Universidade Estadual Paulista

Câmpus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Discriminante mínimo de corpos Abelianos de grau primo

Ruikson Sillas de Oliveira Nunes

Orientador: Prof. Dr. Trajano Pires da Nóbrega Neto

Dissertação apresentada ao Instituto de Biologia, Letras e Ciências Exatas da Universidade Estadual Paulista, Câmpus São José do Rio Preto, como parte dos requisitos para a obtenção do título de Mestre em Matemática

São José do Rio Preto

Abril - 2009

A minha mãe

dedico.

Agradecimentos

Ao concluir este trabalho agradeço:

A Deus por ter me concedido sabedoria e me dado forças para realizar este trabalho.

A minha mãe agradeço por sempre ter me auxiliado em meus estudos.

Aos meus professores de graduação, em especial, ao professor Marcelo Polezzi *(in memorian)* por suas motivações quando eu ainda estava na graduação.

Ao professor Trajano pela disposição em me orientar e por suas importantes sugestões durante a elaboração deste trabalho.

Aos professores, José Othon Dantas Lopes e Clotilzio Moreira dos Santos por terem aceitado o convite em participar da banca examinadora deste trabalho.

Ao professor Cláudio agradeço, por ele ter estado sempre disposto a dialogar e ter me dado algumas sugestões no decorrer deste curso.

Aos meus professores de pós-graduação, que tanto contribuiram para a minha formação.

Agradeço aos meus amigos e colegas, em especial, Tiago, Oyran (o chifre), Ana Paula, Rodiak por seus auxílios e companheirismo.

A CAPES pelo auxílio financeiro

“A vida não entrega nada ao mortal se não em troca de grandes esforços.”

(Horácio)

Resumo

Dado um número inteiro positivo d, encontrar um corpo de grau d que tenha, em valor absoluto, o menor discriminante é um problema clássico e poucos resultados se tem até hoje no sentido de se resolver tal desafio. O principal interesse deste trabalho consiste em estudar o problema acima sobre os corpos de números Abelianos, particularmente aqueles de grau primo. Para tanto será preciso dominar algumas técnicas referentes ao cálculo do discriminante de corpos de números, em especial, dos corpos Abelianos.

Palavras chave: Discriminante, Discriminante Mínimo, Caracteres de Dirichlet, Corpos Abelianos.

Abstract

Given a positive interger d, finding a field of degree d which has, to absolute value, the smallest discriminant it is a classical problem and few results has been got until at present time, to solve this challenge. The main purpose of this paper it is to study the problem above on Abelian numbers fields, in special that ones of prime degree. However, it is necessary to know any techniques for calculating the numbers field discriminant, specially, to Abelian fields.

Key words: Discriminant, Minimal Discriminant, Modular Caracteres, Abelian Fields.

Sumário

Lista de Símbolos

$\mathbb{N}$: Conjunto dos números naturais

$\mathbb{Z}$: Conjunto dos números inteiros

$\mathbb{Q}$: Conjunto dos números racionais

$\mathbb{R}$: Conjunto dos números reais

$\mathbb{C}$: Conjunto dos números complexos

$\mathbb{O}_A(B)$: Conjunto dos elementos inteiros do anel A sobre o anel B

K: Corpo de Números

$\mathbb{O}_K$: Anel de inteiros de K

σ_i: Imersão de K em $\mathbb{C}$

σ_K: Homomorfismo canônico

$\Delta[\alpha_1, \cdots, \alpha_n]$: Discriminante da n-upla $\{\alpha_1, \cdots, \alpha_n\}$

$\Delta(K)$: Discriminante do corpo K

$[K : \mathbb{Q}]$: Grau da extensão de K sobre $\mathbb{Q}$

$det(a_{ij})$: Determinante da matriz (a_{ij})

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

L/K: L extensão de K

$N_{A/B}$: Norma em relação a extensão A/B

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

ζ_n: $e^{\frac{2\pi}{n}} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$

$\mathbb{Q}(\zeta_n)$: n-ésimo corpo ciclotômico

U_n: Grupo das raízes n-ésimas da unidade

$|G|$: Ordem do grupo G

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

$\varphi(n)$: Função de Euler

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

$\Delta(K/L)$: Discriminante em relação a extensão K/L

log: Função logarítma

$Gal(K/L)$: Grupo de Golois de K sobre L

$\delta(\wedge)$: Densidade de centro do reticulado $\wedge$

$\mathbb{C}^*$: Grupo multiplicativo dos elementos inversíveis de $\mathbb{C}$

χ: Caracter

f_χ: Condutor do caracter χ

$\widehat{G}$: Grupo de caracteres de G

X_K: grupo de caracteres associados a K

$Ker(f)$: Núcleo do homomorfismo f

$Aut_K L$: Grupo dos K-automorfismos de L

$G = \langle a \rangle$: Grupo gerado por a

$(G : H)$: Índice do subgrupo H em G

$d \mid p$: d divide p

Introdução

O cálculo do discriminante de corpos de números é um assunto antigo, mas ainda é um problema não totalmente resolvido. Muitos matemáticos da Teoria dos Números dedicaram tempo ao estudo desse desafio, embora não se tenha obtido resultados gerais, porém já foram conseguidos resultados importantes para uma classe significativa de corpos de números, os corpos de números Abelianos. Estudar esses corpos traz uma grande satisfação no que diz respeito a obtenção de resultados esperados, uma vez que esse assunto conduz a Teoria de Galois e assim, os processos algébricos originais para o cálculo do discriminante ganha novos conceitos os quais possibilitam obter ferramentas mais vantajosas na determinação explícita do discriminante.

Entretanto, o estudo do discriminante ganha força quando se olha a sua aplicabilidade nos mais variados ramos da matemática. Entre elas pode-se destacar na Teoria dos Códigos Corretores de Erro, de Empacotamento de Esferas, via a representação geométrica dos ideais de um corpo de números. Com respeito aos reticulados (subgrupos discretos do $\mathbb{R}^n$), existe uma dependência muito grande do conceito de discriminante de um corpo de números, no processo de encontrar a sua densidade de empacotamento ou densidade de centro.

Motivados então pela abrangência existente do conceito, é que este trabalho tem sido preparado. Aqui será estudado o discriminante de um corpo de números Abeliano K, isto é, uma extensão galoisiana dos racionais cujo grupo do automorfismos é abeliano. A definição original do discriminante de um corpo de números, implica na necessidade de se conhecer uma base integral do corpo, bem como todos

os monomorfismos de K no corpo complexo $\mathbb{C}$. Daí então, há uma dificuldade no cálculo do discriminante de corpos de números, uma vez que encontrar uma base integral para um corpo de números não é uma tarefa simples, assim como não é fácil descrever os monomorfismos de K em $\mathbb{C}$. No entanto, para os corpos ciclotômicos $\mathbb{Q}(\zeta_n)$ se conhece uma base integral e, sendo assim, com um pouco mais de trabalho, podemos também expressar o seu discriminante.

Tendo em vista que todo subcorpo K de $\mathbb{Q}(\zeta_n)$ é uma extensão abeliana de $\mathbb{Q}$, a recíproca é uma questão interessante cuja a resposta afirmativa é assegurada pelo Teorema de Kronecker-Weber [Teorema 2.1.2]. Com o objetivo de estudar um método para calcular o discriminante de um corpo ciclotômico que extenda para os seus subcorpos, ou seja, com o propósito de calcular o discriminante dos corpos abelianos, existe um resultado que é a fórmula Condutor-Discriminante [Teorema 2.3.3] que possibilita calcular o discriminante de um corpo de números Abeliano sem precisar ter conhecimento de uma base integral.

Um outro problema antigo, relacionado ao discriminante de corpos de números e que até então não está totalmente resolvido é o de saber qual o menor discriminante absoluto assumido por corpos de uma dada dimensão. Esse assunto ganha importância no ambiente dos reticulados algébricos, pois no processo de maximizar a densidade de centro de um reticulado, (para se obter reticulados de altas densidades) é necessário a minimização do discriminante absoluto do corpo que gera o reticulado.

Tendo em vista a complexidade existente em resolver o problema do discriminante mínimo de modo geral, com respeito a obtenção de resultados, restringiremos tal problema para a classe dos corpos Abelianos. Embora neste ambiente o problema ainda não esteja totalmente resolvido, podemos encontrar alguns resultados para casos particulares dentro desta classe de corpos de números, mais precisamente para os corpos Abelianos de grau primo.

A principal meta deste trabalho consiste em estudar o problema do discriminante mínimo de corpos abeliano de grau primo. Porém, além de calcularmos o discriminante mínimo estaremos interessados também em saber qual é a extensão

ciclotômica mínima que contém o corpo com tal discriminante.

Pensando em atingir tais propósitos de modo satisfatório, este trabalho foi dividido em três capítulos. É interessante ressaltar que para o leitor sentir-se mais confortável na leitura deste texto, será requerido que ele tenha um prévio conhecimento de alguns conceitos de álgebra, como grupos, anéis, ideais e demais conceitos algébricos deste nível.

O primeiro capítulo é dedicado substancialmente a lançar base aos conceitos introdutórios referentes a Teoria dos Números Algébricos. Tendo como objetivo principal dar conhecimento a definição original de discriminante [Definição 1.2.4] de um corpo de números e além disso, é objetivo ainda a obtenção de fórmulas alternativas, que sob determinadas circunstâncias, são mais eficazes para o cálculo do discriminante de corpos de números. Além disto, neste capítulo, é dedicada uma seção para um breve estudo a respeito dos reticulados algébricos, onde ali expressaremos uma fórmula [Fórmula 1.1, pag. 39], a qual se constitui como um dos principais problemas para a aplicação do discriminante mínimo.

Já, o segundo capítulo é destinado a estabelecer alguns importantes conceitos como; Teorema Fundamental da Teoria de Galois e Caracteres Modulares. Tudo isto será feito buscando atingir um outro resultado importante que é a fórmula do Condutor-Discriminante [Teorema 2.3.3]. Essa fórmula nos concede um novo método para o cálculo do discriminante de corpos que estão contidos em alguma extensão ciclotômica. Embora diante desta restrição, com respeito a sua aplicabilidade, a fórmula do Condutor-Discriminante desempenhará aqui neste trabalho um papel importante, a qual será a principal ferramenta para o cálculo do discriminante dos específicos corpos com os quais trabalharemos, a saber, os corpos Abelianos. Isto é garantido via um resultado conhecido como o Teorema de Kronecker-Weber, o qual garante que todo corpo de números Abeliano está contido em uma extensão ciclotômica.

Por fim, no último capítulo, buscaremos atingir os principais resultados propostos para este trabalho. Em primeiro instante será mostrado um resultado que expressa uma fórmula [Teorema 3.3.1] para o discriminante de corpos de números Abelianos.

Em seguida, são estabelecidos alguns resultados que são consequências imediatas dessa fórmula, entre esses podemos destacar o Corolário 3.3.5 que explicita um fórmula para o discriminante de corpos abelianos de grau primo. E, finalizando o capítulo, bem como o corpo deste trabalho, nos direcionaremos ao estudo do discriminante mínimo de corpos abeliano de grau primo. Primeiramente, obteremos este resultado para os corpos quadráticos [Teorema 3.4.1], neste caso mostraremos que o corpo $\mathbb{Q}(\sqrt{-3})$ é o corpo quadrático que possui o menor discriminante, em valor absoluto. Em seguida, faremos o caso geral [Teorema 3.4.4], de ordem prima. Diferentemente do caso quadrático, no caso geral não será estabelecido o corpo que possui o menor discriminante. No entanto, estaremos interessados em calcular o menor discriminante assumido por tais corpos e também investigar qual a extensão ciclotômica mínima que contém o referido corpo.

Capítulo 1

Corpos de Números e Discriminante

Este capítulo foi preparado com o objetivo de apresentar conceitos introdutórios à Teoria dos Números Algébricos tendo como meta principal apresentar a definição original de discriminante de um corpo de números, estabelecida na Definição 1.3.3. No entanto, diante da dificuldade existente em aplicar a fórmula original, é ainda um propósito aqui neste capítulo apresentar uma fórmula alternativa para o discriminante,[vide Proposição 1.4.3] onde esta, do ponto de vista aplicativo, se torna mais eficaz do que a estabelecida pela definição.

Além disso, serão feitas algumas implementações para o uso de tais fórmulas, onde serão computados o discriminante de duas classes importantes de corpos de números, a saber, os corpos quadráticos e ciclotômicos, onde esta última desempenhará um importante papel no decorrer deste trabalho.

Enfim, o capítulo é terminado com uma seção específica tratando de alguns conceitos referentes aos reticulados algébricos. Esta seção tem por objetivo apresentar um problema [Equação 1.1, pag. 39] que a sua solução implica a necessidade de se obter o discriminante mínimo, em valor absoluto, de corpos de números. Para atingir os propósitos acima descritos foram utilizados partes substanciais das referências [1] à [6].

1.1 Elementos algébricos e inteiros sobre um anel

Pretendemos nesta seção introduzir os conceitos básicos relativos a teoria dos números algébricos. Iniciaremos definindo elemento algébrico e inteiro sobre anéis e trabalharemos também alguns propriedades que os relacionam com o conceito de módulo, temos como principal meta nesta seção mostrar que o conjunto dos elementos inteiros sobre um anel é também um anel.

Definição 1.1.1 *Considerando A um anel e B um subanel de A. Um elemento $\beta \in A$ é dito ser algébrico sobre B, se β é raiz de algum polinômio não nulo com coeficientes em B.*

Caso um elemento de A não seja algébrico sobre B dizemos que tal elemento é transcendente sobre B. Quando todos os elementos de A são algébricos sobre B dizemos que o anel A é algébrico sobre B.

Definição 1.1.2 *Sejam A um anel e B um subanel de A. Um elemento $\alpha \in A$ é inteiro sobre B, se α é raiz de algum polinômio mônico com coeficiêntes em B, ou seja, existem $b_0, b_1, \cdots, b_{n-1} \in B$ tal que $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} + \alpha^n = 0$, essa equação é chamada de equação de dependência inteira de α.*

Exemplo 1.1.1 *Seja $\alpha = \sqrt[3]{2} \in \mathbb{R}$, então α é inteiro sobre $\mathbb{Z}$, uma vez que α é raiz de $p(x) = x^3 - 2$.*

Considerando os anéis A e B, tais que $B \subseteq A$, tomando um elemento $\alpha \in A$, inteiro sobre B, adjuntando o anel B com o elemento α o anel $B[\alpha]$ pode ser considerado como um módulo finitamente gerado e, isto pode ser visto no;

Teorema 1.1.1 *{[2], pag. 7} Sejam A um anel e B um subanel de A e $\alpha \in A$. Então as seguintes condições são equivalentes;*

(i) *α é inteiro sobre B;*

(ii) *O anel $B[\alpha]$ é um B-módulo finitamente gerado;*

(iii) *Existe um subanel R do anel A, tal que R é um B-módulo finitamente gerado contendo o elemento α.*

Proposição 1.1.1 {*[2], pag. 8*} *Sejam A um anel, B um subanel de A e $\alpha_1, \cdots, \alpha_n$ elementos de A tal que α_i é inteiro sobre $B[\alpha_1, \cdots, \alpha_{i-1}]$, $i = 2, \cdots, n$. Então, $B[\alpha_1, \cdots, \alpha_n]$ é um B-módulo finitamente gerado.*

Sendo α e β elementos de A inteiros sobre B, como consequência desta última proposição temos que $\alpha + \beta$, $\alpha - \beta$ e $\alpha.\beta$ são também elementos de A inteiros sobre B. E consequêntemente temos que o conjunto de elementos de A inteiros sobre o anel B, denotado por $\mathbb{O}_A(B)$, é ainda um anel. E este fato é assegurado pela;

Proposição 1.1.2 {*[2],pag. 9* } *Sejam A um anel e B um subanel de A. O conjunto $\mathbb{O}_A(B)$, é um subanel de A que contém B.*

Sendo o conjunto $\mathbb{O}_A(B)$ um anel e $B \subseteq \mathbb{O}_A(B)$, como consequência do Corolário 1.1.1 temos que o anel $\mathbb{O}_A(B)$ pode ser considerado como um módulo finitamente gerado sobre B. Com esta estrutura estaremos aptos a falar sobre base e dimensão, porém por agora não é este o nosso propósito, mas voltaremos a retomar este assunto numa próxima seção, quando formos tratar de bases integrais de um corpo de números.

Definição 1.1.3 *Sejam A um anel e B um subanel de A. O conjunto $\mathbb{O}_A(B)$ é também chamado de fecho integral de B em A. Agora, se B for um anel de integridade e A for o seu corpo de frações, $\mathbb{O}_A(B)$ é chamado simplesmente de fecho integral de B. Dizemos que A é inteiro sobre B, se todo elemento de A é inteiro sobre B .*

Exemplo 1.1.2 *O anel $\mathbb{Q}[\sqrt{d}]$ é inteiro sobre $\mathbb{Q}$, pois todo elemento $a+b\sqrt{d}$, $a, b \in \mathbb{Q}$ é raiz do polinômio $x^2 - 2ax + (a - b^2d)$ o qual pertence à $\mathbb{Q}[x]$.*

Proposição 1.1.3 {*[2], pag. 9*} *Sejam A um anel e B um subanel de A, e C um subanel de B. A é inteiro sobre B e B é inteiro sobre C se, e somente se, A é inteiro sobre C.*

Definição 1.1.4 *Seja A um anel, dizemos que A é integralmente fechado quando $A = \mathbb{O}_A(B)$, em outras palavras, um anel A é integralmente fechado se todo elemento de seu corpo de frações que é inteiro sobre A está em A.*

Exemplo 1.1.3 *Todo anel fatorial é integralmente fechado. Em particular todo anel principal é integralmente fechado. De fato, sejam A um anel fatorial e $\alpha = \frac{a}{b}$, onde $mdc(a,b) = 1$, um elemento de seu corpo de frações que é inteiro sobre A, existe $a_0, a_1, \cdots, a_{n-1} \in A$, onde $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$, que é $a_0 + a_1\frac{a}{b} + \cdots + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \frac{a^n}{b^n} = 0$, multiplicando esta última equação por b^n, temos $b^n a_0 + a_1 ab^{n-1} + \cdots + a_{n-1}a^{n-1}b + a^n = 0$, daí $a^n = -(b^n a_0 + a_1 ab^{n-1} + \cdots + a_{n-1}a^{n-1}b) = -b(b^{n-1}a_0 + a_1 ab^{n-2} + \cdots + a_{n-1}a^{n-1})$, isso mostra que $b \mid a^n$, assim, temos que $a = b.k$, com $k \in A$. Como $mdc\,(a,b) = 1$, segue que $ax_0 + by_0 = 1$ para algum $x_0, y_0 \in A$. Assim, $bk_1x_0 + by_0 = 1$, então $b(k_1x_0 + y_0) = 1$, logo b é inversível em A, daí $\alpha \in A$.*

1.2 Conjugados, corpos de números e discriminante

Nesta seção será definido corpos de números e serão estudadas algumas propriedades das imersões de tais corpos no corpo complexo $\mathbb{C}$. Além disso, ainda nesta seção temos por meta principal definir o conceito de discriminante de uma base de um corpo de números.

