é 2^{t-2} e portanto $b \equiv 0(mod\ 2^{t-2})$. Reciprocamente, se a for par e $b \equiv 0(mod\ 2^{t-2})$, então pelo Corolário 3.4.1 temos que $(-1)^a 5^b \equiv 1(mod\ 2^t)$.* ∎

Temos que $(\mathbb{Z}/2^r\mathbb{Z})^* = \langle \overline{-1}, \bar{5} \rangle = \{(\overline{-1})^a \bar{5}^b; a \in \{1,2\} \text{ e } b \in \{1,2,\ldots,2^{r-2}\}\}$. Assim, um caracter de $(\mathbb{Z}/2^r\mathbb{Z})^*$ é completamente determinado pelas imagens de $\overline{-1}$ e $\bar{5}$. Pelo Corolário 3.4.1 temos que a ordem de $5(mod\ 2^t)$ é 2^{t-2} e a ordem de $-1(mod\ 2^t)$ é 2. Assim dado $\chi \in \widehat{(\mathbb{Z}/2^r\mathbb{Z})^*}$ temos que $\chi(\overline{-1}) = (-1)^i$, para $i \in \{1,2\}$ e $\chi(\bar{5}) = \zeta_{2^{r-2}}^l$, para $l \in \{1,2,\ldots,2^{r-2}\}$. Denotaremos esses caracteres por $\chi_{i,l}$.

Teorema 3.4.1 *[13, Lemma 2.2] Se $\chi_{i,l}$ é um caracter de $(\mathbb{Z}/2^r\mathbb{Z})^*$, então o condutor $f_{\chi_{i,l}}$ de $\chi_{i,l}$, para $l = 2^{r-2}$, é dado por*

$$f_{\chi_{i,l}} = \begin{cases} 1 \text{ se } i = 2 \\ 4 \text{ se } i = 1. \end{cases}$$

Demonstração: *Se $\bar{x} \in (\mathbb{Z}/2^r\mathbb{Z})^*$, então $\bar{x} = (\overline{-1})^a \bar{5}^b$.*

- *Se $i = 2$, então $\chi_{i,l}(\bar{x}) = \chi_{i,l}((\overline{-1}^a \bar{5}^b)) = (-1)^{2a} \zeta_{2^{r-2}}^{2^{r-2}} = 1$. Assim o caracter $\chi_{i,l}$ é o trivial e $f_{\chi_{i,l}} = 1$.*
- *Se i=1, então $\chi_{i,l}(\bar{x}) = \chi_{i,l}((\overline{-1}^a \bar{5}^b)) = (-1)^a \zeta_{2^{r-2}}^{2^{r-2}} = (-1)^a = \begin{cases} 1 \text{ se } \bar{x} = \bar{5}^b (a = 2) \\ -1 \text{ se } \bar{x} = \overline{-1}\bar{5}^b (a = 1), \end{cases}$ e portanto $\chi_{i,l}$ não é trivial. Se $x \equiv 1(mod\ 4)$, então $\bar{x} = \bar{5}^b$, pois $5^b \equiv 1(mod\ 4)$ e $-5^b \equiv -1(mod\ 4)$. Assim, para todo x tal que $x \equiv 1(mod\ 4)$ temos que $\chi_{i,l}(\bar{x}) = 1$, e portanto $f_{\chi_{i,l}} = 4$.* ∎

Teorema 3.4.2 *[13, Lemma 2.2] Se $\chi_{i,l}$ é um caracter de $(\mathbb{Z}/2^r\mathbb{Z})^*$, então o condutor $f_{\chi_{i,l}}$ de $\chi_{i,l}$, para $l \neq 2^{r-2}$ é dado por*

$$f_{\chi_{i,l}} = \frac{2^r}{mdc(l, 2^l)}.$$

Demonstração: *Como $\chi_{i,l}(\bar{5}) = \zeta_{2^{r-2}}^l \neq 1$, para $0 \leq l < 2^{r-2}$, segue que $f_{\chi_{i,l}} > 4$, uma vez que $5 \equiv 1(mod\ 4)$. Assim, $f_{\chi_{i,l}} = 2^u$, onde $u > 2$. Seja $\bar{x} = (\overline{-1}^a \bar{5}^b) \in (\mathbb{Z}/2^r\mathbb{Z})^*$. Se*

$x \equiv 1(mod\ 2^u)$, *então pela Proposição 3.4.2, temos que* $(-1)^a 5^b \equiv 1(mod\ 2^u)$, $b \equiv 0(mod\ 2^{u-2})$ *e* $a = 2$. *Portanto,* $\bar{x} = \bar{5}^{t2^{u-2}}$, *onde* $t \in \{1, 2, \ldots, 2^{r-u}\}$. *Como* $f_{\chi_{i,l}} = 2^u$, *se* $x \equiv 1(mod\ 2^u)$ *segue que, devemos ter* $\chi_{i,l}(\bar{x}) = \chi_{i,l}(\bar{5}^{2^{u-2}}) = \zeta_{2^{r-2}}^{l2^{u-2}} = 1$. *Assim* $l2^{u-2} \equiv 0(mod\ 2^{r-2})$, *ou seja,* $l2^{u-2} = 2^{r-2}t$. *Logo* $l = 2^{r-u}t$ *e assim* $l \equiv 0(mod\ 2^{r-u})$. *Por outro lado, devemos ter* $\chi_{i,l}(\bar{5}^{2^{u-3}}) \neq 1$, *uma vez que se* $\chi_{i,l}(\bar{5}^{2^{u-3}}) = 1$, *então para* $x \equiv 1(mod\ 2^{u-1})$ *temos, pela Proposição 3.4.2, que* $\bar{x}\bar{5}^{t2^{u-3}}$ *e portanto* $\chi_{i,l}(\bar{x}) = (\chi_{i,l}(\bar{5}^{2^{u-3}}))^t = 1$, *o que contradiz o fato de* 2^u *ser o condutor de* $\chi_{i,l}$. *Mas,* $\chi_{i,l}(\bar{5}^{2^{u-3}}) = \zeta_{2^{r-2}}^{l2^{u-3}} \neq 1$ *se, e somente se,* $l2^{u-3} \not\equiv 0(mod\ 2^{r-2})$. *Assim,* $l2^{u-3} \neq 2^{r-2}t$ *e deste modo* $l \neq 2^{r-u+1}t$, *ou seja,* $l \not\equiv 0(mod\ 2^{r-u+1})$. *Agora, como* $l \equiv 0(mod\ 2^{r-u})$ *e* $l \not\equiv 0(mod\ 2^{r-u+1})$, *segue que* $mdc(l, 2^r) = 2^{r-u}$ *e assim* $2^u = \frac{2^r}{mdc(l,2^r)}$. *Reciprocamente, se* $2^u = \frac{2^r}{mdc(l,2^r)}$, *mostremos que* $f_{\chi_{i,l}} = 2^u$. *De fato, se* $mdc(l, 2^r) = 2^{r-u}$ *então* $l \equiv 0(mod\ 2^{r-u})$ *e* $l \not\equiv 0(mod\ 2^{r-u+1})$. *Deste modo, temos que*

- *Se* $x \equiv 1(mod\ 2^u)$ *então* $\bar{x} = \bar{5}^{t2^{u-2}}$ *e* $\chi_{i,l}(\bar{x}) = \zeta_{2^{r-2}}^{t2^{u-2}k2^{r-u}} = \zeta_{2^{r-2}}^{tk2^{r-2}} = 1$.

- *Se* $x \equiv 1(mod\ 2^{u-1})$ *e* $x \not\equiv 1(mod\ 2^u)$ *então* $\bar{x} = \bar{5}^{t2^{u-3}}$ *e* $\bar{5}^{t2^{u-3}} \not\equiv 1(mod\ 2^u)$. *Assim, pela Proposição 3.4.2, temos que* $t2^{u-3} \not\equiv 0(mod\ 2^{u-2})$, *ou seja,* $t2^{u-3} \neq 2^{u-2}t_0$, *para qualquer* $t_0 \in \mathbb{Z}$. *Logo* $t \neq 2t_0$ *e deste modo* t *é ímpar. Portanto* $l \not\equiv 0(mod\ 2^{r-u+1})$ *e* t *é ímpar, e assim*

$$\chi_{i,l}(\bar{x}) = \chi_{i,l}(\bar{5}^{t2^{u-3}}) = \zeta_{2^{r-2}}^{tl2^{u-3}} \neq 1.$$

Assim, $\chi_{i,l}(\bar{x}) = 1$ *para todo* $x \equiv 1(mod\ 2^u)$ *e existe* $\bar{x}$ *tal que* $x \equiv 1(mod\ 2^{u-1})$, $x \equiv 1(mod\ 2^u)$ *e* $\chi_{i,l}(\bar{x}) \neq 1$. *Logo,* $f_{\chi_{i,l}} = 2^u$. ∎

Observação 3.4.1 *Observe que não existe caracter com condutor* 2, *uma vez que todo caracter definido módulo* 2 *é trivial e assim tem condutor* 1.

Exemplo 3.4.1 *Se* $n = 2^4$, *então o grupo* G *tem ordem* $2^{r-1} = 2^3$ *e é dado por* $G = (\mathbb{Z}/16\mathbb{Z})^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$. *O grupo de Galois de* $\mathbb{Q}(\zeta_{16})$ *sobre* $\mathbb{Q}$ *é* $\{\sigma_1, \sigma_3, \sigma_5, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{15}, \}$.

O grupo $\hat{G}$ é caracterizado pela tabela abaixo.

	$\chi_{2,4}$	$\chi_{2,3}$	$\chi_{2,2}$	$\chi_{2,1}$	$\chi_{1,4}$	$\chi_{1,3}$	$\chi_{1,2}$	$\chi_{1,1}$	
$1=(-1)^2$	1	1	1	1	1	1	1	1	σ_1
$3=-1.5^3$	1	ζ_4	-1	ζ_4^3	-1	$-\zeta_4$	1	$-\zeta_4^3$	σ_3
$5=(-1)^2 5$	1	ζ_4^3	-1	ζ_4	1	ζ_4^3	-1	ζ_4	σ_5
$7=-1.5^2$	1	-1	1	-1	-1	1	-1	1	σ_7
$9=(-1)^2 5^2$	1	-1	1	-1	1	-1	1	-1	σ_9
$11=-1.5$	1	ζ_4^3	-1	ζ_4	-1	$-\zeta_4^3$	1	$-\zeta_4$	σ_{11}
$13=(-1)^2 5^3$	1	ζ_4	-1	ζ_4^3	1	ζ_4	-1	ζ_4^3	σ_{13}
$15=-1$	1	1	1	1	-1	-1	-1	-1	σ_{15}
	1	2^4	2^3	2^4	2^2	2^4	2^3	2^4	

Pelo Teorema 3.4.1, temos que o condutor $f_{\chi_{2,4}}$ de $\chi_{2,4}$ é 1, pois $l=2^{r-2}=4$ e $i=2$, e o condutor $f_{\chi_{1,4}}$ de $\chi_{1,4}$ é 4, pois $l=2^{r-2}=4$ e $i=1$. Agora, pelo Teorema 3.4.2, temos que o condutor de $\chi_{2,3}$, $\chi_{2,1}$, $\chi_{1,3}$ e $\chi_{1,1}$ é 2^4, pois $mdc(l,2^l)=1$ e o condutor de $\chi_{2,2}$ e $\chi_{1,2}$ é 2^3, pois $mdc(l,2^l)=2$. Os subgrupos multiplicativos do grupo de Galois são:

$$\begin{aligned} H_0&=\{\sigma_1\} & H_3&=\{\sigma_1,\sigma_7,\sigma_9,\sigma_{13}\}\\ H_1&=\{\sigma_1,\sigma_{15}\} & H_4&=\{\sigma_1,\sigma_5,\sigma_9,\sigma_{13}\}\\ H_2&=\{\sigma_1,\sigma_7\} & H_5&=\{\sigma_1,\sigma_3,\sigma_9,\sigma_{11}\}\\ H_6&=G. \end{aligned}$$

Assim, temos que $\mathbb{K}_0=\mathbb{Q}(\zeta_{16})$ é fixado por H_0, $\mathbb{K}_1$ é fixado por H_1, $\mathbb{K}_2$ é fixado por H_2, $\mathbb{K}_3$ é fixado por H_3, $\mathbb{K}_4$ é fixado por H_4, $\mathbb{K}_5$ é fixado por H_5 e $\mathbb{Q}$ é fixado por G. Dessa forma os caracteres associados a $\mathbb{K}_0$ são $H_0^{\perp}=\hat{G}$, a $\mathbb{K}_1$ são $H_1^{\perp}=\{\chi_{2,4},\chi_{2,3},\chi_{2,2},\chi_{2,1}\}$, a $\mathbb{K}_2$ são $H_2^{\perp}=\{\chi_{2,4},\chi_{2,2},\chi_{1,3},\chi_{1,1}\}$, a $\mathbb{K}_3$ são $H_3^{\perp}=\{\chi_{2,4}\}$, a $\mathbb{K}_4$ são $H_4^{\perp}=\{\chi_{2,4},\chi_{1,4}\}$, a $\mathbb{K}_5$ são $H_5^{\perp}=\{\chi_{2,4},\chi_{1,2}\}$ e a $\mathbb{Q}$ são $H_5^{\perp}=\{\chi_{2,4}\}$.

Capítulo 4

Discriminante de corpos de números abelianos via caracteres de Dirichlet

4.1 Introdução

Neste capítulo veremos como calcular o discriminante de corpos de números abelianos via caracteres de Dirichlet fazendo uso da fórmula do condutor discriminante, ou seja, do seguinte teorema.

Teorema 4.1.1 *[10, Theorem 3.11] (Fórmula do condutor discriminante) Se $\mathbb{K}$ é um corpo de números associado a um grupo X de caracteres de Dirichlet, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$D(\mathbb{K}/\mathbb{Q}) = (-1)^{r_2} \prod_{\chi \in X} f_\chi,$$

onde r_2 é a metade do número de automorfismos complexos de $\mathbb{K}$.

Deste modo, na Seção 4.2 veremos o cálculo do discriminante de subcorpos de $\mathbb{Q}(\zeta_{p^r})$, onde ζ_{p^r} é uma raiz p^r-ésima primitiva da unidade com p um primo ímpar e r um inteiro positivo. Na Seção 4.3, veremos o cálculo do discriminante de subcorpos de $\mathbb{Q}(\zeta_{2^r})$, onde ζ_{2^r} é uma raiz 2^r-ésima primitiva da unidade com r um inteiro positivo. Na Seção 4.4, fazendo uso do Teorema de Kroenecker-Weber [10, Theorem 6, p. 341], veremos o cálculo do discriminante de corpos de números abelianos. Na Seção 4.5, veremos o cálculo do discriminante mínimo de alguns corpos de números. Neste capítulo foram utilizadas as referências [10], [12], [13], [14], [15] e [16].

4.2 Discriminante de subcorpos de $\mathbb{Q}(\zeta_{p^r})$

Nesta seção apresentamos o discriminante de um corpo de números $\mathbb{K}$, contido em uma extensão ciclotômica do tipo $\mathbb{Q}(\zeta_{p^r})$.

Sejam p um primo ímpar, r um inteiro positivo e $\mathbb{K}$ um subcorpo de $\mathbb{Q}(\zeta_{p^r})$. Como o grau de $\mathbb{K}$ sobre $\mathbb{Q}$ é um divisor de $(p-1)p^{r-1}$, segue que $[\mathbb{K}:\mathbb{Q}] = up^j$, onde u é um divisor de $p-1$ e $0 < j \leq r-1$. Sejam H o subgrupo de Galois $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ isomorfo a $(\mathbb{Z}/p^r\mathbb{Z})^*$que fixa $\mathbb{K}$ e $X_{\mathbb{K}}$ o grupo dos caracteres associados a $\mathbb{K}$, isto é, $X_{\mathbb{K}} = \{\chi \in \widehat{(\mathbb{Z}/p^r\mathbb{Z})}^* \text{ tal que } \chi(i) = 1, \text{ para todo } i \in H\}$.

Lema 4.2.1 *Se j é um inteiro positivo e p é um número primo, então*

$$1 + 2p + 3p^2 + \ldots + jp^{j-1} + (j+1)p^j = \frac{(j+2)p^{j+1}(p-1) - (p^{j+2}-1)}{(p-1)^2}.$$

Demonstração: *Se $S_{j+1} = 1+p+p^2+\ldots+p^{j+1}$, então $pS_{j+1} = p+p^2+\ldots+p^{j+2}$. Subtraindo a primeira equação da segunda obtemos que $S_{j+1} = \frac{p^{j+2}-1}{p-1}$. Portanto*

$$1 + p + p^2 + \ldots + p^{j+1} = \frac{p^{j+2}-1}{p-1}.$$

Assim, derivando ambos os lados obtemos que

$$1 + 2p + 3p^2 + \ldots + jp^{j-1} + (j+1)p^j = \frac{d}{dp}\left(\frac{p^{j+2}-1}{p-1}\right) = \frac{(j+2)p^{j+1}(p-1) - (p^{j+2}-1)}{(p-1)^2},$$

o que prova o lema. ∎

Teorema 4.2.1 *[12, Theorem 4.1] Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_{p^r})$ com $[\mathbb{K}:\mathbb{Q}] = up^j$, onde p é um primo ímpar, r um inteiro positivo, u um divisor de $(p-1)$ e $0 < j \leq r-1$, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$|D(\mathbb{K}/\mathbb{Q})| = p^{\beta_{(u,j)}},$$

onde $\beta_{(u,j)} = u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}] - 1$.

Demonstração: *Como $[\mathbb{Q}(\zeta_{p^r}):\mathbb{Q}] = (p-1)p^{r-1}$ segue que o grupo de Galois $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ é cíclico de ordem $(p-1)p^{r-1}$. Seja $g \in \mathbb{Z}$ tal que sua classe $\bar{g}$ é um gerador do grupo multiplicativo $(\mathbb{Z}/p^r\mathbb{Z})^*$. Se H é um subgrupo do grupo $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ que fixa $\mathbb{K}$, então H é cíclico de ordem*

$$\frac{(p-1)p^{r-1}}{up^j} = \frac{p-1}{u}p^{r-j-1} = (p-1)p^{r-j-1}u^{-1}.$$

Se σ_a é um gerador de H, então pelo Teorema 3.2.1 temos que um caracter χ módulo p^r associado a $\mathbb{K}$ (ou seja, $\chi \in X_{\mathbb{K}}$) se, e somente se, $\chi(\sigma_a) = 1$. Como a ordem de a módulo p^r

é igual a ordem de H, segue que a ordem de a é $(p-1)p^{r-j-1}u^{-1}$. Assim podemos supor sem perda de generalidade que $a \equiv g^d (mod\ p^r)$, onde $d = up^j$, uma vez que

$$a^{(p-1)p^{r-j-1}u^{-1}} \equiv g^{(p-1)p^{r-1}} \equiv 1 (mod\ p^r).$$

Deste modo, temos que

$$\chi_i(\bar{a}) = \chi_i(\bar{g}^d) = (\zeta^i_{(p-1)p^{r-1}})^d = \zeta^{di}_{(p-1)p^{r-1}}.$$

Logo, se χ_i é um caracter definido módulo p^r, pelo Lema 3.3.1, temos que $\chi_i(a) = 1$, ou seja, χ_i é associado a $\mathbb{K}$ se, e somente se, $di \equiv 0 (mod\ (p-1)p^{r-1})$, ou equivalentemente $i = \frac{(p-1)p^{r-1}t}{d}$, com $0 \leq t \leq d-1$. Como $d = up^j$, segue que $\chi_i(\bar{a}) = 1$ se, e somente se, $i = \frac{(p-1)p^{r-1}t}{up^j} = (p-1)p^{r-j-1}tu^{-1}$, com $0 \leq t \leq up^j - 1$. Se $t = 0$, então $i = 0$ e o condutor de χ_i é $f_{\chi_i} = 1$. Se $t \neq 0$, então $t = p^l t_k$, onde $l \in \mathbb{Z}$, $0 \leq l \leq j$ e $mdc(t_k, p) = 1$. Observe que para cada $0 \leq l \leq j-1$ existem $up^{j-l-1}(p-1)$ elementos t_k nessas condições. Assim, pelo Teorema 3.3.1, temos que os condutores dos correspondentes χ_i são todos iguais a p^{j+1-l}. Se $l = j$, então existem $u-1$ elementos t_k com $mdc(t_k, p) = 1$, e os condutores dos correspondentes χ_i são todos iguais a p. A tabela abaixo resume esses resultados.

l	*número de* χ_i	$f_{\chi_{i,l}} = p^{j+1-l}$
0	$up^{j-1}(p-1)$	p^{j+1}
1	$up^{j-2}(p-1)$	p^j
$\vdots$	$\vdots$	$\vdots$
j-1	$up^0(p-1) = u(p-1)$	p^2
j	*u-1*	p

Na primeira coluna temos os possíveis valores de l, na segunda os números de caracteres não triviais para os quais $i = (p-1)p^{r-j-1+l}t_k u^{-1}$ e $mdc(t_k, p) = 1$, e na terceira o condutor desses caracteres. Pelo Teorema 4.1.1 (Fórmula do condutor discriminante) temos que o discriminante de $\mathbb{K}$, é a menos de sinal, igual ao produto dos condutores dos caracteres χ_i que são associados a $\mathbb{K}$. Usando este resultado e a tabela obtemos:

$$\begin{aligned}
|D(\mathbb{K}/\mathbb{Q})| = \prod_{\chi_i \in X_k} f_{\chi_i} &= \underbrace{(p^{j+1} \dots p^{j+1})}_{up^{j-1}(p-1)} \underbrace{(p^j \dots p^j)}_{up^{j-2}(p-1)} \dots \underbrace{(p^2 \dots p^2)}_{u(p-1)} \underbrace{(p \dots p)}_{u-1} \\
&= (p^{j+1})^{up^{j-1}(p-1)} (p^j)^{up^{j-2}(p-1)} \dots (p^2)^{u(p-1)} p^{u-1} \\
&= p^{(j+1)up^{j-1}(p-1)} p^{jup^{j-2}(p-1)} \dots p^{2u(p-1)} p^{u-1} \\
&= p^{\beta_{(u,j)}},
\end{aligned}$$

onde

$$\begin{aligned}
\beta_{(u,j)} &= (j+1)up^{j-1}(p-1) + jup^{j-2}(p-1) + \ldots + 2u(p-1) + (u-1) \\
&= u(p-1)[(j+1)p^{j-1} + jp^{j-2} + \ldots + 2] + u - 1 \\
&= \tfrac{u(p-1)}{p}[(j+1)p^{j} + jp^{j-1} + \ldots + 2p] + u - 1 \\
&= \tfrac{u(p-1)}{p}\left[\sum_{i=0}^{j}(i+1)p^i - 1\right] + u - 1 = \tfrac{u(p-1)}{p}\sum_{i=0}^{j}(i+1)p^i - \frac{u(p-1)}{p} + u - 1 \\
&= \tfrac{u(p-1)}{p}\sum_{i=0}^{j}(i+1)p^i + \frac{-up+u+up}{p} - 1 = \frac{u(p-1)}{p}\sum_{i=0}^{j}(i+1)p^i + \frac{u}{p} - 1 \\
&= \tfrac{u(p-1)}{p}[1 + 2p + 3p^2 + \ldots + jp^{j-1} + (j+1)p^j] + \tfrac{u}{p} - 1.
\end{aligned}$$