Definição 1.2.1 *Sejam K, L corpos e $f(x) \in K[x]$ um polinômio não constante, se L é o menor corpo tal que $K \subset L$ e possui todos as raízes de $f(x)$, então L é denominado o corpo de raízes de $f(x)$.*

Exemplo 1.2.1 *Consideremos o polinômio $f(x) = x^3 - 3 \in \mathbb{Q}[x]$ temos que $L = \mathbb{Q}[\sqrt[3]{3}, \zeta]$ é o corpo de raízes de $f(x) = x^3 - 3$, onde $\zeta = cos\frac{2\pi}{3} + isen\frac{2\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$.*

Definição 1.2.2 *Um corpo K é dito ser algébricamente fechado se todo polinômio não constante sobre K possui todas as suas raízes em K. Em outras palavras, K é algébricamente fechado se para quaisquer $f(x) \in K[x]$, K é corpo de raízes de $f(x)$.*

Exemplo 1.2.2 *O corpo $\mathbb{C}$ dos números complexos é algebricamente fechado. Já o corpo $\mathbb{R}$ dos números reais não é, pois $f(x) = x^2 + 1 \in \mathbb{R}[x]$ não possui raízes em $\mathbb{R}$*

Consideremos agora dois subcorpos L e M de $\mathbb{C}$, contendo um corpo K. Chamamos de K-isomorfismo de L sobre M a todo isomorfismo $\varphi : L \longrightarrow M$, $\varphi(\alpha) \longrightarrow \alpha$ para todo α em K. Assim, sob tais condições dizemos que L e M são K-isomorfos, ou que eles são conjugados sobre K. Portanto, dados duas extensões L e M de um corpo K, dizemos que os elementos $\alpha \in L$ e $\beta \in M$ são conjugados se existe um K-isomorfismo $\varphi : K[\alpha] \longrightarrow K[\beta]$, tal que $\varphi(\alpha) = \beta$. A existência de tal isomorfismo φ nos garante que α e β são ambos algébricos ou ambos transcendente.

A partir do próximo parágrafo vamos nos direcionar ao estudo de propriedades e conceitos sobre alguns subcorpos de $\mathbb{C}$, denominados corpos de números.

Definição 1.2.3 *Um corpo $K \subset \mathbb{C}$ é dito ser um corpo de números se K é uma extensão finita do corpo $\mathbb{Q}$ dos racionais.*

A partir de agora, todo corpo aqui mencionado, a menos de alguma observação, será considerado como um corpo de números.

Da definição acima vemos que todo corpo de números é uma extensão algébrica de $\mathbb{Q}$. Sendo K um corpo de números segue que $K = \mathbb{Q}[\alpha_1, \cdots, \alpha_n]$ para um número finito de elementos algébricos $\alpha_1, \cdots, \alpha_n$ sobre $\mathbb{Q}$ e daí temos que para todo corpo de números K existe θ algébrico sobre $\mathbb{Q}$, onde $K = \mathbb{Q}[\theta]$, e isto pode ser visto no

Teorema 1.2.1 *{[1], pag. 40} Se K é um corpo de números, então $K = \mathbb{Q}[\theta]$ para algum número algébrico θ sobre $\mathbb{Q}$.*

Observação 1.2.1 *Sendo K é um corpo de números, a expressão $\mathbb{Q}[\theta]$ de K não é única, pois $\mathbb{Q}[\theta] = \mathbb{Q}[-\theta] = \mathbb{Q}[\theta + q]$, onde $q \in \mathbb{Q}$.*

Exemplo 1.2.3 *Seja* $K = \mathbb{Q}[\sqrt{2}, \sqrt[3]{3}]$*, temos que* $\alpha = \sqrt{2}$ *e* $\beta = \sqrt[3]{3}$ *são elementos algébricos sobre* $\mathbb{Q}$*. Assim, pela observação anterior temos que* $K = \mathbb{Q}[\sqrt{2} + \sqrt[3]{3}]$*.*

Anteriormente fizemos menção a respeito dos corpos conjugados. Se considerarmos um corpo $K = \mathbb{Q}[\theta]$, em geral existirá vários monomorfismos distintos $\sigma : K \longrightarrow \mathbb{C}$, e a quantidade destes depende do grau de K, como por exemplo, $K = \mathbb{Q}[\sqrt{2}]$, temos que σ_1 e σ_2 são monomorfismos de $\mathbb{Q}[\sqrt{2}]$ em $\mathbb{C}$, onde σ_1 define o automorfismo idêntico em K e σ_2 a conjugação sobre K.

Teorema 1.2.2 *{[1], pag. 41} Seja* $K = \mathbb{Q}[\theta]$ *um corpo e números de grau* n *sobre* $\mathbb{Q}$*. Então existem exatamente* n *monomorfismos distintos* $\sigma_i : K \longrightarrow \mathbb{C}$*,* $i = 1, \cdots, n$*. Os elementos* $\sigma_i(\theta) = \theta_i$ *são raízes distintas em* $\mathbb{C}$ *do polinômio minimal de* θ *sobre* $\mathbb{Q}$ *.*

Considerando um corpo de números K de grau n, seja $\alpha \in K$, temos que se α é raíz de um polinômio $h(x)$ sobre K, então $\sigma_i(\alpha)$ é também uma raiz de $h(x)$. Por este fato, os elementos $\sigma_i(\alpha)$ $i = 1, \cdots, n$ são chamados de K-conjugados de α. Observemos que neste caso os $\sigma_i's(\alpha)$ podem não ser distintos, por exemplo se $\alpha \in \mathbb{Q}$, então $\sigma_i(\alpha) = \alpha \ \forall \ i = 1, \cdots, n$.

Definição 1.2.4 *Seja* K *um corpo de números de grau* n *e* $\{\alpha_1, \cdots, \alpha_n\}$ *uma base de* K *(como um espaço vetorial sobre* $\mathbb{Q}$*). Definimos o discriminante desta base por;*

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

Esta difinição expressa um método para o cálculo do discriminante de uma base de um corpo de números, mas em muitos casos este método se torna de difícil aplicabilidade, uma vez que determinar as imersões σ_i não é um processo muito simples, e além disso, para corpos de alto grau calcular o determinante acima se torna um processo muito árduo.

Exemplo 1.2.4 *Consideremos o corpo* $K = Q[\sqrt{3}]$*. O conjunto* $\{1, \sqrt{3}\}$ *é uma base de* K *sobre* $\mathbb{Q}$*. Com* $i = 1, 2$ *e* $j = 1, 2$*, temos que* $\sigma_i(1) = 1$ $i = 1, 2$ *e* $\sigma_1(\sqrt{3}) = \sqrt{3}$

e $\sigma_2(\sqrt{3}) = -\sqrt{3}$ *, então;*

$$\Delta[1,\sqrt{3}] = \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{3}) \\ \sigma_2(1) & \sigma_2(\sqrt{3}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{vmatrix}^2 = [-\sqrt{3}-\sqrt{3}]^2 = (-2\sqrt{3})^2 = 2^2.3$$

O próximo resultado, mostra uma importante relação existente entre o discriminante de duas quaisquer bases de um corpo de números.

Proposição 1.2.1 *{[1], pag. 44} Sejam* $\{\beta_1, \cdots, \beta_n\}$ *e* $\{\alpha_1, \cdots, \alpha_n\}$ *bases de um corpo de números* K *tal que* $\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i$*, onde* $c_{ij} \in \mathbb{Q}$ *e* $k = 1, \cdots, n$*, então;*

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

Exemplo 1.2.5 $K = \mathbb{Q}[\sqrt{3}]$*, o conjunto* $\{3+\sqrt{3}, 3-2\sqrt{3}\}$ *é uma outra base para* K*, daí;* $\Delta[2+\sqrt{3}, 3-2\sqrt{3}] = \begin{vmatrix} 2 & 1 \\ 3 & -2 \end{vmatrix}^2 .\Delta[1,\sqrt{3}] = (-4-3)^2.2^2.3 = 7^2.2^2.3.$

Até o momento ainda não sabemos muito sobre as características do discriminante de uma base de um corpo de números, porém o próximo teorema concede duas importantes informações; uma que o discriminante é um número racional e outra com respeito ao sinal do discriminante de uma base de um corpo de números.

Teorema 1.2.3 *{[1], pag. 44} O discriminante de uma base de um corpo* K *é um número racional não nulo. Se todos os* K*-conjugados de* θ *são reais então os discriminantes das bases de* K *são positivos.*

O fato de o discriminante de uma base de um corpo de números ser um número racional é uma importante informação, pois isto mostra que o discriminante é um número algébrico sobre o corpo $\mathbb{Q}$.

1.3 Anéis de inteiros, base integral e discriminante absoluto

Até o presente momento já sabemos calcular o discriminante das bases de um corpo de números, mas pelo que vimos, para quaisquer duas base o discriminante

assume um certo valor, não necessariamente iguais entre si. Por este fato, passaremos agora nos direcionar em busca de bases de um corpo de números K que possuem o mesmo discriminante.

Definição 1.3.1 *Ao conjunto dos elementos de K que são inteiros sobre $\mathbb{Z}$, denominaremos o anel de inteiros algébricos de K o qual será denotado por $\mathbb{O}_K$. Os elementos de K que são inteiros algébricos sobre $\mathbb{Z}$ são chamados simplesmente, elementos inteiros de K.*

Em alguns casos o anel $\mathbb{O}_K$ será denominado somente com o anel de inteiros de K, ao invés de inteiros algébricos.

Observação 1.3.1 *Determinar o anel de inteiros de um corpo de números não é uma tarefa muito simples, em geral não temos calculados os anéis de inteiros dos corpos de números, mas podemos encontrar algumas particularidades como para os corpos ciclotômicos e corpos quadráticos, que analisaremos com maiores detalhes na próxima seção.*

Considerando $K = \mathbb{Q}[\theta]$ onde θ é um inteiro algébrico, temos que $\mathbb{O}_K$ contém $\mathbb{Z}[\theta]$, onde $\mathbb{Z}[\theta]$ é o conjunto dos elementos $p(\theta)$, onde $p(x) \in \mathbb{Z}[x]$. Porém, nem sempre temos $\mathbb{Z}[\theta] = \mathbb{O}_K$, por exemplo, se considerarmos o corpo de números $\mathbb{Q}[\sqrt{5}]$, temos que $\frac{1+\sqrt{5}}{2}$ é um inteiro algébrico, pois é raíz do polinômio $x^2 - x - 1$, logo $\frac{1+\sqrt{5}}{2}$ é um elemento de $\mathbb{O}_K$, porém não é um elemento de $\mathbb{Z}[\sqrt{5}]$.

Vamos agora dar um critério bastante útil, em termos de polinômio minimal, para que um certo número seja um inteiro algébrico.

Proposição 1.3.1 *{[1], pag. 49} Um número algébrico α é um inteiro algébrico se, e somente se o seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.*

É ainda interessante saber a característica dos elementos racionais, que são inteiros algébricos. Esta informação é obtidas como consequência imediata da proposição acima.

Corolário 1.3.1 {*[1], pag. 50*} *Um inteiro algébrico α é um número racional se, e somente se α é um elemente de $\mathbb{Z}$.*

Seja K um corpo de grau n, uma base para K é uma base de K como um espaço vetorial sobre $\mathbb{Q}$. Vimos no Teorema 1.2.1 que $K = \mathbb{Q}[\theta]$ onde θ é um inteiro algébrico, sendo assim $\{1, \theta, \cdots, \theta^{n-1}\}$ é uma base de K sobre $\mathbb{Q}$. O anel de inteiros $\mathbb{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n este fato implica que $\mathbb{O}_K$ possui uma base com n elementos sobre $\mathbb{Z}$. Tais bases possuem características especiais em relação a seus discriminantes e por isso recebem nome especial que é;

Definição 1.3.2 *Uma $\mathbb{Z}$ base de $\mathbb{O}_K$ é chamada de base integral de K.*

Desta forma, $\{\alpha_1, \cdots, \alpha_n\}$ é uma base integral para um corpo K se, e somente todo elemento de $\mathbb{O}_K$ é escrito unicamente da forma $a_1\alpha_1 + \cdots + a_n\alpha_n$ com $a_1, \cdots, a_n$ em $\mathbb{Z}$.

Uma base integral de um corpo K, é uma base de K sobre $\mathbb{Q}$. Mas o recíproco não é verdadeiro, ou seja, nem sempre uma $\mathbb{Q}$-base para K é uma base integral de K. Por exemplo, $K = \mathbb{Q}[\sqrt{5}]$, temos que $\{1, \sqrt{5}\}$ é uma base de K sobre $\mathbb{Q}$ mas não é uma base integral, pois o inteiro $\frac{1+\sqrt{5}}{2} \notin \mathbb{Z}.1 + \mathbb{Z}\sqrt{5}$.

Sabendo que uma base integral de um corpo de números K é uma base para K sobre $\mathbb{Q}$, é natural aparecer a pergunta, todo corpo de números possui uma base integral? A resposta para esta questão é verdadeira e comprovada pelo;

Teorema 1.3.1 {*[1], pag. 51*} *Todo corpo de números possui uma base integral e $\mathbb{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n, onde $n = [K : \mathbb{Q}]$.*

O próximo resultado nos concede uma importante relação entre os discriminantes das bases integrais de um corpo de números. Isso nos conduzirá a ter um tratamento especial para o discriminante de tais bases.

Proposição 1.3.2 *Sejam $\{\alpha_1, \cdots, \alpha_n\}$ e $\{\beta_1, \cdots, \beta_n\}$ duas bases integrais de um corpo K, então $\Delta[\alpha_1, \cdots, \alpha_n] = \Delta[\beta_1, \cdots, \beta_n]$.*

Definição 1.3.3 *Seja um corpo K de grau n, o discriminante de uma base integral de K é chamado absoluto, ou simplesmente o discriminante de K e é denotado por $\Delta(K)$.*

Encontrar uma base de um corpo de números K de certo modo, é uma tarefa simples, no entanto, saber se tal base é integral já implica um pouco mais de trabalho. No próximo teorema veremos uma condição suficiente para que uma base de um corpo de números K seja uma base integral.

Teorema 1.3.2 *{[1], pag. 53} Suponha $\{\alpha_1, \cdots, \alpha_n\}$ seja uma $\mathbb{Q}$-base para K, onde $\alpha_i \in \mathbb{O}_K$, $i = 1, \cdots, n$. Se $\Delta[\alpha_1, \cdots, \alpha_n]$ é livre de quadrado então $\{\alpha_1, \cdots, \alpha_n\}$ é uma base integral.*

A recíproca do teorema acima não é verdadeira, uma vez que existem corpos que possuem bases integrais cujo o discriminante não são livres de quadrados, como por exemplo o corpo $\mathbb{Q}[\sqrt{3}]$ tem $\{1, \sqrt{3}\}$ por base integral, porém seu discriminante não é livre de quadrados, vide Exemplo 1.2.4.

É ainda interessante notar, para fechar esta seção, que o discriminante de um corpo de números é um inteiro algébrico, daí, como consequência do Teorema 1.2.3 e do Corolário 1.3.1, temos que este é um elemento de $\mathbb{Z}$.

1.4 Polinômio característico, norma e traço

Definiremos nesta seção o conceito de norma e traço de um elemento de um corpo de números com o objetivo de relacionar tais conceitos com a idéia de discriminante vista anteriormente. O intuito aqui consiste em estabelecer fórmulas alternativas para o discriminante, em relação a definição original, usando os conceitos de norma e traço.

Definição 1.4.1 *Seja K um corpo de grau n e $\alpha \in K$ um elemento qualquer, denominamos o polinômio característico de α sobre $\mathbb{Q}$ o polinômio $f_\alpha = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$, onde os σ_i's são os monomorfismos de K em $\mathbb{C}$.*

O resultado que será visto no próximo teorema faz relação entre o polinômio característico f_α de α, com o seu polinômio minimal. Observando assim que algumas das propriedades do polinômio minimal de α são herdadas por f_α.

Teorema 1.4.1 {*[1], pag. 43*} *Seja K um corpo, consideremos respectivamente $f_\alpha(x)$ e $p(x)$ os polinômios característico e minimal de α, então;*

(a) *O polinômio característico $f_\alpha(x)$ é uma potência do polinômio minimal $p(x)$;*

(b) *Os K-conjugados de α são raízes de $p(x)$ em $\mathbb{C}$ e cada uma delas se repete $\frac{n}{m}$ vezes, onde $m = deg(p(x))$ e $n = deg(f_\alpha)$ e $m \mid n$.*

(c) *O elemento $\alpha \in \mathbb{Q}$ se, e somente se todos os seus K-conjugados são iguais;*

(d) *$K = \mathbb{Q}[\alpha]$ se, e somente se todos os K-conjugados de α são distintos.*

O fato de o polinômio característico de um elemento de um corpo de números ser uma potência de seu polinômio minimal implica que algumas das propriedades do polinômio minimal são herdades pelo característico, em especial quando este elemento for um inteiro algébrico.

Proposição 1.4.1 *Um elemento $\alpha \in K$ é um inteiro algébrico se, e somente se os coeficientes do polinômio característico f_α são elementos de $\mathbb{Z}$.*

Consideremos agora K um corpo de números de grau n e sejam $\sigma_1, \cdots, \sigma_n$ os monomorfismos de K sobre $\mathbb{C}$.

Definição 1.4.2 *Seja $\alpha \in K$ definimos, respectivamente, traço e norma de α com respeito a K, por $Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$ e $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.*

O próximo resultado determina uma característica especial para a norma e o traço de um inteiro algébrico, é que estes semelhantemente ao discriminante de um corpo de números, são elementos de $\mathbb{Z}$.

Corolário 1.4.1 {*[2], pag. 17*} *Se $\alpha \in K$ é um inteiro algébrico então $N_{K/\mathbb{Q}}(\alpha)$ e $Tr_{K/\mathbb{Q}}(\alpha)$ são inteiros algébricos e são elementos de $\mathbb{Z}$.*

Seja o corpo K de grau n, relativamente a norma e o traço de elementos de K, temos as seguintes propriedades;

(1) Sejam α e β elementos de K, temos que:

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

(2) se $\alpha,\ \beta \in K$, então;

$$Tr_{K/\mathbb{Q}}(\alpha + \beta) = Tr_{K/\mathbb{Q}}(\alpha) + Tr_{K/\mathbb{Q}}(\beta)$$

(3) Se $a \in \mathbb{Q}$ e $\alpha \in K$, então;

$N_{K/\mathbb{Q}}(a) = a^n$, $Tr_{K/\mathbb{Q}}(a) = n.a$ e $Tr_{K/\mathbb{Q}}(a.\alpha) = a.Tr_{K/\mathbb{Q}}(\alpha)$

Trabalhando com a norma e o traço podemos ainda conseguir importantes resultados que relacionam tais conceitos com o de discriminante, ou seja, são obtidos fórmulas para o discriminante de certos corpos de números usando os conceitos de norma e traço.

Proposição 1.4.2 *{[1], pag. 56} Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base de K sobre $\mathbb{Q}$, então $\Delta[\alpha_1, \cdots, \alpha_n] = det(Tr(\alpha_i.\alpha_j))$.*

Exemplo 1.4.1 *Seja $K = \mathbb{Q}[\sqrt{3}]$, temos que $\sigma_1 = id$ e $\sigma_2 = conj.$, considerando a base $\{1, \sqrt{3}\}$ de K, temos que $\sigma_1(1) = 1$, $\sigma_2(1) = 1$, $\sigma_1(\sqrt{3}) = \sqrt{3}$ e $\sigma_2(\sqrt{3}) = -\sqrt{3}$, daí;*

$$\Delta[1, \sqrt{3}] = \begin{vmatrix} Tr(1.1) & Tr(1.\sqrt{3}) \\ Tr(\sqrt{3}.1) & Tr(\sqrt{3}.\sqrt{3}) \end{vmatrix} = \begin{vmatrix} Tr(1) & Tr(\sqrt{3}) \\ Tr(\sqrt{3}) & Tr(3) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 6 \end{vmatrix} = 2.6 =$$

$$= 2^2.3$$

Analogamente ao caso do traço, conseguimos obter uma fórmula importante para o discriminante de uma base usando o conceito de norma. A qual pode ser vista na;

Proposição 1.4.3 *{[1], pag. 55} Sejam $K = \mathbb{Q}[\theta]$ um corpo de grau n e $f(x)$ o polinômio minimal de θ. A base $\{1, \theta, \cdots, \theta^{n-1}\}$ de K sobre $\mathbb{Q}$ tem discriminante*

$$\Delta[1, \theta, \cdots, \theta^{n-1}] = (-1)^{\frac{n.(n-1)}{2}}.N(f'(\theta))$$

onde $f'(x)$ é a derivada formal de $f(x)$.

Exemplo 1.4.2 *Consideremos o corpo $K = \mathbb{Q}[\sqrt{3}]$, temos que $p(x) = x^2 - 3$ é o polinômio minimal de $\theta = \sqrt{3}$, então; $\Delta[1, \sqrt{3}] = (-1)^{\frac{2.(2-1)}{2}}.N(p'(\sqrt{3})) = (-1)N(2.\sqrt{3}) = (-1)N(2).N(\sqrt{3}) = (-1).2^2.(-3) = 2^2.3$.*

A fórmula obtida na Proposição 1.4.3 acima, é de mais simples aplicação do que a fórmula original de discriminante para corpos de números, no entanto existe uma restrição, pois ela só é aplicável para corpos de números $\mathbb{Q}[\theta]$ cujo o anel de inteiros algébrico é da forma $\mathbb{Z}[\theta]$

1.5 Corpos quadráticos e ciclotômicos

Esta seção será destinada ao estudo de duas importantes classes de corpos de números, os corpos Quadráticos e Ciclotômicos. Temos com isto dois objetivos específicos, primeiro determinar o anel de inteiros algébrico destes corpos e em seguida, explicitar uma fórmula para o seu discriminante via os métodos vistos nas seções anteriores.

Definição 1.5.1 *Um corpo K é dito ser quadrático se K é uma extensão de grau 2 de $\mathbb{Q}$.*

Sendo $K = \mathbb{Q}[\alpha]$, um corpo quadrático, o polinômio minimal de α sobre $\mathbb{Q}$ tem grau 2, suponhamos que $x^2 + bx + c \in \mathbb{Q}[x]$, seja o polinômio minimal de α, então então $2\alpha = -b \pm \sqrt{b^2 - 4c}$, daí temos que $K = \mathbb{Q}[\sqrt{b^2 - 4c}]$. Por outro lado temos que $b^2 - 4c \in \mathbb{Q}$ então $b^2 - 4c = \frac{p}{q}$, onde $p, q \in \mathbb{Z}$ e $mdc(p, q) = 1$, daí $\mathbb{Q}[\sqrt{b^2 - 4c}] = \mathbb{Q}[\sqrt{\frac{p}{q}}] = \mathbb{Q}[\sqrt{\frac{p.q}{q^2}}] = \mathbb{Q}[\sqrt{p.q}]$, se decompormos $p.q$ em fatores primos, temos que

$p.q = k^2.d$, onde d é livre de quadrados, assim $\mathbb{Q}[\sqrt{p.q}] = \mathbb{Q}[\sqrt{k^2.d}] = \mathbb{Q}[\sqrt{d}]$, logo $K = \mathbb{Q}[\sqrt{d}]$.

O resultado acima, mostra que todo corpo quadrático é da forma $\mathbb{Q}[\sqrt{d}]$, onde d é um número inteiro livre de quadrado.

A partir de agora, vamos caminhar objetivando determinar o anel de inteiros de um corpo quadrático, que será estabelecido pelo seguinte;

Teorema 1.5.1 {*[1], pag.60*} *Seja $d \in \mathbb{Z}$ livre de quadrado. Então o anel de inteiro de $\mathbb{Q}[\sqrt{d}]$ é:*

(a) $\mathbb{Z}[\sqrt{d}]$, *se* $d \not\equiv 1 \ (mod\, 4)$;

(b) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ *se* $d \equiv 1 (mod\, 4)$.

Observação 1.5.1 *Se $d > 0$, dizemos que o corpo $K = \mathbb{Q}[\sqrt{d}]$ é um corpo quadrático real, de $d < 0$ o corpo $K = \mathbb{Q}[\sqrt{d}]$ é dito imaginário.*

O corpo $K = \mathbb{Q}[\sqrt{i}]$ é chamado o corpo de Gauss, que é um corpo quadrático imaginário, e $\mathbb{Z}[i]$ é o anel dos inteiros desse corpo, que é chamado de anel de inteiros de Gauss. O próximo teorema concede uma fórmula para o discriminante dos corpos quadráticos.

Teorema 1.5.2 {*[1], pag.61*}

(a) *Se $d \not\equiv 1 \ (mod\, 4)$ então $\{1, \sqrt{d}\}$ é uma base integral para o corpo $\mathbb{Q}[\sqrt{d}]$ e seu discriminante é $4d$.*

(b) *Se $d \equiv 1 (mod\, 4)$, então $\{1, \frac{1+\sqrt{d}}{2}\}$ é uma base integral de $\mathbb{Q}[\sqrt{d}]$ e o seu discriminante é d.*

Demonstração: **(a)** Se $d \not\equiv 1 \ (mod\, 4)$ pelo Teorema 1.5.1 temos que $\mathbb{Z}[\sqrt{d}]$ é o anel de interios de $\mathbb{Q}[\sqrt{d}]$, isto implica que $\{1, \sqrt{d}\}$ é uma $\mathbb{Z}$-base de $\mathbb{Z}[\sqrt{d}]$ e

$$\Delta[1, \sqrt{d}] = \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -(\sqrt{d}) \end{vmatrix}^2 = (-\sqrt{d}-\sqrt{d})^2 = (-2\sqrt{d})^2 =$$

$$= 4.d$$

(b) Se $d \equiv 1(mod\,4)$ pelo Teorema 1.5.1, temos que $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ é o anel de inteiros de $\mathbb{Q}[\sqrt{d}]$ e $\{1, \frac{1+\sqrt{d}}{2}\}$ é uma $\mathbb{Z}$-base para $\mathbb{Q}[\sqrt{d}]$ e daí;

$$\Delta[1, \frac{1}{2}+\frac{1}{2}\sqrt{d}] = \begin{vmatrix} \sigma_1(1) & \sigma_1(\frac{1}{2}+\frac{1}{2}\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\frac{1}{2}+\frac{1}{2}\sqrt{d}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = (-\sqrt{d})^2 = d$$

□

Seja K um corpo e n um inteiro positivo, um elemento $\zeta \in K$ é dito ser uma raiz n-ésima da unidade se $\zeta^n = 1$. Caso n seja o menor inteiro positivo que satisfaz esta propriedade, dizemos que ζ é uma raiz n-ésima primitiva da unidade.

Exemplo 1.5.1 *O elemento* $\zeta_n = e^{2i\pi/n} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$ *é uma raiz n-ésima primitiva da unidade.*

Pode se observar então que uma raiz n-ésima da unidade é raiz do polinômio $x^n - 1$, caso K seja um corpo algebricamente fechado segue que todas as raízes de $x^n - 1$ são distintas e, para este caso temos que o grupo multiplicativo $U_n = \{\zeta, \zeta^2, \cdots, \zeta^{n-1}, 1\}$ é cíclico, e ζ^a é um gerador de U_n se e somente se a e n são relativamente primos.

Observação 1.5.2 *Neste caso temos que o número de raízes n-ésimas primitivas da unidade é dado pela função*

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

ou seja, φ *é a função de Euler.*

Definição 1.5.2 *O polinômio* $\phi_n(x) = \prod_{j=1,\, mdc(n,j)=1}^{n} (x - \zeta_n^j)$ *será chamado o n-ésimo polinômio ciclotômico.*

Observação 1.5.3 *Pela forma em que foi definido o n-ésimo polinômio ciclotômico temos que* $deg(\phi_n(x)) = \varphi(n)$.

É interessante muitas vezes expressar o polinômio $x^n - 1$ de um modo diferente, fazendo um agrupamento das raízes da unidade que possuem o mesmo período. Este fato é mostrado através da;

Proposição 1.5.1 *{[5], pag.43} Se n é um inteiro positivo, então;*

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

Demonstração: Seja $p(x) = x^n - 1$, temos que as raízes de $p(x) = x^n - 1$ são $1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}$. Logo $x^n - 1 = (x-1).(x-\zeta_n).(x-\zeta_n^2).\cdots.(x-\zeta_n^{n-1})$, se tomarmos as raízes de mesmo período, podemos escrevê-las como polinômio $\phi_d(x) = \prod_{d=periodo\ \zeta_n} (x - \zeta_n^d)$ e $d \mid n$, portanto temos que $x^n - 1 = \prod_{d|n} \phi_d(x)$. □

Exemplo 1.5.2 *Consideremos o polinômio $p(x) = x^6 - 1$, temos que as raízes de $p(x)$ são, $1, \zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5$, possuem períodos 1,2,3 e 6. $\phi_1(x) = x - 1$, $\phi_2(x) = x - \zeta_6^3$, $\phi_3(x) = (x - \zeta_6^2).(x - \zeta_6^4)$ e $\phi_6(x) = (x - \zeta_6).(x - \zeta_6^5)$, portanto $x^6 - 1 = \phi_1(x).\phi_2(x).\phi_3(x).\phi_6(x) = (x-1).(x-\zeta_6^3).(x-\zeta_6^2).(x-\zeta_6^4).(x-\zeta_6).(x-\zeta_6^5)$.*

O próximo resultado concede um método prático para a obtenção do n-ésimo polinômio ciclotômico.

Corolário 1.5.1 *{[5], pag.43} Sendo n inteiro positivo, temos que*

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

.

Demonstração: Como $\phi_n(x) = \prod_{i=1,\, mdc(n,j)=1}^{n} (x - \zeta_n^j)$, então

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

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

Exemplo 1.5.3 *De acordo com o Corolário 1.5.1, temos que* $\phi_1(x) = x-1$, $\phi_2(x) = \frac{x^2-1}{x-1}$, $\phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1$, $\phi_4(x) = \frac{x^4-1}{(x-1).(x+1)} = \frac{x^4-1}{x^2-1} = x^2+1$ *e* $\phi_8(x) = \frac{x^8-1}{\phi_1(x)\phi_2(x)\phi_4(x)} = \frac{x^8-1}{(x^2-1)(x^2+1)} = \frac{x^8-1}{x^4-1} = x^4+1$.

Observação 1.5.4 *Quando* $n = p$, *onde* p *é um número primo, o* p*-ésimo polinômio ciclotômico é dado por*

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

.

No próximo parágrafo será definido corpos ciclotômicos, o qual desempenhará nesta seção o principal objeto de estudo. O objetivo é encontrar o anel de inteiros algébricos para esta classe de corpos de números e a partir daí calcular o seu discriminante.

Definição 1.5.3 *Consideremos a raiz* n*-ésima primitiva da unidade* ζ_n, *chamamos de o* n*-ésimo corpo ciclotômico, e denotamos por* $\mathbb{Q}(\zeta_n)$, *o corpo gerado por* ζ_n *sobre* $\mathbb{Q}$.

Exemplo 1.5.4 *O corpo* $\mathbb{Q}(-\frac{1}{2} + i\frac{\sqrt{3}}{2})$ *é um corpo ciclotômico, pois* $\alpha = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ *é uma raiz cúbica da unidade.*

Teorema 1.5.3 *{[5], pag.44} O* n*-ésimo polinômio ciclotômico* $\phi_n(x)$ *é irredutível sobre* $\mathbb{Q}$.

Demonstração: Seja $p_{\zeta_n}(x)$ o polinômio irredutível de ζ_n, assim $p_{\zeta_n}(x)$ é o polinômio de menor grau tal que $p_{\zeta_n}(\zeta_n) = 0$. Como $\phi_n(\zeta_n) = 0$, segue que $\phi_n(x) = g(x).p_{\zeta_n}(x)$, onde $g(x) \in \mathbb{Q}[x]$ e $deg(g(x)) < deg(p_{\zeta_n}(x))$, como ζ_n^j, $mdc(j,n) = 1$, é raiz de $\phi_n(x)$, temos que $g(\zeta_n^j).p_{\zeta_n}(\zeta_n^j) = 0$, se $g(\zeta_n^j) = 0$, teríamos que $g(\zeta_n) = 0$, que contradiz a minimalidade de $p_{\zeta_n}(x)$, assim temos que $p_{\zeta_n}(\zeta_n^j) = 0$ para todo j, tal que $mdc(j,n) = 1$, sendo assim, segue que $\phi_n(x) = p_{\zeta_n}(x)$, ou seja, o n-ésimo polinômio ciclotômico $\phi_n(x)$ é irredutível sobre $\mathbb{Q}$. □

Como o resultado obtido acima, juntamente com o da Observação 1.5.2, vamos obter um importante resultado com respeito ao grau do corpo $\mathbb{Q}(\zeta_n)$, que é;

Corolário 1.5.2 *{[5], pag.44} 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.*

Antes de nos concentrarmos ao estudo das características gerais dos corpos ciclotômicos, vamos considerar um caso particular destes corpos, que é o p-ésimo corpo ciclotômico, onde p é um número primo.

Lema 1.5.1 *{[5], pag. 45} Se ζ_p é uma raiz p-ésima primitiva da unidade e $K = \mathbb{Q}(\zeta_p)$, e p é um número primo, entâo;*

(1) $Tr_{K/\mathbb{Q}}(\zeta_p^j) = -1$, $j = 1, \cdots, p-1$

(2) $Tr_{K/\mathbb{Q}}(1 - \zeta_p^j) = p$ *para* $j = 1, \cdots, p-1$

(3) $N_{K/\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}.p$ *e* $N_{K/\mathbb{Q}}(1 - \zeta_p) = p$

(3) $p = (1 - \zeta_p).(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1})$.

Teorema 1.5.4 *{[1], pag. 65} Seja $K = \mathbb{Q}(\zeta_p)$, onde p é um número primo. O anel de inteiros de K é $\mathbb{Z}[\zeta_p]$.*

Este teorema nos concede uma importante informação a respeito do anel de inteiros dos corpos $\mathbb{Q}(\zeta_p)$, pois sendo este $\mathbb{Z}[\zeta_p]$, isto nos possibilita a aplicação da fórmula obtida na Proposição 1.4.3 para o cálculo do discriminante de $\mathbb{Q}(\zeta_p)$.

A partir de agora tomaremos rumo à um traçado mais geral referente a este conceito, isto é, buscaremos encontrar o anel de inteiros, e consequêntemente uma base integral para um corpo ciclotômico qualquer. Mas para isso, é necessário que façamos um estudo a respeito dos corpos compostos KL.

Definição 1.5.4 *Sejam K, L corpos, o corpo composto KL é o menor subcorpo de $\mathbb{C}$ que contém K e L, formado por todas as somas finitas*

$$\alpha_1\beta_1 + \cdots + \alpha_n\beta_n, \text{ onde } \alpha_i \in K \text{ e } \beta_i \in L,\ i = 1, 2, \cdots, n$$

Sejam $\mathbb{O}_K$, $\mathbb{O}_L$ e $\mathbb{O}_{KL}$ os anéis de inteiros de K,L e KL respectivamente. Temos que o anel $\mathbb{O}_{KL}$ contém o anel $\mathbb{O}_L\mathbb{O}_K = \{\alpha_1\beta_1 + \cdots + \alpha_n\beta_n\}$, onde $\alpha_i \in \mathbb{O}_K$ e $\beta_i \in \mathbb{O}_L$, para $i = 1, 2, \cdots, n$. Em geral não temos a igualdade entre os anéis $\mathbb{O}_L\mathbb{O}_K$ e $\mathbb{O}_{KL}$, mas podemos ter $\mathbb{O}_L\mathbb{O}_K = \mathbb{O}_{KL}$, sob algumas circunstâncias dos corpos ciclotômicos. Sejam m e n o grau de K e L respectivamente, seja $d = mdc(d_1, d_2)$, onde d_1 e d_2 são os discriminantes de K e L respectivamente .

Teorema 1.5.5 *{[5], pag. 53} Se $[KL : \mathbb{Q}] = m.n$, então $\mathbb{O}_{KL} \subseteq \frac{1}{d}\mathbb{O}_K\mathbb{O}_L$.*

Corolário 1.5.3 *{[5], pag. 54} Se $[KL : \mathbb{Q}] = m.n$ e $d = 1$, ou seja, o discriminante de K e L são relativamente primos, então $\mathbb{O}_{KL} = \mathbb{O}_K\mathbb{O}_L$.*

Demonstração: Temos que $\mathbb{O}_K\mathbb{O}_L \subseteq \mathbb{O}_{KL}$ e pelo teorema anterior temos que $\mathbb{O}_{KL} \subseteq \frac{1}{d}\mathbb{O}_K\mathbb{O}_L$, como $d = 1$, segue que $\mathbb{O}_{KL} \subseteq \mathbb{O}_K\mathbb{O}_L$, portanto $\mathbb{O}_{KL} = \mathbb{O}_K\mathbb{O}_L$ □

Se considerarmos ζ_m e ζ_n raízes m, n-ésimas da unidade e se $m.n = w$ e $mdc(m, n) = 1$, teremos que o corpo $\mathbb{Q}(\zeta_w)$ é o corpo composto $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$. Com isto, o próximo lema será de fundamental importância na obtenção do anel de inteiros de um corpo ciclotômico.

Lema 1.5.2 *{[5], pag. 41} 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 m.n-ésima primitiva da unidade se, e somente se ζ_m^k é uma raíz m-ésima primitiva da unidade e ζ_n^l é uma raíz n-ésima primitiva da unidade.*

Teorema 1.5.6 *{[5], pag. 55} O anel de inteiros de $K = \mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$.*

Demonstração: Suponhamos $n = n_1.n_2$, onde $mdc(n_1, n_2) = 1$ sendo ambos, n_1, n_2, maiores que um. Sendo assim, em conformidade com o Lema 1.5.2 temos $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$ e ainda $\varphi(n) = \varphi(n_1).\varphi(n_2)$. De acordo a Proposição 1.4.3 temos $\Delta[1, \alpha, \cdots, \alpha^{n-1}] = (-1)^{\frac{n.(n-1)}{2}}.N(p'_\alpha(\alpha))$, onde $p_\alpha(x)$ é o polinômio minimal de α. Sejam d_{n_1} e d_{n_2} os discriminantes de $\mathbb{Q}(\zeta_{n_1})$ e $\mathbb{Q}(\zeta_{n_2})$ respectivamente. Sendo $p_\alpha(x) = x^{n_1} - 1$, segue que $p'_\alpha(x) = n_1.x^{n_1-1}$, aplicando ζ_{n_1} teremos $p'_\alpha(\zeta_{n_1}) =$

$n_1.\zeta_{n_1}^{n_1-1} = \frac{n_1}{\zeta_{n_1}}$, então $N(p'_\alpha(\zeta_{n_1})) = \frac{N(n_1)}{N(\zeta_{n_1})} = \frac{n_1^{\varphi(n_1)}}{\pm 1} = \pm n_1^{\varphi(n_1)}$, daí, $d_{n_1} = \pm n_1^{\varphi(n_1)}$, ou seja, $d_{n_1} \mid n_1^{\varphi(n_1)}$. De modo análogo, temos $d_{n_2} \mid n_2^{\varphi(n_2)}$. Sendo $mdc(d_{n_1}, d_{n_2}) = d$ segue que $\begin{cases} d \mid d_{n_1} \text{ e } d_{n_1} \mid n_1^{\varphi(n_1)} \Longrightarrow d \mid n_1^{\varphi(n_1)} \\ d \mid d_{n_2} \text{ e } d_{n_2} \mid n_2^{\varphi(n_2)} \Longrightarrow d \mid n_2^{\varphi(n_2)} \end{cases}$

Como $mdc(n_1^{\varphi(n_1)}, n_2^{\varphi(n_2)}) = 1$, segue que $d = 1$, Assim, pelo Corolário 1.5.3 segue que $\mathbb{Z}(\zeta_n) = \mathbb{Z}(\zeta_{n_1})\mathbb{Z}(\zeta_{n_2})$, portanto $\mathbb{O}_K = \mathbb{Z}(\zeta_n)$ □

Nos parágrafos anteriores desta seção nos exercitamos basicamente em expressar uma base integral e encontrar o anel de inteiros algébricos dos corpos ciclotômicos. A partir de agora, já sabedores dos resultados anteriores, partamos em busca de expressar uma fórmula geral para o discriminante destes corpos. Porém antes será feito o caso especial que estamos considerando $\mathbb{Q}(\zeta_p)$.