Agora, pelo Lema 4.2.1, segue que

$$\begin{aligned}
\beta_{(u,j)} &= \tfrac{u(p-1)}{p}\left[\tfrac{(j+2)p^{j+1}(p-1)-(p^{j+2}-1)}{(p-1)^2}\right] + \tfrac{u}{p} - 1 = u\left[(j+2)p^j - \tfrac{(p^{j+2}-1)}{p(p-1)} + \tfrac{1}{p}\right] - 1 \\
&= u\left[(j+2)p^j - \tfrac{(p^{j+2}-1+p-1)}{p(p-1)}\right] - 1 = u\left[(j+2)p^j - \tfrac{p(p^{j+1}+1)-2}{p(p-1)}\right] - 1 \\
&= u\left[(j+2)p^j - \tfrac{(p^{j+1}-1)}{(p-1)}\right] - 1.
\end{aligned}$$

Assim, $|D(\mathbb{K}/\mathbb{Q})| = p^{\beta_{(u,j)}}$*, onde* $\beta_{(u,j)} = u\left[(j+2)p^j - \tfrac{(p^{j+1}-1)}{(p-1)}\right] - 1$*, o que prova o teorema.* ■

Corolário 4.2.1 *[12, corollary 4.1] O discriminante do corpo ciclotômico* $\mathbb{Q}(\zeta_{p^r})$*, onde* p *é um primo ímpar e* r *é um inteiro positivo, é dado por*

$$|D(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})| = p^{\beta_{(p-1,r-1)}},$$

onde $\beta_{(p-1,r-1)} = (p-1)\left[(r+1)p^{r-1} - \tfrac{p^r-1}{p-1}\right] - 1$*.*

Demonstração: *Nas condições do Teorema 4.2.1 temos que* $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = (p-1)p^{r-1}$*, e deste modo* $u = p-1$ *e* $j = r-1$*. Assim, aplicando o resultado obtemos que* $|D(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})| = p^{\beta^{(p-1,r-1)}}$*, onde* $\beta^{(p-1,r-1)} = (p-1)\left[(r+1)p^{r-1} - \tfrac{p^r-1}{p-1}\right] - 1$*, o que prova o corolário.* ■

Corolário 4.2.2 *[16, corolário 14] Se* $\mathbb{K}$ *é um subcorpo de* $\mathbb{Q}(\zeta_{p^r})$ *com* $[\mathbb{K} : \mathbb{Q}] = 3$*, ou seja,* $\mathbb{K}$ *é uma cúbica, então* $D(\mathbb{K}/\mathbb{Q}) = p^2$ *se* $p \neq 3$ *ou* $D(\mathbb{K}/\mathbb{Q}) = 81$ *se* $p = 3$*.*

Demonstração: *Temos que* $[\mathbb{K} : \mathbb{Q}] = 3 = up^j$*, e deste modo se* $p \neq 3$*, nas condições do Teorema 4.2.1 temos que* $u = 3$ *e* $j = 0$*. Assim, aplicando o resultado obtemos que* $|D(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})| = p^{\beta_{(3,0)}}$*, onde* $\beta_{(3,0)} = 3[2p^0 - \tfrac{p^1-1}{p-1}] - 1 = 2$*. Portanto* $|D(\mathbb{K}/\mathbb{Q})| = p^2$*. Agora, se* $p = 3$*, então* $u = 1$ *e* $j = 1$*. Assim,* $|D(\mathbb{K}/\mathbb{Q})| = 3^{\beta^{(1,1)}}$*, onde* $\beta^{(1,1)} = [3.3 - \tfrac{3^2-1}{3-1}] - 1 = 4$*. Portanto* $|D(\mathbb{K}/\mathbb{Q})| = 3^4 = 81$*.* ■

Corolário 4.2.3 *[12, corollary 4.2] Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_p)$, onde p é um primo ímpar, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$|D(\mathbb{K}/\mathbb{Q})| = p^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Demonstração: *Novamente nas condições do Teorema 4.2.1 temos que $r = 1$, e deste modo $j = 0$ e $[\mathbb{K} : \mathbb{Q}] = u$. Aplicando o resultado obtido temos que $|D(\mathbb{K}/\mathbb{Q})| = p^{u(2-\frac{p-1}{p-1})-1} = p^{u(2-1)-1} = p^{u-1} = p^{[\mathbb{K}:\mathbb{Q}]-1}$, o que prova o corolário.* ∎

Observação 4.2.1 *Pelo Corolário 4.2.3 temos que o discriminante do corpo $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ é dado por*

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

Exemplo 4.2.1 *Se $n = 3^2$, então o grupo G tem ordem $(p-1)p^{r-1} = 2.3 = 6$ e é dado por $G = (\mathbb{Z}/9\mathbb{Z})^* = \{1, 2, 4, 5, 7, 8\}$. O grupo de Galois de $\mathbb{Q}(\zeta_9)$ sobre $\mathbb{Q}$ é $\{\sigma_1, \sigma_2, \sigma_4, \sigma_5, \sigma_7, \sigma_8\}$. Caracterizamos o grupo $\hat{G}$ pela tabela :*

	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5	
$2^0 = 1$	*1*	*1*	*1*	*1*	*1*	*1*	σ_1
$2^1 = 2$	*1*	ζ_6	ζ_6^2	*-1*	ζ_6^4	ζ_6^5	σ_2
$2^2 = 4$	*1*	ζ_6^2	ζ_6^4	*1*	ζ_6^2	ζ_6^4	σ_4
$2^3 = 8$	*1*	*-1*	*1*	*-1*	*1*	*-1*	σ_8
$2^4 = 7$	*1*	ζ_6^4	ζ_6^2	*1*	ζ_6^4	ζ_6^2	σ_7
$2^5 = 5$	*1*	ζ_6^5	ζ_6^4	*-1*	ζ_6^2	ζ_6	σ_5
f_{χ_i}	*1*	*3*	3^2	*3*	3^2	*3*	

Os subgrupos multiplicativos do grupo de Galois são:

$$H_0 = \{\sigma_1\} \qquad H_2 = \{\sigma_1, \sigma_4, \sigma_7\}$$
$$H_1 = \{\sigma_1, \sigma_8\} \quad H_3 = G = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8, \sigma_7, \sigma_5\}.$$

Assim, temos que $\mathbb{K}_0 = \mathbb{Q}(\zeta_9)$ é fixado por H_0, $\mathbb{K}_1$ é fixado por H_1, $\mathbb{K}_2$ é fixado por H_2 e $\mathbb{Q}$ é fixado por G. Dessa forma os caracteres associados a $\mathbb{K}_0$ são $H_0^\perp = \hat{G}$, a $\mathbb{K}_1$ são $H_1^\perp = \{\chi_0, \chi_2, \chi_4\}$, a $\mathbb{K}_2$ são $H_2^\perp = \{\chi_0, \chi_3\}$ e a $\mathbb{Q}$ são $H_3^\perp = \{\chi_0\}$. Agora, para $\mathbb{K}_1$ temos que $[\mathbb{K}_1 : \mathbb{Q}] = 3$, e deste modo nas condições do Teorema 4.2.1 temos que $u = 1$ e $j = 1$. Assim $|D(\mathbb{K}_1/\mathbb{Q})| = 3^{\beta_{(1,1)}}$, onde $\beta_{(1,1)} = (3.3 - \frac{3^2-1}{2}) - 1 = (9-4) - 1 = 4$. Portanto $|D(\mathbb{K}_1/\mathbb{Q})| = 3^4$. Analogamente para $\mathbb{K}_2$ temos que $[\mathbb{K}_2 : \mathbb{Q}] = 2$, e novamente nas condições do Teorema 4.2.1 temos que $u = 2$ e $j = 0$ e segue que $|D(\mathbb{K}_2/\mathbb{Q})| = 3^{\beta_{(2,0)}}$, onde $\beta_{(2,0)} = 2(3.1 - \frac{2}{2}) - 1 = 2 - 1 = 1$. Portanto $|D(\mathbb{K}_2/\mathbb{Q})| = 3$. Para $\mathbb{K}_0 = \mathbb{Q}(\zeta_9)$ podemos aplicar o Corolário 4.2.1 e assim segue que $|D(\mathbb{K}_0/\mathbb{Q})| = 3^{\beta_{(1,1)}}$, onde $\beta_{(1,1)} = 2(3.3 - \frac{3^2-1}{3-1}) - 1 = 2(9-4) - 1 = 9$. Portanto $|D(\mathbb{K}_0/\mathbb{Q})| = 9$.

Exemplo 4.2.2 *Se $n = 3^3$, então o grupo G tem ordem $(p-1)p^{r-1} = 2.3^2 = 18$ e é dado por $G = (\mathbb{Z}/27\mathbb{Z})^* = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$. O grupo de Galois de $\mathbb{Q}(\zeta_{27})$ sobre $\mathbb{Q}$ é dado por $\{\sigma_1, \sigma_2, \sigma_4, \sigma_5, \sigma_7, \sigma_8, \sigma_{10}, \sigma_{11}, \sigma_{13}, \sigma_{14}, \sigma_{16}, \sigma_{17}, \sigma_{19}, \sigma_{20}, \sigma_{22}, \sigma_{23}, \sigma_{25}, \sigma_{26}\}$. O grupo $\hat{G}$ é caracterizado pela tabela abaixo.*

	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5	χ_6	χ_7	χ_8	χ_9	χ_{10}	χ_{11}	χ_{12}	χ_{13}	χ_{14}	χ_{15}	χ_{16}	χ_{17}
2^0=1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$2^1 = 2$	1	ζ_{18}	ζ_{18}^2	ζ_{18}^3	ζ_{18}^4	ζ_{18}^5	ζ_{18}^6	ζ_{18}^7	ζ_{18}^8	-1	ζ_{18}^{10}	ζ_{18}^{11}	ζ_{18}^{12}	ζ_{18}^{13}	ζ_{18}^{14}	ζ_{18}^{15}	ζ_{18}^{16}	ζ_{18}^{17}
$2^2 = 4$	1	ζ_{18}^2	ζ_{18}^4	ζ_{18}^6	ζ_{18}^8	ζ_{18}^{10}	ζ_{18}^{12}	ζ_{18}^{14}	ζ_{18}^{16}	1	ζ_{18}^2	ζ_{18}^4	ζ_{18}^6	ζ_{18}^8	ζ_{18}^{10}	ζ_{18}^{12}	ζ_{18}^{14}	ζ_{18}^{16}
$2^3 = 8$	1	ζ_{18}^3	ζ_{18}^6	-1	ζ_{18}^{12}	ζ_{18}^{15}	1	ζ_{18}^3	ζ_{18}^6	-1	ζ_{18}^{12}	ζ_{18}^{15}	1	ζ_{18}^3	ζ_{18}^6	-1	ζ_{18}^{12}	ζ_{18}^{15}
$2^4 = 16$	1	ζ_{18}^4	ζ_{18}^8	ζ_{18}^{12}	ζ_{18}^{16}	ζ_{18}^2	ζ_{18}^6	ζ_{18}^{10}	ζ_{18}^{14}	1	ζ_{18}^4	ζ_{18}^8	ζ_{18}^{12}	ζ_{18}^{16}	ζ_{18}^2	ζ_{18}^6	ζ_{18}^{10}	ζ_{18}^{14}
$2^5 = 5$	1	ζ_{18}^5	ζ_{18}^{10}	ζ_{18}^{15}	ζ_{18}^2	ζ_{18}^7	ζ_{18}^{12}	ζ_{18}^{17}	ζ_{18}^4	-1	ζ_{18}^{14}	ζ_{18}	ζ_{18}^6	ζ_{18}^1	ζ_{18}^{16}	ζ_{18}^3	ζ_{18}^8	ζ_{18}^{13}
$2^6 = 10$	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}
$2^7 = 20$	1	ζ_{18}^7	ζ_{18}^{14}	ζ_{18}^3	ζ_{18}^{10}	ζ_{18}^{17}	ζ_{18}^6	ζ_{18}^{13}	ζ_{18}^2	-1	ζ_{18}^{16}	ζ_{18}^5	ζ_{18}^{12}	ζ_{18}	ζ_{18}^8	ζ_{18}^{15}	ζ_{18}^{15}	ζ_{18}^4
$2^8 = 13$	1	ζ_{18}^8	ζ_{18}^{16}	ζ_{18}^6	ζ_{18}^{14}	ζ_{18}^4	ζ_{18}^{12}	ζ_{18}^2	ζ_{18}^{10}	1	ζ_{18}^8	ζ_{18}^{16}	ζ_{18}^6	ζ_{18}^{14}	ζ_{18}^4	ζ_{18}^{12}	ζ_{18}^2	ζ_{18}^{10}
$2^9 = 26$	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1
$2^{10} = 25$	1	ζ_{18}^{10}	ζ_{18}^2	ζ_{18}^{12}	ζ_{18}^4	ζ_{18}^{14}	ζ_{18}^6	ζ_{18}^{16}	ζ_{18}^8	1	ζ_{18}^{10}	ζ_{18}^2	ζ_{18}^{12}	ζ_{18}^4	ζ_{18}^{14}	ζ_{18}^6	ζ_{18}^{16}	ζ_{18}^8
$2^{11} = 23$	1	ζ_{18}^{11}	ζ_{18}^4	ζ_{18}^{15}	ζ_{18}^8	ζ_{18}	ζ_{18}^{12}	ζ_{18}^5	ζ_{18}^{16}	-1	ζ_{18}^4	ζ_{18}^{17}	ζ_{18}^{12}	ζ_{18}^7	ζ_{18}^2	ζ_{18}^{15}	ζ_{18}^{10}	ζ_{18}^7
$2^{12} = 19$	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6
$2^{13} = 11$	1	ζ_{18}^{13}	ζ_{18}^8	ζ_{18}^3	ζ_{18}^6	ζ_{18}^{11}	ζ_{18}^6	ζ_{18}	ζ_{18}^{14}	-1	ζ_{18}^4	ζ_{18}^{17}	ζ_{18}^{12}	ζ_{18}^7	ζ_{18}^2	ζ_{18}^{15}	ζ_{18}^{10}	ζ_{18}^5
$2^{14} = 22$	1	ζ_{18}^{14}	ζ_{18}^{10}	ζ_{18}^6	ζ_{18}^2	ζ_{18}^{16}	ζ_{18}^{12}	ζ_{18}^8	ζ_{18}^4	1	ζ_{18}^{14}	ζ_{18}^{10}	ζ_{18}^6	ζ_{18}^2	ζ_{18}^{16}	ζ_{18}^{12}	ζ_{18}^8	ζ_{18}^4
$2^{15} = 17$	1	ζ_{18}^{15}	ζ_{18}^{12}	-1	ζ_{18}^6	ζ_{18}^3	1	ζ_{18}^{15}	ζ_{18}^{12}	-1	ζ_{18}^6	ζ_{18}^3	1	ζ_{18}^{15}	ζ_{18}^{12}	-1	ζ_{18}^6	ζ_{18}^3
$2^{16} = 7$	1	ζ_{18}^{16}	ζ_{18}^{14}	ζ_{18}^{12}	ζ_{18}^{10}	ζ_{18}^8	ζ_{18}^6	ζ_{18}^4	ζ_{18}^2	1	ζ_{18}^{16}	ζ_{18}^{14}	ζ_{18}^{12}	ζ_{18}^{10}	ζ_{18}^8	ζ_{18}^6	ζ_{18}^4	ζ_{18}^2
$2^{17} = 14$	1	ζ_{18}^{17}	ζ_{18}^{16}	ζ_{18}^{15}	ζ_{18}^{14}	ζ_{18}^{13}	ζ_{18}^{12}	ζ_{18}^{11}	ζ_{18}^{10}	-1	ζ_{18}^8	ζ_{18}^7	ζ_{18}^6	ζ_{18}^5	ζ_{18}^4	ζ_{18}^3	ζ_{18}^2	ζ_{18}
f_{χ_i}	1	3^3	3^3	3^2	3^3	3^3	3^2	3^3	3^3	3	3^3	3^3	3^2	3^3	3^3	3^2	3^3	3^3

Os subgrupos multiplicativos do grupo de Galois G são:

$$H_0 = \{\sigma_1\} \qquad H_3 = \{\sigma_1, \sigma_8, \sigma_{10}, \sigma_{26}, \sigma_{19}, \sigma_{17}\}$$
$$H_1 = \{\sigma_1, \sigma_{26}\} \qquad H_4 = \{\sigma_1, \sigma_4, \sigma_{16}, \sigma_{10}, \sigma_{13}, \sigma_{25}, \sigma_{19}, \sigma_{22}, \sigma_7\}$$
$$H_2 = \{\sigma_1, \sigma_{10}, \sigma_{19}\} \quad H_5 = G$$

Assim, temos que $\mathbb{K}_0 = \mathbb{Q}(\zeta_{27})$ é fixado por H_0, $\mathbb{K}_1$ é fixado por H_1, $\mathbb{K}_2$ é fixado por H_2, $\mathbb{K}_3$ é fixado por H_3, $\mathbb{K}_4$ é fixado por H_4 e $\mathbb{Q}$ é fixado por G. Dessa forma os caracteres associados a $\mathbb{K}_0$ são $H_0^\perp = \hat{G}$, a $\mathbb{K}_1$ são $H_1^\perp = \{\chi_0, \chi_2, \chi_4, \chi_6, \chi_8, \chi_{10}, \chi_{12}, \chi_{14}, \chi_{16}\}$, a $\mathbb{K}_2$ são $H_2^\perp = \{\chi_0, \chi_3, \chi_6, \chi_9, \chi_{12}, \chi_{15}\}$, a $\mathbb{K}_3$ são $H_3^\perp = \{\chi_0, \chi_6, \chi_{12}\}$, a $\mathbb{K}_4$ são $H_4^\perp = \{\chi_0, \chi_9, \}$ e a $\mathbb{Q}$ são $H_5^\perp = \{\chi_0\}$. Agora, para $\mathbb{K}_1$ temos que $[\mathbb{K}_1 : \mathbb{Q}] = 9 = 3^2$, e deste modo nas condições do Teorema 4.2.1 temos que $u = 1$ e $j = 2$. Assim segue que $|D(\mathbb{K}_1/\mathbb{Q})| = 3^{\beta_{(1,2)}}$, onde $\beta_{(1,2)} = (4.3^2 - \frac{3^3-1}{2}) - 1 = 22$. Portanto $|D(\mathbb{K}_1/\mathbb{Q})| = 3^{22}$. Para $\mathbb{K}_2$ temos que $[\mathbb{K}_2 : \mathbb{Q}] = 6 = 2.3$, e assim nas condições do Teorema 4.2.1 temos que $u = 2$ e $j = 1$. Assim $|D(\mathbb{K}_2/\mathbb{Q})| = 3^{\beta_{(2,1)}}$, onde $\beta_{(2,1)} = 2(3.3 - \frac{3^2-1}{2}) - 1 = 9$. Portanto $|D(\mathbb{K}_2/\mathbb{Q})| = 3^9$. Analogamente para $\mathbb{K}_3$ temos que $[\mathbb{K}_3 : \mathbb{Q}] = 3$, e deste modo $u = 1$ e $j = 1$. Assim segue que $|D(\mathbb{K}_3/\mathbb{Q})| = 3^{\beta_{(1,1)}}$, onde $\beta_{(1,1)} = (3.3 - \frac{3^2-1}{2}) - 1 = 4$. Finalmente, para $\mathbb{K}_4$ temos que $[\mathbb{K}_4 : \mathbb{Q}] = 2$, e deste modo $u = 2$ e $j = 0$. Assim segue que $|D(\mathbb{K}_4/\mathbb{Q})| = 3^{\beta_{(2,0)}}$, onde $\beta_{(2,0)} = 2(2 - \frac{3-1}{3-1}) - 1 = 1$. Portanto $|D(\mathbb{K}_4/\mathbb{Q})| = 3$. Para $\mathbb{K}_0 = \mathbb{Q}(\zeta_{27})$ podemos aplicar o Corolário 4.2.1 e assim segue

que $|D(\mathbb{K}_0/\mathbb{Q})| = 3^{\beta_{(1,2)}}$, *onde* $\beta_{(1,2)} = 2(4.9 - \frac{3^3-1}{3-1}) - 1 = 2(36-13) - 1 = 45$. *Portanto* $|D(\mathbb{K}_0/\mathbb{Q})| = 3^{45}$.

Corolário 4.2.4 *O discriminante do subcorpo maximal real* $\mathbb{K} = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ *do corpo* $\mathbb{Q}(\zeta_{p^r})$ *sobre* $\mathbb{Q}$ *é dado por*

$$|D(\mathbb{K}/\mathbb{Q})| = p^{\beta_{(\frac{p-1}{2},r-1)}},$$

onde $\beta_{(\frac{p-1}{2},r-1)} = \frac{1}{2}[(r+1)(p-1)p^{r-1} - p^r - 1]$.