Proposição 1.5.2 *{[5], pag. 65} Seja $K = \mathbb{Q}(\zeta_p)$, onde p é um número primo ímpar, então o discriminante de K é expresso por;*

$$\Delta[1, \zeta_p, \cdots, \zeta_p^{p-2}] = (-1)^{\frac{p-1}{2}}.p^{p-2}$$

Demonstração: Conforme o Teorema 1.5.4 segue que $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ é uma base integral para $\mathbb{Q}(\zeta_p)$. Assim, pela Proposição 1.4.3 segue que $\Delta[1, \zeta_p, \cdots, \zeta_p^{p-2}] = (-1)^{\frac{(p-2).(p-1)}{2}}.N_{K/\mathbb{Q}}(\phi'_p(\zeta_p))$.

Como $\phi_p(x) = \frac{x^p-1}{x-1}$, segue que $\phi'_p(\zeta_p) = \frac{p.\zeta_p^{p-1}.(\zeta_p-1)-[(\zeta_p^p-1).1]}{(\zeta_p-1)^2} = \frac{p.\zeta_p^{p-1}.(\zeta_p-1)}{(\zeta_p-1)^2} = \frac{p.\zeta_p^{p-1}}{\zeta_p-1} = -\frac{p.\zeta_p^{p-1}}{1-\zeta_p}$. Daí, $N_{K/\mathbb{Q}}(\phi'_p(\zeta_p)) = N_{K/\mathbb{Q}}(-\frac{p.\zeta_p^{p-1}}{1-\zeta_p}) = \frac{N_{K/\mathbb{Q}}(-p).N(\zeta_p)^{p-1}}{N_{K/\mathbb{Q}}(1-\zeta_p)} =$
$= \frac{(-p)^{p-1}.1^{p-1}}{p} = (-1)^{p-1}.p^{p-2} = p^{p-2}$. Assim, $\Delta[1, \zeta_p, \cdots, \zeta_p^{p-2}] =$
$= (-1)^{\frac{(p-1).(p-2)}{2}}.p^{p-2} = (-1)^{\frac{p-1}{2}}.p^{p-2}$ □

Um caso interessante que também merece ser retratado é a obtenção de uma fórmula para o discriminante de um p^r-ésimo corpo ciclotômico que é expresso pela seguinte;

Proposição 1.5.3 *{[5], pag. 65} Se $K = \mathbb{Q}(\zeta_{p^r})$, onde $1 < r \in \mathbb{Z}$ e p um número primo ímpar, então o discriminante de $K = \mathbb{Q}(\zeta_{p^r})$ é dado por;*

$$\Delta[1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{(p-1).p^{r-1}-1}] = \pm p^{p^{r-1}.[r(p-1)-1]}$$

Para finalizarmos esta seção, falta então um último resultado que é a fórmula do discriminante dos corpos ciclotômicos $\mathbb{Q}(\zeta_n)$. Para alcançarmos então os nossos objetivos vamos passar por alguns resultados que serão importantes na computação da fórmula do discriminante dos corpos $\mathbb{Q}(\zeta_n)$.

Definição 1.5.5 *Sejam K e L corpos de números, $\{\alpha_1, \cdots, \alpha_n\}$ e $\{\beta_1, \cdots, \beta_m\}$, bases de K e L sobre $\mathbb{Q}$ respectivamente. Dizemos que K e L são linearmente disjuntos quando $\{\alpha_1\beta_1, \cdots, \alpha_n\beta_m\}$ é uma base de KL sobre $\mathbb{Q}$.*

Exemplo 1.5.5 *Sejam ζ_n e ζ_m raízes n, m-ésimas primitivas da unidade, respectivamente, caso $mdc(m, n) = 1$ temos que os corpos $\mathbb{Q}(\zeta_n)$ e $\mathbb{Q}(\zeta_m)$ são linearmente disjuntos.*

Para os próximos parágrafos vamos escrever $\Delta(L/K)$ para denotar o discriminante de uma base integral de L sobre K, e $N_{L/K}$ para denotar a norma de L sobre K.

Proposição 1.5.4 *{[5], pag. 66} Sejam K, L e M corpos de números tais que $K \subseteq L \subseteq M$. Se $[L : K] = n$ e $[M : L] = m$, então;*

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

Proposição 1.5.5 *{[5], pag. 68} Sejam K e L corpos de números, tais que $K \subseteq L$. Se $[KL : L] = n$ e $[KL : K] = m$, então $N_{L/\mathbb{Q}}(\Delta(KL/L))$ divide $\Delta(K)^m$ e $N_{K/\mathbb{Q}}(\Delta(KL/K))$ divide $\Delta(L)^n$.*

Considerando corpos K, L tais que sejam linearmente disjuntos, o discriminante dos composto KL, denota um produto entre potências dos discriminantes de K e L. Mas é claro, isso só vai ocorrer sob a circunstância de o discriminante de ambos os corpos sejam primos entre si, como pode ser visto na;

Proposição 1.5.6 *{[5], pag. 68} Sejam K e L corpos de graus n e m respectivamente. Se $\Delta(K)$ e $\Delta(L)$ são relativamente primos e K, L linearmente disjuntos, então;*

$$\Delta(KL) = \Delta(K)^m.\Delta(L)^n$$

Enfim, agora temos informações o suficiente para estabelecer uma fórmula para o discriminante de um corpo ciclotômico qualquer, isto será feito através do próximo teorema.

Teorema 1.5.7 {*[5], pag. 69*} *Se $K = \mathbb{Q}(\zeta_n)$, onde n é um inteiro maior que 1, então o discriminante de $\mathbb{Q}(\zeta_n)$ é dado por;*

$$\Delta[1, \zeta_n, \cdots, \zeta_n^{\varphi(n)-1}] = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}$$

Demonstração: Se $n = p_1^{\alpha_1}.p_2^{\alpha_2}$, considerando $K_1 = \mathbb{Q}(\zeta_{p_1^{\alpha_1}})$ e $K_2 = \mathbb{Q}(\zeta_{p_2^{\alpha_2}})$, da Proposição 1.5.6 segue que $\Delta(K_1K_2) = \Delta(K_1)^{[K_2:\mathbb{Q}]}.\Delta(K_2)^{[K_1:\mathbb{Q}]}$, aplicando a função logaritmo na igualdade acima, segue que $log|\Delta(K_1K_2)| = [K_2 : \mathbb{Q}].log|\Delta(K_1)| + [K_1 : \mathbb{Q}].log|\Delta(K_2)|$, como K_1 e K_2 são linearmente independentes, então $[K_1K_2 : \mathbb{Q}] = [K_1 : \mathbb{Q}].[K_2 : \mathbb{Q}]$, daí,

$$\frac{log|\Delta(K_1K_2)|}{[K_1K_2 : \mathbb{Q}]} = \frac{log|\Delta(K_1)|}{[K_1 : \mathbb{Q}]} + \frac{log|\Delta(K_2)|}{[K_2 : \mathbb{Q}]}$$

daí, de um modo geral, se $n = \prod_{i=1}^{n} p_i^{\alpha_i}$ teremos;

$$\frac{log|\Delta(K_1)}{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]} = \frac{log|\Delta(K_1)|}{[\mathbb{Q}(\zeta_{p_1^{\alpha_1}}) : \mathbb{Q}]} + \cdots + \frac{log|\Delta(K_n)|}{[\mathbb{Q}(p_n^{\alpha_n}) : \mathbb{Q}]} = \sum_{i=1}^{n} \frac{log|\Delta(K_i)|}{\varphi(p_i^{\alpha_i})}$$

onde $K_i = \mathbb{Q}(\zeta_{p_i^{\alpha_i}})$, $i = 1, \cdots, n$. Assim, pelo Proposição 1.5.3, segue que

$$\frac{log|\Delta(K)|}{\varphi(n)} = \sum_{i=1}^{n} \frac{logp_i^{p_i^{\alpha_i-1}.[\alpha_i(p_i-1)-1]}}{p_i^{\alpha_i-1}.(p_i-1)} = \sum_{i=1}^{n} \frac{p_i^{\alpha_i-1}.[\alpha_i(p_i-1)-1].logp_i}{p_i^{\alpha_i-1}.(p_i-1)}$$

$$= \sum_{i=1}^{n} (\alpha_i - \frac{1}{p_i - 1}).log\, p_i = \sum_{i=1}^{n} \alpha_i.log\, p_i - \sum_{i=1}^{n} \frac{log\, p_i}{p_i - 1} = \sum_{i=1}^{n} log\, p_i^{\alpha_i} - \sum_{i=1}^{n} log\, p_i^{\frac{1}{p_i-1}}$$

$$= log\,(\prod_{i=1}^{n} p_i^{\alpha_i}) - log\,(\prod_{i=1}^{n} p_i^{\frac{1}{p_i-1}}) = log(n) - log\,(\prod_{i=1}^{n} p_i^{\frac{1}{p_i-1}})$$

Daí, $log\,|\Delta(K)| = \varphi(n).[log(n) - log(\prod_{i=1}^{n} p_i^{\frac{1}{p_i-1}})] = log[\frac{n}{\prod_{i=1}^{n} p_i^{\frac{1}{p_i-1}}}]^{\varphi(n)}$, portanto;

$$\Delta(K) = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}$$

□

1.6 Reticulados algébricos: uma aplicação para o discriminante mínimo

Nesta seção vamos mostrar alguns tópicos referentes aos reticulados algébricos que mostram a importância do conceito de discriminante de corpos de números. Entre tais, enfatizaremos o problema da maximização da densidade de centro de um reticulado. Onde este é apontado como sendo uma das principais aplicações do conceito de discriminante mínimo de corpos de números de mesmo grau. Seja A um ideal de $\mathbb{O}_K$, o conceito de norma de um ideal é importante e será útil dentro dos propósitos aqui estabelecidos.

Definição 1.6.1 *Seja $\mathcal{A}$ um subanel de $\mathbb{O}_K$. Definimos por norma do ideal $\mathcal{A}$, e denotamos por $N(\mathcal{A})$, o número de elementos do anel quociente $\mathbb{O}_K/\mathcal{A}$, ou seja $|N(\mathcal{A})| = \#(\mathbb{O}_K/\mathcal{A})$.*

Proposição 1.6.1 *{[2], pag. 34} Seja $\mathcal{A}$ um ideal não nulo de $\mathbb{O}_K$. Então $N(\mathcal{A})$ é finita.*

Proposição 1.6.2 *{[2], pag. 33} Se $x \in \mathbb{O}_K$, $x \neq 0$, então $|N(x)| = \#(\mathbb{O}_K/\mathbb{O}_K x)$.*

Consideremos agora um corpo de números K de grau n, conforme o Teorema 1.2.2, existem n monomorfismos distintos $\sigma_i : K \longrightarrow \mathbb{C}$. Sendo $K = \mathbb{Q}[\theta]$, então o polinômio minimal $p(x)$ de θ sobre $\mathbb{Q}$ possui grau n, logo possui n raízes distintas, assim segue que $\sigma_i(\theta)$, $i = 1, \cdots, n$ são raizes de $p(x)$. Lembrando que se um polinômio $f(x)$ possui uma raiz complexa, então o conjugado desta raiz é também raiz de $f(x)$, isso implica que um polinômio possui um número par de raizes complexas.

Sendo $\sigma_i(K) \subset \mathbb{R}$, dizemos que σ_i é real, se não, σ_i é imaginário. Se todos os n-monomorfismos de K forem reais, dizemos que K é um corpo totalmente real e analogamente, se são todos imaginários, K é denominado totalmente imaginário. Se

$\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ é a conjugação complexa, temos que para todo i, $\alpha \circ \sigma_i = \sigma_j$, para algum $j = 1, \cdots, n$ e $\alpha \circ \sigma_i = \sigma_i$ se, e somente se, σ_i é real. Denotemos por r_1 o número de índices i, para os quais σ_i seja real, da observação feita no parágrafo acima temos que o número de σ_i's imaginários é par e denotemos por $2r_2$ o número destes σ_i imaginários.

Se enumerarmos os σ_i's reais para $1 \leq i \leq r_1$ e os σ_j's imaginários para $r_1 + 1 \leq j \leq r_1 + r_2$ e como $\sigma_{j+r_2} = \overline{\sigma_j}$ temos que os $r_1 + r_2$ primeiros monomorfismos σ_i determinam os outros r_2. Daí a função $\sigma_K : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definida por $\sigma_K(x) = (\sigma_1(x), \cdots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \cdots, \sigma_{r_1+r_2}(x))$, $\in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ é um homomorfismo, e é definida como homomorfismo canônico de K em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, o qual é injetivo.

Exemplo 1.6.1 *Consideremos o corpo $K = \mathbb{Q}[\sqrt{2}]$, $\{\sigma_0, \sigma_1\}$ é o grupo dos $\mathbb{Q}$-monomorfismos de K sobre $\mathbb{C}$, onde σ_0 é a inclusão e σ_1 é a conjugação. Assim, $\sigma_0(a+b\sqrt{2}) = a+b\sqrt{2}$ e $\sigma_1(a+b\sqrt{2}) = a-b\sqrt{2}$, portanto, $\sigma_K(x) = (\sigma_0(x), \sigma_1(x)) = (a + b\sqrt{2}, a - b\sqrt{2})$.*

No Teorema 1.2.3 foi dado implicitamente uma informação a respeito do sinal do discriminante de um corpo de números, no entanto, com o próximo teorema, é dado um resultado mais geral envolvendo este conceito.

Teorema 1.6.1 *{[4], pag. 13} Se K é um corpo de números então o sinal do discriminante de K é $(-1)^{r_2}$.*

Se K for um corpo de números tal que r_2 seja par, então seu discriminante é positivo, em particular se K for totalmente real, então seu discriminante é positivo pois neste caso $r_2 = 0$.

Exemplo 1.6.2 *Consideremos $K = \mathbb{Q}[i]$, temos que os monomorfismos de K em $\mathbb{C}$ são σ_1 e σ_2, que são respectivamente a identidade e a conjugação complexa,temos assim que K é totalmente imaginário e $r_2 = 1$, logo o discriminante de $K = \mathbb{Q}[i]$ é negativo.*

Os homomorfismos canônicos têm uma aplicabilidade de grande importância que consiste na geração de reticulados no $\mathbb{R}^n$. Embora neste trabalho não tomaremos rumo aos reticulado, é importante a esta altura fazer uma breve explanação relativo a este assunto, uma vez que o discriminante desempenha um papel importante dentro deste campo.

Consideremos L um espaço vetorial sobre $\mathbb{R}$ de dimensão n, então L é isomorfo ao $\mathbb{R}^n$. Se considerarmos $\{l_i, \cdots, l_n\} \subset L$, e se os l_i's forem linearmente independentes em $\mathbb{R}$, então o conjunto $H = \mathbb{Z}l_1 + \cdots + \mathbb{Z}l_n = \{\sum_{i=1}^{n} \alpha_i l_i \ \alpha_i \in \mathbb{Z}\}$ é denominado Reticulado de L. Desta forma, podemos dizer que um Reticulado é um subgrupo discreto do $\mathbb{R}^n$ e é gerado como um $\mathbb{Z}$-módulo por uma base de $\mathbb{R}^n$. Ao conjunto $T_L = \{\sum_{i=1}^{n} \alpha_i l_i,\ 0 \leq \alpha_i < 1,\ i = 1, \cdots, m\}$ denominamos região fundamental do reticulado H, associado a base $\{l_i, \cdots, l_n\}$.

Exemplo 1.6.3 *$\mathbb{Z}$ é um reticulado em $\mathbb{R}$ e $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$ é um reticulado em $\mathbb{R}^n$ gerado por $\{e_i, \cdots, e_n\}$, a base canônica do $\mathbb{R}^n$.*

Além da região fundamental T_L o reticulado H possui ainda outras regiões $l+T_L$, onde $l \in H$ e a união de todos estas regiões $l + T_L$ cobre todo o espaço L.

O volume da região T_L é calculado por $Vol(T_L) = |det(\alpha_{ij})|$, $l_i = \sum_{j=1}^{l} \alpha_{ij} e_j$, $\alpha_{ij} \in \mathbb{R}$, onde $\{e_j\}$, $j = 1, \cdots, n$ é a base canônica do $\mathbb{R}^n$, e tal volume é denominado o volume do reticulado H e será denotado por $\mathcal{V}(H)$.

Os reticulados ganha interesse neste trabalho quando é direcionado a estudar os reticulados sobre um corpo de números K. Tais reticulados são gerados pelos ideais do anel de inteiros de K via o homomorfismo Canônico. O volume desta classe de reticulados depende diretamente do discriminante do corpo de números envolvido, como pode ser visto no;

Teorema 1.6.2 *{[4], pag. 14} Sejam K um corpo de grau n, $\mathbb{O}_K$ o seu anel de inteiros algébricos e A um ideal de $\mathbb{O}_K$. Então $\sigma_K(\mathbb{O}_K)$ e $\sigma_K(A)$ são reticulados em $\mathbb{R}^n$ e, temos*

$$\mathcal{V}(\sigma_K(\mathbb{O}_K)) = 2^{-r_2}\sqrt{|\Delta(K)|} \ e \ \ \mathcal{V}(\sigma_K(A)) = 2^{-r_2}\sqrt{|\Delta(K)|}.N(A)$$

Um outro problema importante é o do empacotamento de esferas de mesmo raio em $\mathbb{R}^n$. Os centros destas esferas formam um reticulado, denominado reticulado de empacotamento, denotado por H_E. Assim, se tem um outro problema que é a obtenção de um bom empacotamento, ou seja, uma disposição de esferas de mesmo raio, duas a duas se interceptando em um único ponto, que melhor se aproxime do espaço $\mathbb{R}^n$. Deste modo é preciso encontrar um reticulado de empacotamento H_E de maior densidade. Esta densidade é calculada pelo quociente do volume da esfera pelo volume do reticulado.

Assim, no processo de maximização da densidade de um reticulado, obtemos um outro parâmetro que é a maximização da densidade de centro, dado pela fórmula;

$$\delta(H_E) = \frac{2^{r_2}}{\sqrt{|\Delta(K)|}} . \frac{\rho^n}{N(\mathcal{A})} \tag{1.1}$$

Onde r_2 é a metade do número de imersões complexas de K em $\mathbb{C}$ e ρ é o raio das esferas do empacotamento e $N(\mathcal{A})$ é a norma do ideal $\mathcal{A}$.

No entanto, existem vários formas para se maximizar $\delta(H_E)$; fazendo a expansão do raio ρ e outra é fazendo a minimização de $\sqrt{|\Delta(K)|}$ que consiste em minimizar $|\Delta(K)|$, onde $\Delta(K)$ é o discriminante do corpo que contém o ideal $\mathcal{A}$.

O problema da maximização da densidade de centro de um reticulado, caracterizada pela fórmula acima, é o principal problema em que se aplica o conceito do discriminante mínimo de um corpo de números. Aí então é que surge a importância e a principal motivação para estudar este conceito.

Capítulo 2

Caracteres Modulares e a Fórmula do Condutor-Discriminante

Neste capítulo serão expostos importantes conceitos sobre a teoria de caracteres, em especial, os caracteres de Derichlet ou Modulares. Isto será feito com o objetivo de estabelecer uma outra fórmula que possibilita calcular o discriminante de subcorpos de $\mathbb{Q}(\zeta_n)$, a qual é conhecida como a fórmula do Condutor-Discriminante [Teorema 2.3.3]. No entanto, para atingir este propósito satisfatoriamente, será necessário nos apropriarmos de alguns conceitos da Teoria de Galois, em especial, o teorema fundamental desta teoria [Teorema 2.1.1].

Em suma, a fórmula do Condutor-Discriminante possibilita calcular o discriminante de um corpo de números abeliano qualquer. Uma vez que o Teorema de Kronecker-Weber [Teorema 2.1.2], nos assegura que todo corpo abeliano esta contido em uma extensão ciclotômica. É interessante ressaltar que, aqui, neste trabalho não serão feitos as demonstrações dos respectivos teoremas citados a cima. Uma vez que o nosso propósito é, apropriarmos das informações neles contidas para alcançarmos a principal meta estabelecida para este trabalho.

No final deste capítulo é feito uma seção destinada ao estudo dos caracteres de Dirichlet definidos módulo p^r, onde p é um número primo. Isto será feito com o intuito de estabelecer uma fórmula para discriminante dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$. Para

desenvolvermos os conceitos apresentados neste capítulo, foram utilizados partes substanciais das referências [3] à [8].

2.1 Teoremas; Fundamental de Galois e Kronecker-Weber

É oportuno o momento começarmos este capítulo enunciando os teoremas Fundamental de Galois e Kronecker-Weber que são alguns dos principais teoremas encontrados nos textos de algebra e teoria dos números os quais serão de fundamental importância para obtenção de um dos grandes resultados deste trabalho, a saber, a Fórmula do Condutor-Discriminante. Toda teoria que é apresentada aqui nesta seção é considerada sobre corpos de característica zero, mas é claro não poderíamos deixar de destacar a sua validade para corpos finitos em geral.

Definição 2.1.1 *Sejam L e K corpos, tais que L/K, dizemos que L é uma extensão galoisiana de K quando L é corpo de raízes para algum polinômio não nulo pertencente a $K[x]$. Por outro lado, L é chamada de extensão normal de K se L é corpo de raízes para quaisquer polinômio irredutível de $K[x]$ sobre K.*

Proposição 2.1.1 {*[3], pag.170*} *Seja L/K uma extensão finita. Então L/K é galoisiana se, e somente se L/K é normal*

Exemplo 2.1.1 *Consideremos os corpos $K = \mathbb{Q}$, $M = \mathbb{Q}[\sqrt[3]{2}]$ e $L = \mathbb{Q}[\sqrt[3]{2}, \omega]$, sendo $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{3}i$. Observe que $K \subset M \subset L$. Como $p(x) = x^3 - 2$ é o polinômio irredutível de L sobre K, assim temos que L é uma extensão galoisiana de K, porém M não é galoisiana em relação a K.*

Sendo $G = Aut_K L$, dizemos que K é o corpo dos invariantes por G, se H é subgrupo de G, o conjunto dos invariantes por H é um corpo intermediário da extensão L/K.

Sejam L, M, K corpos tais que $L \supset M \supset K$ e $[L : K] < \infty$, se L/K é galoisiana, então L/M é também galoisiana, mas nem sempre M/K será uma extensão galoisiana, como pode ser observado no Exemplo 2.1.1. Assim, M/K é galoisiana se, e somente se o grupo $H = Aut_M L$ é um subgrupo normal de G.

Definição 2.1.2 *Seja L/K uma extensão galoisiana. O grupo $G = Aut_K L$ é chamado o grupo de Galois desta extensão e é denotado por $G = Gal(L/K)$. Se G é abeliano então dizemos que L/K é uma extensão abeliana.*

Denotemos que $\mathcal{I}(L/K)$ o conjunto dos corpos intermediários da extensão L/K e por $\mathcal{S}(G)$ o conjunto dos subgrupos de G. Consideremos também as seguintes correspandências; $\psi : \mathcal{I}(L/K) \longrightarrow \mathcal{S}(G)$, $\psi(M) = Aut_M L$ e $\varphi : \mathcal{S}(G) \longrightarrow \mathcal{I}(L/K)$, $\varphi(H) = \{a \in L : \gamma(a) = a,\ \gamma \in H\}$.

Proposição 2.1.2 *{[3], pag. 180} Com as notações acima, temos;*

(a) *Se $M_1, M_2 \in \mathcal{I}(L/K)$ e $M_1 \subseteq M_2$, então $\psi(M_2) \subseteq \psi(M_1)$*

(a) *Se $H_1, H_2 \in \mathcal{S}(G)$ e $H_1 \leq H_2$, então $\varphi(H_2) \subseteq \varphi(H_1)$*

(c) *$\forall\, M \in \mathcal{I}(L/K)$ tem-se $(\varphi \circ \psi)(M) \supseteq M$*

(d) *$\forall\, H \in \mathcal{S}(G)$, tem-se $H \leq (\psi \circ \varphi)(H)$*

O próximo Teorema é um resultado devido a Evarist Galois, este resultado é de grande importância em vários ramos da algebra em especial na teoria de Grupos e Corpos. Iremos usá-lo mais a frente para estudar a teoria dos caracteres de Dirichlet.

Teorema 2.1.1 *(Teorema Fundamental de Galois) {[3], pag. 181} Seja L/K uma extensão galoisiana, então:*

(1) *$\forall\, M \in \mathcal{I}(L/K)$, tem-se $[L : M] = |\psi(M)|$ e $[M : K] = (G : \psi(M))$*

(2) *$\forall\, H \in \mathcal{S}(G)$, tem-se $[L : \varphi(H)] = |H|$ e $[\varphi(H) : K] = (G : H)$*

(3) *$\psi \circ \varphi = I_{\mathcal{S}(G)}$ e $\varphi \circ \psi = I_{\mathcal{I}(L/K)}$*

(4) $\forall\, M \in \mathcal{I}(L/K)$, M/K, *é galoisiana se, e somente se* $\psi(M) = Aut_M L$ *é um subgrupo normal de* G

(5) *Seja* $M \in \mathcal{I}(L/K)$. *Se* M/K *é galoisiana, então* $[M : K] = |Aut_K M|$ *e* $G/\psi(M) \simeq Aut_K M$

O teorema acima diz que se L/K é uma extensão galoisiana então ψ e φ são bijetivas e inversas entre si. Isso mostra a existência de uma correspondência bijetiva a qual é denominada, correspondência de Galois.

Em suma, o que este último teorema apresenta é uma relação entre os subcorpos de uma extensão L/K com os subgrupos de $Gal(L/K)$. Logo, isto permite obter informações de subcorpos de L/K, via seus subgrupos correspondente em $Gal(L/K)$.

É oportuno neste momento enunciarmos o teorema de Kronecker-Weber, o qual por sua força constitui um dos pilares fundamentais deste trabalho e que o mesmo esta íntimamente ligado com os conceitos da Teoria de Galois.

Teorema 2.1.2 *(Kroncker-Weber)* {*[6], pag.319*} *Seja* K *um corpo de números Abeliano, então* K *está contido em algum corpo ciclotômico.*

Este último teorema é um importante resultado dentro da teoria dos números e neste trabalho, o mesmo desempenhará um papel fundamental na obtenção do discriminante de um corpo abeliano. Pois, considerando um corpo abeliano K, ele garante a existência de um corpo ciclotômico $\mathbb{Q}(\zeta_m)$ onde $K \subseteq \mathbb{Q}(\zeta_m)$, daí o cálculo do discriminante K é feito aproveitando algumas propriedades aritméticas de $\mathbb{Q}(\zeta_m)$.

2.2 Caracteres em grupos abelianos finitos

Apresentaremos nesta seção as principais propriedades dos caracteres de um grupo Abeliano, em especial estaremos interessados em informações a respeito do conjunto que forma o núcleo de um caracter.

Definição 2.2.1 *Um caracter de um grupo Abeliano finito* G *é um homomorfismo* $\chi : G \longrightarrow \mathbb{C}^*$.

Exemplo 2.2.1 *Seja $G = U_n = \{1, \zeta_n, \cdots, \zeta_n^{n-1}\}$ o grupo das raízes n-ésima da unidade, o homomorfismo $\chi_i : G \longrightarrow \mathbb{C}^*$ dado por $\chi_i(\zeta_n) = \zeta_n^i$, é um caracter, com $0 \leq i \leq n-1$.*

Sendo G um grupo de ordem n, denotaremos por $\widehat{G}$ o conjuntos dos caracteres de G. Tomando $\chi \in \widehat{G}$ e $a \in G$, temos que $1 = \chi(e) = \chi(a^n) = \chi(a)^n$, onde e é o elemento neutro de G. Isso mostra que $\chi(a)$ é uma raiz n-ésima da unidade e $\chi(G)$ é um subgrupo das raízes n-ésima da unidade contidas em $\mathbb{C}^*$.

Agora, consideremos H um subgrupo de G; pelo fato de cada caracter de G ser um homomorfismo, temos que um caracter de G restrito a H é ainda um caracter de H.

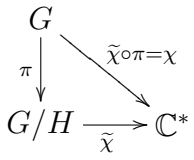
Consideremos os caracteres χ, χ' pertencentes a $\widehat{G}$ e definamos $\chi.\chi' : G \longrightarrow \mathbb{C}^*$ por $\chi.\chi'(x) = \chi(x).\chi'(x)$, $\forall x \in G$. Temos que $\chi.\chi'(x) = \chi(x).\chi'(x) = \chi'(x).\chi(x) = \chi'(x).\chi(x) = \chi'.\chi(x)$ e $\chi_0 : G \longrightarrow \mathbb{C}^*$, tal que $\chi_0(x) = 1$ $\forall x \in G$ é o elemento neutro de $\widehat{G}$, e a conjugação complexa $\overline{\chi} : G \longrightarrow \mathbb{C}^*$, $\overline{\chi}(g) = \overline{\chi(g)}$, é o elemento inverso de χ em $\widehat{G}$. Assim, com todas estas propriedades constatamos que $\widehat{G}$ é um grupo Abeliano, com a operação acima descrita.

Consideremos agora H e G grupos abeliano finito, se $\varphi : H \longrightarrow G$ é um homomorfismo, então φ induz o homomorfismo $\widehat{\varphi} : \widehat{G} \longrightarrow \widehat{H}$ dado por $\widehat{\varphi}(\chi) = \chi \circ \varphi$. Este homomorfismo na verdade é um caracter de H induzido pelo homomorfismo φ via a composição de um caracter de G. Assim, segue que $Ker(\widehat{\varphi}) = \{\chi \in \widehat{G} : \widehat{\varphi}(\chi) = 1\} = \{\chi \in \widehat{G} : \chi(\varphi(a)) = 1, \forall a \in H\}$, ou seja, o núcleo de $\widehat{\varphi}$ é o conjunto dos caracteres de G que restritos a imagem de φ é o caracter trivial

Agora, pensando em H como um subgrupo de G e φ como sendo a inclusão, podemos extrair algumas propriedades importantes a respeito do núcleo de $\widehat{\varphi}$. Denotando neste caso $Ker(\widehat{\varphi})$ por $H^\perp$, pelo fato de $\varphi : H \hookrightarrow G$ ser a inclusão, concluímos que $H^\perp$ é o conjunto dos caracteres de G cuja a restrição a H é o caracter trivial.

Proposição 2.2.1 *Sendo G um grupo Abeliano e H um subgrupo de G, temos que $H^\perp \simeq \widehat{G/H}$.*

Demonstração: Consideremos o homomorfismo canônico $\pi : G \longrightarrow G/H$ e a aplicação $\psi : H^{\perp} \longrightarrow \widehat{G/H}$, definidos por $\psi(\chi) = \widetilde{\chi}$



Temos assim que ψ é um homomorfismo, basta então mostrar que ψ é bijetor. Para isso, $Ker\psi = \{\chi \in H^{\perp} : \psi(\chi) = 1\} = \{\chi \in H^{\perp} : \ \widetilde{\chi}(aH) = 1\} = \{\chi_0 \in G\}$ portanto $Ker\psi = \{\chi_0\}$, ou seja, ψ é injetor. Como $\widetilde{\chi}(\bar{g}) = \widetilde{\chi}(\pi(g)) = (\widetilde{\chi} \circ \pi)(g) = \chi(g)$. Isso mostra que ψ é sobrejetiva, logo ψ é um isomorfismo. □

Teorema 2.2.1 *{[4], pag. 17} O número de caracteres de um grupo abeliano finito G é igual a sua ordem, ou seja, $|\widehat{G}| = |G|$*

Demonstração: Sendo G um grupo abeliano finito, então $G = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle$, assim todo elemento $x \in G$ pode ser escrito da forma $x = a_1^{k_1} \cdots a_n^{k_n}$. Considerando χ um caracter de G, segue que $\chi(x) = \chi(a_1)^{k_1} \cdots \chi(a_n)^{k_n}$, assim, χ fica completamente determinado pelos valores $\chi(a_i)$, $i = 1, \cdots, n$. Agora, se a_i tem ordem m_i, então G tem ordem $m_1 \cdots m_n$ e $\chi(a_i)$ é uma raiz m_i-ésima da unidade, assim temos m_i possibilidades para $\chi(a_i)$ num total de $m_1 \cdots m_n$ caracteres em G. Logo $|\widehat{G}| = |G|$. □

Teorema 2.2.2 *{[4], pag. 19} Se G é um grupo cíclico de ordem n, então $G \simeq \widehat{G}$*

Demonstração: Considerando g um gerador de G e ζ_n uma raiz n-ésima primitiva da unidade. Seja $\chi : G \longrightarrow G^*$ dado por $\chi(g^k) = \zeta_n^k$. Temos que χ é um caracter de G. Desde que $\chi^r(g^k) = \zeta_n^{rk}$ os caracteres $\chi, \chi^2, \cdots, \chi^{n-1}, \chi^n = \chi_0$ são dois a dois distintos. Agora, como $|\widehat{G}| = |G| = n$, temos que $\widehat{G} = \{\chi, \chi^2, \cdots, \chi^{n-1}, \chi^n = \chi_0\}$, e, sendo assim $\widehat{G}$ é um grupo cíclico de ordem n, gerado por χ. Logo $G \simeq \widehat{G}$. □

Enfim, desta seção podemos extrair uma importante informação a respeito dos caracteres de um grupo abeliano finito, a saber, que o número de caracteres de tal

grupo é igual a sua ordem. Este fato será importante mais a frente, pois umas das necessidades consiste em saber qual a quantidade de caracteres associados a um determinado corpo números.

2.3 Caracteres de Dirichlet

Vamos estudar nesta seção os caracteres do grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$, este grupo é formado pelos elementos inversíveis do anel $(\mathbb{Z}/n\mathbb{Z})$, tais caracteres são chamados de caracteres de Dirichlet. Estaremos interessados nos condutores desses caracteres e algumas propriedades que serão úteis para o cálculo do discriminante de um corpo de números Abeliano K.

Definição 2.3.1 *Um homomorfismo $\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ é denominado caracter de Dirichlet definido módulo n.*

Caso exista um inteiro m que divide n, o caracter $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ induz o caracter $\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ através do homomorfismo $\pi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$, isto é, $\chi = \chi' \circ \pi$;

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & & \\ \Big\downarrow{\scriptstyle \pi} & \searrow^{\chi=\chi'\circ\pi} & \\ (\mathbb{Z}/m\mathbb{Z})^* & \xrightarrow[\chi']{} & \mathbb{C}^* \end{array}$$

Se m for minimal, dizemos que m é o condutor do caracter χ o qual será denotado por f_χ. Desta forma, se χ e χ' forem ambas a mesma aplicação podemos considerar χ como definido módulo m.

Exemplo 2.3.1 *Sejam $G = (\mathbb{Z}/10\mathbb{Z})^* = \{1, 3, 7, 9\}$ e $\{\chi_0, \chi_1, \chi_2, \chi_3\}$ o grupo dos*

caracteres de G, dado na tabela abaixo

	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*

No exemplo acima vimos os caracteres definidos módulo 10, porém, temos que 1,2,5,10 são divisores de 10, como estabelecer então qual será o condutor de χ_i ?. Uma informação importante é que o condutor f_{χ_i} de χ_i será o menor m que faz comutar o diagrama;

$$\begin{array}{ccc} (\mathbb{Z}/10\mathbb{Z})^* & & \\ \downarrow{\scriptstyle \pi} & \searrow^{\chi=\chi'\circ\pi} & \\ (\mathbb{Z}/m\mathbb{Z})^* & \xrightarrow[\chi']{} & \mathbb{C}^* \end{array}$$

Porém, uma outra ferramenta para encontrar o condutor f_{χ_i} de um caracter χ_i é dado no;

Teorema 2.3.1 {*[4], pag. 20*} *Sejam m e n inteiros positivos e χ um caracter de Dirichlet definido módulo n. O condutor de χ é m se, e somente se m é o menor inteiro dividindo n que satisfaz a condição: para todo a tal que $mdc(a,n) = 1$ e $a \equiv 1(mod\, m)$ tem-se $\chi(\bar{a}) = 1$*

Considerando ainda os caracteres do Exemplo 2.3.1, temos que o condutor de χ_3 é 5, pois $1 \equiv 1(mod\, 5)$ e $\chi_3(1) = 1$. Analogamente, o condutor dos caracteres χ_2 e χ_1 é 5, logo os caracteres de Dirichlet definidos módulo 10, podem ser considerados como definidos módulo 5.

Um caracter definido módulo n pode ser visto como uma aplicação de $\mathbb{Z}$ em $\mathbb{C}$, pondo $\chi(a) = 0$ se $mdc(a, f_\chi) \neq 1$. Um caracter definido módulo seu condutor é denominado caracter primitivo.

Exemplo 2.3.2 *Seja χ um caracter definido módulo 8, dado por $\chi(1) = 1$, $\chi(3) = 1$, $\chi(5) = -1$ e $\chi(7) = -1$, temos que $f_\chi = 8$, logo χ é um caracter primitivo.*

É interessante notar que dados χ e ψ caracteres primitivos de condutores f_χ e f_ψ respectivamente o caracter $\chi\psi$ definido módulo $mmc(f_\chi, f_\psi)$ é um caracter primitivo.

Exemplo 2.3.3 *Consideremos o caracter ψ definido módulo 4, dado por $\psi(1) = 1$ e $\psi(3) = -1$ e daí $f_\psi = 4$, então ψ é um caracter primitivo. Como o caracter do Exemplo 2.3.2 é um caracter primitivo, sendo o caracter $\chi\psi$ definido módulo 8 dado por;*

. $\chi\psi(1) = \chi(1)\psi(1) = 1.1 = 1$

. $\chi\psi(3) = \chi(3)\psi(3) = 1.(-1) = -1$

. $\chi\psi(5) = \chi(5)\psi(5) = (-1).1 = -1$

. $\chi\psi(7) = \chi(7)\psi(7) = (-1).(-1) = 1$ *e como $f_{\chi\psi} = 8$, segue que $\chi\psi$ definido módulo 8 é um caracter primitivo.*

Proposição 2.3.1 {*[5], pag. 75*} *Sejam χ e ψ caracteres de Dirichlet primitivos com condutores f_χ e f_ψ, respectivamente. Se $mdc(f_\chi, f_\psi) = 1$, então $f_{\chi\psi} = f_\chi.f_\psi$.*

As vezes é conveniente classificar os caracteres de Dirichlet em dois grupos; se $\chi(-1) = 1$, dizemos que o caracter χ é um caracter par, caso $\chi(-1) = -1$, o caracter χ é um caracter ímpar.

Exemplo 2.3.4 *O caracter χ do Exemplo 2.3.2 é um caracter ímpar pois $7 \equiv -1(mod\,8)$ e $\chi(7) = -1$, já, o caracter χ_3 do Exemplo 2.3.1 é um caracter par pois $9 \equiv -1(mod\,10)$ e $\chi_3(9) = 1$*

Sabendo que o grupo $(\mathbb{Z}/n\mathbb{Z})^*$ é um grupo abeliano, tomando o caso particular em que $n = p^r$, é interessante saber em qual circunstâncias $(\mathbb{Z}/p^r\mathbb{Z})^*$ é cíclico. Este fato vai nos auxiliar no determinação dos caracteres definidos módulo p^r, isto será determinada na proposição abaixo.

O próximo teorema irá auxiliar na classificação do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$, p-primo, ou seja, saber sob quais condições ele será ou não cíclico.

Proposição 2.3.2 {*[8], pag. 163*}

(a) Se p é um número primo ímpar e r um inteiro positivo, temos que $(\mathbb{Z}/p^r\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)p^{r-1}\mathbb{Z}$.