Demonstração:

$$\begin{array}{c} \mathbb{Q}(\zeta_{p^r}) \\ |_2 \\ \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1}) \\ |_{\frac{\varphi(p^r)}{2}} \\ \mathbb{Q} \end{array}$$

Temos que

Como $[\mathbb{K} : \mathbb{Q}] = \frac{(p-1)p^{r-1}}{2}$, *pelas hipóteses do Teorema 4.2.1, segue que* $u = \frac{p-1}{2}$ *e* $j = r-1$. *Assim, aplicando o resultado obtemos que* $|D(\mathbb{K}/\mathbb{Q})| = p^{\beta_{(\frac{p-1}{2},r-1)}}$, *onde*

$$\begin{aligned} \beta_{(\frac{p-1}{2},r-1)} &= \tfrac{p-1}{2}\left[(r-1+2)p^{r-1} - \tfrac{p^{r-1+1}-1}{p-1}\right] - 1 \\ &= \tfrac{p-1}{2}\left[(r+1)p^{r-1} - \tfrac{p^r-1}{p-1}\right] - 1 \\ &= \tfrac{r+1}{2}(p-1)p^{r-1} - \tfrac{p^r-1}{2} - 1 \\ &= \tfrac{1}{2}[(r+1)(p-1)p^{r-1} - p^r - 1], \end{aligned}$$

o que prova o corolário. ∎

Observação 4.2.2 *Pelo Corolário 4.2.4 temos que o discriminante do subcorpo* $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ *de* $\mathbb{Q}(\zeta_p)$ *sobre* $\mathbb{Q}$ *é dado por*

$$|D(\mathbb{Q}(\zeta_p + \zeta_p^{-1})/\mathbb{Q})| = p^{\frac{p-3}{2}}.$$

Exemplo 4.2.3 *Para* $n = 3^2$, *o discriminante do subcorpo* $\mathbb{K} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ *do corpo* $\mathbb{Q}(\zeta_9)$ *sobre* $\mathbb{Q}$ *é dado por* $|D(\mathbb{K}/\mathbb{Q})| = 3^{\beta_{(1,1)}}$, *onde* $\beta_{(1,1)} = \frac{1}{2}(3.2.3 - 9 - 1) = \frac{1}{2}(18-10) = \frac{1}{2}(8) = 4$. *Portanto,* $|D(\mathbb{K}/\mathbb{Q})| = 3^4$.

Exemplo 4.2.4 *Para* $n = 3^3$, *o discriminante do subcorpo* $\mathbb{K} = \mathbb{Q}(\zeta_{27} + \zeta_{27}^{-1})$ *do corpo* $\mathbb{Q}(\zeta_{27})$ *sobre* $\mathbb{Q}$ *é dado por* $|D(\mathbb{K}/\mathbb{Q})| = 3^{\beta_{(1,2)}}$, *onde* $\beta_{(1,2)} = \frac{1}{2}(4.2.9 - 27 - 1) = \frac{1}{2}(44) = 22$. *Portanto,* $|D(\mathbb{K}/\mathbb{Q})| = 3^{22}$.

4.3 Discriminante de subcorpos de $\mathbb{Q}(\zeta_{2^r})$

Nesta seção veremos o discriminante de subcorpos de $\mathbb{Q}(\zeta_{2^r})$, onde r é um inteiro positivo. Deste modo, para calcularmos tal discriminante trabalhamos com o grupo dos caracteres de $(\mathbb{Z}/2^r\mathbb{Z})^*$.

Assim, sejam $\mathbb{K}$ um subcorpo de $\mathbb{Q}(\zeta_{2^r})$ e o subgrupo H do grupo de Galois de $\mathbb{Q}(\zeta_{2^r})$ sobre $\mathbb{Q}$, que fixa $\mathbb{K}$. Tomando o subgrupo $X_{\mathbb{K}}$ do grupo dos caracteres de $(\mathbb{Z}/2^r\mathbb{Z})^*$ cujo núcleo contém H temos que o discriminante de $\mathbb{K}$ será o produto dos condutores desses caracteres. Como $\mathbb{Q}(\zeta_{2^r})$ tem grau 2^{r-1}, segue que o subgrupo H do grupo de Galois $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ que fixa $\mathbb{K}$ tem ordem 2^{r-m} e satisfaz uma das seguintes formas:

1. $H \simeq \langle \bar{5}^{2^{m-2}} \rangle$,
2. $H \simeq \langle -\bar{5}^{2^{m-2}} \rangle$,
3. $H \simeq \langle -\bar{1}, \bar{5}^{2^{m-1}} \rangle$.

Lema 4.3.1 *[14, Lema 3.6] Se m é um número inteiro tal que $m > 1$, então*

$$m2^{m-2} + (m-1)2^{m-3} + \ldots + 3.2 + 2.1 = 2^{m-1}(m-1).$$

Demonstração: *Se $x \neq 1$, então*

$$x^m + x^{m-1} + \ldots + x^3 = \frac{x^{m+1} - x^3}{x-1}.$$

Derivando ambos os lados obtemos que

$$mx^{m-1} + (m-1)x^{m-2} + \ldots + 3x^2 = \frac{mx^{m+1} - (m+1)x^m - 2x^3 + 3x^2}{(x-1)^2},$$

para todo $x \neq 1$. Tomando $x = 2$, temos que

$$m2^{m-1} + (m-1)2^{m-2} + \ldots + 12 = m2^{m+1} - (m+1)2^m - 16 + 12.$$

Assim

$$m2^{m-1} + (m-1)2^{m-2} + \ldots + 12 = 2^m(2m - m - 1) - 4,$$

e deste modo

$$m2^{m-1} + (m-1)2^{m-2} + \ldots + 12 + 4 = 2^m(m-1).$$

Assim, dividindo ambos os lados por 2, obtemos que

$$m2^{m-2} + (m-1)2^{m-3} + \ldots + 6 + 2 = 2^{m-1}(m-1),$$

o que prova o lema. ∎

Teorema 4.3.1 *[13, Theorem 3.1] Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_{2^r})$, com $[\mathbb{K}:\mathbb{Q}]=2^{m-1}$, e se H é o subgrupo de $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ que fixa $\mathbb{K}$ e $H \simeq \langle \bar{5}^{2^{m-2}} \rangle$, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$|D(\mathbb{K}/\mathbb{Q})| = 2^{2^{m-1}(m-1)}.$$

Demonstração: *Sejam $H \simeq \langle \bar{5}^{2^{m-2}} \rangle$ e $\chi_{i,l}$ um caracter de Dirichlet associado a $\mathbb{K}$, ou seja, $\chi_{i,l}(\bar{x})=1$, para todo $\bar{x} \in H$. Mas, temos que $\chi_{i,l}(\bar{x})=1$, para todo $\bar{x} \in H$ se, e somente se, $\chi_{i,l}(\bar{5}^{2^{m-2}}) = \zeta_{2^{r-2}}^{l2^{m-2}} = 1$ se, e somente se, $l2^{m-2} \equiv 0 (mod\ 2^{r-2})$. Assim $l \equiv 0 (mod\ 2^{r-m})$, ou seja, $l = k2^{r-m}$, onde $k \in \{1,2,\ldots,2^{m-2}\}$, e deste modo os caracteres associados a $\mathbb{K}$ são os $\chi_{i,l}$ tais que $i \in \{1,2\}$ e $l \in \{2^{r-m}, 2.2^{r-m}, 3.2^{r-m}, \ldots, 2^{m-2}.2^{r-m}\}$. Portanto, temos que existem $2.2^{m-2} = 2^{m-1}$ caracteres associados a $\mathbb{K}$. Se $l = 2^{r-m}$, então existem $2\frac{2^{m-2}}{2} = 2^{m-2}$ caracteres $\chi_{i,l}$ com condutor 2^m. Se $l = 2^{r-m+1}$ e $k = 2$ ou 2^{m-3}, então existem $2\frac{2^{m-3}}{2}$ caracteres. A tabela abaixo resume esses resultados.*

$mdc(l, 2^r)$	*número de* $\chi_{i,l}$	$f_{\chi_{i,l}}$
2^{r-m}	$2.\frac{2^{m-2}}{2} = 2^{m-2}$	$\frac{2^r}{2^{r-m}} = 2^m$
2^{r-m+1}	$2.\frac{2^{m-3}}{2} = 2^{m-3}$	$\frac{2^r}{2^{r-m+1}} = 2^{m-1}$
$\vdots$	$\vdots$	$\vdots$
2^{r-3}	$2.\frac{2^{m-(m-1)}}{2} = 2$	$\frac{2^r}{2^{r-3}} = 2^3$
2^{r-2} *e* $i=1$	1	2^2
2^{r-2} *e* $i=2$	1	1

Pelo Teorema 4.1.1(Fórmula do condutor discriminante) temos que o discriminante de $\mathbb{K}$ é a menos de sinal, igual ao produto dos condutores dos caracteres $\chi_{i,l}$ que são associados a $\mathbb{K}$. Portanto usando este resultado e a tabela obtemos

$$\begin{aligned}
|D(\mathbb{K}/\mathbb{Q})| &= \prod_{\chi_{i,l} \in X_{\mathbb{K}}} f_{\chi_{i,l}} = 2^{\alpha} = \underbrace{(2^m \ldots 2^m)}_{2^{m-2}} \underbrace{(2^{m-1} \ldots 2^{m-1})}_{2^{m-3}} \ldots (2^3.2^3)2^2.1 \\
&= (2^m)^{2^{m-2}} (2^{m-1})^{2^{m-3}} \ldots (2^3)^2.2^2.1 \\
&= 2^{m2^{m-2}}.2^{(m-1)2^{m-3}} \ldots (2^3)^2.2^2.1 \\
&= 2^{m2^{m-2}+(m-1)2^{m-3}+\ldots+3.2+2.1}.
\end{aligned}$$

Assim, $\alpha = m2^{m-2}+(m-1)2^{m-3}+\ldots+3.2+2.1$. Pelo Lema 4.3.1, segue que $\alpha = 2^{m-1}(m-1)$. Portanto, $|D(\mathbb{K}/\mathbb{Q})| = 2^{2^{m-1}(m-1)}$, o que prova o teorema. ∎

Lema 4.3.2 *Se m é um número inteiro tal que $m > 1$, então*

$$(m+1)2^{m-2} + m2^{m-3} + (m-1)2^{m-4} + \ldots + 3 = m2^{m-1} - 1.$$

Demonstração: *Se $x \neq 1$, então*

$$x^{m+1} + x^m + \ldots + x^3 = \frac{x^{m+2} - x^3}{x - 1}.$$

Derivando ambos os lados temos que

$$(m+1)x^m + mx^{m-1} + \ldots + 3x^2 = \frac{((m+2)x^{m+1} - 3x^2)(x-1) - x^{m+2} + x^3}{(x-1)^2}.$$

Logo,

$$(m+1)x^m + mx^{m-1} + \ldots + 3x^2 = \frac{((m+1)x^{m+2} - (m+2)x^{m+1}) - 2x^3 + 3x^2}{(x-1)^2},$$

para todo $x \neq 1$. Tomando $x = 2$, temos que

$$\begin{aligned}(m+1)2^m + m2^{m-1} + \ldots + 12 &= (m+1)2^{m+2} - (m+2)2^{m+1} - 4 \\ &= 2^{m+1}[2(m+1) - (m+2)] - 4 \\ &= 2^{m+1}m - 4 = 2^2(m2^{m-1} - 1).\end{aligned}$$

Assim, temos que

$$(m+1)2^m + m2^{m-1} + \ldots + 12 = 2^2(m2^{m-1} - 1).$$

Portanto, dividindo ambos os lados por 2^2 obtemos que

$$(m+1)2^{m-2} + m2^{m-3} + \ldots + 3 = m2^{m-1} - 1,$$

o que prova o lema. ∎

Teorema 4.3.2 *[13, Theorem 3.1] Seja $\mathbb{K}$ um subcorpo de $\mathbb{Q}(\zeta_{2^r})$ com $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$. Se H é o subgrupo de $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ que fixa $\mathbb{K}$ e $H \simeq \langle -\bar{5}^{2^{m-2}} \rangle$ ou $H \simeq \langle \bar{-1}, \bar{5}^{2^{m-1}} \rangle$, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$|D(\mathbb{K}/\mathbb{Q})| = 2^{m2^{m-1}-1}.$$

Demonstração:

- *Se $H \simeq \langle -\bar{5}^{2^{m-2}} \rangle$ e se $\chi_{i,l} \in X_{\mathbb{K}}$, então $\chi_{i,l}(\bar{x}) = 1$ para todo $\bar{x} \in H$, se, e somente se,*

$$\chi_{i,l}(-\bar{5}^{2^{m-2}}) = (-1)^i \zeta_{2^{r-2}}^{l2^{m-2}} = 1,$$

  se, e somente se,

$$\zeta_{2^{r-2}}^{l2^{m-2}} = (-1)^i.$$

Se $i = 1$, *então* $\zeta_{2^{r-2}}^{l2^{m-2}} = -1$, *e assim* $l2^{m-2} \equiv 0(mod\ \frac{2^{r-2}}{2} = 2^{r-3})$, *ou seja,* $l2^{m-2} = 2^{r-3}t$, *para algum* $t \in \mathbb{Z}$. *Assim* $l = 2^{r-m-1}t$, *ou seja,* $l \equiv 0(mod\ 2^{r-m-1})$ *e deste modo* $l \in \{2^{r-m}, 3.2^{r-m-1}, 5.2^{r-m-1}, \ldots, (2^{m-1}-1)2^{r-m-1}\}$, *e neste caso temos que existem* $\frac{2^{m-1}-1+1}{2} = 2^{m-2}$ *caracteres associados a* $\mathbb{K}$. *Se* $i = 2$, *então* $\zeta_{2^{r-2}}^{l2^{m-2}} = 1$, *e assim* $l2^{m-2} \equiv 0(mod\ 2^{r-2})$, *ou seja,* $l2^{m-2} = 2^{r-2}t$, *para algum* $t \in \mathbb{Z}$. *Assim* $l = 2^{r-m}t$, *ou seja,* $l \equiv 0(mod\ 2^{r-m})$ *e deste modo* $l \in \{2^{r-m}, 2.2^{r-m}, 3.2^{r-m}, \ldots, 2^{m-2}2^{r-m}\}$, *e neste caso temos que existem* 2^{m-2} *caracteres. Assim, no total temos* $2.2^{m-2} = 2^{m-1}$ *caracteres associados a* $\mathbb{K}$. *A tabela abaixo nos ajudará a calcular o discriminante, para isto usaremos novamente a fórmula do condutor discriminante.*

$mdc(l, 2^r)$	*número de* $\chi_{i,l}$	$f_{\chi_{i,l}}$
2^{r-m-1}	2^{m-2}	2^{m+1}
2^{r-m}	2^{m-3}	2^m
2^{r-m+1}	2^{m-4}	2^{m-1}
2^{r-m+2}	2^{m-5}	2^{m-2}
$\vdots$	$\vdots$	$\vdots$
2^{r-3}	*1*	2^3

Assim,

$$|D(\mathbb{K}/\mathbb{Q})| = 2^{\alpha} = 2^{(m+1)2^{m-2}}2^{m2^{m-3}}2^{(m-1)2^{m-1}}2^3 2^0 = 2^{(m+1)2^{m-2}+m2^{m-3}+(m-1)2^{m-1}+\ldots+3},$$

onde $\alpha = (m+1)2^{m-2} + m2^{m-3} + (m-1)2^{m-1} + \ldots + 3$. *Pelo Lema 4.3.2, temos que* $\alpha = m2^{m-1} - 1$. *Portanto,* $|D(\mathbb{K}/\mathbb{Q})| = 2^{m2^{m-1}-1}$.

- *Se* $H \simeq \langle \bar{-1}, \bar{5}^{2^{m-1}} \rangle$ *e se* $\chi_{i,l} \in X_{\mathbb{K}}$, *então* $\chi_{i,l}(\bar{x}) = 1$ *para todo* $\bar{x} \in H$, *se, e somente se,*

$$\chi_{i,l}(\bar{-1}) = \chi_{i,l}(\bar{5}^{2^{m-1}}) = 1$$

se, e somente se,

$$(-1)^i = \zeta_{2^{r-2}}^{l2^{m-1}} = 1,$$

se, e somente se,

$$i = 2 \ e\ l \equiv 0(mod\ 2^{r-m-1}).$$

Assim, $i = 2$ *e* $l \in \{2^{r-m-1}, 2.2^{r-m-1}, 3.2^{r-m-1}, \ldots, 2^{m-1}2^{r-m-1}\}$. *Novamente usamos a*

fórmula do condutor discriminante e a tabela abaixo.

$mdc(l, 2^r)$	*número de* $\chi_{i,l}$	$f_{\chi_{i,l}}$
2^{r-m-1}	2^{m-2}	2^{m+1}
2^{r-m}	2^{m-3}	2^m
2^{r-m+1}	2^{m-4}	2^{m-1}
2^{r-m+2}	2^{m-5}	2^{m-2}
$\vdots$	$\vdots$	$\vdots$
2^{r-3}	*1*	2^3
2^{r-2}	*1*	*1*

Assim,

$$|D(\mathbb{K}/\mathbb{Q})| = 2^{\alpha} = 2^{(m+1)2^{m-2}} 2^{m2^{m-3}} 2^{(m-1)2^{m-1}} 2^3 2^0 = 2^{(m+1)2^{m-2}+m2^{m-3}+(m-1)2^{m-1}+\ldots+3},$$

onde $\alpha = (m+1)2^{m-2} + m2^{m-3} + (m-1)2^{m-1} + \ldots + 3$. *Analogamente ao caso anterior obtemos que* $\alpha = m2^{m-1} - 1$. *Portanto,* $|D(\mathbb{K}/\mathbb{Q})| = 2^{m2^{m-1}-1}$, *o que prova o teorema.* ■

Corolário 4.3.1 *Se* $\mathbb{K}$ *é um subcorpo de* $\mathbb{Q}(\zeta_{2^r})$, *com* $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$, *e se* H *é o subgrupo de* $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ *que fixa* $\mathbb{K}$ *e* $H \simeq \langle \bar{5}^{2^{m-2}} \rangle$, *então o corpo fixo por* H *é* $\mathbb{K} = \mathbb{Q}(\zeta_{2^m})$.

Demonstração: *Seja* $\sigma_{\bar{5}^{2^{m-2}}}$ *o automorfismo gerador de* H. *Pela Proposição 3.4.1, temos que* $5^{2^{m-2}} \equiv 1 (mod\ 2^m)$, *ou seja,* $5^{2^{m-2}} = 1 + 2^m k$, *para algum* $k \in \mathbb{Z}$. *Assim* $\sigma_{5^{2^{m-2}}}(\zeta_{2^m}) = \zeta_{2^m}^{1+2^m k} = \zeta_{2^m}$, *e deste modo o corpo fixo por* H *é* $\mathbb{Q}(\zeta_{2^m})$, *o que prova o corolário.* ■

Corolário 4.3.2 *Seja* $\mathbb{K}$ *um subcorpo de* $\mathbb{Q}(\zeta_{2^r})$, *com* $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$. *Se* H *é o subgrupo de* $Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ *que fixa* $\mathbb{K}$ *e* $H \simeq \langle -\bar{5}^{2^{m-2}} \rangle$ *ou* $H \simeq \langle -\bar{1}, \bar{5}^{2^{m-1}} \rangle$, *então o corpo fixo por* H *é* $\mathbb{K} \neq \mathbb{Q}(\zeta_{2^m})$.

Demonstração: *Seja* $\sigma_{-\bar{5}^{2^{m-2}}}$ *o automorfismo gerador de* H. *Pela Proposição 3.4.1, temos que* $-\bar{5}^{2^{m-2}} \not\equiv 1 (mod\ 2^m)$, *ou seja,* $-\bar{5}^{2^{m-2}} \neq 1 + 2^m k$, *para todo* $k \in \mathbb{Z}$. *Assim* $\sigma_{-\bar{5}^{2^{m-2}}}(\zeta_{2^m}) \neq \zeta_{2^m}^{1+2^m k} = \zeta_{2^m}$, *e deste modo* H *não fixa* ζ_{2^m}. *Portanto, o corpo fixo por* $H \simeq \langle \bar{5}^{2^{m-2}} \rangle$ *é diferente de* $\mathbb{Q}(\zeta_{2^m})$. *Analogamente, tomando* $\sigma_{-\bar{1},\bar{5}^{2^{m-1}}}$ *temos o resultado.* ■

Corolário 4.3.3 *[13, Theorem 3.2] Se* $\mathbb{K} = \mathbb{Q}(\zeta_{2^m})$ *é um subcorpo de* $\mathbb{Q}(\zeta_{2^r})$ *tal que* $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$, *então o discriminante de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por* $|D(\mathbb{K}/\mathbb{Q})| = 2^{2^{m-1}(m-1)}$.

Demonstração: *Se* $\mathbb{K} = \mathbb{Q}(\zeta_{2^m})$, *então pelo Corolário 4.3.1, temos que* $\mathbb{K}$ *é fixado por* $H \simeq \langle \bar{5}^{2^{m-2}} \rangle$. *Logo, pelo Teorema 4.3.1, segue que* $|D(\mathbb{K}/\mathbb{Q})| = 2^{2^{m-1}(m-1)}$, *o que prova o corolário.* ■

Corolário 4.3.4 *[13, Theorem 3.2] Se $\mathbb{K} \neq \mathbb{Q}(\zeta_{2^m})$ é um subcorpo de $\mathbb{Q}(\zeta_{2^r})$ tal que $[\mathbb{K}:\mathbb{Q}] = 2^{m-1}$, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por $|D(\mathbb{K}/\mathbb{Q})| = 2^{m2^{m-1}-1}$.*

Demonstração: *Se $\mathbb{K} \neq \mathbb{Q}(\zeta_{2^m})$, então pelo Corolário 4.3.2, temos que $\mathbb{K}$ é fixado por $H \simeq \langle -\bar{5}^{2^{m-2}} \rangle$ ou $H \simeq \langle -\bar{1}, \bar{5}^{2^{m-1}} \rangle$. Assim, pelo Teorema 4.3.2, segue que $|D(\mathbb{K}/\mathbb{Q})| = 2^{m2^{m-1}-1}$, o que prova o corolário.* ■

Exemplo 4.3.1 *Se $n = 2^3$, então o grupo G tem ordem $2^{r-1} = 2^2 = 4$ e é dado por $G = (\mathbb{Z}/8\mathbb{Z})^* = \{1,3,5,7\}$. O grupo de $Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ é $\{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$. Além disso, temos que $\bar{-}1 = 7$ e assim segue que $1 = \bar{-}1^2$, $3 = \bar{-}1^3$, $5 = \bar{5}^4$ e $7 = \bar{-}1$. Portanto $G \simeq \langle \bar{-}1, \bar{5}^4 \rangle$. Caracterizamos o grupo $\hat{G}$ pela tabela:*

	χ_0	χ_1	χ_2	χ_3	
$7^1 = 7$	*1*	ζ_4	*-1*	ζ_4^3	σ_7
$7^2 = 1$	*1*	*-1*	*1*	*-1*	σ_1
$7^3 = 3$	*1*	ζ_4^3	*-1*	ζ_4	σ_3
$5^4 = 5$	*1*	*1*	*1*	*1*	σ_5
f_{χ_i}	*1*	*1*	*1*	*1*	

Os subgrupos multiplicativos do grupo de Galois são:

$$H_0 = \{\sigma_5\} \simeq \langle \bar{5}^2 \rangle$$
$$H_1 = \{\sigma_1, \sigma_5\} \simeq \langle \bar{-}1, \bar{5}^4 \rangle$$
$$H_2 = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\} \simeq \langle \bar{-}1, \bar{5}^4 \rangle.$$

Assim, temos que $\mathbb{K}_0 = \mathbb{Q}(\zeta_8)$ é fixado por $H_0 \simeq \langle \bar{5}^2 \rangle$, $\mathbb{K}_1$ é fixado por $H_1 \simeq \langle \bar{-}1, \bar{5}^4 \rangle$ e $\mathbb{Q}$ é fixado por G. Dessa forma os caracteres associados a $\mathbb{K}_0$ são $H_0^\perp = \hat{G}$, a $\mathbb{K}_1$ são $H_1^\perp = \{\chi_0, \chi_2\}$ e a $\mathbb{K}_2$ é $H_2^\perp = \{\chi_0\}$. Agora, para $\mathbb{K}_1$ temos que $[\mathbb{K}_1 : \mathbb{Q}] = 2$, e deste modo nas condições do Teorema 4.3.2 segue que $m = 2$. Como $H_1 \simeq \langle \bar{-}1, \bar{5}^4 \rangle$ segue que $|D(\mathbb{K}_1/\mathbb{Q})| = 2^{m2^{m-1}-1} = 2^{2.2-1} = 2^3$. Portanto $|D(\mathbb{K}_1/\mathbb{Q})| = 2^3$. Para $\mathbb{K}_0 = \mathbb{Q}(\zeta_8)$ podemos aplicar o Corolário 4.3.3 e assim segue que $|D(\mathbb{K}_0/\mathbb{Q})| = 2^{2^{m-1}(m-1)} = 2$. Portanto $|D(\mathbb{K}_0/\mathbb{Q})| = 2$.