(b) $(\mathbb{Z}/2^r\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{r-2}\mathbb{Z})$ para cada inteiro $r \geq 2$.

Esta proposição nos chama a atenção à alguns fatos que serão de grande utilidade na obtenção de subcorpos de $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{2^r})$, a parte (a) diz que $(\mathbb{Z}/p^r\mathbb{Z})^*$, p-primo ímpar é um grupo cíclico, sendo assim, para cada divisor m da ordem de $(\mathbb{Z}/p^r\mathbb{Z})^*$ existe um único subgrupo de $(\mathbb{Z}/p^r\mathbb{Z})^*$ com ordem m. Logo, pela correspondência de Galois, existe um único subcorpo K de $\mathbb{Q}(\zeta_{p^r})$ cujo o grau é m. Já, a parte (b) diz que $(\mathbb{Z}/2^r\mathbb{Z})^*$ é um grupo abeliano não cíclico, assim, para este caso não é válido o resultado acima, ou seja, para cada divisor m da ordem de $(\mathbb{Z}/2^r\mathbb{Z})^*$ podem existir mais que um subcorpo de $\mathbb{Q}(\zeta_{2^r})$ de ordem m.

Seja $m = p_1^{e_1} \cdots p_r^{e_r}$ uma decomposição em fatores primos, consideremos o isomorfismo de grupo

$$\theta : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \prod_{i=1}^{r} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$$

Dado por $\widehat{\theta(x(mod\, m))} = (x(mod\, p_1^{e_1}), \cdots, x(mod\, p_r^{e_r}))$. Considerando $\chi \in \widehat{\prod_{i=1}^{r} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*}$, dado por $\chi(\bar{x_1}, \cdots, \bar{x_r}) = \chi((x_1, \cdots, 1) \cdots (1, \cdots, x_r)) = \chi(x_1, \cdots, 1) \cdots \chi(1, \cdots, x_r)$. Seja $\chi_i \in \widehat{(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*}$ dado por $\chi_i(x_i) = \chi(1, \cdots, x_i, \cdots, 1)$. Desta forma, $\chi(\bar{x_1}, \cdots, \bar{x_r}) = \chi_1(\bar{x_1}) \cdots \chi_r(\bar{x_r})$. Considerando ainda o homomorfismo de grupos $\widehat{\theta} : \widehat{\prod_{i=1}^{r} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*} \longrightarrow \widehat{(\mathbb{Z}/m\mathbb{Z})^*}$, onde $\widehat{\theta} = \chi_1 \cdots \chi_r$ com $\chi_i \in \widehat{(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*}$ tem-se, $\widehat{\theta}(\chi) = \chi \circ \theta$. Assim, $(\chi \circ \theta)(x) = \chi(\theta(x)) = \chi(\bar{x_1}, \cdots, \bar{x_r}) = \chi_1(\bar{x_1}) \cdots \chi_r(\bar{x_r})$. Desta forma, todo caracter ψ de $(\mathbb{Z}/m\mathbb{Z})^*$ pode ser escrito da forma $\psi = \chi_1 \cdots \chi_r = \prod_{i=1}^{r} \chi_i$, onde χ_i é um caracter definido módulo $p_i^{e_i}$.

Sendo assim, para conhecermos um caracter de $(\mathbb{Z}/m\mathbb{Z})^*$, basta conhecer os caracteres de $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$. Vamos por enquanto nos deter com respeito a este assunto,

mas voltaremos a retomá-lo na seção seguinte, objetivando conhecer mais detalhadamente os caracteres do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$.

No próximo teorema vamos determinar uma relação que existe entre os grupos $Gal(\mathbb{Q}(\zeta_n/\mathbb{Q}))$ e $(\mathbb{Z}/n\mathbb{Z})^*$. Isto vai nos possibilitar trabalhar com os elementos de $Gal(\mathbb{Q}(\zeta_n/\mathbb{Q}))$ ao invés dos elementos de $(\mathbb{Z}/n\mathbb{Z})^*$.

Teorema 2.3.2 {*[6], pag. 11*} *O grupo* $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *é isomorfo ao grupo* $(\mathbb{Z}/n\mathbb{Z})^*$, *através da aplicação* $\theta(\sigma_i) = \bar{i}(mod\, n)$, *onde* $\sigma_i(\zeta_n) = \zeta_n^i$, *para* $0 < i < n$ *e* $mdc(i, n) = 1$

Este teorema nos garante que existe uma correspondência bijetiva de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ em $(\mathbb{Z}/n\mathbb{Z})^*$, sendo assim, os caracteres definidos módulo n, são também chamados de caracteres de Galois.

Considerando um caracter χ do grupo $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ o núcleo de χ, denotado por $Ker\,\chi$ é um subgrupo do grupo $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, assim o subcorpo K de $\mathbb{Q}(\zeta_n)$ fixo por $Ker\,\chi$ é denominado o corpo associado ao caracter χ.

Sendo X um grupo finito de caracteres de Dirichlet e n o mínimo múltiplo comum dos condutores dos caracteres de X, temos que X é um subgrupo do grupo dos caracteres de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Seja H a intersecção dos núcleos dos caracteres de X, temos que H é um subgrupo do grupo $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e o corpo K, fixo por H, é também denominado o corpo associado ao grupo X.

Agora, se considerarmos K um subcorpo de $\mathbb{Q}(\zeta_n)$ e H o subgrupo de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa K, denotamos por X_K o conjunto dos caracteres de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que restritos a H são os caracteres triviais.

$$X_K = \{\chi \in \widehat{Gal(\mathbb{Q}(\zeta_n)}/\mathbb{Q}) : \chi(h) = 1 \quad \forall h \in H\}$$

O conjunto X_K, é denominado o grupo de caracteres de Dirichlet associados a K. E além disso, temos que $X_K \simeq Gal(K/\mathbb{Q})$, ou seja, $|X_K| = |Gal(K/\mathbb{Q})|$.

Exemplo 2.3.5 *Seja* $K = \mathbb{Q}(\zeta_8)$, *temos que* $(\mathbb{Z}/8\mathbb{Z})^* \simeq Gal(\mathbb{Q}(\zeta_8)\ /\mathbb{Q})$, *assim Gal* $(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$ *e* $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, *assim* $\zeta_8^4 = i^2$ *e dai* $\zeta_8^2 = i$. *Como*

o grupo $Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ *é não cíclico e tem ordem 4, segue que os monomorfismos* $\sigma_3, \sigma_5, \sigma_7$ *tem ordem 2. Assim os subgrupos do grupo de Galois de* K *são;* $\langle \sigma_1 = id \rangle$, $\langle \sigma_3 \rangle$, $\langle \sigma_5 \rangle$, $\langle \sigma_7 \rangle$ *e* $Gal(K/\mathbb{Q})$. *Isso implica que cada um dos subcorpos próprios de* K *tem grau 2. O corpo* $\mathbb{Q}(i)$ *é um subcorpo de* K *e o grupo associado a* $\mathbb{Q}(i)$ *é* $\langle \sigma_5 \rangle$, *pois* $\sigma_5(i) = \sigma_5(\zeta_8^2) = \zeta_8^{10} = \zeta_8^2$. *O corpo* $\mathbb{Q}(\sqrt{2})$ *é corpo de ordem 2 e como* $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, *como* σ_7 *fixa* $\sqrt{2}$, *assim o corpo* $\mathbb{Q}(\sqrt{2})$ *é o corpo associado ao grupo* $\langle \sigma_7 \rangle$. *Como* $i, \sqrt{2} \in K$, *o corpo* $\mathbb{Q}(\sqrt{-2})$ *é o subcorpo de* K *associado ao grupo* $\langle \sigma_3 \rangle$, *pois* σ_3 *fixa* $\sqrt{-2} = \zeta_8 + \zeta_8^3$. *Portanto, os subcorpos de* $K = \mathbb{Q}(\zeta_8)$, *são* $K, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$ *e* $\mathbb{Q}$. *Assim, temos que* $K = \mathbb{Q}(\sqrt{2}, i)$

Para finalizar esta seção, como havíamos proposto anteriormente, vamos enunciar a célebre fórmula do Condutor-Discriminante. Esta fórmula concede uma alternativa muito valiosa no processo do cálculo do discriminante de um corpo de números abeliano K, pois através dela conseguimos calcular o discriminante de K, sem precisar ter conhecimento de uma base integral, usando apenas o grupo dos caracteres associados a K e seu condutores.

Teorema 2.3.3 *(Fórmula do Condutor-Discriminante)* {*[4], pag.24*} *Sejam* K *um corpo de números, tal que* $K \subset \mathbb{Q}(\zeta_n)$, r_2 *o número de monomorfismos complexos de* K *não conjugados entre si, e* X *o grupo dos caracteres de Dirichlet associados a* K. *Então o discriminante de* K *é dado por*

$$\Delta(K) = (-1)^{r_2} \prod_{\chi \in X} f_\chi$$

Onde f_χ *é o condutor do caracter* χ.

Podemos observar que esta fórmula é de mais aplicação do que a Definição 1.2.4, uma vez que ela calcula o discriminante de um corpo de números sem tomar conhecimento de uma base integral do corpo e também não implica a necessidade de calcular o determinante de uma matriz. No entanto, ela só é aplicável para corpos de números que estejam contidos em alguma extensão ciclotômica. Logo, através desta, obtemos uma ferramenta para o cálculo do discriminante de corpos abeliano,

pois o teorema de Kronecker-Weber garante que todo corpo abeliano está contido em uma extensão ciclotômico.

Exemplo 2.3.6 *Seja $K = \mathbb{Q}(\zeta_p)$, p:primo, os condutores dos caracteres associados a K são 1 ou p. Como o grupo destes caracteres possui $p-1$ elementos, temos $p-2$ caracteres de condutor p e um caracter trivial, logo aplicando a fórmula do teorema acima temos $|\Delta(K)| = p^{p-2}$.*

2.4 Caracteres de Dirichlet módulo p^r

Nesta seção temos por objetivo calcular os condutores dos caracteres definidos módulo p^r, onde p é seja um número primo. Isto será feito graças a possibilidade que temos em determinar explicitamente quem são tais caracteres. No entanto, para conseguir tal resultado, será necessário considerar separadamente o caso $p = 2$ e o caso p ímpar.

Consideremos primeiramente o caso p-ímpar, porém antes de nos direcionarmos efetivamente ao cálculo destes caracteres, vamos expor alguns resultados que serão importantes, aritmeticamente, na computação dos mesmos.

Lema 2.4.1 *{[7], pag. 320} Sejam p um número primo ímpar, r um inteiro positivo e g um inteiro tal que $\bar{g} \equiv g\,(mod\,p^r)$ é um gerador do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$. Então para todo j tal que $0 < j \leq r$, tem-se $g^k \equiv 1\,(mod\,p^j)$ se, e somente se, $k \equiv 0(mod(p-1).p^j)$.*

Sejam $\chi : (\mathbb{Z}/p^r\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ um caracter de Dirichlet e $\bar{g} \equiv g\,(mod\,p^r)$ um gerador do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$, então todos os $(p-1).p^{r-1}$ caracteres deste grupo são determinados por $\bar{g}$, e $\chi(\bar{g})$ é uma raiz $(p-1).p^{r-1}$-ésima da unidade. Sendo assim, dado um caracter de Dirichlet definido módulo p^r, existe um inteiro i, onde $0 \leq i \leq (p-1)p^{r-1} - 1$, tal que $\chi(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$. Assim, podemos concluir que todos os caracteres definidos módulo p^r são da forma;

$$\chi_i(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}, \quad i = 0, \cdots, (p-1)p^{r-1} - 1$$

Lema 2.4.2 *{[7], pag. 321} Se i é um inteiro tal que $0 \leq i \leq (p-1)p^{r-1}-1$, então $p^j = mdc(i, p^r)$, se, e somente se o condutor f_{χ_i} de χ_i é p^{r-j}*

Exemplo 2.4.1 *Seja $n = 5^2$, então o grupo de caracteres definidos modulo 25 possui 20 elementos. Daí, o condutor f_{χ_i} de χ_i, é 5^2 para $i = 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19$, pois para cada um destes casos temos $mdc(i, 5^2) = 1 = 5^0$, daí $f_{\chi_i} = 5^{2-0} = 5^2$. Para $i = 5, 10, 15$, temos que $f_{\chi_i} = 5$, pois $mdc(i, 5^2) = 5 = 5^1$, daí $f_{\chi_i} = 5^{2-1} = 5$ e $f_{\chi_0=1}$*

Analogamente ao caso anterior, agora vamos considerar dois importantes resultados os quais auxiliarão na computação dos condutores dos caracteres definidos módulo 2^r.

Lema 2.4.3 *{[4], pag. 32} Seja t um número inteiro, $t \geq 3$. Então, tem-se: $5^{2^{t-3}} \equiv 1 (mod\, 2^{t-1})$ e $5^{2^{t-3}} \not\equiv 1 (mod\, 2^t)$, ou seja, a ordem de $5\,(mod\, 2^t)$ é 2^{t-2}*

Lema 2.4.4 *{[4], pag. 32} Se $t \geq 2$ então $(-1)^a 5^b \equiv 1\,(mod\, 2^t)$ se, e somente se, $b \equiv 0 (mod\, 2^{t-2})$ e a é par.*

O grupo $(\mathbb{Z}/2^r\mathbb{Z})^*$ é um tanto diferente do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$, p primo ímpar. Embora ambos sejam abelianos, porém $(\mathbb{Z}/p^r\mathbb{Z})^*$ é cíclico, enquanto $(\mathbb{Z}/2^r\mathbb{Z})^*$ não é. E, além disso temos que

$$(\mathbb{Z}/2^r\mathbb{Z})^* = \{(-1)^a 5^b : \ \ a \in \{1, 2\} \text{ e } b \in \{1, 2, \cdots, 2^{r-2}\}\}$$

Daí, um caracter de Dirichlet definido módulo 2^r fica completamente determinado pelas imagens de $\overline{-1}$ e $\bar{5}$. Como a ordem de $5\,(mod\, 2^t)$ é 2^{t-2} e a ordem de $-1\,(mod\, 2^t)$ é 2, dado $\chi \in \widehat{(\mathbb{Z}/2^r\mathbb{Z})^*}$ temos que $\chi(\overline{-1}) = (-1)^i$ para $i \in \{1, 2\}$ e $\chi(\bar{5}) = \zeta_{2^{r-2}}^l$, $l \in \{1, 2, \cdots, 2^{r-2}\}$, assim cada caracter de $\widehat{(\mathbb{Z}/2^r\mathbb{Z})^*}$ será denotado por $\chi_{i,l}$.

Teorema 2.4.1 *{[5], pag. 86} 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*

$$f_{\chi_{i,l}} = \begin{cases} 1 & \text{se} \quad i\text{=}2, \\ 4 & \text{se} \quad i\text{=}1. \end{cases}$$

Demonstração: Consideremos $\bar{x} \in (\mathbb{Z}/2^r\mathbb{Z})^*$, então $\bar{x} = (-1)^a 5^b$, se $i = 2$ e $l = 2^{r-2}$ temos $\chi_{i,l}(\bar{x}) = \chi_{i,l}((-1)^a 5^b) = (\chi_{i,l}(-1))^a.(\chi_{i,l}(\bar{5}))^b = (-1)^{2a}.\zeta_{2^{r-2}}^{2^{r-2}} = 1$, logo $\chi_{i,l}$, $l = 2^{r-2}$ é o caracter trivial. Se $l = 2^{r-2}$ e $i = 1$, temos $\chi_{i,l}(\bar{x}) = \chi_{i,l}((-1)^a 5^b) = (-1)^a.\zeta_{2^{r-2}}^{2^{r-2}} = (-1)^a = \begin{cases} 1, & \text{se } \bar{x} = \bar{5}^b; \\ -1, & \text{se } \bar{x} = \overline{-1}\bar{5}^b. \end{cases}$, logo $\chi_{i,l}$ não é trivial. Se $x \equiv 1(mod\,4)$, temos $\bar{x} = \bar{5}^b$ pois $5^b \equiv 1(mod\,4)$ e $-5^b \equiv -1(mod\,4)$, daí para todo x, satisfazendo $x \equiv 1(mod\,4)$, temos $\chi_{i,l}(\bar{x}) = 1$, logo $f_{\chi_{i,l}} = 4$. □

Teorema 2.4.2 {*[5], pag. 86*} *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: Para $l \neq 2^{r-2}$ temos que $\chi_{i,l}(\bar{5}) = \zeta_{2^{r-2}}^l \neq 1$, como $5 \equiv 1(mod\,4)$ segue que $f_{\chi_{i,l}} > 4$. Temos então que $f_{\chi_{i,l}} = 2^u$, para $u > 2$. Dado $\bar{x} = \overline{(-1)}.5^b \in (\mathbb{Z}/2^r\mathbb{Z})^*$, $x \equiv 1(mod\,2^u)$ implica em $(-1)^a 5^b \equiv 1(mod\,2^u)$ se, e somente se, $b \equiv 0(mod\,2^{u-2})$ e $a = 2$, conforme o Lema 2.4.4. Sendo assim, se $x \equiv 1(mod\,2^u)$ devemos ter; $\chi_{i,l}(\bar{x}) = \chi_{i,l}(\bar{5}^{2^{u-2}}) = \zeta_{2^{r-2}}^{l.2^{u-2}} = 1$, então $l.2^{u-2} \equiv 0(mod\,2^{r-2})$ e portanto, $l \equiv 0(mod\,2^{r-u})$. Agora devemos ter $\chi_{i,l}(\bar{5}^{2^{u-3}}) \neq 1$ pois se $\chi_{i,l}(\bar{5}^{2^{u-2}}) = 1$, dado $x \equiv 1(mod\,2^{u-1})$ pelo Lema 2.4.4 temos que $\bar{x} = \bar{5}^{t.2^{u-3}}$ e daí $\chi_{i,l}(\bar{x}) = (\chi_{i,l}(\bar{5}^{2^{u-3}}))^t = 1$ o que contradiz o fato de 2^u ser condutor de $\chi_{i,l}$. Más, $\chi_{i,l}(\bar{5}^{2^{u-3}}) \neq 1 \Leftrightarrow \zeta_{2^{r-2}}^{2^{u-3}.l} \neq 1 \Leftrightarrow l \not\equiv 0(mod\,2^{r-2-(u-3)}) \Leftrightarrow l \not\equiv 0(mod\,2^{r-u+1})$. Como $l \equiv 0(mod\,2^{r-u})$ e $l \not\equiv 0(mod\,2^{r-u+1})$, temos que $mdc(l, 2^r) = 2^{r-u}$ e daí $2^u = \frac{2^r}{mdc(l,2^r)}$, daí $f_{\chi_{i,l}} = \frac{2^r}{mdc(l,2^r)}$ □

Exemplo 2.4.2 *Seja $n = 2^5$, então o grupo de caracteres definidos módulo n tem 16 elementos. Assim, temos $f_{\chi_{2,5}} = \frac{2^5}{mdc(5,2^5)} = \frac{2^5}{1} = 2^5$, $f_{\chi_{2,4}} = \frac{2^5}{mdc(2^2,2^5)} = \frac{2^5}{2^2} = 2^3$ e $f_{\chi_{1,8}} = 4$, pois $i = 1$ e $l = 2^3$*

Nos últimos parágrafos nos exercitamos basicamente em expressar os caracteres de Dirichlet definidos módulos p^r, p:primo. Isto foi feito com o intuito de expressar uma fórmula para o discriminante dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$, que será feito no próximo capítulo.

Capítulo 3

O Discriminante Mínimo

O objetivo deste capítulo consiste em abordar o principal assunto proposto para este trabalho, que é calcular o discriminante mínimo dos corpos abelianos de grau primo. No entanto, para atingirmos tal propósito se faz necessário passarmos previamente por alguns resultados, os quais possibilitarão atingir com êxito os propósitos estabelecidos.

Dentre estes podemos destacar o Teorema 3.3.1, que estabelece uma fórmula para o discriminante um corpo abeliano qualquer. Este resultado é conseguido, em especial, via a Fórmula do Condutor-Discriminante auxiliado de perto pelo Teorema de Kroncker-Weber. Como consequência do Teorema 3.3.1, serão ainda expostos vários outros resultados, entre os quais se destaca o Corolário 3.3.5, que caracteriza uma fórmula para o discriminante dos corpos abelianos de grau primo.

Porém, em uma última seção será abordado o assunto do discriminante mínimo, o qual foi acima citado. No entanto, primeiramente será feito um estudo para saber a quantidade de subcorpos de grau primo existem em uma extensão ciclotômica $\mathbb{Q}(\zeta_m)$. E, enfim, estudaremos o problema do discriminante mínimo, e paralelamente a isso desejaremos saber qual a extensão ciclotômica mínima onde esta contido o corpo com tal discriminante. Para este capítulo foram utilizados as referência [4] à [10].

3.1 Discriminante dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$

Sendo p um número primo ímpar e r um inteiro positivo, temos que $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = (p-1).p^{r-1}$. Agora, se K é um subcorpo de $\mathbb{Q}(\zeta_{p^r})$ segue $[K : \mathbb{Q}] = up^j$, onde u divide $p-1$ e $0 \leq j \leq r-1$. Da Proposição 2.3.2 temos que o grupo $G = Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ é cíclico, logo todo subgrupo de G é ainda cíclico.

Considerando H o subgrupo de G que fixa K. Então, χ é um caracter associado à K se, e somente se, $H \subseteq Ker\chi$. Assim o grupo X_K dos caracteres associados a K é o conjunto;

$$\{\chi \in \widehat{(\mathbb{Z}/p^r\mathbb{Z})^*} : \ \chi(h) = 1, \ \forall\, h \in H\}$$

Assim, de acordo a Fórmula do Condutor-Discriminante, segue que o discriminante de K é, a menos de sinal, o produto dos condutores dos elementos de X_K.

Através do próximo teorema conseguimos um resultado importante que nos concede uma fórmula para o discriminante de subcorpos K de $\mathbb{Q}(\zeta_{p^r})$. Tal resultado foi conseguido determinando explicitamente os caracteres associados a K e em seguida determinando os condutores de tais caracteres.

Teorema 3.1.1 *{[7], pag.322} Sejam p um número primo ímpar, r um inteiro positivo e K um subcorpo de $\mathbb{Q}(\zeta_{p^r})$, $[K : \mathbb{Q}] = up^j$, onde u divide $p-1$ e $0 \leq j \leq r-1$, então;*

$$|\Delta(K)| = p^{u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}]-1}$$

Decorrente do teorema acima podemos extrair alguns importantes resultados, entre os quais podemos destacar a obtenção de uma fórmula para o discriminante dos corpos $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_p)$, isto será feito nos corolários abaixo.

Corolário 3.1.1 *{[4], pag.31} Sejam p um número primo ímpar e r um inteiro positivo, o discriminante de $\mathbb{Q}(\zeta_{p^r})$ é;*

$$\Delta(\mathbb{Q}(\zeta_{p^r})) = \pm p^{(p-1)[(r+1)p^{r-1} - \frac{p^r-1}{p-1}]-1}$$

Demonstração: Como $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = (p-1).p^{r-1}$, neste caso temos que $u = p-1$ e $j = r-1$, daí usando a fórmula do Teorema 3.1.1, obtemos o resultado. □

Consequentemente ainda podemos expor vários outros resultados decorrentes deste último teorema, entre os quais podemos destacar o discriminante dos subcorpos de $\mathbb{Q}(\zeta_p)$.

Corolário 3.1.2 *{[4], pag.31} Sejam p um número primo ímpar e $K \subseteq \mathbb{Q}(\zeta_p)$, então;*

$$|\Delta(K)| = p^{[K:\mathbb{Q}]-1}$$

Demonstração: Como $[\mathbb{Q}(\zeta_p) : \mathbb{Q})] = p-1$, então $[K : \mathbb{Q}] = up^0$, onde u divide $p-1$. Daí $|\Delta(K)| = p^{u[(0+2)p^0 - \frac{p^{0+1}-1}{p-1}]-1} = p^{u[2-1]-1} = p^{u-1} = p^{[K:\mathbb{Q}]-1}$ □

Considerando o corpo $\mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, que é o subcorpo real maximal de $\mathbb{Q}(\zeta_{p^r})$, podemos determinar o seu discriminante utilizando também o Teorema 3.1.1, como pode ser visto no exemplo abaixo.

Exemplo 3.1.1 *Consideremos o corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$, p-primo ímpar e r um inteiro positivo, calculemos o discriminante de $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$. Como $[K : \mathbb{Q}] = \frac{(p-1)p^r}{2}$, então $u = \frac{(p-1)}{2}$ e $j = r-1$ daí*

$$|\Delta(K)| = p^{\frac{(p-1)}{2}[(r-1+2)p^{r-1} - \frac{p^r-1}{p-1}]-1} = p^{\frac{(p-1)}{2}[(r+1)p^{r-1} - \frac{p^r-1}{p-1}]-1}$$

3.2 Discriminante dos subcorpos de $\mathbb{Q}(\zeta_{2^r})$

O objetivo nesta seção é estabelecer uma fórmula para o discriminante de um subcorpo K de $\mathbb{Q}(\zeta_{2^r})$. Analogamente ao caso anterior, isto será feito obtendo explícitamente os caracteres associados a K, bem como os seus condutores.

O corpo $\mathbb{Q}(\zeta_{2^r})$, r inteiro positivo, é um corpo de números Abeliano não cíclico de ordem 2^{r-1}. Para o cálculo do discriminante dos subcorpos K de $\mathbb{Q}(\zeta_{2^r})$ vamos trabalhar com os caracteres de $(\mathbb{Z}/2^r\mathbb{Z})^*$ associados a K. Seja H um subgrupo de $G = Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ que fixa K, o grupo de caracteres associados a K é o conjunto X_K formado pelos elementos de $\widehat{G}$ cujo o núcleo contém H.

Assim, dado K um subcorpo de $\mathbb{Q}(\zeta_{2^r})$ de grau 2^{m-1}, então o subgrupo H de G, que fixa K tem ordem 2^{r-m} e tem as seguintes formas;

$$H = \langle \bar{5}^{2^{m-2}} \rangle \qquad H = \langle -\bar{5}^{2^{m-2}} \rangle \qquad H = \langle \overline{-1}, \bar{5}^{2^{m-2}} \rangle$$

Diferentemente do caso p^r, p-primo ímpar, o discriminante de $K \subseteq \mathbb{Q}(\zeta_{2^r})$, dependerá diretamente da característica de seu grupo de fixação H, ou seja, vai depender do fato de H ser ou não ser cíclico.

Teorema 3.2.1 *{[4], pag.35} Sejam K um subcorpo de $\mathbb{Q}(\zeta_{2^r})$, com $[K : \mathbb{Q}] = 2^{r-m}$ e H o subgrupo de $G = Gal(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$ que fixa K. Temos;*

(1) Se $H = \langle \bar{5}^{2^{m-2}} \rangle$, então $K = \mathbb{Q}(\zeta_{2^m})$ e $|\Delta(K)| = 2^{(m-1).2^{m-1}}$

(2) se $H = \langle -\bar{5}^{2^{m-2}} \rangle$ ou $H = \langle \overline{-1}, \bar{5}^{2^{m-2}} \rangle$, então $|\Delta(K)| = 2^{m.2^{m-1}-1}$

É interessante notar que como consequência do teorema acima se $K = \mathbb{Q}(\zeta_{2^m})$, então $|\Delta(K)| = 2^{(m-1).2^{m-1}}$, se não, $|\Delta(K)| = 2^{m.2^{m-1}-1}$. Assim, o que este teorema deixa explícito é que o discriminante de um subcorpo K de $\mathbb{Q}(\zeta_{2^r})$ depende do fato de K ser ou não ciclotômico.

Considerando o corpo $K = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, temos que $[\mathbb{Q}(\zeta_{2^r}) : K] = 2$, então $[K : \mathbb{Q}] = 2^{r-2}$, pondo $m = r - 1$ e pelo fato de $K \neq \mathbb{Q}(\zeta_{2^r})$, pois K é totalmente real, segue que $|\Delta(K)| = 2^{m.2^{m-1}-1}$.

O que foi feito nas duas primeiras seções deste capítulo consisti em estabelecer uma fórmula para o discriminante de subcorpos de $\mathbb{Q}(\zeta_{p^r})$, p-primo. Porém, na próxima seção será exposta uma fórmula mais abrangente, que determina o discriminante de um corpo de números contidos em uma extensão ciclotômica qualquer.

3.3 Corpos de números Abelianos

No capítulo inicial deste trabalho, além da definição formal de discriminante, estabelecemos uma outra ferramenta (Proposição 1.4.3), decorrente da norma, que nos auxilia no cálculo do discriminante de um corpo de números K, cujo o anel de

inteiros algébricos é $\mathbb{Z}[\theta]$. No entanto, em sua aplicação, tanto uma quanto a outra encontra limitações no contexto geral para o cálculo do discriminante de um determinado corpo de números. O que vamos fazer nesta seção é efetivamente calcular o discriminante dos corpos abelianos em geral, usando a Fórmula do Condutor-Discriminante.

Seja K um corpo Abeliano, segue que $K \subset \mathbb{Q}(\zeta_m)$, se m for minimal, diremos que m é o condutor de K. Considerando o subgrupo H de $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ que fixa K, pelo fato de $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ ser isomorfo à $(\mathbb{Z}/m\mathbb{Z})^*$, podemos considerar H como um subgrupo de $(\mathbb{Z}/m\mathbb{Z})^*$, assim X_K, o grupo dos caracteres associados a K, é o conjunto de caracteres de $(\mathbb{Z}/m\mathbb{Z})^*$, cujo o núcleo contém H, temos ainda que $X_K \simeq Gal(K/\mathbb{Q})$ e daí $[K : \mathbb{Q}] = |X_K|$. Para então estabelecermos a fórmula do discriminante de um corpo de números Abeliano, vamos determinar os possíveis condutores dos caracteres de X_K, em seguida estabelecer quantos caracteres existem para cada um dos possíveis condutores e assim, usar a Fórmula do Condutor-Discriminante para conseguirmos o resultado esperado. Porém, antes de tudo, vamos necessitar de alguns conceitos que auxiliarão na aritmética da computação da fórmula do discriminante.

Lema 3.3.1 {*[4], pag. 40*} *Se K e L são subcorpos de $\mathbb{Q}(\zeta_m)$, então $K \subset L$ se, e somente se $X_K \subset X_L$.*

Demonstração: Consideremos H_L e H_K os subgrupos de $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ que fixam L e K respectivamente, se $K \subset L \subset \mathbb{Q}(\zeta_m)$, do Teorema Fundamental da Teoria de Galois segue que $H_L \subset H_K$ isso implica que $X_K \subset X_L$, e o recíproco também fica garantido. □

Lema 3.3.2 {*[4], pag. 40*} *Sejam K, L subcorpos de $\mathbb{Q}(\zeta_m)$, então $X_K \cap X_L = X_{K \cap L}$*

Os Lemas seguintes são ferramentas de fundamental importância para obter a fórmula do discriminante de corpos de números Abelianos, uma vez que estes auxiliam simplificar a estrutura dos conjuntos de caracteres associados aos subcorpos de $\mathbb{Q}(\zeta_n)$.

Lema 3.3.3 *{[4], pag. 40} Sejam K um subcorpo de $\mathbb{Q}(\zeta_m)$, s e d divisores de m, temos que $X_{K\cap\mathbb{Q}(\zeta_d)} \cap X_{K\cap\mathbb{Q}(\zeta_s)} = X_{K\cap\mathbb{Q}(\zeta_t)}$, onde $t = mdc(s,d)$.*

Demonstração: $X_{K\cap\mathbb{Q}(\zeta_d)}\cap X_{K\cap\mathbb{Q}(\zeta_s)} = X_{K\cap\mathbb{Q}(\zeta_s)\cap\mathbb{Q}(\zeta_d)=X_{K\cap\mathbb{Q}(\zeta_t)}}$, uma vez que $\mathbb{Q}(\zeta_s)$ $\cap\mathbb{Q}(\zeta_d) = \mathbb{Q}(\zeta_t)$. □

Lema 3.3.4 *{[4], pag. 41} Sejam $A_1, \cdots, A_n$ conjuntos e $B_r = \sum_{i_k=1,\ i_j<i_{j+1}}^{n} |A_{i_1} \cap \cdots \cap A_{i_r}|$, $r = 1, \cdots, n$, então*

$$|A_1 \cap \cdots \cap A_n| = \sum_{k=1}^{n} (-1)^{k+1} B_k$$

Consideremos agora um corpo de números K de condutor m, segue do Lema 3.3.1, que $X_K \subset X_{\mathbb{Q}(\zeta_m)}$, por este fato, temos que os condutores dos caracteres de X_K são divisores de m. Assim, vamos determinar a quantidade de caracteres de X_K cujo o condutor é d, para cada d divisor de m. O conjunto $X_{K\cap\mathbb{Q}(\zeta_d)}$ é formado por todos os caracteres associados a K cujo o condutor é um divisor de d. Sendo assim, segue que o conjunto de caracteres de X_K cujo o condutor é d, esta contido em $X_{K\cap\mathbb{Q}(\zeta_d)}$, e temos ainda que $|X_{K\cap\mathbb{Q}(\zeta_d)}| = [K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}]$.

Desta maneira o número de caracteres de X_K, cujo o condutor é d é dado por $[K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - n(d)$, onde $n(d)$ é o número de caracteres de X_K cujo o condutor é um divisor próprio de d.

Portanto, se χ é um caracter associado a K, cujo o condutor é l, onde l é um divisor próprio de d, segue que; $\chi \in \bigcup_{p|d} X_{K\cap\mathbb{Q}(\zeta_{d/p})}$, onde p é um número primo, daí $n(d) = |\bigcup_{p|d} X_{K\cap\mathbb{Q}(\zeta_{d/p})}|$. Sendo assim o número de caracteres associado a K cujo o condutor é d, d divisor de m, é dado por;

$$[K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - |\bigcup_{p|d} X_{K\cap\mathbb{Q}(\zeta_{d/p})}|$$

.

Assim, pela Fórmula do Condutor-Discriminante, segue que o discriminante de um corpo abeliano K de condutor m, é;

$$|\Delta(K)| = \prod_{d|m} d^{[K\cap\mathbb{Q}(\zeta_d):\mathbb{Q}]-|\bigcup_{p|d} X_{K\cap\mathbb{Q}(\zeta_{d/p})}|} \tag{3.1}$$

Porém, se decompormos m em fatores irredutíveis, podemos ainda tornar a fórmula acima um tanto mais elegante, para isso consideremos o;

Lema 3.3.5 {*[4], pag. 42*} *Se* $d = p_1^{\beta_1}.p_2^{\beta_2}\cdots p_r^{\beta_r}$, *então;* $|\bigcup_{p|d} X_{K\cap\mathbb{Q}(\zeta_{d/p})}| = \sum_{i=1}^{r}|X_{K\cap\mathbb{Q}(\zeta_{d/p_i})}| - \sum_{i_1,i_2=1\ i_1<i_2}^{r}|X_{K\cap\mathbb{Q}(\zeta_{d/p_{i_1}.p_{i_2}})}| + \cdots + (-1)^{r+1}|X_{K\cap\mathbb{Q}(\zeta_{d/p_1\cdots p_r})}|$

Considerando um corpo Abeliano $K \subseteq \mathbb{Q}(\zeta_m)$, através do lema imediatamente anterior a Fórmula (3.1) pode ainda ser melhorada, como pode ser visto no teorema abaixo.

Teorema 3.3.1 {*[4], pag. 42*} *Sejam* $m = p_1^{\alpha_1}.p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ *e* K *um corpo de números abeliano de condutor* m, *então;*

$$|\Delta(K)| = \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\sum_{r=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]}}$$

O Teorema 3.3.1 expressa uma fórmula para o discriminante de um corpo Abeliano qualquer. E, através desta conseguimos obter os resultados das seções 3.1 e 3.2 como uma consequência imediata deste teorema os quais serão expostos nos corolários abaixo.

Corolário 3.3.1 {*[4], pag. 45*} *Seja* K *um subcorpo de* $\mathbb{Q}(\zeta_{p^r})$ *de grau* up^j, *onde* p *é primo ímpar e* u *divide* $p-1$ *e* $0 \leq j \leq r-1$, *então;*

$$|\Delta(K)| = p^{u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}]-1}$$

Demonstração: Como $[K:\mathbb{Q}] = up^j$, então $m = p^{j+1}$ é o menor inteiro tal que $K \subset \mathbb{Q}(\zeta_{p^{j+1}})$. Assim;

$$|\Delta(K)| = \frac{m^{[K:\mathbb{Q}]}}{p^{\sum_{r=1}^{j+1}[K\cap\mathbb{Q}(\zeta_{m/p^r}):\mathbb{Q}]}} = \frac{(p^{j+1})^{up^j}}{p^{\sum_{r=0}^{j}[K\cap\mathbb{Q}(\zeta_{m/p^r}):\mathbb{Q}]}}$$

Como $[K \cap \mathbb{Q}(\zeta_{m/p^j}) : \mathbb{Q}] = up^{j-1}$, $j \geq 1$ e $[K \cap \mathbb{Q}(\zeta_{m/p^0}) : \mathbb{Q}] = 1$, daí

$$|\Delta(K)| = \frac{p^{u(j+1)p^j}}{p^{up^{j-1}+up^{j-2}+\cdots+up+u+1}} = \frac{p^{u(j+1)p^j}}{p^{u(p^{j-1}+p^{j-2}+\cdots+p+1)+1}} = \frac{p^{u(j+1)p^j}}{p^{u(\frac{p^j-1}{p-1})+1}} =$$
$$= p^{u(j+1)p^j-u(\frac{p^j-1}{p-1})-1} = p^{u[(j+1)p^j-(\frac{p^j-1}{p-1})]-1} = p^{u[(j+1)p^j-(\frac{p^j-1}{p-1})-p^j+p^j]-1} =$$
$$= p^{u[(j+2)p^j-(\frac{p^{j+1}-1}{p-1})]-1} \qquad \square$$

Corolário 3.3.2 *{[4], pag. 46} Seja K um subcorpo de $\mathbb{Q}(\zeta_{2^n})$ de grau 2^{m-1}. Se $K = \mathbb{Q}(\zeta_{2^n})$, $|\Delta(K)| = 2^{(m-1).2^{m-1}}$, caso contrário, $|\Delta(K)| = 2^{m.2^{m-1}-1}$*

Demonstração: Suponhamos que $K = \mathbb{Q}(\zeta_{2^n})$, temos que, $[K \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^n}) \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = 2^{i-1}$, $i \geq 1$ e $[\mathbb{Q}(\zeta_{2^0}) : \mathbb{Q}] = 1$, daí $|\Delta(K)| = \frac{2^{n.[K:\mathbb{Q}]}}{\sum_{2}^{m} [K \cap \mathbb{Q}(\zeta_{m/2^r}) : \mathbb{Q}]} = \frac{2^{n.2^{n-1}}}{\sum_{2}^{m-1} [K \cap \mathbb{Q}(\zeta_{2^r}) : \mathbb{Q}]} = \frac{2^{n.2^{n-1}}}{2^{2^{m-2}+2^{m-3}+\cdots+2+1+1}} =$
$= \frac{2^{n.2^{n-1}}}{2^{[2^{n-1}-1]+1}} = \frac{2^{n.2^{n-1}}}{2^{2^{n-1}}} = 2^{(n-1).2^{n-1}}$