Corolário 4.3.5 *O discriminante do subcorpo $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ do corpo $\mathbb{Q}(\zeta_{2^r})$ sobre $\mathbb{Q}$ é dado por*

$$|D(\mathbb{K}/\mathbb{Q})| = 2^{(r-1)2^{r-2}-1}.$$

Demonstração:

Temos que

$$\begin{array}{c} \mathbb{Q}(\zeta_{2^r}) \\ |_2 \\ \mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1}) \\ |_{2^{r-2}} \\ \mathbb{Q} \end{array}$$

Como $[\mathbb{Q}(\zeta_{2^r}):\mathbb{Q}]=2^{r-1}$ *e* $[\mathbb{Q}(\zeta_{2^r}):\mathbb{K}]=2$ *segue que* $[\mathbb{K}:\mathbb{Q}]=2^{r-2}$. *Assim, nas condições do Corolário 4.3.4, temos* $m=r-1$ *e* $\mathbb{K}=\mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1})\neq\mathbb{Q}(\zeta_{2^m})$, *uma vez que* $\mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1})$ *é o subcorpo real. Assim, o discriminante de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por* $|D(\mathbb{K}/\mathbb{Q})|=2^{m2^{m-1}-1}=2^{(r-1)2^{r-2}-1}$, *o que prova o corolário.* ∎

Exemplo 4.3.2 *O discriminante do subcorpo* $\mathbb{K}=\mathbb{Q}(\zeta_2+\zeta_2^{-1})$ *do corpo* $\mathbb{Q}(\zeta_2)$ *sobre* $\mathbb{Q}$ *é dado por* $|D(\mathbb{K}/\mathbb{Q})|=2^{-1}=1/2$.

4.4 Discriminante de corpos de números abelianos

Nesta seção veremos o discriminante de corpos de números abelianos. Para isso, seja $\mathbb{K}$ um corpo de números abeliano. Pelo Teorema de Kroenecker-Weber, temos que o corpo $\mathbb{K}$ está contido em algum corpo ciclotômico $\mathbb{Q}(\zeta_m)$. No caso de corpos de números não abelianos, não temos conhecimento de um processo para o cálculo de seu discriminante.

Definição 4.4.1 *Seja* $\mathbb{K}$ *um corpo de números abeliano. O menor inteiro* m *tal que* $\mathbb{K}\subseteq\mathbb{Q}(\zeta_m)$ *é chamado de condutor do corpo* $\mathbb{K}$.

Seja $H_{\mathbb{K}}$ o subgrupo do grupo de Galois $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ que fixa $\mathbb{K}$. Como $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})\simeq(\mathbb{Z}/m\mathbb{Z})^*$, segue que $H_{\mathbb{K}}$ pode ser visto como um subgrupo de $(\mathbb{Z}/m\mathbb{Z})^*$. Seja $X_{\mathbb{K}}$ o grupo dos caracteres associados a $\mathbb{K}$, isto é, o conjunto dos elementos de $(\mathbb{Z}/m\mathbb{Z})^*$ cujo núcleo contém $H_{\mathbb{K}}$. Assim, $X_{\mathbb{K}}$ é um subgrupo de $\widehat{(\mathbb{Z}/m\mathbb{Z})^*}$, isomorfo ao grupo de Galois $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Portanto $[\mathbb{Q}(\zeta_m):\mathbb{Q}]=|X_{\mathbb{K}}|$, onde o módulo denota o número de elementos do conjunto. Para o cálculo do discriminante de $\mathbb{K}$, novamente veremos que a idéia de contagem de quantos caracteres existem para cada valor do condutor também será utilizada.

Lema 4.4.1 *[15, Lemma 3] Se* $A_1,A_2,\ldots,A_n$ *são conjuntos e* $B_r=\sum_{i_k=1,\ldots,n}|A_{i_1}\cap A_{i_r}|$, *para* $r=1,\ldots,n$ *e* $i_j<i_{j+1}$, *então*

$$|A_1\cup\ldots\cup A_n|=\sum_{k=1}^{n}(-1)^{k+1}B_k.$$

Demonstração: *A demonstração será feita por indução sobre n. Se $n = 1$, o resultado é válido. Se $n = 2$, então $|A_1 \cup A_2| = |A_{1_1} \cap A_{1_2}| + |A_{2_1} \cap A_{2_2}|$. Para $n > 2$, suponhamos, sem perda de generalidade, que $A_1 \cap A_j = \emptyset$, para todo $j = 2, \ldots, n$. Assim, $|A_1 \cup \ldots \cup A_n| = |A_1| + |A_2 \cup \ldots \cup A_n|$. Por hipótese de indução, temos que $|A_2 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} C_k$, onde $C_r = \sum_{i_k, i_r} |A_{i_1} \cap \ldots \cap A_{i_r}|$, para $r = 1, \ldots, n-1$ e $i_k = 2, \ldots, n$. Mas, como $A_1 \cap A_j = \emptyset$, para todo $j = 2, \ldots, n$, segue que $\sum_{i_k=2,\ldots,n} |A_{i_1} \cap \ldots \cap A_{i_r}| = \sum_{i_k=1,\ldots,n} |A_{i_1} \cap \ldots \cap A_{i_r}|$, pois quando $i_1 = 1$ temos que $A_{i_1} \cap \ldots \cap A_{i_r} = \emptyset$. Assim $|A_{i_1} \cap \ldots \cap A_{i_r}| = 0$, e portanto, $|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} B_k$, o que prova o lema.* ■

Sejam $\mathbb{K}$ um corpo de números abeliano contido no corpo ciclotômico $\mathbb{Q}(\zeta_m)$. Pela Proposição 3.2.5 temos que $X_{\mathbb{K}} \subseteq X_{\mathbb{Q}(\zeta_m)}$, e deste modo os condutores dos caracteres de $X_{\mathbb{K}}$ são divisores de m. Para o cálculo do discriminante de $\mathbb{K}$ teremos que determinar o número de caracteres de $X_{\mathbb{K}}$ cujo condutor é d, para cada d divisor de m. O conjunto $X_{\mathbb{K} \cap \mathbb{Q}(\zeta_d)}$ consiste exatamente de todos os caracteres de $X_{\mathbb{K}}$ cujo condutor divide d, e deste modo os caracteres de $X_{\mathbb{K}}$ de condutor d, pertencem a $X_{\mathbb{K} \cap \mathbb{Q}(\zeta_d)}$, cuja ordem é $[\mathbb{K} \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}]$. Assim, o número de caracteres de $\mathbb{K}$ que tem condutor d é $[\mathbb{K} \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - n(d)$, onde $n(d)$ é o número de caracteres de $X_{\mathbb{K}}$ cujo condutor é um divisor próprio de d. Se l é um divisor próprio de d, então l é um divisor de d/p, para algum p primo divisor de d. Assim, um caracter χ associado a $\mathbb{K}$ tem condutor l, se, e somente se, $\chi \in \bigcup_{p|d} X_{\mathbb{K} \cap \mathbb{Q}(\zeta_{d/p})}$. Por outro lado, $n(d) = |\bigcup_{p|d} X_{\mathbb{K} \cap \mathbb{Q}(\zeta_{d/p})}|$. Assim, o número de caracteres associados a $\mathbb{K}$ de condutor d é $[\mathbb{K} \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - |\bigcup_{p|d} X_{\mathbb{K} \cap \mathbb{Q}(\zeta_{d/p})}|$. Logo, pela fórmula do condutor discriminante, temos que se $\mathbb{K}$ é um corpo de números abeliano de condutor m, então

$$|D(\mathbb{K}/\mathbb{Q})| = \prod_{d|m} d^{\alpha_d}, \text{ onde } \alpha_d = [\mathbb{K} \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - |\bigcup_{p|d} X_{\mathbb{K} \cap \mathbb{Q}(\zeta_{d/p})}| .$$

O nosso objetivo agora é vermos um método para simplificar esta fórmula.

Lema 4.4.2 *[14, Lema 3.10] Se $d = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, então*

$$|\bigcup_{p|d} X_{\mathbb{K} \cap \mathbb{Q}(\zeta_{d/p})}| = \sum_{i=1}^{r} |X_{\mathbb{K} \cap \mathbb{Q}(\zeta_{d/p})}| - \sum_{i_1, i_2 = 1}^{r} |X_{\mathbb{K} \cap \mathbb{Q}(\zeta_{d/p_{i_1} p_{i_2}})}| + \ldots + (-1)^{n+1} |X_{\mathbb{K} \cap \mathbb{Q}(\zeta_{d/p_1 \ldots p_n})}|,$$

onde $i_1 < i_2$.

Demonstração: *Segue do ítem 2 da Prosição 3.2.5, do Corolário 3.2.1 e do Lema 4.4.1* ■

Teorema 4.4.1 *[15, Theorem 1] Se $\mathbb{K}$ é um corpo de números abeliano de condutor m, onde $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, então*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\beta_i}},$$

onde $\beta_i = \sum_{n=1}^{\alpha_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^n}) : \mathbb{Q}]$.

Demonstração: *Seja d um divisor de m, onde $d = p_1^{t_1} p_2^{t_2} \dots p_n^{t_n}$, com $0 \leq t_i \leq \alpha_i$. O número de caracteres associados a $\mathbb{K}$ de condutor d é*

$$[\mathbb{K} \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - |\bigcup_{p|d} X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p})}|,$$

onde p é um primo ímpar. Mas pelo Lema 4.4.2, temos que

$$\begin{aligned}[\mathbb{K} \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - |\bigcup_{p|d} X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p})}| &= |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)}| - \sum_i |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p})}| - \sum_{i_1,i_2} |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p_{i_1}p_{i_2}})}| - \dots \\ &\quad -(-1)^{n+1} |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p_1\dots p_n})}| = |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)}| - |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p_1})}| \\ &\quad - |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p_1p_2})}| - \dots - (-1)^{n+1} |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p_1\dots p_n})}|.\end{aligned}$$

Assim, $|D(\mathbb{K}/\mathbb{Q})| = \prod_{d|m} d^{\alpha_d}$, onde

$$\alpha_d = |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)}| - |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p_1})}| - |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p_1p_2})}| - \dots - (-1)^{n+1} |X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{d/p_1\dots p_n})}|.$$

Dessa forma, $|D(\mathbb{K}/\mathbb{Q})| = \prod_{d|m} h_d^{|X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)}|}$, e temos as seguintes possibilidades para h_d :

1. *Se $d = p_1^{t_1} p_2^{t_2} \dots p_n^{t_n}$, onde $0 \leq t_i \leq \alpha_i$, para $i = 1, 2, \dots, k$, então*

$$\begin{aligned}h_d &= d\left(\prod_{i=1}^{n} p_i d\right)^{-1} \left(\prod_{i,j=1}^{n} p_i p_j d\right) \dots \left(\prod_{i_1\dots i_n=1}^{n} p_{i_1} \dots p_{i_k} d\right)^{(-1)k+1} \\ &= d^{\sum_{i=0}^{n}(-1)^i \binom{k}{i}} \prod_{i=1}^{k} p_i^{\sum_{i=0}^{n}(-1)^i \binom{k-1}{i}} = 1.\end{aligned}$$

2. *Se $d = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$, onde $t_{i_1} = \alpha_{i_1}$ para algum i_1 e $0 \leq t_i \leq \alpha_i$, para $i \neq i_1$, então*

$$\begin{aligned}h_d &= d\left(\prod_{j=2}^{k} p_{i_j} d\right)^{-1} \left(\prod_{i,j=2}^{k} p_i p_j d\right) \dots \left(\prod_{i_1\dots i_k=2}^{k} p_{i_1} \dots p_{i_{k-1}} d\right)^{(-1)k} \\ &= d^{\sum_{i=0}^{k-1}(-1)^i \binom{k-1}{i}} \prod_{i=1}^{k} p_i^{\sum_{i=0}^{k-1}(-1)^i \binom{k-2}{i}} = 1.\end{aligned}$$

Analogamente, se $t_{i_1} = \alpha_{i_1}$, $t_{i_2} = \alpha_{i_2}, \ldots, t_{i_s} = \alpha_{i_s}$, *onde* $0 \leq t_i \leq \alpha_i$, *para* $i \neq i_1, i_2, \ldots, i_s$ *e* $2 \leq s \leq k-2$, *temos* $h_d = 1$.

3. *Se* $t_{i_1} = \alpha_{i_1}$, $t_{i_2} = \alpha_{i_2}, \ldots, t_{i_s} = \alpha_{i_s}$, *onde* $0 \leq t_i \leq \alpha_i$, *para* $i \neq i_1, i_2, \ldots, i_s$ *e* $s = k-1$, *ou seja,* $d = m/p_i^n$, *para* $1 \leq n\alpha_i$, $1 \leq j \leq k$, *temos que* $h_d = d(p_i d)^{-1} = p_i^{-1}$.

4. *Se* $t_i = \alpha_i$, *para* $i = 1, 2, \ldots, k$, *ou seja,* $d = m$ *então* $h_d = m$.

Resumindo, temos

$$h_d = \begin{cases} m & se \;\; d = m, \\ p_i^{-1} & se \;\; d = mp_i^n, \; para \; 1 \leq n \leq \alpha_i \; e \; 1 \leq i \leq k, \\ 1 & se \;\; d \neq m \; e \; d \neq mp_i^n, \; para \; 1 \leq n \leq \alpha_i \; e \; 1 \leq i \leq k. \end{cases}$$

Assim,

$$\begin{aligned} |D(\mathbb{K}/\mathbb{Q})| &= \prod_{d|m} h_d^{|X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)|}} = h_m^{|X_{\mathbb{K}\cap\mathbb{Q}(\zeta_d)|}} \prod_{i=1}^{k} \left(\prod_{n=1}^{\alpha_i} h_{m/p_i^n}^{|X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{p_i^n})|}} \right) = m^{[\mathbb{K}:\mathbb{Q}]} \prod_{i=1}^{k} \left(\prod_{n=1}^{\alpha_i} p_i^{-|X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{p_i^n})|}} \right) \\ &= m^{[\mathbb{K}:\mathbb{Q}]} \prod_{i=1}^{k} \left(p_i^{-\sum_{n=1}^{\alpha_i} | \, X_{\mathbb{K}\cap\mathbb{Q}(\zeta_{p_i^n})} \, |} \right) = m^{[\mathbb{K}:\mathbb{Q}]} \prod_{i=1}^{k} \left(p_i^{-\sum_{n=1}^{\alpha_i} [\mathbb{K}\cap\mathbb{Q}(\zeta_{m/p_i^n}) : \mathbb{Q}]} \right) \\ &= \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{k}, \\ &\quad \prod_{i=1}^{} p_i^{\beta_i} \end{aligned}$$

onde $\beta_i = \sum_{n=1}^{\alpha_i} [\mathbb{K}\cap\mathbb{Q}(\zeta_{m/p_i^n}) : \mathbb{Q}]$, *o que prova o teorema.* ∎

Corolário 4.4.1 *[14, Corolário 3.5] Se* $\mathbb{K}$ *é um subcorpo de* $\mathbb{Q}(\zeta_{p^r})$ *com* $[\mathbb{K} : \mathbb{Q}] = up^j$, *onde* p *é um primo ímpar,* r *um inteiro positivo,* u *um divisor de* $(p-1)$ *e* $0 < j \leq r-1$, *então o discriminante de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por*

$$|D(\mathbb{K}/\mathbb{Q})| = p^{\beta_{(u,j)}},$$

onde $\beta_{(u,j)} = u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}] - 1$.

Demonstração: *Como* $[\mathbb{K} : \mathbb{Q}] = up^j$, *segue que o menor inteiro* m *tal que* $\mathbb{K} \subset \mathbb{Q}(\zeta_m)$ *é* $m = p^{j+1}$. *Assim, pelo Teorema 4.4.1, temos que*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{k}, \\ \prod_{i=1}^{} p_i^{\beta}$$

onde $\beta = \sum_{n=1}^{\alpha_{j+1}} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p^n}) : \mathbb{Q}]$. *Mas, temos que*

$$\sum_{n=1}^{\alpha_{j+1}} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p^n}) : \mathbb{Q}] = \sum_{n=1}^{\alpha_{j+1}} [\mathbb{K} \cap \mathbb{Q}(\zeta_{p^{j+1}/p^n}) : \mathbb{Q}] = \sum_{n=0}^{\alpha_j} [\mathbb{K} \cap \mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}].$$

Como $[\mathbb{K} \cap \mathbb{Q}(\zeta_{p^0}) : \mathbb{Q}] = 1$, $[\mathbb{K} \cap \mathbb{Q}(\zeta_p) : \mathbb{Q}] = u$, $[\mathbb{K} \cap \mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}] = up$, $\ldots$, $[\mathbb{K} \cap \mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}] = up^{n-1}$, *para* $n \geq 1$, *segue que*

$$\sum_{n=0}^{\alpha_j} [\mathbb{K} \cap \mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}] = 1+u+up+\ldots+up^{j-2}+up^{j-1} = 1+u(1+p+\ldots+p^{j-2}+p^{j-1}) = 1+u\left(\frac{p^j-1}{p-1}\right).$$

Portanto,

$$\begin{aligned} |D(\mathbb{K}/\mathbb{Q})| &= \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{k\prod_{i=1}^{\beta} p_i} = \frac{(p^{j+1})^{up^j}}{p^{1+u(\frac{p^j-1}{p-1})}} = \frac{p^{(j+1)up^j}}{p^{1+u(\frac{p^j-1}{p-1})}} = p^{(j+1)up^j - u(\frac{p^j-1}{p-1})} = p^{u((j+1)\frac{p^j-1}{p-1})-1} \\ &= p^{u[(j+1)p^j - \frac{p^j-1}{p-1} + p^j - p^j]-1} = p^{u[(j+2)p^j - (\frac{p^j-1}{p-1}+p^j)]-1} = p^{u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}]-1}, \end{aligned}$$

o que prova o corolário. ∎

Corolário 4.4.2 *[14, Corolário 3.6] Se* $\mathbb{K} = \mathbb{Q}(\zeta_{2^m})$ *é um subcorpo de* $\mathbb{Q}(\zeta_{2^r})$ *tal que* $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$, *então o discriminante de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por* $|D(\mathbb{K}/\mathbb{Q})| = 2^{2^{m-1}(m-1)}$.

Demonstração: *Se* $\mathbb{K} = \mathbb{Q}(\zeta_{2^m})$, *então temos que o condutor de* $\mathbb{K}$ *é* 2^m *e* $[\mathbb{K} \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^m}) \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = 2^{i-1}$, *para* $i \geq 1$ *e* $[\mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = 1$, *para* $i = 0$. *Assim, pelo Teorema 4.4.1, temos que*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{(2^m)^{[\mathbb{K}:\mathbb{Q}]}}{2^\beta},$$

onde

$$\begin{aligned} \beta &= \sum_{n=1}^{m} [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^m/p_i^n}) : \mathbb{Q}] = \sum_{n=0}^{m-1} [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^n}) : \mathbb{Q}] \\ &= 1+1+2+2^2+\ldots+2^{m-3}+2^{m-2} \\ &= 1+\tfrac{2^{m-1}-1}{2-1} = 1+2^{m-1}-1 = 2^{m-1}. \end{aligned}$$

Portanto,

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{(2^m)^{[\mathbb{K}:\mathbb{Q}]}}{2^{2^{m-1}}} = \frac{2^{m2^{m-1}}}{2^{2^{m-1}}} = 2^{(m-1)2^{m-1}},$$

o que prova o corolário. ∎

Corolário 4.4.3 *[14, Corolário 3.6] Se* $\mathbb{K} \neq \mathbb{Q}(\zeta_{2^m})$ *é um subcorpo de* $\mathbb{Q}(\zeta_{2^r})$ *tal que* $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$, *então o discriminante de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por* $|D(\mathbb{K}/\mathbb{Q})| = 2^{m2^{m-1}-1}$.

Demonstração: *Se* $\mathbb{K} \neq \mathbb{Q}(\zeta_{2^m})$, *então* 2^{m+1} *é o menor inteiro tal que* $\mathbb{K} \subset \mathbb{Q}(\zeta_{2^{m+1}})$. *Assim*

$$\begin{array}{c} \mathbb{Q}(\zeta_{2^r}) \\ | \\ \mathbb{Q}(\zeta_{2^{m+1}}) \\ |_2 \\ \mathbb{K} \\ |_{2^{m-1}} \\ \mathbb{Q} \end{array}$$

Como $[\mathbb{Q}(\zeta_{2^{m+1}}) : \mathbb{Q}] = 2^m$ *e* $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$, *segue que* $[\mathbb{Q}(\zeta_{2^{m+1}}) : \mathbb{K}] = 2$. *Logo,* $[\mathbb{Q}(\zeta_{2^i}) : \mathbb{K} \cap \mathbb{Q}(\zeta_{2^i})] = 2$, *para todo* $i \in \{1, 2, \ldots, m\}$. *Assim,* $[\mathbb{K} \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_{2^i}):\mathbb{Q}]}{2} = \frac{2^{i-1}}{2} = 2^{i-2}$, *para* $i \geq 2$, *e* $[\mathbb{K} \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = 1$, *para* $i = 0, 1$. *Portanto, novamente pelo Teorema 4.4.1, temos que*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{(2^{m+1})^{[\mathbb{K}:\mathbb{Q}]}}{2^\beta},$$

onde

$$\begin{aligned} \beta &= \sum_{n=1}^{m+1} [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^m/p_i^n}) : \mathbb{Q}] = \sum_{n=0}^{m} [\mathbb{K} \cap \mathbb{Q}(\zeta_{2^n}) : \mathbb{Q}] \\ &= 1 + 1 + 1 + 2 + 2^2 + \ldots + 2^{m-3} + 2^{m-2} \\ &= 2 + \tfrac{2^{m-1}-1}{2-1} = 2 + 2^{m-1} - 1 = 2^{m-1} + 1. \end{aligned}$$

Assim,

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{(2^{m+1})^{[\mathbb{K}:\mathbb{Q}]}}{2^{2^{m-1}+1}} = \frac{2^{(m+1)2^{m-1}}}{2^{2^{m-1}+1}} = 2^{(m+1)2^{m-1}-2^{m-1}-1} = 2^{m2^{m-1}-1},$$

o que prova o corolário. ∎

Corolário 4.4.4 *[14, Corolário 3.7] O discriminante do corpo* $\mathbb{K} = \mathbb{Q}(\zeta_m)$, *onde* $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, *é dado por*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\frac{\varphi(m)}{p-1}}}.$$

Demonstração: *Temos que* $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$. *Além disso, temos que* $\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^j}) = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_{m/p_i^j}) = \mathbb{Q}(\zeta_{m/p_i^n})$. *Logo,* $[\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}] = \varphi(m/p_i^n)$. *Assim, pelo Teorema 4.4.1, temos que*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\beta_i}},$$

onde

$$\begin{aligned}
\beta_i &= \sum_{n=1}^{\alpha_i}[\mathbb{K}\cap\mathbb{Q}(\zeta_{m/p_i^j}):\mathbb{Q}] = \sum_{n=1}^{\alpha_i}\varphi(m/p_i^n) = \varphi(m/p_i)+\varphi(m/p_i^2)+\ldots+\varphi(m/p_i^{\alpha_i})\\
&= \varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_i^{\alpha_i-1}\ldots p_k^{\alpha_k})+\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_i^{\alpha_i-2}\ldots p_k^{\alpha_k})+\ldots+\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_i^{\alpha_i-\alpha_i}\ldots p_k^{\alpha_k})\\
&= \varphi(p_i^{\alpha_i-1})\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})+\varphi(p_i^{\alpha_i-2})\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})+\ldots\\
&+ \varphi(p_i^{\alpha_i-\alpha_i})\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})\\
&= \varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})(\varphi(p_i^{\alpha_i-1})+\varphi(p_i^{\alpha_i-2})+\ldots+\varphi(p_i^{\alpha_i-\alpha_i}))\\
&= \varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})((p_i-1)p_i^{\alpha_i-2}+\ldots+(p_i-1)p_i+(p_i-1)+1)\\
&= \varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})[1+(p_i-1)(1+p_i+p_i^2+\ldots+p_i^{\alpha_i-3}+p_i^{\alpha_i-2})]\\
&= \varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})\left[1+(p_i-1)\left(\tfrac{p_i^{\alpha_i-1}}{p_i-1}\right)\right]\\
&= \varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})(1+p_i-1) = p_i^{\alpha_i-1}\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})\\
&= \tfrac{\varphi(p_i^{\alpha_i})}{p_i-1}\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})\\
&= \tfrac{\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{i-1}^{\alpha_{i-1}}p_i^{\alpha_i}p_{i+1}^{\alpha_{i+1}}\ldots p_k^{\alpha_k})}{p_i-1}\\
&= \tfrac{\varphi(m)}{p_i-1}.
\end{aligned}$$

Portanto,

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\frac{\varphi(m)}{p_i-1}}} = \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\frac{\varphi(m)}{p-1}}},$$

o que prova o corolário. ∎

Corolário 4.4.5 *[14, Corolário 3.8] Seja $\mathbb{K}$ um corpo de números abeliano de condutor m. Se $\mathbb{K}\cap\mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$, para todo primo p divisor de m, então*

$$|D(\mathbb{K}/\mathbb{Q})| = m^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Demonstração: *Pelo Teorema 4.4.1, temos que*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\beta_i}},$$

onde $\beta_i = \sum_{n=1}^{\alpha_i}[\mathbb{K}\cap\mathbb{Q}(\zeta_{m/p_i^n}):\mathbb{Q}]$. Assim, se $\mathbb{K}\cap\mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$, para todo primo p divisor de m, então $\beta_i = \sum_{n=1}^{\alpha_i}[\mathbb{K}\cap\mathbb{Q}(\zeta_{m/p_i^n}):\mathbb{Q}] = \sum_{n=1}^{\alpha_i}[\mathbb{Q}:\mathbb{Q}] = \sum_{n=1}^{\alpha_i}1 = \alpha_i$. Portanto,

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i}} = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{m} = m^{[\mathbb{K}:\mathbb{Q}]-1},$$

o que prova o corolário. ∎

Corolário 4.4.6 *[14, Corolário 3.9] Seja $\mathbb{K}$ um corpo de números abeliano de condutor m. Se $[\mathbb{K}:\mathbb{Q}] = p$ é primo, então*

$$|D(\mathbb{K}/\mathbb{Q})| = m^{p-1}.$$

Demonstração: *Temos que $\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p})$ é um subcorpo de $\mathbb{K}$ e diferente de $\mathbb{K}$, uma vez que se $\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p}) = \mathbb{K}$, teríamos que $\mathbb{K} \subset \mathbb{Q}(\zeta_{m/p})$, o que contraria a minimalidade de m. Além disso, como $[\mathbb{K}:\mathbb{Q}] = p$ é primo, segue que $\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$. Assim, pelo Corolário 4.4.5, segue que*

$$|D(\mathbb{K}/\mathbb{Q})| = m^{[\mathbb{K}:\mathbb{Q}]} = m^{p-1},$$

o que prova o corolário. ∎

4.5 Discriminante mínimo

Nesta seção, veremos alguns fatos sobre o cálculo do discriminante mínimo de corpos de números abelianos. Esses resultados serão de bastante utilidade para encontrarmos reticulados algébricos com maior densidade de centro.

Proposição 4.5.1 *[14, Corolário 3.10] Se $\mathbb{K}$ é um corpo de números abeliano de condutor m e $[\mathbb{K}:\mathbb{Q}] = p$ é primo, então o discriminante mínimo de $\mathbb{K}$ é o menor valor entre $p^{2(p-1)}$ e $(kp+1)^{p-1}$, onde k é inteiro positivo e $kp+1$ é primo.*

Demonstração: *Temos que $|D(\mathbb{K}/\mathbb{Q})| = m^2$, onde m é o condutor do corpo $\mathbb{K}$. Vamos procurar o menor inteiro possível para o condutor m. Se $m = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, então $\varphi(m) = (p_1-1)p_1^{\alpha_1-1}(p_2-1)p_2^{\alpha_2-1}\dots(p_k-1)p_k^{\alpha_k-1}$. Temos que $p|\varphi(m)$ se, e somente se, $p|(p_i-1)$, para algum i, ou $p|p_j^{\alpha_j-1}$, para algum j. Para que m seja mínimo devemos ter $m = p^2$ ou $m = kp+1$, onde $kp+1$ é primo. Como as extensões $\mathbb{Q}(\zeta_{kp+1})$ e $\mathbb{Q}(\zeta_p)$ são cíclicas, uma vez que p e $kp+1$ são primos, segue que elas contém subcorpos de grau p, pois $p|\varphi(kp+1)$ e $p|\varphi(p^2)$, e assim segue o resultado.* ∎

Corolário 4.5.1 *[14, Corolário 3.11] O discriminante mínimo de uma cúbica galoisiana é 49.*

Demonstração: *O discriminante mínimo de uma cúbica é o menor elemento do conjunto $\{3^{2(3-1)}, (3.2+1)^{(3-1)}\} = \{81, 49\}$. Logo, o menor valor possível para o discriminante de uma cúbica é 49.* ∎

Exemplo 4.5.1 *Alguns discriminantes mínimos encontrados utilizando a Proposição 4.5.1,*

para corpos $\mathbb{K}$ com dimensão p primo:

p	$\mid D(\mathbb{K}) \mid$
2	*3*
3	*49*
5	*14641*
7	*20124293*
11	$6,727499949 \times 10^{20}$

Usando a idéia de contar os elementos do grupo de caracteres associado a um corpo de números abeliano $\mathbb{K}$ temos o seguinte resultado.

Proposição 4.5.2 *[14, Proposição 3.1] Se $\mathbb{K}$ e $\mathbb{L}$ são corpos de números linearmente disjuntos sobre $\mathbb{Q}$, ou seja, $[\mathbb{KL} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}][\mathbb{L} : \mathbb{Q}]$ e $D(\mathbb{K}/\mathbb{Q})$ e $D(\mathbb{L}/\mathbb{Q})$ são relativamente primos, então*

$$|D(\mathbb{KL}/\mathbb{Q})| = |D(\mathbb{K}/\mathbb{Q})|^{[\mathbb{L}:\mathbb{Q}]}|D(\mathbb{L}/\mathbb{Q})|^{[\mathbb{K}:\mathbb{Q}]}.$$

Demonstração:

Temos o seguinte diagrama

$$\begin{array}{ccc} & \mathbb{KL} & \\ / & & \backslash \\ \mathbb{K} & & \mathbb{L} \\ \backslash & & / \\ & \mathbb{Q} & \end{array}$$

Sejam $X_{\mathbb{K}}$ e $X_{\mathbb{L}}$ os grupos de caracteres associados a $\mathbb{K}$ e a $\mathbb{L}$, respectivamente. Pela Proposição 3.2.5 temos que, o grupo de caracteres $X_{\mathbb{KL}}$ associado ao corpo composto $\mathbb{KL}$ é gerado por $X_{\mathbb{K}}$ e $X_{\mathbb{L}}$. Mas, como $X_{\mathbb{K}}$ e $X_{\mathbb{L}}$ são abelianos segue que $X_{\mathbb{KL}}$ é gerado por $X_{\mathbb{K}}X_{\mathbb{L}}$. Tomando, $[\mathbb{K} : \mathbb{Q}] = r$ e $[\mathbb{L} : \mathbb{Q}] = s$, temos que $X_{\mathbb{K}} = \{\chi_0, \chi_1, \ldots, \chi_{r-1}\}$ e $X_{\mathbb{L}} = \{\psi_0, \psi_1, \ldots, \psi_{s-1}\}$. Assim, pela fórmula do condutor discriminante, temos que $D(\mathbb{K}/\mathbb{Q}) = \prod_{i=0}^{r-1} f_{\chi_i}$, e $D(\mathbb{L}/\mathbb{Q}) = \prod_{j=0}^{s-1} f_{\psi_j}$. Por outro lado, temos que $\chi_0 = \psi_0$, $\chi_i \neq \psi_j$, para $i \neq j$, uma vez que $D(\mathbb{K}/\mathbb{Q})$ e $D(\mathbb{L}/\mathbb{Q})$ são relativamente primos, e $\chi_i\psi_j \neq \chi_l\psi_m$, para $i \neq j$ ou $l \neq m$, pois a ordem de $X_{\mathbb{K}}X_{\mathbb{L}}$ é rs, já que $[\mathbb{KL} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}][\mathbb{L} : \mathbb{Q}]$. Assim, $X_{\mathbb{KL}} = X_{\mathbb{K}}X_{\mathbb{L}} = \{\chi_i\psi_j;\ 0 \leq i \leq r-1,\ e\ 0 \leq j \leq s-1\}$, e segue novamente pela fórmula do condutor discriminante, que $D(\mathbb{KL}/\mathbb{Q}) = \prod_{i,j} f_{\chi_i\psi_j}$. Agora, como $D(\mathbb{K}/\mathbb{Q})$ e $D(\mathbb{L}/\mathbb{Q})$ são relativamente primos, segue que f_{χ_i} e f_{ψ_j} também são

relativamente primos. Assim $f_{\chi_i\psi_j} = f_{\chi_i} f_{\psi_j}$ *e deste modo*

$$\prod_{i,j} f_{\chi_i\psi_j} = \prod_{i,j} f_{\chi_i} f_{\psi_j} = \left(\prod_{i=0}^{r-1} f_{\chi_i}\right)^{[\mathbb{L}:\mathbb{Q}]} \left(\prod_{j=0}^{s-1} f_{\psi_j}\right)^{[\mathbb{K}:\mathbb{Q}]} = |D(\mathbb{K}/\mathbb{Q})|^{[\mathbb{L}:\mathbb{Q}]} |D(\mathbb{L}/\mathbb{Q})|^{[\mathbb{K}:\mathbb{Q}]}.$$

Portanto,

$$|D(\mathbb{KL}/\mathbb{Q})| = |D(\mathbb{K}/\mathbb{Q})|^{[\mathbb{L}:\mathbb{Q}]} |D(\mathbb{L}/\mathbb{Q})|^{[\mathbb{K}:\mathbb{Q}]},$$

o que prova a proposição. ∎

Corolário 4.5.2 *[14, Corolário 3.12] Se* m *e* n *são relativamente primos, então*

$$|D(\mathbb{Q}(\zeta_{mn})/\mathbb{Q})| = |D(\mathbb{Q}(\zeta_m)/\mathbb{Q})|^{\varphi(n)} |D(\mathbb{Q}(\zeta_n)/\mathbb{Q})|^{\varphi(m)}.$$

Demonstração: *Sejam* X_m, X_n *e* X_{mn} *os grupos de caracteres associados a* $\mathbb{Q}(\zeta_m)$, $\mathbb{Q}(\zeta_n)$ *e* $\mathbb{Q}(\zeta_{mn})$, *respectivamente. Como* m *e* n *são relativamente primos, segue que* $X_m \cap X_n = \{\chi_0\}$. *Por outro lado, o grupo gerado por* X_m *e* X_n *é* X_{mn}. *Assim, os corpos* $\mathbb{Q}(\zeta_m)$ *e* $\mathbb{Q}(\zeta_n)$ *são linearmente disjuntos e* $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$. *Assim, pela Proposição 4.5.2, temos que*

$$\begin{aligned} |D(\mathbb{Q}(\zeta_{mn})/\mathbb{Q})| &= |D(\mathbb{Q}(\zeta_m)/\mathbb{Q})|^{[\mathbb{Q}(\zeta_n):\mathbb{Q}]} |D(\mathbb{Q}(\zeta_n)/\mathbb{Q})|^{[\mathbb{Q}(\zeta_m):\mathbb{Q}]} \\ &= |D(\mathbb{Q}(\zeta_m)/\mathbb{Q})|^{\varphi(n)} |D(\mathbb{Q}(\zeta_n)/\mathbb{Q})|^{\varphi(m)}, \end{aligned}$$

o que prova o corolário. ∎

Teorema 4.5.1 *[14, Teorema 3.5] Se* $\mathbb{K}$ *é um corpo de números abeliano de condutor* m, *onde* $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, *então*

$$\frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\varphi(m)}} \leq |D(\mathbb{K}/\mathbb{Q})| \leq m^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Demonstração: *Pelo Teorema 4.4.1, temos que*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\beta_i}},$$

onde $\beta_i = \sum_{n=1}^{\alpha_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^n}) : \mathbb{Q}]$. *Como*

$$\alpha_i = \sum_{n=1}^{\alpha_i} [\mathbb{Q} : \mathbb{Q}] \leq \beta_i = \sum_{n=1}^{\alpha_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^n}) : \mathbb{Q}] \leq \sum_{n=1}^{\alpha_i} [\mathbb{Q}(\zeta_{m/p_i^n}) : \mathbb{Q}] = \sum_{n=1}^{\alpha_i} \varphi(m/p_i^n) = \frac{\varphi(m)}{p_i - 1},$$

segue que

$$\frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\varphi(m)}} \leq \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\beta_i}} \leq \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i}} = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{m} = m^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Portanto,

$$\frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\varphi(m)}} \leq |D(\mathbb{K}/\mathbb{Q})| \leq m^{[\mathbb{K}:\mathbb{Q}]-1},$$

o que prova o teorema. ∎

Teorema 4.5.2 *[14, Teorema 3.6] Se $\mathbb{K}$ é um corpo de números abeliano de condutor m, onde $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, então*

$$m^{(1-\frac{1}{p})[\mathbb{K}:\mathbb{Q}]} \leq |D(\mathbb{K}/\mathbb{Q})| \leq m^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Demonstração: *Pelo Teorema 4.4.1, temos que*

$$|D(\mathbb{K}/\mathbb{Q})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\beta_i}},$$

onde $\beta_i = \sum_{n=1}^{\alpha_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^n}) : \mathbb{Q}]$. *Por outro lado, temos que*

$$\alpha_i = \sum_{n=1}^{\alpha_i} [\mathbb{Q} : \mathbb{Q}] \leq \beta_i = \sum_{n=1}^{\alpha_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^n}) : \mathbb{Q}] \leq \sum_{n=1}^{\alpha_i} \frac{[\mathbb{K} : \mathbb{Q}]}{p} = \frac{\alpha_i [\mathbb{K} : \mathbb{Q}]}{p},$$

e deste modo

$$\frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i [\mathbb{K}:\mathbb{Q}]/p}} \leq \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\beta_i}} \leq \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i}} = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{m} = m^{[\mathbb{K}:\mathbb{Q}]-1},$$

assim

$$\frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i [\mathbb{K}:\mathbb{Q}]/p}} = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{m^{[\mathbb{K}:\mathbb{Q}]/p}} = m^{(1-\frac{1}{p})[\mathbb{K}:\mathbb{Q}]},$$

e portanto

$$m^{(1-\frac{1}{p})[\mathbb{K}:\mathbb{Q}]} \leq |D(\mathbb{K}/\mathbb{Q})| \leq m^{[\mathbb{K}:\mathbb{Q}]-1},$$

o que prova o teorema. ∎

Corolário 4.5.3 *[14, Teorema 3.7] Se $\mathbb{K}$ é um corpo de números abeliano de condutor m, onde $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, então*

$$max\left\{ \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\varphi(m)}}, m^{(1-\frac{1}{p})[\mathbb{K}:\mathbb{Q}]} \right\} \leq |D(\mathbb{K}/\mathbb{Q})| \leq m^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Demonstração: *Segue dos Teoremas 4.5.1 e 4.5.2.* ■

Capítulo 5

Reticulados

5.1 Introdução

Os reticulados têm se mostrado bastante úteis em aplicações na Teoria das Comunicações. Intuitivamente, um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de forma regular. Deste modo, no presente capítulo faremos um estudo sobre reticulados no $\mathbb{R}^n$, explicitando alguns reticulados construtivos conhecidos na literatura, e a obtenção de reticulados via o homomorfismo canônico. Nas Seções 5.2 e 5.3 apresentamos os conceitos de reticulado, empacotamento esférico, densidade de empacotamento e densidade de centro. Em seguida, na Seção 5.4 veremos o homomorfismo canônico, e através dele obtemos um método de gerar reticulados no $\mathbb{R}^n$. Os reticulados obtidos desta maneira dependem diretamente do anel dos inteiros de um corpo de números. O grande desafio é encontrar o anel dos inteiros de qualquer corpo de números, uma vez que são conhecidos apenas o anel dos inteiros dos corpos quadráticos e dos corpos ciclotômicos. Na Seção 5.5, faremos o estudo em particular de reticulados de posto 3 utilizando as cúbicas reais e as abelianas. Neste capítulo utilizamos as referências [3], [5], [16], [17], [18] e [19].

5.2 Reticulados

Nesta seção apresentamos o conceito de reticulados, enfocando suas principais propriedades.

Definição 5.2.1 *Sejam $\mathbb{K}$ um corpo, $R \subseteq \mathbb{K}$ um anel, V um espaço vetorial de dimensão finita n sobre $\mathbb{K}$ e $\{v_1, \ldots, v_m\}$ vetores de V linearmente independentes sobre $\mathbb{K}$, com $m \leq n$.*

O conjunto dos elementos de V da forma

$$\left\{ x = \sum_{i=1}^{m} a_i v_i, \ \ com\ a_i \in R \right\},$$

é chamado reticulado com base $\beta = \{v_1, \ldots, v_m\}$ e será denotado por Λ_β.

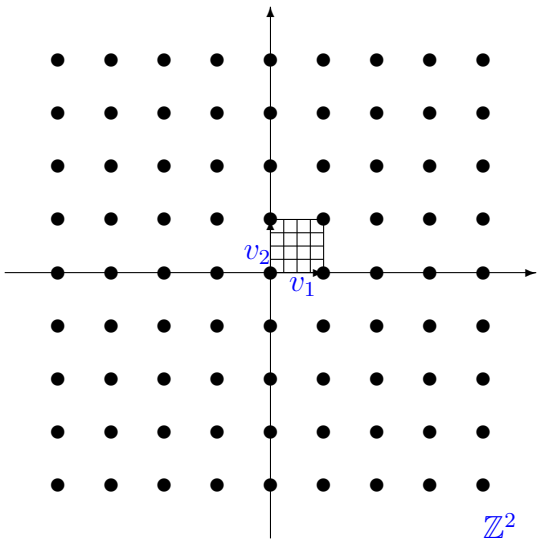
Observação 5.2.1 *Estamos interessados nos casos em que $\mathbb{K} = \mathbb{R}$, $R = \mathbb{Z}$, $V = \mathbb{R}^n$ e $m = n$.*

Definição 5.2.2 *Seja $\beta = \{v_1, \ldots, v_n\}$ uma $\mathbb{Z}$-base do reticulado $\Lambda_\beta \subset \mathbb{R}^n$. O conjunto*

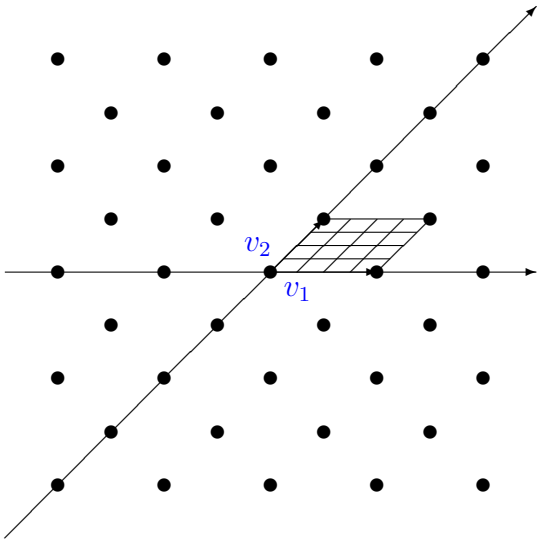
$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n : \ x = \sum_{i=1}^{n} \lambda_i v_i, \ 0 \leq \lambda_i < 1 \right\},$$

é chamado região fundamental de Λ_β.

Exemplo 5.2.1 *Temos que $\Lambda_\beta = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $v_1 = (1, 0)$ e $v_2 = (0, 1)$ com região fundamental descrita na figura abaixo.*



Exemplo 5.2.2 *Temos que $\Lambda_\beta = \{(a, b) \in \mathbb{Z}^2;\ a + b \equiv 0 (mod\, 2)\}$ é um reticulado gerado pelos vetores $v_1 = (2, 0)$ e $v_2 = (1, 1)$ com região fundamental descrita pela figura abaixo.*



Observação 5.2.2 *Seja Λ_β um reticulado do $\mathbb{R}^n$ com base $\beta = \{v_1, \ldots, v_n\}$. Se $c_1, \ldots, c_n$ são elementos quaisquer de Λ_β, então $c_i = \sum_{j=1}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Assim, temos que $\{c_1, \ldots, c_n\}$ é uma base de Λ_β se, e somente se, $\det(a_{ij})$ é um elemento inversível de $\mathbb{Z}$.*

Definição 5.2.3 *Seja $\Lambda \subseteq \mathbb{R}^n$ um subgrupo. Se $\Lambda \cap \mathbb{K}$ é finito, para todo subconjunto compacto $\mathbb{K}$ do $\mathbb{R}^n$, então Λ é chamado discreto.*

Exemplo 5.2.3 *Temos que $\mathbb{Z}^n$ é um subconjunto discreto do $\mathbb{R}^n$.*

Lema 5.2.1 *[5, Lema 2.6.1] O conjunto dos pontos de um reticulado Λ no $\mathbb{R}^n$ é discreto.*

Demonstração: *Seja $\{v_1, \ldots, v_n\}$ uma base do reticulado Λ. Temos que as condições$\langle x, v_2\rangle = 0, \ldots, \langle x, v_n\rangle = 0$ fornecem um sistema linear com $n-1$ equações lineares homogêneas e n incógnitas. Como este sistema tem uma solução não nula, segue que existe um vetor x ortogonal aos vetores $v_2, \ldots, v_n$. Se $\langle x, v_1\rangle = 0$, então o vetor x seria ortogonal a todos os vetores do $\mathbb{R}^n$, o que é impossível. Assim, $\langle x, v_1\rangle \neq 0$. O vetor $s_1 = [1/\langle x, v_1\rangle]/x$ também é ortogonal a todos os vetores $v_2, \ldots, v_n$, e $\langle s_1, v_1\rangle = 1$. Deste modo, para todo $1 \leq i \leq n$, podemos escolher um vetor s_i tal que $\langle s_i, v_i\rangle = 1$ e $\langle s_j, v_i\rangle \neq 1$, para $i \neq j$. Agora, suponhamos, que o vetor $z = a_1 z_1 + \ldots + a_n z_n$ de Λ, com $a_i \in \mathbb{Z}, i = 1, 2 \ldots, n$, pertence a uma bola de raio r. Como $a_k = \langle z, s_k\rangle$, pela inequação de Cauchy-Schwartz, segue que*

$$||a_k|| = ||\langle z, s_k\rangle|| \leq ||z||||s_k|| < r||s_k||,$$

onde $r||s_k||$ não depende de z. Portanto, existe um número finito de possibilidades para a_k e o conjunto de todos os $z \in \Lambda$ tal que $||z|| < r$ é finito. ∎

O próximo teorema diz que um reticulado é gerado sobre $\mathbb{Z}$ por uma base do $\mathbb{R}^n$, ou seja, por uma $\mathbb{Z}$-base do reticulado dado.

Teorema 5.2.1 *[3, Theorem 1, p.53] Se Λ é um subgrupo discreto do $\mathbb{R}^n$, então Λ é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.*

Demonstração: *Sejam $\beta = \{v_1, \ldots, v_r\}$ um conjunto de vetores de Λ que são linearmente independentes sobre $\mathbb{R}$, onde r é o maior possível com $r \leq n$, e*

$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n : \, x = \sum_{i=1}^{r} \alpha_i v_i, \, 0 \leq \alpha_i \leq 1 \right\}$$

o paralelepípedo construído a partir destes vetores. Temos que $\mathcal{P}_\beta$ é fechado e limitado, logo $\mathcal{P}_\beta$ é compacto. Agora, como Λ é discreto, segue que $\mathcal{P}_\beta \cap \Lambda$ é finito. Tomando $x \in \Lambda$, pela maximalidade de r, segue que $\{x, v_1, \ldots, v_r\}$ é linearmente dependente. Assim, existem $\lambda_i \in \mathbb{R}$, $i = 1, \ldots, r$, não todos nulos, tal que $x = \sum_{i=1}^{r} \lambda_i v_i$. Para cada $j \in \mathbb{N}$, seja

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] v_i \, \in \, \Lambda, \tag{5.1}$$

onde $[k]$ denota o maior inteiro menor ou igual a k. Assim,

$$x_j = j \sum_{i=1}^{r} \lambda_i v_i - \sum_{i=1}^{r} [j\lambda_i] v_i = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) v_i \in \mathcal{P}_v \cap \Lambda.$$

Deste modo, tomando $j = 1$ na Equação (5.1) obtemos que

$$x_1 = x - \sum_{i=1}^{r} [\lambda_i] v_i, \;\; \textit{ou seja,} \;\; x = x_1 + \sum_{i=1}^{r} [\lambda_i] v_i.$$

Assim, como $x_1 \in \mathcal{P}_v \cap \Lambda$ e este é finito, segue que Λ é finitamente gerado como um $\mathbb{Z}$-módulo. Por outro lado, do fato de $\mathcal{P}_v \cap \Lambda$ ser finito e $\mathbb{N}$ ser infinito, existem inteiros j e k, tais que $x_j = x_k$. Da Equação (5.1), segue que $x_j = x_k \implies jx - \sum_{i=1}^{r} [j\lambda_i] v_i = kx - \sum_{i=1}^{r} [k\lambda_i] v_i \implies (j-k)x = \sum_{i=1}^{r} ([j\lambda_i] - [k\lambda_i]) v_i \implies (j-k) \sum_{i=1}^{r} \lambda_i v_i = \sum_{i=1}^{r} ([j\lambda_i] - [k\lambda_i]) v_i \implies (j-k)\lambda_i = [j\lambda_i] - [k\lambda_i] \implies \lambda_i = \dfrac{[j\lambda_i] - [k\lambda_i]}{(j-k)}$, ou seja, $\lambda_i \in \mathbb{Q}$. Assim, Λ é gerado como um $\mathbb{Z}$-módulo por um número finito de elementos, que são combinações lineares com coeficientes racionais dos $v_i's$. Seja $d \neq 0$ um denominador comum destes coeficientes. Consideremos o conjunto $d\Lambda$. Temos que $d\Lambda \subset \sum_{i=1}^{r} \mathbb{Z} v_i$. Daí, pelo Teorema 1.2.2, segue que existe uma base $\{s_1, \ldots, s_r\}$ do

$\mathbb{Z}$-módulo $\sum_{i=1}^{r} \mathbb{Z}v_i$ *e inteiros* α_i*, tal que* $\{\alpha_1 s_1, \ldots, \alpha_r s_r\}$ *gera* $d\Lambda$ *sobre* $\mathbb{Z}$*. Como o* $\mathbb{Z}$*-módulo* $d\Lambda$ *tem o mesmo posto de* Λ *e como* $\sum_{i=1}^{r} \mathbb{Z}v_i \subset \Lambda$*, segue que o posto de* $d\Lambda \geq r$*. Pela maximalidade de* r *decorre que o posto de* $d\Lambda$ *é* r *e os* $\alpha_i' s$ *são não nulos, pois caso contrário* $d\Lambda$ *não teria posto* r*. Assim os* $s_i' s$ *são linearmente independentes sobre* $\mathbb{R}$*, uma vez que* $\{v_1, \ldots, v_r\}$ *é linearmente independente sobre* $\mathbb{R}$*. Portanto,* $d\Lambda$ *é gerado por* r *vetores linearmente independentes sobre* $\mathbb{R}$ *e consequentemente* Λ *também é gerado por* r *vetores linearmente independentes sobre* $\mathbb{R}$*.* ■

Observação 5.2.3 *Segue do Teorema* 5.2.1 *que um subconjunto discreto do* $\mathbb{R}^n$ *é um reticulado.*

5.3 Empacotamento esférico

Nesta seção apresentamos os conceitos de empacotamento esférico, densidade de empacotamento e densidade de centro, relacionando-os e enfocando algumas das principais propriedades.

Definição 5.3.1 *Um empacotamento esférico, ou simplesmente um empacotamento no* $\mathbb{R}^n$*, é uma distribuição de esferas de mesmo raio no* $\mathbb{R}^n$ *de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

Um problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço Euclidiano n-dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Isto pode ser visto como a versão euclidiana do 18º Problema de Hilbert, proposto em 1900.

A Teoria dos Códigos Corretores de Erros nasceu em 1948, com o famoso trabalho de Shannon, onde foi demonstrado o Teorema da Capacidade do Canal. Em linhas gerais, este resultado diz que para transmissão de dados abaixo de uma certa taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter a probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

A prova do Teorema da Capacidade do Canal implica que no caso de valores altos da relação sinal-ruído (SNR), um código de bloco ótimo para um canal com ruído gaussiano branco (AWGN), limitado em faixa consiste em um empacotamento denso de sinais dentro de uma esfera, no espaço euclidiano n-dimensional, para n suficientemente grande. Assim, se estabeleceu o vínculo entre empacotamento esférico e Teoria da Informação.

Para cada n, Minkowski provou a existência de reticulados no espaço euclidiano n-dimensional com densidade de empacotamento esférico Δ satisfazendo

$$\Delta \geq \frac{\xi(n)}{2^{n-1}},$$

onde ξ é a função zeta de Riemann. Como consequência, obtêm-se

$$\frac{1}{n} log_2 \Delta \geq -1. \tag{5.2}$$

Depois disto, Leech mostrou como usar códigos corretores de erros para construir empacotamentos esféricos densos no $\mathbb{R}^n$, e Conway e Sloane provaram que reticulados satisfazendo a cota de Minkowski, dada pela Equação (5.2) são equivalentes a códigos atingindo a capacidade do canal.

Dentre os métodos de geração de reticulados, o homomorfismo de Minkowski apresenta características interessantes. Usando Teoria Algébrica dos Números, Craig reproduziu o reticulado de Leech Λ_{24} através da representação geométrica de um ideal do anel dos inteiros de $\mathbb{Q}(\zeta_{39})$. Com o mesmo método, ainda obteve a família A_n^m em dimensões $n = p - 1$, através de $\mathbb{Q}(\zeta_p)$, onde p é um número primo.

Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis. Lembramos que os reticulados de maior interesse são aqueles com maior densidade de empacotamento.

Para que possamos prosseguir no estudo de reticulados, precisamos da noção de volume. O volume no $\mathbb{R}^n$ é bem conhecido e pode ser facilmente transferido para o $\mathbb{R}$-espaço V através do isomorfismo natural entre $\mathbb{R}^n$ e V, e definido por meio de uma base $\{v_1, \ldots, v_n\}$. Além disso, é possível restringir a subconjuntos C de V que são reuniões finitas da região fundamental, usando apenas as seguintes propriedades de volume.

1. $vol(x + C) = vol(C)$, para todo $x \in V$.

2. $vol(\gamma C) = \gamma^n vol(C)$, para todo $\gamma \in \mathbb{R},\ \gamma > 0$.

3. Se $C \cap C' = \emptyset$, então $vol(C \cup C') = vol(C) + vol(C')$.

Definição 5.3.2 *Sejam $\{v_1, \ldots, v_n\}$ uma base de um reticulado $\Lambda \subseteq \mathbb{R}^n$ e $\mathcal{P}_v$ a sua região fundamental. Se $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, para $i = 1, 2, \ldots, n$, então o volume da região fundamental $\mathcal{P}_v$, denotado por $vol(\mathcal{P}_v)$, é definido por*

$$vol(\mathcal{P}_v) = |det(B)|,$$

onde

$$B = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}.$$

Proposição 5.3.1 *[3, Lemma 1, p.55] O volume da região fundamental independe da base do reticulado.*

Demonstração: *Seja* $v = \{v_1, \ldots, v_n\}$ *uma base de um reticulado* $\Lambda \subseteq \mathbb{R}^n$. *Se* $s = \{s_1, \ldots, s_n\}$ *é uma outra base de* Λ, *então,* $s_i = \sum_{j=1}^{n} \alpha_{ij} v_j$, *com* $\alpha_{ij} \in \mathbb{Z}$. *Assim,*

$$vol(\mathcal{P}_s) = |\det(\alpha_{ij})| vol(\mathcal{P}_v).$$

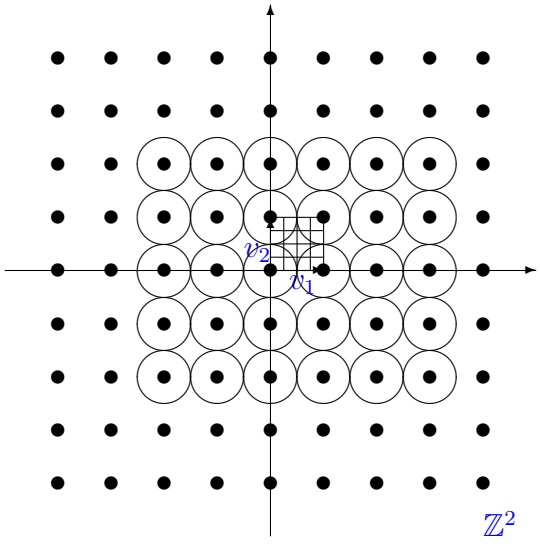
Como a matriz de mudança de base (α_{ij}) *é inversível, segue que* $\det(\alpha_{ij}) = \pm 1$. *Portanto,* $vol(\mathcal{P}_s) = vol(\mathcal{P}_v)$. ■

Observação 5.3.1 *Sendo* β' *uma outra base para* Λ_β, *segue que* $vol(\Lambda_\beta) = vol(\Lambda_{\beta'})$, *pois* β *e* β' *diferem pelo produto de uma matriz inversível com entradas inteiras. Deste modo, podemos definir o volume de* Λ_β *como o volume de uma região fundamental.*

Definição 5.3.3 *Seja* $\beta = \{v_1, v_2, \ldots, v_n\}$ *uma base de um reticulado* $\Lambda \subseteq \mathbb{R}^n$. *O volume do reticulado* Λ_β *é definido por* $vol(\Lambda_\beta) = vol(\mathcal{P}_v)$.

Definição 5.3.4 *Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* Λ_β *de* $\mathbb{R}^n$.

Exemplo 5.3.1 *Empacotamento do reticulado* $\Lambda_\beta = \mathbb{Z}^2$.



Definição 5.3.5 *Dado um empacotamento no $\mathbb{R}^n$, associado a um reticulado Λ_β, com $\beta = \{v_1, \ldots, v_n\}$ uma $\mathbb{Z}$-base, definimos a sua densidade de empacotamento como a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.*

Estamos interessados nos empacotamentos associados a um reticulado Λ_β em que as esferas tenham raio máximo, onde consigamos cobrir a maior área possível. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n;\ |x| \leq k\}$ com o reticulado Λ_β é um conjunto finito, de onde segue que o número $\Lambda_{\beta_m} = min\{|\lambda|;\ \lambda \in \Lambda_\beta,\ \lambda \neq 0\}$ está bem definido e $(\Lambda_{\beta_m})^2$ é chamado de norma mínima. Observamos que $\rho = \Lambda_{\beta_m}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ_β e obter um empacotamento. Dessa forma, o estudo dos empacotamentos reticulados é equivalente ao estudo dos reticulados.

A densidade de empacotamento de um reticulado Λ_β é definida por

$$\Delta(\Lambda_\beta) = \frac{\text{Volume de uma esfera de raio } \rho}{\text{Volume do reticulado}}.$$

Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que o seu volume é dado por

$$vol(\mathcal{B}(\rho)) = vol(\mathcal{B}(1))\rho^n,$$

onde $vol(\mathcal{B}(1))$ é o volume de uma esfera de raio 1. Assim, a densidade de empacotamento é dada por

$$\Delta(\Lambda_\beta) = vol(\mathcal{B}(1))\frac{\rho^n}{vol(\Lambda_\beta)}.$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de densidade de centro, que é dado por

$$\delta(\Lambda_\beta) = \frac{\rho^n}{vol(\Lambda_\beta)}.$$

Exemplo 5.3.2 *Seja $\Lambda_\beta = \mathbb{Z}^2$ um reticulado do $\mathbb{R}^2$ gerado pelos vetores $(1,0)$ e $(0,1)$. Temos que o raio de empacotamento é $\rho = 1/2$, e $vol(\mathcal{B}(1)) = \pi.1 = \pi$. Assim, o volume do reticulado é $vol(\Lambda_\beta) = 1$, a densidade de empacotamento é*

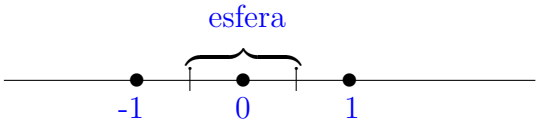
$$\Delta(\Lambda_\beta) = vol(\mathcal{B}(1)).\frac{\rho^2}{vol(\Lambda_\beta)} = \pi\frac{1}{4} = \frac{\pi}{4}$$

e a densidade de centro é $\delta(\Lambda_\beta) = 1/4$.

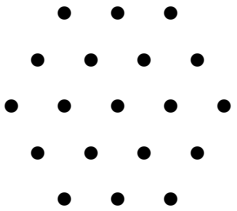
Exemplo 5.3.3 *Seja $\Lambda_\beta = \mathbb{Z}^n$ um reticulado do $\mathbb{R}^n$, gerado pelos vetores $v_1 = (1, 0, \ldots, 0)$, $(0, 1, \ldots, 0), \ldots, v_n = (0, 0, \ldots, 1)$. A forma quadrática $|v|^2 = x_1^2 + \ldots + x_n^2$ assume o valor*

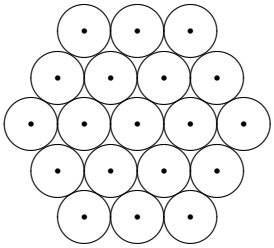
mínimo quando $x_i = 1$ *para algum* $i = 1, \ldots, n$, *e os demais são nulos. Assim* $|v|^2 = 1$ *e* $\rho = \dfrac{1}{2}$. *Visto que* $v(\Lambda_\beta) = |\det B|$, *e* B *neste caso é a matriz identidade, temos que o* $vol(\Lambda_\beta) = 1$, *e portanto,* $\delta(\Lambda_\beta) = \dfrac{1}{2^n}$.

Um dos problemas de empacotamento esférico de um reticulado Λ_β do $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade. Em dimensão um, temos que os pontos de coordenadas inteiras da reta formam um reticulado cuja a densidade de empacotamento é a melhor possível dada por $\Delta = 1$. Neste caso as "esferas" são intervalos como podemos ver na figura abaixo.



A resposta também é conhecida para dimensão dois, o reticulado hexagonal com base $\beta = \left\{(1,0), (-\frac{1}{2}, \frac{\sqrt{3}}{2})\right\}$ e $\rho = \frac{1}{2}$ é o de maior densidade, dada por $\Delta = \dfrac{\pi}{\sqrt{12}} \approx 0,9069$. O empacotamento deste reticulado é dado por





Em dimensão três *Gauss* mostrou em 1831 que o reticulado denominado $face-centered-cubic$, denotado por fcc (pilha de laranjas ou bala de canhões) é o empacotamento com maior densidade), sendo $\Delta = \dfrac{\pi}{\sqrt{18}} \approx 0,7405$.

Já para dimensões $n \geq 4$ conhece-se apenas algumas densidades de determinados empacotamentos, mais ainda não se sabe qual a melhor densidade. O empacotamento mais denso conhecido é o reticulado denominado *checkerboard* D_4. Analogamente ao anterior, este reticulado consiste de todos os pontos $(x, y, z, w) \in \mathbb{R}^4$ tais que $x + y + z + w = 2k$, com $x, y, z, w, k \in \mathbb{Z}$.

5.4 Reticulados via corpos de números

Nesta seção descrevemos o método de *Minkowski*, que consiste na obtenção de um homomorfismo de um corpo de números $\mathbb{K}$ no $\mathbb{R}^n$, de modo que a imagem de um ideal não nulo do anel dos inteiros $I_{\mathbb{K}}(\mathbb{Z})$ por este homomorfismo é um reticulado de posto n no $\mathbb{R}^n$.

Para isso, seja $\mathbb{K}$ um corpo de números de grau n. Temos que existem n monomorfismos distintos $\sigma_j : \mathbb{K} \to \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Assim, σ_j é chamado real, se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$, caso contrário, σ_j é chamado imaginário. Quando todos os monomorfismos são reais o corpo $\mathbb{K}$ é chamado totalmente real e quando os monomorfismos são todos imaginários o corpo $\mathbb{K}$ é chamado totalmente imaginário.

Se $\alpha : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$, temos que $\alpha \circ \sigma_j = \sigma_k$, para algum $1 \leq k \leq n$, e que $\sigma_j = \sigma_k$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices, tal que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de tal modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$. Assim $n - r_1$ é um número par e deste modo podemos escrever $r_1 + 2r_2 = n$. Daí, para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido por

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2},$$

é um homomorfismo injetivo de anéis, chamado de homomorfismo canônico de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$, ou homomorfismo de *Minkowski*. Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ com $\mathbb{R}^n$, e este homomorfismo pode também ser visto como

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

onde $\Re(x)$ e $\Im(x)$ representam, respectivamente, as partes real e imaginária do número complexo x.

Exemplo 5.4.1 *Sejam $\mathbb{K}$ o corpo quadrático dado por $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, onde $\sigma_1(a + b\sqrt{-7}) = a + b\sqrt{-7}$ e $\sigma_2(a + b\sqrt{-7}) = a - b\sqrt{-7}$, com $a, b \in \mathbb{Q}$. Como $\mathbb{K}$ é totalmente imaginário temos que, $r_1 = 0$ e $r_2 = 1$. Assim, para $x = a + b\sqrt{-7} \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, temos $\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x)) = (a, b)$.*

Exemplo 5.4.2 *Sejam $\mathbb{K}$ o corpo ciclotômico dado por $\mathbb{K} = \mathbb{Q}(\zeta_5)$, onde $\zeta_5 = e^{\frac{2\pi i}{5}}$ e $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Como $\mathbb{K}$ é um corpo totalmente complexo, temos que $s = 0$ e $t = 2$. Os 4 monomorfismos são dados por $\sigma_1(\zeta_5) = \zeta_5$, $\zeta_2(\zeta_5) = \zeta_5^2$, $\zeta_3(\zeta_5) = \zeta_5^3$, $\sigma_4(\zeta_5) = \zeta_5^4$. Se $x = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4 \in \mathbb{K}$, com a, b, c, d, $e \in \mathbb{Q}$, temos que $\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x), \Re\sigma_2(x), \Im\sigma_2(x))$.*

Uma das aplicações deste homomorfismo é a geração de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser obtidos via teoria algébrica dos números, através de propriedades herdadas de $\mathbb{K}$. Isto pode ser visto de maneira formal nos seguintes resultados.

Proposição 5.4.1 *[3, Proposition 1, p.56] Seja $\mathbb{K}$ um corpo de números de grau n. Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $(x_i)_{1\leq i\leq n}$, então*

1. *$\sigma_{\mathbb{K}}(M)$ é um reticulado no $\mathbb{R}^n$,*
2. *$vol(\sigma_{\mathbb{K}}(M)) = 2^{-r_2}|det(\sigma_i(x_j))|$.*

Demonstração:

1. *Para cada i fixo temos que*

$$\sigma_{\mathbb{K}}(x_i) = (\sigma_1(x_i), \ldots, \sigma_{r_1}(x_i), \Re\sigma_{r_1+1}(x_i), \Im\sigma_{r_1+1}(x_i), \ldots, \Re\sigma_{r_1+r_2}(x_i), \Im\sigma_{r_1+r_2}(x_i)), \quad (5.3)$$

onde $\Re$ e $\Im$ denotam, respectivamente, as partes real e imaginária do número complexo x_i. Agora, tomamos a matriz que tem a i-ésima coluna dada pela Equação (5.3), e calculamos o seu determinante d. Como

$$\begin{cases} \Re(z) &= \dfrac{1}{2}(z+\overline{z}) \\ \Im(z) &= \dfrac{1}{2i}(z-\overline{z}), \end{cases}$$

para $z \in \mathbb{C}$, e fazendo transformações elementares no determinante, a saber, a adição da $(s+2l)$-ésima linha a sua anterior e em seguida a subtração da (r_1+2l-1)-ésima coluna a sua posterior, para $l = 1, \ldots, r_2$, segue que

$$d = \begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_i) & \ldots & \sigma_1(x_n) \\ \sigma_2(x_1) & \ldots & \sigma_2(x_i) & \ldots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_i) & \ldots & \sigma_{r_1}(x_n) \\ \Re(\sigma_{r_1+1}(x_1)) & \ldots & \Re(\sigma_{r_1+1}(x_i)) & \ldots & \Re(\sigma_{r_1+1}(x_n)) \\ \Im(\sigma_{r_1+1}(x_1)) & \ldots & \Im(\sigma_{r_1+1}(x_i)) & \ldots & \Im(\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \Re(\sigma_{r_1+r_2}(x_1)) & \ldots & \Re(\sigma_{r_1+r_2}(x_i)) & \ldots & \Re(\sigma_{r_1+r_2}(x_n)) \\ \Im(\sigma_{r_1+r_2}(x_1)) & \ldots & \Im(\sigma_{r_1+r_2}(x_i)) & \ldots & \Im(\sigma_{r_1+r_2}(x_n)) \end{vmatrix}$$

$$= \left(\frac{1}{2}\right)^{\frac{r_2}{2}} \left(\frac{1}{2i}\right)^{\frac{r_2}{2}} \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}$$

$$= \left(\frac{1}{2}\right)^{\frac{r_2}{2}} \left(\frac{1}{2i}\right)^{\frac{r_2}{2}} 2^{r_2} \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_i) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_i) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_i) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_i) & \dots & \sigma_{r_1+1}(x_n) \\ \overline{\sigma_{r_1+1}(x_1)} & \dots & \overline{\sigma_{r_1+1}(x_i)} & \dots & \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_i) & \dots & \sigma_{r_1+r_2}(x_n) \\ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \overline{\sigma_{r_1+r_2}(x_i)} & \dots & \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}$$

$$= \left(\frac{1}{2i}\right)^{t} \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_i) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_i) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_i) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_i) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_i) & \dots & \sigma_{r_1+2}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_i) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix}$$

$$= (2i)^{-r_2} \det(\sigma_i(x_j)).$$

Assim, $d = (2i)^{-r_2} \det(\sigma_i(x_j))$*, para* $i, j = 1, \dots, n$*. Como* $(x_i)_{1 \le i \le n}$ *é uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$*, segue da Proposição* 1.7.3 *que* $\det(\sigma_i(x_j)) \neq 0$*, e portanto,* $d \neq 0$*. Assim, os*

vetores $\sigma_{\mathbb{K}}(x_i)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{\mathbb{K}}(M)$, ou seja, $\sigma_{\mathbb{K}}(M)$ é um reticulado do $\mathbb{R}^n$.

2. *Se $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de M, então $m = \sum_{i=1}^{n} a_i x_i$, com $a_i \in \mathbb{Z}$, e assim, $m \in M$. Logo, $\sigma_{\mathbb{K}}(m) = \sum_{i=1}^{n} a_i \sigma_{\mathbb{K}}(x_i)$, com $a_i \in \mathbb{Z}$, ou seja, $\sigma_{\mathbb{K}}(M) = \left\{ \sum_{i=1}^{n} a_i \sigma_{\mathbb{K}}(x_i);\ a_i \in \mathbb{Z} \right\}$. Portanto, $vol(\sigma_{\mathbb{K}}(M)) = |d| = 2^{-r_2} |det(\sigma_i(x_j))|$.* ■

Exemplo 5.4.3 *Se $\mathbb{K} = \mathbb{Q}(\sqrt{7})$, então seu anel dos inteiros é $\mathbb{Z}[\sqrt{7}]$ e $\{1, \sqrt{7}\}$ é uma $\mathbb{Z}$-base. Como $\mathbb{K}$ é totalmente real, segue que $r_2 = 0$, e assim*

$$vol(\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{7}]) = \left| \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\sqrt{7}) \\ \sigma_2(1) & \sigma_2(\sqrt{7}) \end{pmatrix} \right| = \left| \det \begin{pmatrix} 1 & \sqrt{7} \\ 1 & -\sqrt{7} \end{pmatrix} \right| = 2\sqrt{7}.$$

Portanto, a imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{7}]) \subseteq \mathbb{R}^2$ é um reticulado de posto 2 do $\mathbb{R}^2$, cujo volume é $2\sqrt{7}$.

Exemplo 5.4.4 *Se $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, então seu anel dos inteiros é $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ e $\left\{1, \frac{1+\sqrt{-7}}{2}\right\}$ é uma $\mathbb{Z}$-base. Como $\mathbb{K}$ é totalmente imaginário, segue que $r_2 = 1$, e assim*

$$vol(\sigma_{\mathbb{K}}(\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]) = \frac{1}{2} \left| \det \begin{pmatrix} 1 & \frac{1+\sqrt{-7}}{2} \\ 1 & \frac{1-\sqrt{-7}}{2} \end{pmatrix} \right| = \frac{1}{2}\sqrt{7}.$$

Portanto, $\sigma_{\mathbb{K}}(\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]) \subseteq \mathbb{R}^2$ é um reticulado de posto 2 do $\mathbb{R}^2$ com volume $\frac{1}{2}\sqrt{7}$.

Exemplo 5.4.5 *Se $\mathbb{K} = \mathbb{Q}(\zeta_5)$, onde $\zeta_5 = e^{\frac{2\pi i}{5}}$, então seu anel dos inteiros é $\mathbb{Z}[\zeta_5]$ e $\{1, \zeta_5\}$ é uma $\mathbb{Z}$-base. Como $\mathbb{K}$ é totalmente imaginário, segue que $r_2 = 1$, e assim*

$$\begin{aligned} vol(\sigma_{\mathbb{K}}(\mathbb{Z}[\zeta_5]) &= \frac{1}{2} \left| \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\zeta_5) \\ \sigma_2(1) & \sigma_2(\zeta_5) \end{pmatrix} \right| = \frac{1}{2} \left| \det \begin{pmatrix} 1 & \zeta_5 \\ 1 & \overline{\zeta_5} \end{pmatrix} \right| \\ &= \frac{1}{2} \left| -\frac{1}{2} - \frac{i\sqrt{5}}{2} - \left(-\frac{1}{2} + \frac{i\sqrt{5}}{2} \right) \right| = \frac{1}{2}\sqrt{5}. \end{aligned}$$

Portanto, a imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{5}])$ é um reticulado de posto 2 no $\mathbb{R}^2$, cujo volume é $\frac{\sqrt{5}}{2}$.

Proposição 5.4.2 *[3, Proposition 2, p.57] Sejam $\mathbb{K}$ um corpo de números de grau n e $D(\mathbb{K}/\mathbb{Q})$ o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$. Se $I_{\mathbb{K}}(\mathbb{Z})$ é o anel dos inteiros de $\mathbb{K}$, $\mathcal{A}$ um ideal não nulo de $I_{\mathbb{K}}(\mathbb{Z})$ e r_2 o número de monomorfismos imaginários, então*

1. *$\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z}))$ é um reticulado com volume $vol(\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z}))) = 2^{-r_2}|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}$.*

2. *$\sigma_{\mathbb{K}}(\mathcal{A})$ é um reticulado com volume $vol(\sigma_{\mathbb{K}}(\mathcal{A})) = 2^{-r_2}|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})$.*

Demonstração:

1. *Temos que $I_{\mathbb{K}}(\mathbb{Z})$ é um $\mathbb{Z}$-módulo livre de posto n. Assim pela Proposição* 5.4.1 *segue que $\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z}))$ é um reticulado do $\mathbb{R}^n$ e $vol(\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z}))) = 2^{-r_2}|\det(\sigma_i(x_j))|$, com $\{x_1, \ldots, x_n\}$ uma $\mathbb{Z}$-base de $I_{\mathbb{K}}(\mathbb{Z})$. Pela Proposição 1.7.3, temos que $D(\mathbb{K}/\mathbb{Q}) = \det(\sigma_i(x_j))^2$, e assim segue que $vol(\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z}))) = 2^{-r_2}|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}$.*

2. *Analogamente, temos que $\sigma_{\mathbb{K}}(\mathcal{A})$ é um reticulado do $\mathbb{R}^n$. Como $I_{\mathbb{K}}(\mathbb{Z})/\mathcal{A}$ é isomorfo a $\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z}))/\sigma_{\mathbb{K}}(\mathcal{A})$, segue que $\sigma_{\mathbb{K}}(\mathcal{A})$ é um subgrupo de $\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z}))$ de índice $N(\mathcal{A})$. Além disso, como um domínio fundamental de $\sigma_{\mathbb{K}}(\mathcal{A})$ é a união disjunta de $N(\mathcal{A})$ cópias de um domínio fundamental de $\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z}))$, segue que $vol(\sigma_{\mathbb{K}}(\mathcal{A})) = 2^{-r_2}|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})$.* ∎

Definição 5.4.1 *O reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ é chamado de realização geométrica do ideal $\mathcal{A}$.*

Observação 5.4.1 *Segue das Proposições* 5.4.1 *e* 5.4.2*, que a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{A})) = \frac{2^{r_2}\rho^n}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})}. \tag{5.4}$$

Proposição 5.4.3 *[17, p. 225] Se $\mathbb{K}$ é um corpo de números e $x \in \mathbb{K}$, então*

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}}.Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

onde

$$c_{\mathbb{K}} = \begin{cases} 1, \text{ se } \mathbb{K} \text{ for totalmente real, ou seja, } r_2 = 0, \\ \dfrac{1}{2}, \text{ se } \mathbb{K} \text{ for totalmente imaginário, ou seja, } r_1 = 0. \end{cases}$$

Demonstração: *Seja $\mathbb{K}$ um corpo de números de grau n tal que $r_1+2r_2 = n$. Como $\sigma_{\mathbb{K}}(x) \in \mathbb{R}^n$, segue que*

$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \ldots + (\sigma_{r_1}(x))^2 + \Re(\sigma_{r_1+1}(x))^2 + \Im(\sigma_{r_1+1}(x))^2 + \ldots + \Re(\sigma_{r_1+r_2}(x))^2 + \Im(\sigma_{r_1+r_2}(x))^2$.

Observe que $\Re(\sigma_k(x))^2 + \Im(\sigma_k(x))^2 = \sigma_k(x)\overline{\sigma_k(x)} = \sigma_k(x\overline{x})$, para $r_1 + 1 \leq k \leq r_1 + r_2$. Logo,

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \ldots + (\sigma_{r_1}(x))^2 + \sigma_{r_1+1}(x\overline{x}) + \cdots + \sigma_{r_1+r_2}(x\overline{x}).$$

Assim, se $r_1 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(x\overline{x}) = \sigma_{r_2+1}(x\overline{x}) + \cdots + \sigma_{r_2+r_2}(x\overline{x}),$$

uma vez que, sendo $\overline{\sigma}$ a conjugação complexa, temos que

$$\sigma_{r_2+j}(x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(x\overline{x}) = \sigma_j(x\overline{x}),$$

para $j = 1, \ldots, r_2$. Logo,

$$2|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(x\overline{x}) + \sigma_{r_2+1}(x\overline{x}) + \cdots + \sigma_{r_2+r_2}(x\overline{x}) = \sum_{i=1}^{n} \sigma_i(x\overline{x}),$$

e como os $\sigma_i(x\overline{x})$ são os conjugados de $x\overline{x}$, segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}).$$

Analogamente, se $r_2 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2,$$

e como

$$\sigma_i(x) = (\overline{\sigma} \circ \sigma_i)(x) = \sigma_i(\overline{x})$$

segue que $\sigma_i(x\overline{x}) = \sigma_i(x)\sigma_i(\overline{x}) = \sigma_i(x)\sigma_i(x) = (\sigma_i(x))^2$ e assim, $|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \ldots + \sigma_{r_1}(x\overline{x})$. Portanto,

$$|\sigma_{\mathbb{K}}(x)|^2 = \sum_{i=1}^{n} \sigma_i(x\overline{x}) = Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}).$$

■

Exemplo 5.4.6 *Se $\mathbb{K} = \mathbb{Q}(\sqrt{7})$, pelo Teorema 1.8.1, temos que o seu anel de inteiros é $\mathbb{Z}[\sqrt{7}]$, e pela Proposição 2.4.1 segue que $D(\mathbb{K}/\mathbb{Q}) = 28$. Logo, dado $x = a + b\sqrt{7} \in \mathbb{Z}[\sqrt{7}]$, obtemos que $x\bar{x} = a^2 + 2ab\sqrt{7} + 7b^2$. Assim,*

$$|\sigma_{\mathbb{K}}(x)|^2 = Tr_{\mathbb{K}/\mathbb{Q}}(x\bar{x}) = 2(a^2 + 7b^2),$$

e esta forma quadrática assume valor mínimo 2 quando $a = 1$ e $b = 0$. Portanto,

$$\delta(\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{7}])) = \frac{1}{4\sqrt{7}} \approx 0,09449.$$

Observação 5.4.2 *Se $\mathbb{K}$ é um corpo de números e $\mathcal{A}$ é um ideal não nulo do anel dos inteiros $I_{\mathbb{K}}(\mathbb{Z})$, então o raio de empacotamento do reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ pode ser reescrito da forma:*

$$\rho(\sigma_{\mathbb{K}}(\mathcal{A})) = \frac{1}{2} min\{|\sigma_{\mathbb{K}}(x)|,\, x \in \mathcal{A},\, x \neq 0\} = \frac{1}{2} min\left\{\sqrt{c_{\mathbb{K}} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})},\, x \in \mathcal{A},\, x \neq 0\right\}.$$

Fazendo $t_{\mathcal{A}} = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),\, x \in \mathcal{A},\, x \neq 0\}$ temos que:

1. Se $\mathbb{K}$ é totalmente real, então

$$\delta(\sigma_{\mathbb{K}}(\mathcal{A})) = \frac{(\frac{\sqrt{t_{\mathcal{A}}}}{2})^n}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})} = \frac{\left(\sqrt{\frac{t_{\mathcal{A}}}{4}}\right)^n}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})} = \frac{\left(\frac{t_{\mathcal{A}}}{4}\right)^{\frac{n}{2}}}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})}$$

2. Se $\mathbb{K}$ é totalmente imaginário, então

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathcal{A})) &= \frac{2^{\frac{n}{2}}(\frac{\sqrt{\frac{1}{2}t_{\mathcal{A}}}}{2})^n}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})} = \frac{\frac{2^{\frac{n}{2}}t_{\mathcal{A}}^{\frac{n}{2}}}{2^{\frac{3n}{2}}}}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})} = \frac{\frac{t_{\mathcal{A}}^{\frac{n}{2}}}{2^n}}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}\mathcal{N}(\mathcal{A})} \\ &= \frac{\frac{t_{\mathcal{A}}^{\frac{n}{2}}}{(\sqrt{4})^n}}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})} = \frac{\frac{t_{\mathcal{A}}^{\frac{n}{2}}}{4^{\frac{n}{2}}}}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})} = \frac{(\frac{t_{\mathcal{A}}}{4})^{\frac{n}{2}}}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})}.\end{aligned}$$

Portanto a densidade de centro é a mesma para ambos os casos.

Exemplo 5.4.7 *Se $\mathbb{K} = \mathbb{Q}(i)$, então o seu anel dos inteiros é $\mathbb{Z}[i]$ e $D(\mathbb{K}/\mathbb{Q}) = -4$. Logo, dado $x = a + bi \in \mathbb{Z}[i]$, temos que $x\overline{x} = (a+bi)(a-bi) = a^2 - abi + abi + b^2 = a^2 + b^2$, $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 2(a^2+b^2)$ e $t_A = 2$, para $a = 1$ e $b = 0$. Portanto,*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{Z}[i])) = \frac{\left(\frac{2}{4}\right)}{\sqrt{4}} = \frac{\left(\frac{1}{2}\right)}{2} = \frac{1}{4} = 0,25.$$

5.5 Reticulados de posto 3

Nesta seção veremos a construção de reticulados de posto 3 no $\mathbb{R}^3$ de 2 maneiras. Na primeira partimos de um polinômio irredutível de grau 3 que possua as 3 raízes reais. Na segunda partimos de uma extensão cúbica galoisiana dos racionais que está contida numa extensão p-ciclotômica. Em ambos os casos explicitamos alguns fatos sobre o reticulado obtido, e através do primeiro método conseguimos obter o reticulado que possui a maior densidade de centro conhecida.

5.5.1 Cúbicas reais

Sejam $f(x) = x^3 + ax^2 + bx + c$ um polinômio com coeficientes inteiros e α, β e γ as raízes reais de f. Temos que α, β e γ são reais se, e somente se, a derivada $f'(x)$ possui duas raízes x_1 e x_2, reais distintas, e $f(x_1)$ e $f(x_2)$ tenham sinais distintos, ou seja, $f(x_1) < 0 < f(x_2)$. Podemos escrever este resultado da seguinte maneira:

Proposição 5.5.1 *[16, Lema 1] Se $f(x) = x^3 + ax^2 + bx + c$ é um polinômio com coeficientes inteiros, então suas raízes α, β e γ são reais se, e somente se $a^2 - 3b > 0$ e $\sqrt{(a^2-3b)^3} > |\frac{2a^3-9ab+27c}{2}|$.*

Demonstração: *Seja $f(x) = x^3 + ax^2 + bx + c$. Temos que a sua derivada é dada por $f'(x) = 3x^2 + 2ax + b$, e suas raízes são $x_1 = \frac{-a-\sqrt{a^2-3b}}{3}$ e $x_2 = \frac{-a+\sqrt{a^2-3b}}{3}$. Assim $a^2 - 3b$ deve ser um número positivo. Aplicando x_1 e x_2 no polinômio $f(x)$, obtemos*

$$\begin{aligned} f(x_1) &= (\tfrac{-a-\sqrt{a^2-3b}}{3})^3 + a(\tfrac{-a-\sqrt{a^2-3b}}{3})^2 + b(\tfrac{-a-\sqrt{a^2-3b}}{3}) + c \\ &= \tfrac{1}{27}(2a^3 + 2\sqrt{a^2-3b}a^2 - 9ab - 6\sqrt{(a^2-3b)b} + 27c) \\ &= \tfrac{1}{27}(2a^3 + 2(a^2-3b)\sqrt{(a^2-3b) - 9ab + 27c}), \end{aligned}$$

e deste modo $f(x_1) > 0$ se, e somente se $\sqrt{(a^2-3b)^3} > \frac{2a^3-9ab+27c}{2}$. Analogamente, para x_2 obtemos

$$\begin{aligned} f(x_2) &= (\tfrac{-a+\sqrt{a^2-3b}}{3})^3 + a(\tfrac{-a+\sqrt{a^2-3b}}{3})^2 + b(\tfrac{-a+\sqrt{a^2-3b}}{3}) + c \\ &= \tfrac{1}{27}(2a^3 - 2\sqrt{a^2-3b}a^2 - 9ab + 6\sqrt{(a^2-3b)b} + 27c) \\ &= \tfrac{1}{27}(2a^3 - 2(a^2-3b)\sqrt{(a^2-3b) - 9ab - 27c}), \end{aligned}$$

e deste modo $f(x_2) < 0$ se, e somente se $\sqrt{(a^2-3b)^3} > -\frac{2a^3-9ab+27c}{2}$. Portanto,

$$\sqrt{(a^2-3b)^3} > |\frac{2a^3-9ab+27c}{2}|.$$

■

Corolário 5.5.1 *[16, Corolário 2] Se $f(x) = x^3+ax^2+bx+c$ é um polinômio com coeficientes inteiros, então suas raízes α, β e γ são reais se, e somente se $a^2-3b > 0$ e $c(27c+4a^3-18ab) < b^2(a^2-4b)$.*

Demonstração: *Considerando a desigualdade $\sqrt{(a^2-3b)^3} > |\frac{2a^3-9ab+27c}{2}|$ da Proposição 5.5.1 e elevando ambos os membros ao quadrado obtemos*

$$(a^2-3b)^3 > (\frac{2a^3-9ab+27c}{2})^2.$$

Logo

$$a^6 - 9a^4b + 27a^2b^2 - 27b^3 > \frac{4a^6 - 36a^4b + 108a^3c + 81a^2b^2 - 486abc + 729c^2}{4},$$

e assim

$$108a^2b^2 - 108b^3 - 81a^2b^2 > 108a^3c - 486abc + 729c^2.$$

Deste modo,

$$27a^2b^2 - 108b^3 > c(108a^3 - 486ab + 729c),$$

e dividindo ambos os membros por 27 *obtemos que*

$$b^2(a^2 - 4b) > c(4a^3 - 18ab + 27c).$$

■

Se α, β e γ são raízes reais do polinômio mônico $f(x) = x^3 + ax^2 + bx + c$, então pela relação de Girard obtemos que

$$\begin{cases} \alpha + \beta + \gamma = -a \\ \alpha\beta + \alpha\gamma + \beta\gamma = b \\ \alpha\beta\gamma = -c. \end{cases}$$

Sejam v_1, v_2 e v_3 vetores do $\mathbb{R}^3$ que geram um reticulado Λ do $\mathbb{R}^3$, onde $v_1 = (\alpha, \beta, \gamma), v_2 = (\gamma, \alpha, \beta)$ e $v_3 = (\beta, \gamma, \alpha)$. Assim, o volume do reticulado é dado por

$$vol(\Lambda) = |det(M)|,$$

onde

$$M = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{pmatrix}.$$

Logo, a densidade de centro de Λ é dada por

$$\delta(\Lambda) = \frac{\rho^n}{vol(\Lambda)} = \frac{\rho^3}{|det(M)|},$$

onde ρ é o raio de empacotamento de Λ, que é dado por $\rho = \frac{1}{2} min\{|\lambda|, \lambda \in \Lambda, \lambda \neq 0\}$.

Lema 5.5.1 *[16, Lema 3] O determinante da matriz M definida acima é dado por*

$$\det(M) = -a(a^2 - 3b).$$

Demonstração: *Temos que $det(M) = \alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma$. Por outro lado, como $\alpha + \beta + \gamma = -a$, segue que*

$$\alpha^2 + \beta^2 + \gamma^2 + 2(\alpha\beta + \alpha\gamma + \beta\gamma) = a^2, \tag{5.5}$$

e desta forma obtemos $\alpha^2 + \beta^2 + \gamma^2 = a^2 - 2b$. Multiplicando o lado direito da Equação (5.5) por $-a$ e o lado esquerdo por $\alpha + \beta + \gamma$, que são equivalentes, obtemos a seguinte equação

$$\begin{aligned} \alpha^3 + \beta^3 + \gamma^3 + \alpha\beta^2 + \alpha\gamma^2 + \alpha^2\beta + \beta\gamma^2 + \alpha^2\gamma + \beta^2\gamma &= \\ \alpha^3 + \beta^3 + \gamma^3 + \alpha\beta(\alpha + \beta) + \alpha\gamma(\alpha + \gamma) + \beta\gamma(\beta + \gamma) &= \\ \alpha^3 + \beta^3 + \gamma^3 - \alpha\beta(\gamma + a) - \alpha\gamma(\beta + a) - \beta\gamma(\alpha + a) &= \\ -a(a^2 - 2b) = -a^3 + 3ab, & \end{aligned}$$

e deste modo

$$\alpha^3+\beta^3+\gamma^3-3\alpha\beta\gamma-a(\alpha\beta+\alpha\gamma+\beta\gamma)=-a^3+2ab.$$

Portanto, $\alpha^3+\beta^3+\gamma^3-3\alpha\beta\gamma=-a^3+3ab$, *e segue que,* $det(M)=-a^3+3ab=-a(a^2-3b)$.■

Lema 5.5.2 *[16, Lema 4] Se* $v=xv_1+yv_2+zv_3$ *é um vetor do reticulado* Λ, *então*

$$|v|^2=(a^2-2b)(x^2+y^2+z^2)+2b(xy+xz+yz).$$

Demonstração: *Se* $v=(\alpha x+\beta y+\gamma z,\alpha x+\beta y+\gamma z,\alpha x+\beta y+\gamma z)$, *então*

$$\begin{aligned}|v|^2 &= (\alpha^2+\beta^2+\gamma^2)(x^2+y^2+z^2)+2(\alpha\beta+\alpha\gamma+\beta\gamma)(xy+xz+yz)\\ &= (a^2-2b)(x^2+y^2+z^2)+2b(xy+xz+yz),\end{aligned}$$

o que prova o lema. ■

Exemplo 5.5.1 *Seja* $f(x)=x^3+6x^2+9x+1$. *Temos que* f *é irredutível e satisfaz a Proposição* 5.5.1. *Pelo lema* 5.5.2, *a forma quadrática que mede o quadrado do comprimento dos vetores do reticulado é dada por*

$$Q(x,y,z)=18(x^2+y^2+z^2+xy+xz+yz),$$

que assume o valor mínimo 18 *para a entrada* $(1,0,0)$. *Dessa forma, obtemos que o raio de empacotamento é* $\rho=\frac{1}{2}min\{|\lambda|;\lambda\in\Lambda\}=\frac{\sqrt{18}}{2}$. *Agora, pelo Lema* 5.5.1, *temos que* $\det(M)=-54$. *Portanto, a densidade de centro de* Λ *é dada por*

$$\delta(\Lambda)=\frac{(\frac{\sqrt{18}}{2})^3}{54}\approx 0,17678,$$

que é a maior densidade de centro conhecida, para reticulados de posto 3, *cujo reticulado é o da família dos Laminados.*

Exemplo 5.5.2 *Seja* $f(x)=x^3-9x^2+23x-15$. *Temos que* f *é irredutível e satisfaz a Proposição* 5.5.1. *A forma quadrática que mede o quadrado do comprimento dos vetores do reticulado é dada por*

$$Q(x,y,z)=35(x^2+y^2+z^2)+46(xy+xz+yz),$$

que assume o valor mínimo 24 *para a entrada* $(1,-1,0)$. *Dessa forma, obtemos que o raio de empacotamento é* $\rho=\frac{1}{2}min\{|\lambda|;\lambda\in\Lambda\}=\frac{\sqrt{24}}{2}$. *Agora, pelo Lema* 5.5.1, *temos que* $\det(M)=108$. *Portanto, a densidade de centro de* Λ *é dada por*

$$\delta(\Lambda)=\frac{(\frac{\sqrt{24}}{2})^3}{108}\approx 0,136.$$

Exemplo 5.5.3 *Seja* $f(x) = x^3+4x^2+4x+1$. *Temos que* f *é irredutível e satisfaz a Proposição* 5.5.1. *A forma quadrática que mede o quadrado do comprimento dos vetores do reticulado é dada por*

$$Q(x, y, z) = 8(x^2 + y^2 + z^2 + xy + xz + yz),$$

que assume o valor mínimo 8 *para a entrada* $(1, 0, 0)$. *Dessa forma, obtemos que o raio de empacotamento é* $\rho = \frac{1}{2}min\{|\lambda|; \lambda \in \Lambda\} = \frac{\sqrt{8}}{2}$. *Agora, pelo Lema* 5.5.1, *temos que* $\det(M) = 16$. *Portanto, a densidade de centro de* Λ *é dada por*

$$\delta(\Lambda) = \frac{(\frac{\sqrt{8}}{2})^3}{16} \approx 0,17678.$$

Teorema 5.5.1 *[18, Teorema 3.3.1] Seja* $f(x) = x^3 + ax^2 + bx + c$, *onde* $a, b, c \in \mathbb{Z}$ *e* Λ *um reticulado. Se* $f(x)$ *satisfaz* $(\frac{a}{2})^2 = b$ *e* $c(27c + 4a^3 - 18ab) < 0$, *então o reticulado* Λ *possui densidade de centro recorde.*

Demonstração: *Temos que sua forma quadrática é dada por*

$$|v|^2 = 2b(x^2 + y^2 + z^2 + xy + xz + yz),$$

que assume o valor mínimo $2b$ *na coordenada* $(1, 0, 0)$. *Assim,* $\rho = \frac{\sqrt{2b}}{2}$ *e* $|det(M)| = |a|b$, *e deste modo a densidade de centro é dada por*

$$\delta(\Lambda) = \frac{\sqrt{2b}/2}{|a|b} = \frac{\sqrt{2b\sqrt{2b}}}{8|a|b} = \frac{\sqrt{2}\sqrt{b}}{8\sqrt{b}} = \frac{\sqrt{2}}{8} = \frac{1}{4\sqrt{2}} \approx 0,17678.$$

■

Este Teorema diz que se $f(x)$ satisfaz as condições dadas, obtemos uma família de reticulados cuja densidade de centro é recorde, como podemos notar nos Exemplos 5.5.1 e 5.5.3, ressaltando que para cada polinômio obtemos reticulados diferentes.

5.5.2 Cúbicas abelianas

Teorema 5.5.2 *[19, Teorema 3.2.3] Se* $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ *é a fatoração de* n *em fatores primos e*

$$r = \#\{p_i;\ 3|\varphi(p_i^{\alpha_i}), i = 1, 2 \dots, s\},$$

então existem $\frac{3^r-1}{2}$ *cúbicas em* $\mathbb{Q}(\zeta_n)$.

Demonstração: *Pelo Teorema Fundamental da Teoria de Galois temos que existe uma correspondência biunívoca entre corpos e grupos. Assim, tomando* $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, *temos que*

$$[\mathbb{K} : \mathbb{Q}] = (G : H),\ \ onde\ G = Gal(\mathbb{Q}(\zeta_n/\mathbb{Q})) \simeq (\mathbb{Z}/n\mathbb{Z})^*.$$

Assim, o objetivo é encontrar a quantidade de subgrupos de $(\mathbb{Z}/n\mathbb{Z})^*$ *de índice* 3*, o que equivale a determinar a quantidade de subgrupos de ordem* 3*. Seja* $\bar{G}$ *este subgrupo. Sendo* $\bar{G} = \{e, x, x^2\}$*, onde a ordem de* x *é* 3*. A ordem de* x^2 *também é* 3 *e assim* $\bar{G}$ *tem ordem* 3*. Assim, temos que cada subgrupo é formada pelo elemento neutro mais um par de elementos de ordem* 3 *cada. Assim, existem* $s/2$ *subgrupos de ordem* 3*, onde* s *é a quantidade de elementos de ordem* 3 *que vão formar os subgrupos. Se* $n = 2^c p_i^{a_i} \dots p_s^{a_s}$*, então pelo Teorema Fundamental dos Grupos Abelianos Finitos temos que*

$$(\frac{\mathbb{Z}}{n\mathbb{Z}})^* \simeq G \times (\frac{\mathbb{Z}}{p_1^{a_1}\mathbb{Z}})^* \times \ldots \times (\frac{\mathbb{Z}}{p_s^{a_s}\mathbb{Z}})^*,$$

onde G *é um grupo, cuja ordem é uma potência de* 2*. Assim, dado um elemento* g *tal que* $g \in G \times (\frac{\mathbb{Z}}{p_1^{a_1}\mathbb{Z}})^* \times \ldots \times (\frac{\mathbb{Z}}{p_s^{a_s}\mathbb{Z}})^*$*, temos que* g *é da forma* $(g_0, g_1, \ldots, g_s)$*. Deste modo,* g *tem ordem* 3 *se, e somente se,* $(g_0, g_1, \ldots, g_s) = (1, 1, \ldots, 1) \Leftrightarrow$

$$\begin{cases} g_0^3 &= 1, \\ g_1^3 &= 1, \\ \vdots &\vdots \quad \vdots \\ g_s^3 &= 1. \end{cases}$$

Encontrar o número de soluções para este sistema é equivalente a resolver a equação $x_i^3 = 1$*, para todo* $i = 1, \ldots, s$*. Se* $3 \nmid o(H_i)$*, então* $x_i^3 = 1$ *possui somente a solução trivial, onde* $H_i \simeq (\frac{\mathbb{Z}}{p_i^{a_i}\mathbb{Z}})^*$*, para todo* $i = 1, \ldots, s$*. Se* $3 \mid o(H_i)$ *e* H_i *é cíclico, então existem* 3 *soluções para* $x_i^3 = 1$*. Por outro lado,* $o(H_i) = \varphi(p_i^{a_i})$ *e deste modo temos que* $3 \mid \varphi(p_i^{a_i})$*. Portanto, a solução do sistema é uma s-upla, onde cada coordenada pode ser* 1 *ou* 3 *elementos e estas possibilidades equivalem a quantidade de primos tais que* $3 \mid \varphi(p_i^{a_i})$*.* ∎

Observação 5.5.1 *Seja* $n = pq$*, com* p *e* q *números primos distintos. Temos que* $\varphi(n) = (p-1)(q-1)$ *e deste modo, se* $3 \nmid (p-1)$ *e* $3 \nmid (q-1)$*, então* $r = 0$*, e assim segue que existe* $\frac{3^0-1}{2} = 0$ *cúbica na extensão Galoisiana* $\mathbb{Q}(\zeta_{pq})$ *sobre* $\mathbb{Q}$*. Se* $3 \mid (p-1)$ *e* $3 \nmid (q-1)$*, então* $r = 1$ *e assim existe* $\frac{3^1-1}{2} = 1$ *cúbica na extensão Galoisiana* $\mathbb{Q}(\zeta_{pq})$ *sobre* $\mathbb{Q}$*. Ainda, se* $3 \mid (p-1)$ *e* $3 \mid (q-1)$*, então* $r = 2$ *e assim existem* $\frac{3^2-1}{2} = 4$ *cúbicas na extensão Galoisiana* $\mathbb{Q}(\zeta_{pq})$ *sobre* $\mathbb{Q}$*.*

Exemplo 5.5.4 *Seja* $n = 21 = 3.7$*. Temos que* $\varphi(21) = \varphi(3)\varphi(7) = 2.6 = 12$ *e* $3 \nmid 2$*,* $3 \mid 6$*. Assim* $r = 1$ *e segue que existe uma cúbica em* $\mathbb{Q}(\zeta_{21})$ *que está contida em* $\mathbb{Q}(\zeta_7)$*, pois* $\varphi(7) = 6$ *e* $3|6$*. Portanto,* $\mathbb{Q}(\zeta_3)$ *não contribui na quantidade de cúbicas de* $\mathbb{Q}(\zeta_{21})$*.*

Exemplo 5.5.5 *Seja* $n = 55 = 11.5$. *Temos que* $\varphi(55) = \varphi(11)\varphi(5) = 10.4 = 40$ *e* $3 \nmid 10$, $3 \nmid 4$. *Assim* $r = 0$ *e segue que não existe nenhuma cúbica em* $\mathbb{Q}(\zeta_{55})$.

Observação 5.5.2 *Pela Observação* 5.4.1, *dado um ideal* $\mathcal{A}$ *do anel dos inteiros* $I_{\mathbb{K}}(\mathbb{Z})$, *temos que a densidade de centro da realização geométrica de* $\mathcal{A}$ *é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{A})) = \frac{2^{r_2}\rho^n}{|D(\mathbb{K}/\mathbb{Q})|^{\frac{1}{2}}N(\mathcal{A})}.$$

Agora, quando $\mathbb{K}$ *é uma cúbica e tomando o ideal* $I_{\mathbb{K}}(\mathbb{Z})$, *o próprio anel dos inteiros de* $\mathbb{K}$, *temos que* $\mathcal{N}(I_{\mathbb{K}}(\mathbb{Z})) = 1$ *e* $r_2 = 0$. *Portanto,*

$$\delta(\sigma_{\mathbb{K}}(I_{\mathbb{K}}(\mathbb{Z})) = \frac{\rho^3}{|D(\mathbb{K}/\mathbb{Q})|^{1/2}}.$$

Além disso, da Proposição 5.4.3, segue que

$$|\sigma_{\mathbb{K}}(\alpha)|^2 = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\bar{\alpha}).$$

Exemplo 5.5.6 *Seja* $\mathbb{K}$ *uma cúbica tal que* $\mathbb{K} \subseteq \mathbb{Q}(\zeta_9)$. *Como* $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$, *pelo Teorema 5.5.2, segue que* $r = \#\{p_i;\ 3|\varphi(p_i^{\alpha_i}), i = 1, 2 \ldots, s\} = 1$. *Assim existe* $\frac{3^r-1}{2} = 1$ *cúbica em* $\mathbb{Q}(\zeta_9)$, *que é o subcorpo maximal real* $\mathbb{K} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. *Tomando* $\alpha = \zeta_9 + \zeta_9^{-1}$ *teremos* $\mathbb{K} = \mathbb{Q}(\alpha)$ *e* $f(x) = x^3 - 3x + 1$ *é o polinômio irredutível de* α *sobre* $\mathbb{Q}$. *Temos ainda, que o anel de inteiros de* $\mathbb{K}$ *é* $\mathbb{Z}[\alpha]$. *Agora, pelo Corolário 4.2.2, segue que* $D(\mathbb{K}/\mathbb{Q}) = 81$. *Assim, dado* $x = a_0 + a_1\alpha + a_2\alpha^2$, *segue pela Observação 5.5.2, que*

$$|\sigma_{\mathbb{K}}(x)|^2 = Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = 3[(a_0 + 2a_2)^2 + (a_1 - a_2)^2 + a_1^2 + a_2^2].$$

Esta forma quadrática assume valor mínimo 3 *quando* $a_0 = 1$, $a_1 = a_2 = 0$. *Logo, o raio de empacotamento é* $\rho = \frac{1}{2}\sqrt{|\sigma_{\mathbb{K}}(x)|^2} = \frac{\sqrt{3}}{2}$. *Assim,*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{Z}[\alpha])) = \frac{(\frac{\sqrt{3}}{2})^3}{9} \approx 0,07217.$$

Portanto, do ponto de vista de empacotamento esférico este reticulado não tem um bom desempenho, visto que em dimensão 3 *a maior densidade de centro conhecida é aproximadamente* $0,17678$.

Exemplo 5.5.7 *Seja* $\mathbb{K}$ *uma cúbica tal que* $\mathbb{K} \subseteq \mathbb{Q}(\zeta_7)$. *Como* $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$, *pelo Teorema 5.5.2, segue que* $r = \#\{p_i;\ 3|\varphi(p_i^{\alpha_i}), i = 1, 2 \ldots, s\} = 1$. *Assim existe* $\frac{3^r-1}{2} = 1$ *cúbica em* $\mathbb{Q}(\zeta_7)$, *que é o subcorpo maximal real* $\mathbb{K} = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. *Tomando* $\alpha = \zeta_7 + \zeta_7^{-1}$ *teremos* $\mathbb{K} = \mathbb{Q}(\alpha)$ *e* $f(x) = x^3 + x^2 - 2x - 1$ *é o polinômio irredutível de* α *sobre* $\mathbb{Q}$. *Temos ainda, que o anel*

de inteiros de $\mathbb{K}$ *é* $\mathbb{Z}[\alpha]$. *Agora, pelo Corolário 4.2.2, segue que* $D(\mathbb{K}/\mathbb{Q}) = 49$. *Assim, dado* $x = a_0 + a_1\alpha + a_2\alpha^2$, *segue pela Observação 5.5.2, que*

$$|\sigma_{\mathbb{K}}(x)|^2 = Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = 3[(a_0 + 2a_2)^2 + (a_1 - a_2)^2 + a_1^2 + a_2^2].$$

Esta forma quadrática assume valor mínimo 3 quando $a_0 = 1$, $a_1 = a_2 = 0$. *Logo, o raio de empacotamento é* $\rho = \frac{1}{2}\sqrt{|\sigma_{\mathbb{K}}(x)|^2} = \frac{\sqrt{3}}{2}$. *Assim,*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{Z}[\alpha])) = \frac{(\frac{\sqrt{3}}{2})^3}{7} \approx 0,01326.$$

Portanto, este reticulado também não tem um bom desempenho.

Referências Bibliográficas

[1] **Shannon, C.E.**; *A Mathematical Theory of Communications*. BSTJ 27, 1948.

[2] **Ribenboim, P.**; *Algebraic Numbers*. Wiley-Interscience, 1972.

[3] **Samuel, P.**; *Algebraic Theory of Numbers*. Herman, Paris, 1967.

[4] **Endler, O.**; *Teoria dos Números Algébricos*. Projeto Euclides, 1986.

[5] **Oliveira, C. M.**; *Discriminante, Ramificação e Diferente*. Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 2005.

[6] **Stewart, I.; Tall, D.**; *Algebraic Number Theory*, New York: Chapman-Hall, 1987.

[7] **Lang, S.**; *Álgebra*. New York, Addison-Wesley, 1965.

[8] **Alves, C.**; *Reticulados via Corpos Ciclotômicos*. Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 2005.

[9] **Marcus, D. A.**; *Number Fields*. New York: Springer-Verlag, 1977.

[10] **Washington, L. C.**; *Introduction to Cyclotomic Fields*. New York: Board, 1982.

[11] **Cazzeta, M.**; *Caracteres de Dirichlet e Aplicações*. Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 1998.

[12] **Nóbrega, T.P.; Interlando, J.C.; Lopes, J.O.D.**; *On Computing Discriminants of Subfields of* $\mathbb{Q}(\zeta_{p^r})$. Journal of Number Theory, N. 96, pp. $319 - 325$, 2002.

[13] **Lopes, J.O.D.**; *On Computing Discriminants of Subfields of* $\mathbb{Q}(\zeta_{2^r})$. Journal of Algebra And Its Applications, USA, V. 2, N. 4, pp. $463 - 469$, 2003.

[14] **Lopes, J.O.D.**; *Discriminante dos Corpos Abelianos*. Tese de Doutorado, IMECC/UNICAMP, 2003.

[15] **Nóbrega, T.P.; Interlando, J.C.; Lopes, J.O.D.**; *Discriminante de Corpos de Números Abelianos*. to appear.

[16] **Nóbrega, T.P.**; *Cúbicas Reais, Algumas Aplicações*. Anais do VI encontro de Álgebra USP-UNICAMP, 1997.

[17] **Sloane, N.J.A.; Conway, J.H.**; *Sphere Packing, Lattices and Groups*. Springer-Verlag, 1999.

[18] **Souza, T.M.**; *Reticulados Algébricos em Corpos de Números Abelianos*. Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 2004.

[19] **Rodrigues, T.M.**; *Cúbicas Galoisianas*. Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto-SP, 2003.

Índice Remissivo