Se $k \neq \mathbb{Q}(\zeta_{2^n})$, então $K \in \mathbb{Q}(\zeta_{2^{n+1}})$ e $[\mathbb{Q}(\zeta_{2^{n+1}}) : K] = 2$, logo $[\mathbb{Q}(\zeta_{2^i}) : K \cap \mathbb{Q}(\zeta_{2^i})] = 2$ para $i \in 2, \cdots, n$ e portanto, $[K \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}/2] = 2^{i-1}$ $i \geq 2$ e $[K \cap \mathbb{Q}(\zeta_2) : \mathbb{Q}] = [K \cap \mathbb{Q}(\zeta_{2^0}) : \mathbb{Q}] = 1$. Assim, $|\Delta(K)| = \frac{2^{(n+1).[K:\mathbb{Q}]}}{\sum_{2}^{n+1} [K \cap \mathbb{Q}(\zeta_{2^{n+1}/2^r}) : \mathbb{Q}]} = \frac{2^{(n+1).2^n}}{\sum_{2}^{m-1} [K \cap \mathbb{Q}(\zeta_{2^r}) : \mathbb{Q}]} = \frac{2^{(n+1).2^{n-1}}}{2^{2^{m-2}+2^{m-3}+\cdots+2+1+1+1}} =$
$= \frac{2^{n.2^{n-1}}}{2^{[2^{n-1}-1]+2}} = \frac{2^{n.2^{n-1}}}{2^{2^{n-1}+1}} = 2^{(n+1).2^{n-1}-2^{n-1}-1} = 2^{(n-1).2^{n-1}-1}$ $\square$

Pelo fato de um corpo ciclotômico $\mathbb{Q}(\zeta_n)$ ser também um corpo de números Abeliano, podemos determinar o discriminante de $\mathbb{Q}(\zeta_n)$ usando a fórmula descrita pelo Teorema 3.3.1, como pode ser visto no;

Corolário 3.3.3 *{[4], pag. 46} Se $K = \mathbb{Q}(\zeta_m)$, então*

$$|\Delta(K)| = \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\frac{\varphi(m)}{p-1}}}$$

Demonstração: $K \cap \mathbb{Q}(\zeta_{m/p_i^j}) = \mathbb{Q}(\zeta_{m/p_i^j})$ e daí, $[K \cap \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}] = \phi(m/p_i^j)$,

como $[K:\mathbb{Q}] = \varphi(m)$, segue que;

$$|\Delta(K)| = \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\sum_{j=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^j}):\mathbb{Q}]}} = \frac{m^{\varphi(m)]}}{\prod_{i=1}^{k} p_i^{\sum_{j=1}^{\alpha_i}\phi(m/p_i^j)}} =$$

$$= \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{\varphi(m/p_i)+\varphi(m/p_i^2)+\cdots+\varphi(m/p_i^{\alpha_i})}} =$$

$$= \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{\varphi(p_1^{\alpha_1}.p_2^{\alpha_2}\cdots p_i^{\alpha_i-1}\cdots p_k^{\alpha_k})+\varphi(p_1^{\alpha_1}.p_2^{\alpha_2}\cdots p_i^{\alpha_i-2}\cdots p_k^{\alpha_k})+\cdots+\varphi(p_1^{\alpha_1}.p_2^{\alpha_2}\cdots p_i^{\alpha_i-\alpha_i}\cdots p_k^{\alpha_k})}} =$$

$$= \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{\sum_{j=0}^{\alpha_i-1}\varphi(p_i^j)\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}} = \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})\sum_{j=0}^{\alpha_i-1}\varphi(p_i^j)}} =$$

$$= \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{[1+(p_i-1)+(p_i-1).p_i+(p_i-1).p_i^2+\cdots+(p_i-1).p_i^{\alpha_i-2}].\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}} =$$

$$= \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{[1+(p_i-1).(\frac{p_i^{\alpha_i}-1}{p_i-1})].\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}} = \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{[1+p_i^{\alpha_i}-1].\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}} =$$

$$\frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{p_i^{\alpha_i}.\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}} = \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{(p_i-1).\frac{p_i^{\alpha_i}}{(p_i-1)}.\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}} =$$

$$\frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{\frac{\varphi(p_i^{\alpha_i})}{(p_i-1)}.\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}} = \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p_i^{\frac{\varphi(p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}.p_i^{\alpha_i}.p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}{(p_i-1)}}} =$$

$$\frac{m^{\varphi(m)}}{\prod_{p|m} p_i^{\frac{\varphi(m)}{(p_i-1)}}} = \frac{m^{\varphi(m)}}{\prod_{i=1}^{k} p^{\frac{\varphi(m)}{(p-1)}}}$$

□

Como temos o objetivo de estudar o problema do discriminante mínimo sobre corpos Abelianos de grau primo, precisamos então estabelecer uma fórmula para o discriminante desta classe de corpos. E, isto será feito nos corolários abaixo.

Corolário 3.3.4 *{[4], pag. 49} Seja K um corpo de números de condutor m. Se $K \cap \mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$, para todo p primo divisor de m, então*

$$|\Delta(K)| = m^{[K:\mathbb{Q}]-1}$$

Demonstração: Como $K \cap \mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$, para todo p primo, divisor de m, temos que $[K \cap \mathbb{Q}(\zeta_{m/p_i^r}) : \mathbb{Q}] = 1$ e $\sum_{r=1}^{\alpha_i} [K \cap \mathbb{Q}(\zeta_{m/p_i^r}) : \mathbb{Q}] = \alpha_i$, então

$$|\Delta(K)| = \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\sum_{r=1}^{\alpha_i} [K \cap \mathbb{Q}(\zeta_{m/p_i^r}) : \mathbb{Q}]}} = \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i}} = \frac{m^{[K:\mathbb{Q}]}}{m} = m^{[K:\mathbb{Q}]-1}$$

□

Corolário 3.3.5 *{[4], pag. 50} Seja K um corpo de números abeliano de grau primo p, e condutor m, então $|\Delta(K)| = m^{p-1}$.*

Demonstração: Sendo $K \cap \mathbb{Q}(\zeta_{m/p})$ um subcorpo próprio de K então $[K \cap \mathbb{Q}(\zeta_{m/p}) : \mathbb{Q}]$ divide $[K : \mathbb{Q}]$, isso implica que $K \cap \mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$, logo $|\Delta(K)| = m^{[K:\mathbb{Q}]-1} = m^{p-1}$ □

Para os nossos propósitos, o Corolário 3.3.5 se constitui como um dos principais resultados desta seção. Uma vez que estaremos estudando a classe de corpos Abelianos de grau p:primo e este apresenta a fórmula do discriminante para estes corpos.

3.4 Discriminante mínimo de corpos Abelianos de grau p

Na Seção 1.6, foi feito uma breve revisão a respeito de alguns problemas dos reticulados algébricos, sendo apresentado o problema da maximização da densidade

de centro [Fórmula 1.1], sendo visto que uma das maneiras que se tem para se fazer tal maximização é fazendo a minimização do discriminante, em valor absoluto, do corpo em questão. No entanto, esse, pode ser classificado como um dos principais problemas onde se aplica o conceito do discriminante mínimo de um corpo de números. Embora estejamos tratando de um problema ainda não resolvido totalmente, o objetivo nesta seção é estudar esse problema somente sobre os corpos Abelianos de grau p:primo.

Iniciaremos este estudo obtendo um resultado específicos aos corpos quadráticos, onde apresentaremos o corpo quadrático que possui o menor discriminante.

Teorema 3.4.1 *O discriminante mínimo dos corpos de números de grau 2 é, em módulo, igual a 3 e* $\mathbb{Q}(\sqrt{-3})$ *é o corpo quadrático de menor discriminante.*

Demonstração: Consideremos $K = \mathbb{Q}(\sqrt{-3})$, pelo Teorema 1.5.2 segue que $|\Delta(K)| = 3$. Supondo $K = \mathbb{Q}(\sqrt{d})$, também pelo mesmo teorema se $d \not\equiv 1(mod\,4)$, então $|\Delta(K)| = 4|d| > 3$. Se $d \equiv 1(mod\,4)$, temos que $|\Delta(K)| = |d|$, e neste caso, $|\Delta(K)| < 3$ se, e somente se $d = \pm 1$. Mas, $\mathbb{Q}(\sqrt{1})$ não é quadrático e pelo fato de $-1 \not\equiv 1\,(mod\,4)$ o teorema está demonstrado.

□

Agora, o nosso próximo objetivo consiste em calcular o discriminante mínimo dos corpos Abelianos de grau p, com p ímpar, porém, antes disto, vamos estabelecer um resultado interessante que determina a quantidade de corpos de números abelianos de grau p contidos em uma determinada extensão ciclotômica.

Consideremos um corpo de números abeliano K de grau p:primo. Então segue que $Gal(K/\mathbb{Q})$ um grupo abeliano de ordem p. Pelo Teorema de Kronecker-Weber segue que $K \subset \mathbb{Q}(\zeta_n)$, para algum n, isso implica que $p \mid \varphi(n)$. A recíproca deste resultado é também verdadeira, isto é, se $p \mid \varphi(n)$, então $\mathbb{Q}(\zeta_n)$ contém um corpo de grau p.

Lema 3.4.1 *Seja n um inteiro positivo e $L = \mathbb{Q}(\zeta_n)$, então L contém um corpo de grau p se, e somente se p divide $\varphi(n)$.*

Demonstração: Se $[K:\mathbb{Q}] = p$ e $K \subseteq \mathbb{Q}(\zeta_n)$, então $p \mid \varphi(n)$, pela multiplicidade dos graus.

Por outro lado, consideremos $n = \prod_{i=1} p_i^{\alpha_i}$, então $\varphi(n) = \prod_{i=1}(p_i - 1)p_i^{\alpha_i - 1}$, se $p \mid \varphi(n)$, então $p \mid (p_i - 1)$ ou $p = p_i$, com $\alpha_i \geq 2$. Se $p \mid (p_i - 1)$ temos que o corpo $\mathbb{Q}(\zeta_{p_i})$ contém um subcorpo K de grau p, como $\mathbb{Q}(\zeta_{p_i}) \subseteq \mathbb{Q}(\zeta_n)$, segue que $K \subseteq \mathbb{Q}(\zeta_n)$. Se $p = p_i$ com $\alpha_i \geq 2$, temos que o corpo $\mathbb{Q}(\zeta_{p^2})$ contém um subcorpo L de grau p, como $\mathbb{Q}(\zeta_{p^2}) \subseteq \mathbb{Q}(\zeta_n)$, segue que $L \subseteq \mathbb{Q}(\zeta_n)$. Logo se $p \mid \varphi(n)$, então $\mathbb{Q}(\zeta_n)$ contém um subcorpo de grau p.

□

Antes de nos direcionarmos efetivamente para o problema do discriminante mínimo de corpos abelianos de grau p, vamos estabelecer um resultado que nos informa a respeito da quantidade de subcorpos de grau p que existem em uma extensão ciclotômica $\mathbb{Q}(\zeta_n)$. Um problema interessante seria de encontrar o subcorpo que possui o menor discriminante. Porém, não será este aqui o nosso intuito, mas estamos interessados somente em determinar a extensão ciclotômica mínima que contém este corpo.

Com o próximo teorema pretendemos contar a quantidade de corpos de grau p, contidos em uma extensão ciclotômica $\mathbb{Q}(\zeta_n)$.

Teorema 3.4.2 *Sejam $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ a fatoração de n em fatores primos e*

$$r = \#\{p_i : p \mid \varphi(p_i^{\alpha_i}), \quad i = 1, \cdots, k\}$$

Então existem $\frac{p^r - 1}{p-1}$ corpos K de grau p em $\mathbb{Q}(\zeta_n)$

Demonstração: Conforme o Teorema Fundamental da Teoria de Galois existe uma correspondência biunívoca entre os subcorpos de $\mathbb{Q}(\zeta_n)$ e os subgrupos H de $G = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $[K:\mathbb{Q}] = (G:H)$. Como $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ assim, o objetivo será encontrar a quantidade de subgrupos de $(\mathbb{Z}/n\mathbb{Z})^*$ de índice p, o que equivale a determinar a quantidade de subgrupos de $(\mathbb{Z}/n\mathbb{Z})^*$ de índice p.

Consideremos $\overline{G}$, um grupo de ordem p, temos então que $\overline{G} = \{e, x, x^2, \cdots, x^{p-1}\}$, como a ordem do elemento divide a ordem do grupo segue que a ordem dos elementos

$x, x^2, \cdots, x^{p-1}$ é p. Então cada subgrupo de G de ordem p é formado pelo elemento neutro e mais $p-1$ elementos de ordem p. Assim, necessitamos saber quantos elementos de G possuem ordem p.

Seja o conjunto $\{1, x_2, x_3, \cdots, x_m\}$ de elementos de G tais que $x^p = 1$. Então os subgrupos de G de ordem p são;

$\{1, x_2, x_2^2, \cdots, x_2^{p-1}\}$

$\{1, x_3, x_3^2, \cdots, x_3^{p-1}\}$

.....

$\{1, x_m, x_m^2, \cdots, x_m^{p-1}\}$

Isto quer dizer que existem $t(p-1)+1$ elementos tais que $x^p = 1$, onde t é o número de subgrupos cuja a ordem é p. Segue então que $m = t(p-1)+1$, ou seja, $t = \frac{m-1}{p-1}$.

Agora basta determinar o valor de m. Sendo G abeliano segue que $G = (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})^*$, então, determinar m, é determinar o números de soluções da equação $y^p = 1$, $y \in G$, ou seja $(y_1, \cdots, y_s)^p = (1, \cdots, 1)$, onde $y_i^p = 1$, $i = 1, \cdots, s$, e $y_i \in (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ então a equação acima é equivalente ao sistema:

$$\begin{cases} y_1^p = 1 \\ \vdots \\ y_s^p = 1 \end{cases}$$

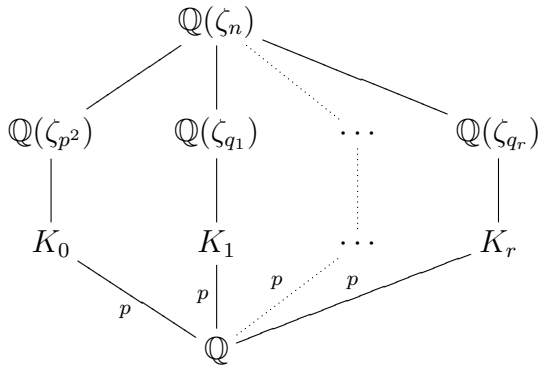
Como $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ é cíclico, se $p \nmid \varphi(p_i^{\alpha_i})$, segue que a equação $y_i^p = 1$ possui somente a solução trivial. Agora, se $p \mid \varphi(p_i^{\alpha_i})$ temos que a solução da equação $(y_1, \cdots, y_s)^p = (1, \cdots, 1)$ é uma s-upla, onde cada coordenada pode ter 1 ou p soluções, e estas possibilidades equivalem a quantidade de $p_i's$, tais que $p \mid \varphi(p_i^{\alpha_i})$, então $m = p^r$, onde

$$r = \#\{p_i : p \mid \varphi(p_i^{\alpha_i}), \quad i = 1, \cdots, k\}$$

Logo $t = \frac{p^r-1}{p-1}$ □

Sabendo a quantidade de subcorpos de grau primo p contidos em uma determinada extensão ciclotômica, o objetivo agora é estabelecer qual será o menor dis-

criminante entre todos estes $\frac{p^r-1}{p-1}$ corpos. Sendo $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, onde $p \mid \varphi(n)$, consideremos o seguinte diagrama;



Onde $q_i \equiv 1\,(mod\,p)$ $i = 1, \cdots, r$, temos que os corpos de grau p contidos em $\mathbb{Q}(\zeta_n)$, são em número $\frac{p^s-1}{p-1}$, sendo $s = \#\{p_i : p \mid \varphi(p_i)\}$. Por outro lado, como $p \mid \varphi(q_i)$ e $p \mid \varphi(p^2)$, pelo Lema 3.4.1 temos que os corpos $\mathbb{Q}(\zeta_{p^2})$, $\mathbb{Q}(\zeta_{q_1})$, $\cdots$, $\mathbb{Q}(\zeta_{q_r})$ são subcorpos de $\mathbb{Q}(\zeta_n)$ que contém algum corpo de grau p. Além disto estas são extensões ciclotômicas de menor grau que contém algum corpo de grau p, ou seja, $p^2, q_1, \cdots, q_r$ são condutores respectivamente dos corpos $K_0, K_1, \cdots, K_r$.

Conforme o Corolário 3.3.5, segue que se m é o condutor de K, onde $[K : \mathbb{Q}] = p$, então $|\Delta(K)| = m^{p-1}$, logo o corpo de números Abeliano de grau p com o menor discriminante, em valor absoluto, é aquele com o menor condutor. Visto que $\mathbb{Q}(\zeta_{p^2})$ tem um corpo K de grau p, cujo o condutor é p^2, e portanto $|\Delta(K)| = (p^2)^{p-1}$ e se $q \equiv 1\,(mod\,p)$, então existe um corpo $K_q \subseteq \mathbb{Q}(\zeta_q)$, cujo o condutor é q, e portanto $|\Delta(K_q)| = q^{p-1}$. Finalmente, se K é um corpo de números Abeliano de grau p cujo o condutor é n, então $p \mid \varphi(n)$, ou seja, p^2 divide n ou existe q primo, $q \equiv 1(mod\,p)$, tal que $q \mid n$; assim o corpo abeliano de grau p com discriminante (em valor absoluto) mínimo ocorre quando o seu condutor é p^2 ou é um menor primo q, tal que $q \equiv 1(mod\,p)$. Com isso temos provado o;

Teorema 3.4.3 {*[4], pag.50*} *O discriminante mínimo, em valor absoluto, dos corpos abelianos de grau primo p é, $p^{2(p-1)}$ ou q^{p-1}, onde q é o menor primo tal que $q \equiv 1\,(mod\,p)$.*

Com o resultado acima, além de estabelecer o discriminante mínimo de um corpo Abeliano de grau primo, fica estabelecido também qual a extensão ciclotômica de

menor grau que contém tal corpo. De acordo ao diagrama acima temos que tal extensão é $\mathbb{Q}(\zeta_{p^2})$ ou $\mathbb{Q}(\zeta_q)$, onde q é o menor primo tal que $q \equiv 1\,(mod\,p)$.

Embora diante da importância de se obter o menor discriminante de corpos de números em uma determinada dimensão, como foi referido na Seção 1.6, ainda não se tem resultados gerais referentes a este assunto. Aqui neste trabalho foi apresentado um caso especifico dentre os corpos abelianos, a saber os corpos de grau primo, porém muita coisa ainda tem para ser feita. No entanto, estamos tratando de um assunto motivante e que ainda demandará muito esforço e empenho para resolvê-lo, pois até mesmo para casos especiais, como por exemplo, para os corpos de números Abelianos, pouca coisa ainda tem sido feito. Desta forma, com este trabalho, deixamos ao leitor um convite para participar entusiasticamente na tentativa de resolver este desafio. Pois, um mistério só é desvendado quando alguém propõe estudá-lo.

Referências Bibliográficas

[1] Stewart, I., Tall,D. **Algebric numbers theory**. New York:Chapman e Hall,1979

[2] Ribeiro, A.C. **Reticulados sobre corpos de números**. Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto,2001.

[3] Gonçalves, A. **Introdução à álgebra**. Instituto de Matemática Pura e Aplicada, Rio de Janeiro,1979.

[4] Lopes, J.O.D. **Discriminante dos corpos Abelianos**. Tese de Doutorado, IMECC/UNICAMP,2003.

[5] Quilles, C.R.O. **Discriminante de corpos de números**. Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto, 2006.

[6] Washington, L.C. **Introduction to ciclotomic fields**. Springer-Verlag, New York, 1982.

[7] Nobrega, T.P.,Interlando, J.C., Lopes, J.O.D. On Computing discriminants of subfields of $\mathbb{Q}(\zeta_{p^r})$. **Jornal of Numbers Theory**, N.96, pp 319-325, 2002.

[8] Garcia, A.; Lequain, Y.**Elementos de Álgebra**. Projeto Euclides, 2002.

[9] Rodrigues, T.M.**Cúbicas Galoisianas**. Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto,2003.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo