Universidade Estadual de Campinas - UNICAMP
Instituto de Matemática, Estatística e Computação Científica IMECC
Programa de Pós-Graduação em Matemática
Curso de Doutorado em Matemática

# Discriminante dos Corpos Abelianos

por

José Othon Dantas Lopes

sob orientação do

Prof. Dr. Paulo Roberto Brumatti

Tese apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - IMECC - UNICAMP, como requisito parcial para obtenção do título de Doutor em Matemática.

Agosto/2003

Campinas - SP

# Discriminante dos Corpos Abelianos

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por José Othon Dantas Lopes e aprovada pela comissão julgadora.

Campinas, 28 de 08 de 2003.

Prof. Dr. Paulo Roberto Brumatti

Orientador

Prof. Dr. Trajano P. Nóbrega Neto

Co-orientador

Banca Examinadora:

1. Prof. Dr. Amilcar Pacheco
2. Prof. Dr. Antonio José Engler
3. Prof. Dr. Hemar Godinho
4. Prof. Dr. José Plínio de Oliveira Santos
5. Prof. Dr. Paulo Roberto Brumatti

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de DOUTOR em Matemática.

## FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Lopes, José Othon Dantas

L881d Discriminante dos corpos abelianos / José Othon Dantas Lopes -- Campinas, [S.P. :s.n.], 2003.

Orientador : Paulo Roberto Brumatti

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Corpos algébricos. 2. Caracteres de grupos. 3. Teoria dos números algébricos. I. Brumatti, Paulo Roberto. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

**Tese de Doutorado defendida em 28 de agosto de 2003 e aprovada**

**Pela Banca Examinadora composta pelos Profs. Drs.**

**Prof (a). Dr (a). PAULO ROBERTO BRUMATTI**

**Prof (a). Dr (a). AMILCAR PACHECO**

**Prof (a). Dr (a). ANTONIO JOSÉ ENGLER**

**Prof (a). Dr (a). HEMAR TEIXEIRA GODINHO**

**Prof (a). Dr (a). JOSÉ PLINIO DE OLIVEIRA SANTOS**

# Agradecimentos

1. Ao Professor Dr. Trajano Pires da Nóbrega Neto, pela orientação, pelo interesse e dedicação com que se envolveu e pela imprescindível colaboração para o desenvolvimento deste trabalho.

2. Ao Professor Dr. Paulo Roberto Brumatti, pela colaboração junto ao IMECC/UNICAMP.

3. Ao Professor Dr. Francisco Thaine Prada, pela leitura crítica do trabalho e pelos ensinamentos durante o curso.

4. Ao Prof. Dr. José Carmelo Interlando pelo apoio e pelas importantes sugestões.

5. Aos colegas do Departamento de Matemática da UFC, em especial ao Chefe do Departamento, Professor Dr. José Fábio Bezerra Montenegro, pela compreensão e boa vontade dispensadas no sentido de me permitir uma maior dedicação na fase de conclusão da Tese.

6. Ao Programa de Pós-graduação em Matemática da UFC, através dos professores Doutores João Lucas Marques Barbosa e Antônio Gervásio Colares.

7. À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES, pelo suporte financeiro.

8. Aos professores José Valter Lopes Nunes, Ciro Nogueira Filho e Dr. Abdênago Alves de Barros, pelo apoio e incentivo, decisivos para que este objetivo fosse alcançado.

9. Ao meu Irmão José Arimatéia Dantas Lopes e à sua esposa Antônia Maria das Graças Lopes Citó, pelo apoio e ambiente fraterno propiciado durante todo o período que convivemos em Campinas.

10. Ao Professor Dr. Antônio de Andrade e Silva, da UFPB, pela valiosa ajuda na edição deste trabalho.

11. À família do Professor Trajano, pela acolhida amiga durante minhas estadias em Rio Preto.

12. A todos aqueles que contribuiram direta ou indiretamente para a realização deste trabalho.

# Dedicatória

À minha mulher Neide
e aos meus filhos
Tetê, Paulinha,
Mariana e Júnior.

# Resumo

O cálculo do discriminante de um Corpo de Números $K$ tem representado um grande desafio para muitos estudiosos e certamente a maior dificuldade consiste em se determinar uma base integral de $K$. Quando tal corpo $K$ é abeliano pode-se recorrer ao Teorema de Kronecker-Weber que assegura que $K$ está contido em alguma extensão ciclotômica $\mathbb{Q}(\zeta_m)$ e, neste caso, pode-se usar a Fórmula do Condutor-Discriminante para calcular o discriminante de $K$.

Os resultados aqui obtidos visam o cálculo efetivo dos Discriminantes dos Corpos de Números Abelianos e faz-se o uso pleno da Fórmula do Condutor-Discriminante, isto é, o discriminante de um corpo $K$ é, a menos de sinal, o produtório dos condutores dos caracteres associados a $K$. Quando o condutor de $K$ é uma potência de primo, ou seja, $K \subseteq \mathbb{Q}(\zeta_{p^r})$ para algum primo $p$ e $r$ um inteiro positivo, então o discriminante de $K$ é uma função do seu grau, quando o primo é ímpar; e tal fórmula é dada pelo Teorema 3.1. Quando tal primo é 2, o Teorema 3.3 determina o discriminante de $K$, distinguindo os casos em que $K$ é um Corpo Ciclotômico e quando não é.

O caso geral foi abordado no Teorema 3.4 e descreve o discriminante de um Corpo de Números Abeliano qualquer, em função do seu grau, do seu condutor e dos graus de subcorpos particulares de $K$.

# Abstract

The computation of the discriminant of a number field $K$ has represented a great challenge to number theorists, and certainly the difficulty lies in determining an integral basis for $K$. When $K$ is Abelian, one can resort to the Kronecker-Weber theorem, which guarantees that $K$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_m)$. In this case, one can use the conductor-discriminant formula for evaluating the discriminant of $K$. The results obtained here aim at efficiently computing the discriminant of any Abelian number field. For that, we will fully use the conductor-discriminant formula, which states that the discriminant of a field $K$ is the product of the conductors of the characters associated to $K$. When the conductor of $K$ is a power of an odd prime $p$, that is, $K \subseteq \mathbb{Q}(\zeta_{p^r})$ for some positive integer $r$, then the discriminant of $K$ is a function of its degree only - see the formula given in Theorem 3.1. When $p = 2$, Theorem 3.3 provides a formula for the discriminant of $K$ which consists of two expressions, depending on whether $K$ is a cyclotomic field. The general case is addressed in Theorem 3.4. It gives the discriminant of any Abelian number field as a function of its degree, its conductor, and the degrees of some particular subfields of $K$.

# Notação

$\widehat{G}$ - Grupo dos caracteres do grupo $G$.

$\langle g \rangle$ - Subgrupo gerado por $g$.

$\mathbb{Z}/n\mathbb{Z}$ - Anel dos inteiros módulo $n$.

$(\mathbb{Z}/n\mathbb{Z})^*$ - Grupo multiplicativo dos elementos inversíveis de $\mathbb{Z}/n\mathbb{Z}$.

$(a, b)$ - Máximo dividor comum de $a$ e $b$.

$[a, b]$ - Mínimo múltiplo comum de $a$ e $b$.

$\phi(n)$ - Função de Euler.

$K^*$ - Grupo cíclico multiplicativo do corpo $K$.

$K[X]$ - Anel dos polinômios sobre o corpo $K$.

$[L : K]$ - Grau de $L$ sobre $K$.

$\mathbb{N}$ - 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.

$\equiv$ - Congruente.

$|$ - Divide.

$\cong$ - Isomorfo.

Disc$(K)$ - Discriminante do corpo $K$.

$Ker(\varphi)$ - Núcleo de $\varphi$.

Im $\varphi$ - Imagem de $\varphi$.

$Tr_{B/A}(x)$ - Traço de $x$ relativamente a $B$ e $A$.

$N_{B/A}(x)$ - Norma de $x$ relativamente a $B$ e $A$.

det $M$ - Determinante da matriz $M$.

$D(x_1, x_2, \ldots, x_n)$ - Discriminante do sistema $(x_1, x_2, \ldots, x_n)$.

$\mathbb{D}_{B/A}$ - Ideal gerado pelo discriminante de qualquer base de $B$ sobre $A$.

$\mathcal{O}_K$ -Anel dos inteiros de um corpo de números $K$.

$Gal(L/K)$ - Grupo de Galois de $L$ sobre $K$.

$X_K$ - Grupo dos caracteres associados a $K$.

$f_\chi$ - Condutor do caracter $\chi$.

$\zeta_m$ - Raiz $m$-ésima primitiva da unidade.

$|A|$ - Cardinalidade do conjunto $A$.

# Sumário


Introdução xi

**1 Resultados Básicos** **1**

1.1 Elementos inteiros sobre um anel e algébricos sobre um corpo . . . . . 1

1.2 Elementos e corpos conjugados . . . . . 4

1.3 Norma, traço e polinômio característico . . . . . 5

1.4 Discriminante . . . . . 6

1.5 Teoria de Galois . . . . . 8

1.6 Corpos de Números . . . . . 9

1.7 Prolongamento Canônico de um Corpo de Números . . . . . 12

1.8 Corpos Ciclotômicos . . . . . 14

**2 Caracteres e a Fórmula do Condutor-Discriminante** **16**

2.1 Caracteres em grupos abelianos finitos . . . . . 16

2.1.1 Caracteres de Dirichlet . . . . . 20

2.1.2 A Fórmula do Condutor-Discriminante . . . . . 23

**3 Discriminantes dos Corpos de Números Abelianos** **26**

3.1 Os subcorpos de $\mathbb{Q}(\zeta_{p^r})$, $p$ primo ímpar . . . . . 27

3.1.1 O cálculo do discriminante . . . . . 28

3.2 Os subcorpos de $\mathbb{Q}(\zeta_{2^r}), r \geq 3$ . . . . . 31

3.2.1 O cálculo do discriminante . . . . . 34

3.3 Os Corpos de Números Abelianos . . . . . 39
3.3.1 O cálculo do discriminante . . . . . 41

**Referências Bibliográficas** **55**

# Introdução

A família dos Corpos Abelianos, certamente, representa uma importante classe na categoria dos Corpos de Números, visto que permite o uso da Teoria de Galois no estudo das extensões de ideais, no cálculo do discriminante, no grupo das classes, etc.

Nesse universo é possível reproduzir modelos matemáticos da Teoria dos Códigos Corretores de Erros, de Empacotamento de Esferas, via a representação Geométrica de Ideais Ordinários de um Corpo de Números e em inúmeras ligações da Teoria dos Números com vários outros ramos da ciência.

Em se tratando de Reticulados, ou seja, subgrupos discretos de $\mathbb{R}^n$, a sua densidade de empacotamento, ou densidade de centro, representa um importante parâmetro, cujo valor depende do discriminante do corpo $K$, da norma do ideal $I$ e da minimização da função traço relativo, quando tal reticulado é a representação geométrica de um ideal ordinário $I$ do anel de inteiros algébricos de um corpo de números $K$. Neste sentido um estudo aprofundado e de resultados significativos assume um papel fundamental no campo científico tendo em vista que tais contribuições exercem uma tarefa de ligação entre variados campos da pesquisa científica, por onde passam desafios e motivações.

Incentivado por essa importância, este trabalho busca contribuir com o item relativo ao discriminante absoluto de um Corpo de Números $K$, quando tal corpo é uma extensão de Galois, com grupo de Galois Abeliano, do corpo dos números racionais. Tais corpos são aqui denominados simplesmente de Corpos Abelianos.

O cálculo do discriminante de um corpo de números $K$, em sua definição original, passa pelo conhecimento de uma base integral do anel dos inteiros algébricos de $K$ e

do conjunto das imersões de $K$ no corpo dos números complexos. Entretanto, em se tratando de Corpos Abelianos, o Teorema de Kronecker-Weber assegura que tal corpo está contido em alguma extensão ciclotômica $\mathbb{Q}(\zeta_n)$ e, para tais casos, a Fórmula do Condutor-Discriminante oferece a possibilidade de se obter o discriminante de $K$ a partir do grupo dos automorfismos de $\mathbb{Q}(\zeta_n)$ que fixa os elementos do corpo $K$.

Com base no Teorema de Kronecker-Weber e na Fórmula do Condutor-Discriminante, dois resultados centrais da Teoria Algébrica dos Números, obtemos diversos resultados auxiliares para explicitar o discriminante de cada Corpo Abeliano.

Tendo como propósito tornar este trabalho o mais auto suficiente possível, sem entretanto alongá-lo em demasia, foi escrito um primeiro capítulo, com o objetivo introdutório, visando atender aos leitores sem formação em Teoria dos Números, porém interessados em melhor compreender as técnicas aqui apresentadas. Tal capítulo aborda os conceitos básicos da Teoria Algébrica dos Números tais como as definições de inteiro algébrico, anéis integralmente fechados, anel dos inteiros algébricos, base integral, prolongamento canônico de um corpo de números, norma e traços relativos, polinômio característico, Teoria de Galois e Corpos Ciclotômicos. As principais referências utilizadas nesse capítulo, tanto no conteúdo como na notação, foram [Rib, Sam, Ste2, Was].

No segundo capítulo são apresentados os principais resultados indispensáveis para o desenvolvimento do capítulo seguinte. O propósito central desse capítulo é o de desenvolver resultados clássicos da Teoria dos Números, todavia com o propósito de atender a parte central desta tese. Atenção especial será dada ao estudo dos caracteres de grupos abelianos finitos, com enfoque para os caracteres de Dirichlet e um tratamento direcionado para o cálculo do condutor de um caracter numérico. A Fórmula do Condutor-Discriminante também é apresentada. As referências principais para os tópicos abordados neste capítulo são os livros [Rib, Was].

O terceiro e último capítulo constitui a parte central desta tese e tem como principal objetivo apresentar contribuições originais no sentido de calcular o discriminante de um

dado Corpo Abeliano $K$.

Uma primeira abordagem é feita sobre os corpos com condutor potência de um número primo ímpar, ou seja, subcorpos de $\mathbb{Q}(\zeta_{p^r})$. Visto que o grupo de Galois de $\mathbb{Q}(\zeta_{p^r})$ sobre os racionais é cíclico então para cada divisor $s$ do grau de $\mathbb{Q}(\zeta_{p^r})$, existe um único subcorpo $K$ de $\mathbb{Q}(\zeta_{p^r})$ com grau $s$ e, certamente, o discriminante de tal corpo poderá ser explicitado em função de $s$. Este resultado corresponde ao Teorema 3.1 onde a fórmula do discriminante de $K$ em função do seu grau é explicitada e de fácil aplicação. Este resultado foi publicado em Journal of Number Theory ([Tra]).

O passo seguinte seria abordar os Corpos Abelianos de condutor potência de 2, ou seja, os subcorpos de $\mathbb{Q}(\zeta_{2^r})$. Uma primeira dificuldade consiste no fato de que o grupo de Galois de $\mathbb{Q}(\zeta_{2^r})$ sobre $\mathbb{Q}$ não é cíclico. Particularmente constatamos que para alguns divisores $s$ do grau de $\mathbb{Q}(\zeta_{2^r})$ existem até 3 subcorpos com grau $s$. Entretanto conseguimos mostrar que dado um divisor $s$ do grau de $\mathbb{Q}(\zeta_{2^r})$, seria suficiente analisar apenas se o subcorpo $K$ de $\mathbb{Q}(\zeta_{2^r})$ de grau $s$ é ciclotômico ou não. Nesta situação também obtivemos explicitamente uma fórmula para o discriminante de $K$ e este resultado será publicado em Journal of Algebra and Its Applications ([Oth]).

Na situação mais geral $K$ será considerado um Corpo Abeliano qualquer. Neste caso a técnica usada foi explorar as propriedades de $X_K$, o grupo dos caracteres associados a $K$. Inicialmente sabemos que o número de elementos de $X_K$ é igual ao grau de $K$ e que os condutores dos seus caracteres são divisores de $m$. Descrevemos o número de caracteres com condutor $d$, para cada divisor $d$ de $m$. Embora não conhecendo explicitamente $X_K$ isto foi possível devido às propriedades dos caracteres de Dirichlet. Mais precisamente, visto que $K \subset \mathbb{Q}(\zeta_m)$, temos $X_K \subset X_{\mathbb{Q}(\zeta_m)}$ e portanto os condutores dos caracteres associados a $K$ são divisores de $m$. Fixado um divisor $d$ de $m$, $X_K \cap X_{\mathbb{Q}(\zeta_d)} = X_{K\cap\mathbb{Q}(\zeta_d)}$, cuja ordem é $[K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}]$, consiste exatamente dos caracteres associados a $K$ cujo condutor é um divisor de $d$ . Assim o número de caracteres cujo condutor é $d$ é igual a

$$[K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - n(d),$$

onde $n(d)$ é o número de caracteres associados a $K$ cujo condutor é um divisor de $d$, diferente de $d$. Mostramos que $n(d)$ é igual ao número de elementos do conjunto

$$\bigcup_{p/d}(K \cap \mathbb{Q}(\zeta_{d/p})$$

e que no cálculo do discriminante de $K$ o resultado depende de alguns subcorpos particulares de $\mathbb{Q}(\zeta_m)$.

O raciocínio empregado é válido para qualquer inteiro $m$ e, particularmente, quando $m$ é o condutor de $K$. Neste caso o grupo de caracteres associados a $K$ pode ser visto como subgrupo de $(\mathbb{Z}/m\mathbb{Z})^*$ e, em conseqüência disto, os condutores de todos os caracteres associados a $K$ são divisores de $m$. Exibimos uma maneira de contar quantos caracteres existem para cada valor possível do condutor. Fazemos essa contagem observando as interseções de $K$ com os subcorpos ciclotômicos de $\mathbb{Q}(\zeta_m)$ e a partir daí obtemos uma fórmula geral para o discriminante de $K$ a qual depende de $m$, do grau de $K$ e dos graus de alguns subcorpos particulares de $K$.

# Capítulo 1

# Resultados Básicos

Apresentaremos neste capítulo algumas definições e resultados básicos da teoria dos números, diretamente relacionados com o conteúdo da tese. O objetivo é que este material seja, na medida do possível, se não autosuficiente, uma sequência que forneça ao leitor informações sobre os principais resultados, definições e idéias básicas que contribuíram para a obtenção dos resultados. Isto faz com que sua leitura se torne menos cansativa e mais estimulante.

Partimos das definições e resultados gerais envolvendo elementos inteiros sobre um anel, elementos algébricos sobre um corpo, norma, traço, polinômio característico e discriminante. Apresentamos em seguida um resumo da Teoria de Galois, destacando o Teorema Fundamental, e finalmente aplicamos os resultados aos Corpos de Números, com atenção especial aos Corpos Ciclotômicos.

## 1.1 Elementos inteiros sobre um anel e algébricos sobre um corpo

**Definição 1.1** *Sejam $B$ um anel e $A$ um subanel de $B$. Um elemento $x \in B$ é inteiro sobre $A$ se $x$ é raiz de um polinômio mônico com coeficientes em $A$. Se todo elemento de $B$ é inteiro sobre $A$ dizemos que $B$ é inteiro sobre $A$.*

**Proposição 1.1** *[Sam, Corolário 2, pag 35] Sejam $B$um anel e $A$ um subanel de $B$. O conjunto $A'$ dos elementos de $B$ que são inteiros sobre $A$ é um subanel de $B$ que contém $A$.*

**Definição 1.2** *O anel $A'$ dos elementos de $B$ inteiros sobre $A$ é chamado de fecho integral de $A$ em $B$. Particularmente se $A$ é um anel de integridade e $B$ é o corpo de frações de $A$, $A'$ é chamado simplesmente de fecho integral de $A$ e se $A' = A$ dizemos que $A$ é integralmente fechado.*

**Proposição 1.2** *[Sam, Proposição 2, pag. 35] Sejam $C$ um anel, $B$ um subanel de $C$ e $A$ um subanel de $B$. Se $B$ é inteiro sobre $A$ e $C$ é inteiro sobre $B$, então $C$ é inteiro sobre $A$.*

**Proposição 1.3** *[Sam, Proposição 3, pag. 35] Sejam $B$ um anel de integridade e $A$ um subanel de $B$ tal que $B$ é inteiro sobre $A$. Para que $B$ seja um corpo é necessário e suficiente que $A$ seja um corpo.*

**Definição 1.3** *Sejam $B$ um anel e $K \subset B$ um corpo. Um elemento $x \in B$ é algébrico sobre $K$ se $x$ é raiz de um polinômio com coeficientes em $K$. Um elemento de $B$ que não é algébrico sobre $K$ é chamado de transcendente sobre $K$.*

Assim, sobre um corpo, um elemento é algébrico se, e somente se , é inteiro.

Temos também que um elemento $x$ é algébrico sobre um corpo $K$, se e somente se, $[K[x] : K]$ é finito(como $K - módulo$).

**Definição 1.4** *Dizemos que um anel $B$ que contém um corpo $K$ é algébrico sobre $K$ se todo elemento de $B$ é algébrico sobre $K$. Neste caso, se $B$ é um corpo dizemos que $B$ é uma extensão algébrica de $K$.*

**Definição 1.5** *Se $L$ é um corpo e $K$ é um subcorpo de $L$, $[L : K]$ (dimensão de $L$ como espaço vetorial sobre $K$) é chamada de grau de $L$ sobre $K$.*

Quando o grau de $L$ sobre $K$ é finito então $L$ é uma extensão algébrica de $K$. A recíproca não é verdadeira.

Sejam $B$ um anel, $K$ um subcorpo de $B$ e $x$ um elemento de $B$ algébrico sobre $K$. Existe um homomorfismo $\varphi : K[X] \to B$ tal que $\varphi(X) = x$ e $\varphi(a) = a$ para todo $a \in K$. A imagem de $\varphi$ é $K[x]$. Podemos então dizer que um elemento $x \in B$ é algébrico sobre $K$ se, e somente se, $Ker(\varphi) \neq (0)$.

Como $K[X]$ é principal, $Ker(\varphi)$ é um ideal principal de $K[X]$. Assim, se $x$ é algébrico sobre $K$, $Ker(\varphi)$ é gerado por um polinômio não nulo $F(X)$, o qual pode ser tomado mônico e neste caso é unicamente determinado e é chamado polinômio minimal de $x$ sobre $K$. Temos também que, se $G(X) \in K[X]$, então $G(x) = 0 \Leftrightarrow F(X)$ divide $G(X)$ em $K[X]$.

Do fato de $\varphi : K[X] \to B$ ser um homomorfismo tal que $Ker(\varphi) = (F(X))$ e $\operatorname{Im}\varphi = K[x]$ temos $K[X]/(F(X)) \cong K[x]$. As equivalências a seguir são conseqüências de proposições anteriores: $K[x]$ é corpo $\Leftrightarrow$ $K[x]$ é anel de integridade $\Longleftrightarrow$ $F(X)$ é irredutível. Particularmente, se $B$ é um corpo e um elemento $x$ de $B$ é algébrico sobre $K$, o polinômio minimal de $x$ sobre $K$ é irredutível.

Por outro lado se $K$ é um corpo e $F(X) \in K[X]$ um polinômio irredutível, então $K[X]/(F(X))$ pode ser visto como um corpo que contém $K$. Denotando por $x$ a classe de $X$ nesse corpo, temos $f(x) = 0$ e assim $F(X)$ é divisível por $X - x$ sobre $K[x]$. Mais geralmente:

**Proposição 1.4** *[Sam, Proposição 3, pag. 38] Sejam $K$ um corpo e $P(X) \in K[X]$ um polinômio não constante. Existe uma extensão algébrica $K'$ de $K$ tal que $P(X)$ se decompõe em fatores lineares em $K'[X]$.*

Dizemos que um corpo $K$ é algebricamente fechado se todo polinômio não constante $P(X) \in K[X]$ se decompõe em fatores do primeiro grau em $K[X]$. Para que um corpo $K$ seja algebricamente fechado é suficiente que todo polinômio não constante $P(X) \in K[X]$ admita uma raiz $x \in K$. O corpo $\mathbb{C}$ dos números complexos é algebricamente fechado.

## 1.2 Elementos e corpos conjugados

Dados dois corpos $L$ e $M$ contendo um corpo $K$, chamamos de $K$-isomorfismo de $L$ sobre $M$ a todo isomorfismo $\varphi$ de $L$ em $M$ tal que $\varphi(a) = a$ para todo $a \in K$. Nestas condições dizemos que $L$ e $M$ são $K$-isomorfos ou, se eles são algébricos sobre $K$, que são corpos conjugados sobre $K$. Dadas duas extensões $L$ e $M$ de $K$ dizemos que dois elementos $x \in L$ e $y \in M$ são conjugados sobre $K$ se existe um $K$-isomorfismo $\varphi : K(x) \to K(y)$ tal que $\varphi(x) = y$. Tal isomorfismo $\varphi$ é único e o fato de dois elementos serem conjugados sobre $K$ significa que ou os dois são transcendentes sobre $K$ ou os dois são algébricos sobre $K$ e, neste caso, têm o mesmo polinômio minimal.

Por exemplo: se $f(X)$ for um polinômio irredutível sobre $K$ e $x_1, x_2, \ldots, x_n$ são suas raízes em uma extensão $L$ de $K$, então os $x_i$ são dois a dois conjugados sobre $K$, bem como os corpos $K(x_i)$ são também dois a dois conjugados sobre $K$.

**Lema 1.1** *[Sam, Lema, pag. 39] Sejam $K$ um corpo finito ou de característica zero, $F(X)$ um polinômio mônico irredutível em $K[X]$,*

$$F(X) = \prod_{i=1}^{n} (X - x_i)$$

*sua decomposição em fatores lineares em uma extensão $K'$ de $K$. Então as $n$ raízes $x_1, x_2, \ldots, x_n$ de $F(X)$ são distintas.*

**Teorema 1.1** *[Sam, Teorema 1, pag. 40] Sejam $K$ um corpo finito ou de característica 0, $L$ uma extensão de $K$ de grau $n$ e $C$ um corpo algebricamente fechado contendo $K$. Então existem $n$ $K$-isomorfismos distintos de $L$ em $C$.*

**Corolário 1.1 (Teorema do Elemento Primitivo)** *[Sam, Corolário, pag. 41] Sejam $K$ um corpo finito ou de característica 0 e $L$ uma extensão de grau finito $n$ de $K$. Então existe um elemento $x$ em $L$ tal que $L = K[x]$. Um tal elemento $x$ é chamado de elemento primitivo.*

## 1.3 Norma, traço e polinômio característico

Sejam $B$ um anel e $A$ um subanel de $B$ tal que $B$ seja um $A$-módulo livre de posto finito $n$ (por exemplo se $A$ é um corpo e $B$ é uma extensão de grau $n$ de $A$). Dado $x \in B$, a aplicação $m_x : B \to B$ dada por $m_x(y) = xy$ é um endomorfismo do $A$-módulo $B$. Seja $\{e_1, e_2, \ldots, e_n\}$ uma base qualquer de $B$ e $(a_{ij})$ a matriz que representa $m_x$ nesta base.

Definimos:

i) O traço de $x$ relativamente a $B$ e $A$ por $\sum_{i=1}^{n} a_{ii}$. Usaremos a notação $Tr_{B/A}(x)$ (ou simplesmente, $Tr(x)$).

ii) A norma de $x$ relativamente a $B$ e $A$ por $\det(a_{ii})$. Usaremos a notação $N_{B/A}(x)$ (ou simplesmente, $N(x)$).

iii) O polinômio característico de $x$ relativamente a $B$ e $A$ por $\det(X.I_B - (a_{ii}))$. Se $x, x' \in B$ e $a \in A$, temos as seguintes propriedades:

$$\begin{aligned} Tr(x+x') &= Tr(x) + Tr(x'),\ Tr(ax) = aTr(x),\ Tr(a) = na, \\ N(xx') &= N(x)N(x'),\ N(ax) = a^n N(x), N(a) = a^n. \end{aligned}$$

**Proposição 1.5** *[Sam, Proposição 1, pag. 44] Sejam $K$ um corpo de característica 0 ou finito, $L$ uma extensão algébrica de grau $n$ de $K$, $x$ um elemento algébrico de $L$, e $x = x_1, x_2, \ldots, x_n$ as raízes do polinômio minimal de $x$ em uma extensão conveniente de $K$, cada uma repetida $[L : K[x]]$ vezes. Então*

$$Tr_{L/K}(x) = x_1 + x_2 + \cdots + x_n, N_{L/K}(x) = x_1 \cdot x_2 \cdots x_n$$

*e o polinômio característico de $x$, relativamente a $L$ e $K$ é*

$$(X - x_1)(X - x_2)\cdots(X - x_n).$$

Desta Proposição segue-se que o polinômio característico é a $[L : K[x]]$-ésima potência do polinômio minimal.

**Proposição 1.6** *[Sam, Proposição 2, pag. 45] Sejam $A$ um anel de integridade, $K$ seu corpo de frações, $L$ uma extensão de grau finito de $K$ e $x$ um elemento de $L$ inteiro sobre $A$. Se $K$ tem característica 0, então os coeficientes do polinômio característico de $x$ relativamente a $L$ e $K$, em particular $Tr_{L/K}(x)$ e $N_{L/K}(x)$, são inteiros sobre $A$.*

**Corolário 1.2** *[Sam, Corolário, pag. 45] Suponha, além disso, que $A$ é integralmente fechado. Então os coeficientes do polinômio característico de $x$ relativamente a $L$ e $K$, em particular $Tr_{L/K}(x)$ e $N_{L/K}(x)$, são elementos de $A$.*

Assim, quando consideramos particularmente $A$ como sendo o anel dos números inteiros, os coeficientes do polinômio característico relativamente a $L$ e $\mathbb{Q}$ de um elemento $x \in L$, inteiro sobre $\mathbb{Z}$, são números inteiros. Conseqüentemente, se L é uma extensão finita dos racionais então $Tr_{L/\mathbb{Q}}(x)$ e $N_{L/\mathbb{Q}}(x)$ são números inteiros.

## 1.4 Discriminante

**Definição 1.6** *Sejam $B$ um anel e $A$ um subanel de $B$ tal que $B$ seja um $A$-módulo livre de posto finito $n$. Para $(x_1, x_2, \ldots, x_n) \in B^n$ chamamos de discriminante do sistema $(x_1, x_2, \ldots, x_n)$ o elemento de $A$ definido por*

$$D(x_1, x_2, \ldots, x_n) = \det(Tr_{B/A}(x_i x_j)).$$

**Proposição 1.7** *[Sam, Proposição 1, pag. 46] Se $(y_1, y_2, \ldots, y_n) \in B^n$ é um outro sistema de elementos de $B$ tal que*

$$y_i = \sum_{j=1}^{n} a_{ij} x_j,$$

*com* $a_{ij} \in A$, *então*

$$D(y_1, y_2, \ldots, y_n) = \det(a_{ij})^2 D(x_1, x_2, \ldots, x_n).$$

Quando dois sistemas são bases então a matriz mudança de uma base para a outra é invertível e portanto seu determinante é invertível. De acordo com a proposição acima os discriminantes dos dois sistemas são associados em $A$ e portanto geram o mesmo ideal de $A$.

Nas condições da definição acima, chamamos de discriminante de $B$ sobre $A$, e denotamos por $\mathbb{D}_{B/A}$, ao ideal gerado pelo discriminante de qualquer base de $B$ sobre $A$.

**Proposição 1.8** *[Sam, Proposição 3, pag. 47] Sejam* $K$ *um corpo finito ou de característica* 0, $L$ *uma extensão de grau finito* $n$ *de* $K$, *e* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *os* $n$ $K$*-isomorfismos distintos de* $L$ *em um corpo algebricamente fechado* $C$ *contendo* $K$. *Então se* $\{x_1, x_2, \ldots, x_n\}$ *é uma base de* $L$ *sobre* $K$, *temos:*

$$D(x_1, x_2, \ldots, x_n) = \det(\sigma_i(x_j))^2 \neq 0.$$

Sob as condições da proposição anterior, a relação $D(x_1, x_2, \ldots, x_n) \neq 0$ revela que a forma bilinear $(x, y) \longmapsto Tr_{L/K}$ é não degenerada, isto é, se $Tr_{L/K}(xy) = 0$ para todo $y \in L$ então $x = 0$. Assim a aplicação $K$-linear que faz corresponder a cada $x \in L$ a forma $K$-linear $s_x : y \to Tr_{L/K}(xy)$ é uma injeção de $L$ em seu dual $Hom_k(L, K)$ ( para a estrutura de espaço vetorial sobre $K$). Como $L$ e $Hom_k(L, K)$ têm mesma dimensão $n$ sobre $K$, temos que $x \longmapsto s_x$ é uma bijeção. A existência de bases duais sobre espaços vetoriais e seu dual mostra então que, para toda base $\{x_1, x_2, \ldots, x_n\}$ de $L$ sobre $K$, existe uma outra base $\{y_1, y_2, \ldots, y_n\}$ de $L$ sobre $K$ tal que $Tr_{L/K}(x_i y_j) = \delta_{ij}$ $(1 \leq i,\ j \leq n)$. Este fato é fundamental na demonstração do teorema a seguir.

**Teorema 1.2** *[Sam, Teorema 1, pag. 48] Sejam* $A$ *um anel integralmente fechado,* $K$ *seu corpo de frações,* $L$ *uma extensão de grau finito* $n$ *de* $K$ *e* $A'$ *o fecho integral de* $A$

*em $L$. Se $K$ tem característica 0 então $A'$ é um sub $A$-módulo de um $A$-módulo livre de posto $n$.*

**Corolário 1.3** *[Sam, Corolário, pag. 48] Nas condições do teorema acima, se $A$ é principal, então $A'$ é um $A$-módulo livre de posto $n$.*

Assim, se $A = \mathbb{Z}$ então $A'$ é um $A$-módulo livre de posto $n$.

**Proposição 1.9** *[Sam, pag. 49] Sejam $K$ um corpo finito ou de característica 0, $L = K[x]$ uma extensão de grau finito $n$ de $K$ e $F(X)$ o polinômio minimal de $x$ sobre $K$. Então*

$$D(1, x, ..., x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(F'(x)).$$

## 1.5 Teoria de Galois

Sejam $L$ um corpo e $G$ um conjunto de automorfismos de $L$. O conjunto dos $x \in L$ tais que $\sigma(x) = x$ para todo $\sigma \in G$ é um subcorpo de $L$, que é chamado de corpo dos invariantes de $G$. Por outro lado, dada uma extensão $L$ de um corpo $K$ o conjunto dos $K$-automorfismos de $L$ é um grupo com a operação de composição.

**Teorema 1.3** *[Sam, Teorema 1, pag. 101] Seja $L$ uma extensão finita de grau $n$ de um corpo $K$ finito ou de característica 0. As seguintes condições são equivalentes:*

*a) $K$ é o corpo dos invariantes do grupo $G$ dos $K$-automorfismos de $L$.*

*b) Para todo $x \in L$ o polinômio minimal de $x$ sobre $K$ tem todas as raízes em $L$.*

*c) $L$ é gerado pelas raízes de um polinômio sobre $K$. Nestas condições o grupo $G$ dos $K$-automorfismos de $L$ possui $n$ elementos.*

**Definição 1.7** *Se as condições do Teorema acima são satisfeitas, dizemos que $L$ é uma extensão de Galois de $K$ e que $G$ é o grupo de Galois de $L$ sobre $K$. Se $G$ é abeliano (respectivamente cíclico), dizemos que $L$ é uma extensão abeliana (respectivamente cíclica) de $K$.*

**Corolário 1.4** *[Sam, Corolário, pag. 102] Sejam $K$ um corpo finito ou de característica 0, $L$ uma extensão de grau finito $n$ de $K$ e $H$ um grupo de automorfismos de $L$ que admitem $K$ como corpo de invariantes. Então $L$ é uma extensão de Galois de $K$ e seu grupo de Galois é $H$.*

**Teorema 1.4 (Fundamental da Teoria de Galois)** *[Sam, Teorema 2, pag. 102] Sejam $K$ um corpo finito ou de característica 0, $L$ uma extensão de Galois de $K$ e $G$ seu grupo de Galois. Para cada subgrupo $G'$ de $G$ seja $k(G')$ o corpo dos invariantes de $G'$ e para cada subcorpo $K'$ de $L$ que contém $K$ seja $g(K')$ o grupo dos $K'$-automorfismos de $L$. Então:*

*a) As aplicações $g$ e $k$ são bijeções inversas uma da outra e invertem a inclusão e $L$ é uma extensão de Galois de todo corpo intermediário $K'$.*

*b) Para que um corpo intermediário $K'$ seja uma extensão de Galois de $K$ é necessário e suficiente que $g(K')$ seja um subgrupo normal de $G$. Neste caso, o grupo de Galois de $K'$ sobre $K$ é isomorfo a $G/g(K')$.*

## 1.6 Corpos de Números

Um Corpo de Números Algébricos $K$ (ou simplesmente Corpo de Números) é uma extensão finita do corpo dos números racionais.

Um número complexo $\alpha$, algébrico sobre $\mathbb{Q}$, é chamado de número algébrico. Um número complexo $\alpha$ que é inteiro sobre $\mathbb{Z}$ é chamado de inteiro algébrico.

Denotaremos por $A$ o conjunto de todos os números algébricos, o qual é um subcorpo do corpo dos números complexos. Denotaremos por $B$ o conjunto de todos os inteiros algébricos, o qual é um subanel de $A$.

Assim todo elemento de um corpo de números $K$ é um número algébrico e daí $K \subseteq A$. Dado um corpo de números $K$ o seu grau, denotado por $[K : \mathbb{Q}]$, é a dimensão de $K$ visto como $\mathbb{Q}$-espaço vetorial. Os Corpos de Números têm característica nula.

**Proposição 1.10** *[Ste2, Lema 2.12, pag. 49] Um número algébrico $\alpha$ é um inteiro algébrico se, e somente se, seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.*

**Proposição 1.11** *[Ste2, Lema 2.13, pag. 50] Um inteiro algébrico é um número racional se, e somente se, é um inteiro. Equivalentemente $B \cap \mathbb{Q} = \mathbb{Z}$.*

Dado um corpo de números $K$, o conjunto dos elementos de $K$ que são inteiros sobre $\mathbb{Z}$ são chamados de inteiros de $K$. Denotaremos este conjunto por $\mathcal{O}_K$ e podemos ver que $\mathcal{O}_K = K \cap B$.

Do parágrafo anterior concluimos que os inteiros de um corpo de números $K$ formam um subanel de $K$, o qual é um $\mathbb{Z}$-módulo livre de posto $[K : \mathbb{Q}]$. O polinômio minimal de um número algébrico é irredutível em $\mathbb{Q}[X]$. Logo o polinômio minimal de um inteiro algébrico é irredutível sobre $\mathbb{Z}[X]$.

Os discriminantes das bases do $\mathbb{Z}$-módulo $\mathcal{O}_K$ diferem por um elemento inversível de $\mathbb{Z}$ e que é um quadrado, sendo portanto igual a 1. Logo os discriminantes das bases do $\mathbb{Z}$-módulo $\mathcal{O}_K$ são iguais. Este valor comum se chama discriminante absoluto de $K$, ou simplesmente discriminante de $K$. O discriminante é sempre um inteiro não nulo. Corpos de Números isomorfos têm o mesmo discriminante.

Visto que um Corpo de Números $K$ determina de forma única o anel $\mathcal{O}_K$, constantemente, para simplificar a linguagem, atribuimos a $K$ noções relativas a $\mathcal{O}_K$. Assim costumamos chamar de ideais de $K$ os ideais de $\mathcal{O}_K$; de unidades de $K$ as unidades de $\mathcal{O}_K$ e assim por diante.

Uma base do $\mathbb{Z}$-módulo $\mathcal{O}_K$ é chamada de base integral de $K$. Uma base integral de $K$ é também uma base de $K$ sobre $\mathbb{Q}$ como espaço vetorial já que tem $[K : \mathbb{Q}]$ elementos linearmente independentes. A recíproca não é verdadeira, isto é, nem toda base de $K$ sobre $\mathbb{Q}$, como espaço vetorial, contida em $\mathcal{O}_K$, é uma base integral. Vejamos por exemplo o caso do Corpo de Números $\mathbb{Q}(\sqrt{5})$. Temos que $\{1, \sqrt{5}\}$ é uma base de $\mathbb{Q}(\sqrt{5})$ sobre $\mathbb{Q}$ formada por inteiros algébricos, entretanto não é uma base integral de $K$. Uma base integral de $K$, neste caso, é $\{1, \frac{1}{2}(1+\sqrt{5})\}$.

Para o caso dos Corpos Quadráticos o teorema a seguir mostra como encontrar uma base integral.

**Teorema 1.5** *[Sam, Teorema 1, pag. 43] Seja $K = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde $d$ é um inteiro sem fator quadrático (e portanto $d \not\equiv 0 \bmod 4$). Então:*

*a) Se $d \equiv 2$ ou $d \equiv 3 \bmod 4$ então $\{1, \sqrt{d}\}$ é uma base integral de $K$.*

*b) Se $d \equiv 1 \bmod 4$ então $\{1, \frac{1}{2}(1+\sqrt{d})\}$ é uma base integral de $K$.*

**Teorema 1.6** *[Rib, pag. 116, M] Sejam $K$ um Corpo de Números, $\mathcal{O}_K$ o seu anel dos inteiros algébricos e $\{x_1, x_2, \ldots, x_n\}$ uma base integral de $K$. Se $y_1, y_2, \ldots, y_n \in \mathcal{O}_K$, então*

$$\mathrm{Disc}(x_1, x_2, \ldots, x_n) = \mathrm{Disc}(y_1, y_2, \ldots, y_n)$$

*se e somente se, $\{y_1, y_2, \ldots, y_n\}$ é uma base integral de $K$.*

Dada uma base $\{x_1, x_2, \ldots, x_n\}$ de $K$ sobre $\mathbb{Q}$, como cada $x_i$ é algébrico sobre $K$, existem $a_j \in \mathbb{Z}$, $j = 1, 2, \ldots, n$ tais que

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

com $a_n \neq 0$ e, multiplicando esta igualdade por $a_n^{n-1}$ vemos que $x_i{}' = a_n x_i$ é inteiro sobre $\mathbb{Z}$ e $(x_1', x_2', \ldots, x_n')$ é uma base de $K$ contida em $\mathcal{O}_K$. Assim temos o seguinte resultado:

**Proposição 1.12** *[Ste2, Lema 2.10, pag. 49] Se $K$ é um corpo de números e $\alpha \in K$ então existe um elemento não nulo $c \in \mathbb{Z}$ tal que $c\alpha \in \mathcal{O}_K$.*

**Corolário 1.5** *[Ste2, Corolário 2.11, pag. 49] Se $K$ é um Corpo de Números, então $K = \mathbb{Q}(\theta)$ para algum inteiro algébrico $\theta$.*

**Teorema 1.7** *[Ste2, Teorema 2.16, pag. 53] Suponhamos que $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{O}_K$ formam uma $\mathbb{Q}$-base para $K$. Se $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é livre de quadrados então $\alpha_1, \alpha_2, \ldots, \alpha_n$ formam uma base integral de $K$.*

Para calcularmos o discriminante de um Corpo de Números de acordo com a definição, precisamos conhecer o anel dos inteiros algébricos de $K$ e, a partir daí, encontrar uma base deste $\mathbb{Z}$-módulo e aplicar a definição de discriminante.

O problema de encontrar uma base integral para um Corpo de Números em geral não é uma tarefa simples, ao contrário do que vimos nos corpos quadráticos e como veremos a seguir nos corpos ciclotômicos. Isto implica numa grande dificuldade para calcularmos o discriminante do referido Corpo de Números. No nosso trabalho buscamos uma forma alternativa de calcular o discriminante sem conhecer uma base integral do mesmo.

## 1.7 Prolongamento Canônico de um Corpo de Números

Quando fixarmos um Corpo de Números $K$, denotaremos a norma de um elemento $x \in K$ por $N(x)$ ao invés de $N_{L/\mathbb{Q}}(x)$.

**Proposição 1.13** *[Sam, Proposição 1, pag. 62] Se $x$ é um elemento não nulo de $\mathcal{O}_K$, então $|N(x)| = Card(\mathcal{O}_K/x\mathcal{O}_K)$ (observe que esta fórmula faz sentido, já que $N(x) \in \mathbb{Z}$).*

**Definição 1.8** *Dado um ideal ordinário não nulo $\mathfrak{a}$ de $\mathcal{O}_K$ chamamos de norma de $\mathfrak{a}$, e denotamos por $N(\mathfrak{a})$, o número $Card(\mathcal{O}_K/\mathfrak{a})$.*

**Proposição 1.14** *[Sam, Proposição 2, pag. 63] Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais ordinários não nulos de $\mathcal{O}_K$ então $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

Considerando um Corpo de Números $K$ de grau $n$ sabemos que existem $n$ isomorfismos distintos $\sigma_i : K \to \mathbb{C}$. Se $\alpha : \mathbb{C} \to \mathbb{C}$ a conjugação complexa, então para todo $i$, $\alpha \circ \sigma_i$ é um dos $\sigma_j$, e é igual a $\sigma_i$ se, e somente se, $\sigma_i(K) \subset \mathbb{R}$. Denotaremos por $r_1$ o número de índices $i$ tais que $\sigma_i(K) \subset \mathbb{R}$. A quantidade de índices $i$ para os quais $\sigma_i(K) \not\subset \mathbb{R}$ é par e a denotaremos por $2r_2$; temos portanto $r_1 + 2r_2 = n$. Se $r_2 = 0$ dizemos que $K$ é totalmente real e quando $r_1 = 0$ dizemos que $K$ é totalmente imaginário. Como $K$ é uma extensão de Galois de $\mathbb{Q}$ temos ou $r_1 = 0$ ou $r_2 = 0$.

**Teorema 1.8** *[Was, Lema 2.2, pag. 10] Se $K$ é um Corpo de Números, então o sinal do discriminante de $K$ é $(-1)^{r_2}$.*

**Corolário 1.6** *Se $K$ é totalmente real, então seu discriminante é positivo.*

Numeraremos os $\sigma_i$ de modo que $\sigma_i(K) \subset \mathbb{R}$ para $1 \leq i \leq r_1$ e que $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$, para $r_1 + 1 \leq j \leq r_1 + r_2$. Assim os $r_1 + r_2$ primeiros isomorfismos $\sigma_i$ determinam os outros $r_2$ .

A função $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definida por

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

é chamada de prolongamento canônico de $K$ em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ e é um homorfismo injetivo de anéis. Frequentemente identificamos $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$.

**Definição 1.9** *Chamamos de reticulado em $\mathbb{R}^n$ qualquer subgrupo discreto de $\mathbb{R}^n$ de posto $n$.*

Um reticulado em $\mathbb{R}^n$ é, portanto, gerado (como $\mathbb{Z}$-módulo) por uma base de $\mathbb{R}^n$. Para cada base

$$e = \{e_1, e_2, ..., e_n\}$$

de um reticulado $H$ em $\mathbb{R}^n$ denotamos por $P_e$ o paralelepípedo semi-aberto

$$P_e = \left\{ \sum_{i=1}^{n} \alpha_i e_i; 0 \leq \alpha_i < 1 \right\}.$$

Todo ponto de $\mathbb{R}^n$ é congruente, módulo $H$, a um único ponto de $P_e$. Dizemos que $P_e$ é um domínio fundamental para $H$.

**Definição 1.10** *O volume de $P_e$ independe da base e escolhida e é chamado de volume do reticulado $H$, que denotaremos por $v(H)$.*

**Teorema 1.9** *[Sam, Proposição 2, pag. 69] Sejam $K$ um Corpo de Números de grau $n$, $\mathcal{O}_K$ o seu anel de inteiros algébricos e $\mathfrak{a}$ um ideal ordinário de $\mathcal{O}_K$. Então $\sigma(\mathcal{O}_K)$ e $\sigma(\mathfrak{a})$ são reticulados em $\mathbb{R}^n$ e, se $d$ é o discriminante de $K$ temos:*

$$v(\sigma(\mathcal{O}_K)) = 2^{-r_2}\,|d|^{1/2} \text{ e } v(\sigma(\mathfrak{a})) = 2^{-r_2}\,|d|^{1/2}\,N(\mathfrak{a}).$$

## 1.8 Corpos Ciclotômicos

Uma raiz $n$-ésima da unidade é uma raiz do polinômio $X^n - 1$. O conjunto das raízes $n$-ésimas da unidade forma um grupo cíclico multiplicativo de ordem $n$. Um gerador deste grupo é chamado de raiz primitiva $n$-ésima da unidade e será denotado por $\zeta_n$. O número complexo $\zeta_n^m$ é uma raiz primitiva da unidade se, e somente se, $(m, n) = 1$. O número de raízes primitivas da unidade é, portanto, $\phi(n)$ e o polinômio minimal de $\zeta_n$ é

$$\prod_{(j,n)=1} (X - \zeta_n^j) \in \mathbb{Z}[X],$$

o qual denotaremos por $\phi_n(X)$ e será chamado de $n$-ésimo polinômio ciclotômico. Temos ainda que

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

Os quatro primeiros polinômios ciclotômicos são

$$\begin{aligned}
\phi_1(X) &= X - 1, \\
\phi_2(X) &= X + 1, \\
\phi_3(X) &= X^2 + X + 1, \\
\phi_4(X) &= X^2 + 1.
\end{aligned}$$

Se $p$ é um número primo temos $p-1$ raízes primitivas $p$-ésimas da unidade e portanto a única raiz $p$-ésima da unidade que não é primitiva é 1. Desta forma

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

Um corpo $K$ é chamado de Ciclotômico se $K = \mathbb{Q}(\zeta_n)$.

**Teorema 1.10** *[Was, Teorema 2.5, pag. 11] O corpo $\mathbb{Q}(\zeta_n)$ é uma extensão de Galois de $\mathbb{Q}$ de grau $\phi(n)$ e*

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Como $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é de Galois, $\mathbb{Q}(\zeta_n)/L$ é de Galois para todo corpo $L$ tal que $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_n)$. Como $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ e $(\mathbb{Z}/n\mathbb{Z})^*$ é abeliano, $\mathbb{Q}(\zeta_n)$ é uma extensão abeliana de $\mathbb{Q}$. Por outro lado $(\mathbb{Z}/n\mathbb{Z})^*$ é cíclico se, e somente se, $n$ vale $1, 2, 4, p^r$ ou $2.p^r$, onde $p$ é um número primo ímpar e $r$ é um número inteiro positivo. Temos também que todo subgrupo de $(\mathbb{Z}/n\mathbb{Z})^*$ é normal em $(\mathbb{Z}/n\mathbb{Z})^*$ e daí $L/\mathbb{Q}$ é de Galois para todo corpo $L \subset \mathbb{Q}(\zeta_n)$.

**Teorema 1.11** *[Was, Teorema 2.16, pag. 16] O anel dos inteiros de $\mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$ e*

$$\{1, \zeta_n, \ldots, \zeta_n^{\phi(n)-1}\}$$

*é uma base integral de $\mathbb{Q}(\zeta_n)$.*

**Teorema 1.12** *[Was, Teorema 2.16, pag. 16] Sejam $\alpha = \zeta_n + \zeta_n^{-1}$ e $K = \mathbb{Q}(\alpha)$. Então o anel dos inteiros algébricos de $K$ é $\mathbb{Z}[\alpha]$ e $\{1, \alpha, \ldots, \alpha^{\frac{\phi(n)}{2}-1}\}$ é uma base integral de $K$.*

Um resultado fundamental envolvendo Corpos Ciclotômicos é o seguinte:

**Teorema 1.13 (Kronecker - Weber)** *[Was, Apêndice, Teorema 6, pag. 401] Seja $K$ uma extensão abeliana dos racionais (isto é, de Galois com grupo de Galois abeliano). Então $K$ está contido em algum Corpo Ciclotômico.*

# Capítulo 2

# Caracteres e a Fórmula do Condutor-Discriminante

Neste capítulo serão apresentados os principais conceitos relacionados com a Teoria dos Caracteres de Grupos Abelianos e alguns resultados da Teoria Analítica dos Números com o propósito de esboçar uma demonstração da Fórmula do Condutor Discriminante. O propósito deste capítulo é mostrar um texto alternativo contemplando de forma concatenada os dois importantes tópicos da Teoria dos Números Algébricos e de vital importância para este trabalho.

## 2.1 Caracteres em grupos abelianos finitos

**Definição 2.1** *Um carater de um grupo finito $G$ é um homomorfismo $\chi : G \to \mathbb{C}^*$.*

Assim $\chi(ab) = \chi(a)\chi(b)$ para $a, b \in G$ e $\chi(e) = 1$, onde $e$ representa o elemento neutro do grupo $G$. Quando $G$ é um grupo de ordem $n$, tem-se que $\chi(a)$ é uma raiz $n$-ésima da unidade para todo $a \in G$, pois $(\chi(a))^n = \chi(a^n) = \chi(e) = 1$. Daí $\chi(G)$ é um subgrupo do grupo cíclico multiplicativo das raízes $n$-ésimas da unidade contidas em $\mathbb{C}^*$. É fácil ver que se $H$ é um subgrupo de $G$ e $\chi$ é um caracter de $G$ então a restrição de $\chi$ a $H$ é um caracter de $H$.

Quando $m$ é o máximo das ordens dos elementos de $G$ (isto é, $m$ é o expoente de $G$), então a ordem de qualquer elemento de $G$ divide $m$ e portanto $\chi(a)$ é uma raiz $m$-ésima da unidade para todo $a \in G$. Podemos pois definir um caracter do grupo $G$ como um homomorfismo de $G$ no grupo das raízes $m$-ésimas da unidade contidas em $\mathbb{C}^*$, onde $m$ é o expoente de $G$.

Denotaremos por $\widehat{G}$ o conjunto de todos os caracteres de $G$. Se $\chi$ e $\chi'$ pertencem a $\widehat{G}$, definimos $\chi\chi' : G \to \mathbb{C}^*$ por $\chi\chi'(x) = \chi(x)\chi'(x)$, $\forall x \in G$. É fácil ver que $\chi\chi'$ é um caracter de $G$ e temos assim definido uma operação em $\widehat{G}$. Esta operação satisfaz às propriedades de um grupo abeliano, onde $\chi_0 : G \to \mathbb{C}^*$, dado por $\chi_0(x) = 1$ $\forall x \in G$, é o elemento neutro e $\overline{\chi} : G \to \mathbb{C}^*$, dado por $\overline{\chi}(x) = \overline{\chi(x)}$ $\forall x \in G$, é o caracter inverso de $\chi$.

**Teorema 2.1** *O número de caracteres de um grupo abeliano finito $G$ é igual à ordem de $G$, isto é, $|G| = \left|\widehat{G}\right|$.*

**Prova.** De fato, $G$ pode ser representado como produto de grupos cíclicos, isto é, $G = \langle a_1 \rangle \times \ldots \times \langle a_1 \rangle$. Daí todo elemento $x \in G$ pode ser representado de modo único (a menos da ordem) na forma $x = a_1^{k_1} \cdots a_s^{k_s}$ e portanto, se $\chi$ é um caracter de $G$, temos $\chi(x) = \chi(a_1)^{k_1} \cdots \chi(a_s)^{k_s}$ e assim $\chi$ é completamente determinado pelos valores de $\chi(a_1), \ldots, \chi(a_s)$. Se $a_i$ tem ordem $m_i$ então $G$ tem ordem $m_1 \cdots m_s$ e $\chi(a_i)$ é uma $m_i$-ésima raiz da unidade e portanto temos $m_i$ possibilidades para $\chi(a_i)$ e um total de $m_1 \cdots m_s$ caracteres em $G$. Logo $|G| = \left|\widehat{G}\right|$. ■

Vamos agora comparar caracteres de dois grupos abelianos finitos distintos. Dados dois grupos abelianos finitos $H$ e $G$, se $\varphi : H \to G$ é um homomorfismo então $\varphi$ induz um homomorfismo $\widehat{\varphi} : \widehat{G} \to \widehat{H}$ dado por $\widehat{\varphi}(\chi) = \chi \circ \varphi (H \xrightarrow{\varphi} G \xrightarrow{\chi} \mathbb{C}^*)$. É imediato observar que $\widehat{\varphi}$ é um homomorfismo. O núcleo de $\widehat{\varphi}$ consiste de todos os caracteres $\chi \in \widehat{G}$ tais que $\widehat{\varphi}(\chi) = \chi_0$ isto é $(\chi \circ \varphi)(a') = \chi(\varphi(a')) = 1$ $\forall a' \in H$ ou seja, de todos os caracteres $\chi \in \widehat{G}$ tais que $\chi(a) = 1$ para todo $a$ pertencente à imagem de $\varphi$. Como a imagem de $\varphi$ é um subgrupo de $G$, sua restrição à imagem de $\varphi$ é um caracter da imagem de $\varphi$ e

assim o núcleo de $\widehat{\varphi}$ consiste de todos os caracteres de $G$ cuja restrição à imagem de $\varphi$ é o caracter trivial .

Particularmente se $H$ é um subgrupo de $G$ e se $\varphi$ é a inclusão, então $\widehat{\varphi}(\chi)$ é a restrição de $\chi$ a $H$. Neste caso o núcleo de $\widehat{\varphi}$, que será denotado por $H^{\perp}$, consiste de todos os caracteres de $G$ cuja retrição a $H$ é o caracter trivial. Uma outra forma de ver $H^{\perp}$, para o caso em que $H$ é um subgrupo de $G$ , é a seguinte:

Se $\psi : G \to G/H$ é o homomorfismo canônico então $\widehat{\psi} : \widehat{G/H} \to \widehat{G}$ (levantamento) é tal que $\widehat{\psi}(\widetilde{\chi}) = \chi = \widetilde{\chi} \circ \psi$ e $\chi(a) = \widetilde{\chi}(\psi(a)) = \widetilde{\chi}(aH)$, $\forall a \in G$ e então $\chi(a) = 1$, $\forall a \in H$, o que significa que $\chi \in H^{\perp}$. Logo $\widehat{\psi}(\widehat{G/H}) \subset H^{\perp}$. Por outro lado, dado $\chi \in H^{\perp}$, temos $\chi(a') = \chi(a)$ sempre que $aH = a'H$ e, portanto, $\widetilde{\chi} : G/H \to \mathbb{C}^*$ definida por $\widetilde{\chi}(aH) = \chi(a)$, é um caracter de $G/H$ tal que $\widehat{\psi}(\widetilde{\chi}) = \widetilde{\chi} \circ \psi = \chi$, pois $\widetilde{\chi} \circ \psi(a) = \widetilde{\chi}(\psi(a) = \widetilde{\chi}(aH) = \chi(a), \forall a \in G$. Assim $H^{\perp} \subset \widehat{\psi}(\widehat{G/H})$ e portanto $\widehat{\psi}(\widehat{G/H}) = H^{\perp}$. Temos ainda que $\widehat{\psi}$ é injetiva pois se $\widehat{\psi}(\widetilde{\chi}) = \widetilde{\chi} \circ \psi = \chi_0$ temos $\widetilde{\chi}(aH) = \widetilde{\chi}(\psi(a)) = \widetilde{\chi} \circ \psi(a) = \chi_0(a) = 1$ para toda classe $aH$ e daí $\widetilde{\chi}$ é o caracter trivial de $G/H$. Portanto $H^{\perp} \cong \widehat{G/H}$ e daí $\left|H^{\perp}\right| = \left|\widehat{G/H}\right| = |G/H| = |G| \,/\, |H|$ o que acarreta $\left|\widehat{G}/H^{\perp}\right| = |H| = \left|\widehat{H}\right|$. Como $\widehat{G}/H^{\perp} \cong \widehat{\varphi}(\widehat{G})$ tem-se $\widehat{\varphi}(\widehat{G}) = \widehat{H}$ implicando que $\widehat{\varphi}$ é sobrejetiva e assim $\widehat{G}/H^{\perp} \cong \widehat{H}$.

Podemos então dizer que todo caracter de $H$ é a restrição de $|G| \,/\, |H|$ caracteres de $G$ ou ainda que cada caracter de $H$ pode ser estendido a $|G| \,/\, |H|$ caracteres de $G$. Este resultado é muitas vezes usado para determinarmos os caracteres de um grupo a partir da extensão dos caracteres de um subgrupo.

Um resultados muito importante sobre caracteres é a propriedade que afirma que existem caracteres que separam elementos de um grupo, mais precisamente: Se $a, a' \in G, a \neq a'$, então existe um caracter $\chi \in \widehat{G}$ tal que $\chi(a) \neq \chi(a')$ ([Rib, pag. 467, E]).

Voltando ao caso geral em que $\varphi : H \to G$ é um homomorfismo vimos que o núcleo de $\widehat{\varphi}$ consiste de todos os caracteres de $G$ cuja retrição á imagem de $\varphi$ é o caracter trivial e portanto $\ker(\widehat{\varphi}) \cong \widehat{G/\operatorname{Im}\varphi}$. Observe que se $\varphi$ for sobrejetiva então $\widehat{\varphi}$ é injetiva (pois $\ker(\widehat{\varphi}) \cong \widehat{G/\operatorname{Im}\varphi} \cong \widehat{G/G}$) e portanto $\widehat{G}$ é isomorfo a um subgrupo de $\widehat{H}$. Temos também

que se $\varphi$ for injetiva então $\widehat{\varphi}$ é sobrejetiva (pois $\varphi$ sendo injetiva $H$ pode ser identificado a um subgrupo de $G$ e temos o caso anterior) e portanto $\widehat{G}/\ker(\widehat{\varphi}) \cong \widehat{H}$. Portanto se $\varphi$ é um isomorfismo então $\widehat{\varphi}$ também é isomorfismo e daí $\widehat{G} \cong \widehat{H}$. Resumindo estes resultados temos que se $1 \longrightarrow H \xrightarrow{\varphi} G \xrightarrow{\psi} G/H \longrightarrow 1$ é uma seqüência exata de grupos abelianos finitos então a sequência $1 \longrightarrow \widehat{G/H} \xrightarrow{\widehat{\psi}} \widehat{G} \xrightarrow{\widehat{\varphi}} \widehat{H} \longrightarrow 1$ também é exata.

Vamos agora descrever explicitamente como obter os caracteres de um grupo abeliano finito. Inicialmente consideremos o caso particular em que $G$ é cíclico, neste caso temos:

**Teorema 2.2** *Se $G$ é um grupo cíclico de ordem $n$, então $G \cong \widehat{G}$.*

**Prova.** Seja $a$ um gerador de $G$ e $\xi$ uma raiz n-ésima primitiva da unidade. Seja $\chi : G \longrightarrow \mathbb{C}^*$ dado por $\chi(a^k) = \xi^k$. Evidentemente $\chi, \chi^2, \chi^3, \ldots, \chi^{n-1}, \chi^n = \chi_0$ são caracteres de $G$. Desde que $\chi^r(a^k) = \xi^{rk}$ os caracteres $\chi, \chi^2, \chi^3, \ldots, \chi^{n-1}, \chi^n = \chi_0$ são dois a dois distintos e como $\left|\widehat{G}\right| = |G| = n$ temos que $\widehat{G} = \{\chi, \chi^2, \chi^3, \ldots, \chi^{n-1}, \chi^m\}$ e, portanto, $\widehat{G}$ é ciclico de ordem $n$ e gerado por $\chi$. Logo $G \cong \widehat{G}$. ■

Note também que a aplicação $\theta : G \longrightarrow \widehat{G}$ dada por $\theta(a^s) = \chi^s$ é um isomorfismo de $G$ em $\widehat{G}$.

**Teorema 2.3** *Se*

$$\theta : G \longrightarrow \prod_{i=1}^{r} G_i$$

*é um isomorfismo de grupos então $\theta$ induz um isomorfismo de grupos*

$$\widehat{\theta} : \widehat{G} \longrightarrow \prod_{i=1}^{r} \widehat{G}_i.$$

**Prova.** (cf. [Rib, pag. 464]). ■

**Teorema 2.4** *Se $G$ é um grupo abeliano finito, então $G \cong \widehat{G}$.*

**Prova.** Como todo grupo abeliano finito é isomorfo ao produto cartesiano de um número finito de grupos cíclicos temos $G \cong \prod_{i=1}^{r} G_i$ onde cada $G_i$ é cíclico e, pelos Teoremas 2.2 e

2.3 temos $\widehat{G} \cong \prod_{i=1}^{r} \widehat{G}_i \cong \prod_{i=1}^{r} G_i \cong G$. ■

**Corolário 2.1** *Seja $G$ um Grupo Abeliano, então $\widehat{\widehat{G}} \cong G$.*

### 2.1.1 Caracteres de Dirichlet

Vamos agora estudar mais detalhadamente os caracteres do grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$ das unidades do anel $\mathbb{Z}/m\mathbb{Z}$, que são chamados de caracteres de Dirichlet. Se $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ é um caracter de Dirichlet e $m \mid n$ então $\chi$ induz um homomorfismo de $(\mathbb{Z}/n\mathbb{Z})^*$ em $\mathbb{C}^*$ pela composição com a aplicação natural de $(\mathbb{Z}/n\mathbb{Z})^*$em $(\mathbb{Z}/m\mathbb{Z})^*$ e assim nós podemos pensar $\chi$ como definido $\bmod m$ ou $\bmod n$ desde que ambas são essencialmente a mesma aplicação. É conveniente escolher $m$ minimal. Neste caso $m$ é chamado de condutor de $\chi$ e é denotado por $f_\chi$. Um caracter definido módulo seu condutor é chamado de caracter primitivo. Muitas vezes vemos $\chi$ como uma aplicação $\mathbb{Z}$ em $\mathbb{C}^*$ fazendo $\chi(a) = 0$ se $(a, f_\chi) \neq 1$. Sempre consideraremos $\chi$ definido módulo seu condutor e é importante que façamos esta escolha já que, neste caso, teremos $\chi(a) = 0$ para um número menor de inteiros e $\chi$ é periódica de período $f_\chi$. No que segue, quando falarmos em caracteres de $(\mathbb{Z}/n\mathbb{Z})^*$ ou de caracteres $\bmod n$ estamos falando dos caracteres cujos condutores dividem $n$, por exemplo do caracter trivial de condutor 1. A convenção de que todos os caracteres são primitivos requer uma observação com relação à multiplicação de caracteres. Se $\chi$ e $\psi$ são caracteres de condutores $f_\chi$ e $f_\psi$, definimos o produto como segue: consideramos o homomorfismo $\gamma : (\mathbb{Z}/[f_\chi, f_\psi]\mathbb{Z})^* \to \mathbb{C}^*$ definido por $\gamma(a) = \chi(a).\psi(a)$ e então $\chi.\psi$ é o caracter primitivo associado a $\gamma$.

**Lema 2.1** *Sejam $n$ e $m$ interos positivos e $\chi$ um Caracter de Dirichlet definido módulo $n$. O condutor de $\chi$ é $m$ se, e somente se, $m$ é o menor inteiro dividindo $n$ que satisfaz a seguinte condição: para todo $a$ tal que $(a, n) = 1$ e $a \equiv 1 (\bmod m)$ tem-se $\chi(\overline{a}) = 1$.*

**Prova.** Seja $m$ um divisor de $n$. Suponha que para todo $a$ tal que $(a, n) = 1$ e $a \equiv 1 (\bmod m)$ tem-se $\chi(\overline{a}) = 1$. Sejam $a, b$ tais que $(a, s) = (b, s) = 1$ e $a \equiv b (\bmod m)$.

Como $a \equiv b (\mathrm{mod}\, m) \Leftrightarrow \overline{a} = \overline{b} \Longleftrightarrow \overline{a}\overline{b}^{-1} = \overline{1}$ temos $\chi(\overline{a}\overline{b}^{-1}) = 1$ e daí $\chi(\overline{a}) = \chi(\overline{b})$. Desta forma $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ dada por $\chi'(\overline{a}) = \chi(\overline{a})$ está bem definida e $\chi'(\overline{a}\overline{b}) = \chi'(\overline{ab}) = \chi(\overline{ab}) = \chi(\overline{a}\overline{b}) = \chi(\overline{a})\chi(\overline{b}) = \chi'(\overline{a})\chi'(\overline{b})$, sendo, portanto, um homomorfismo. Portanto, $\chi$ pode ser visto como um caracter módulo $m$. Por outro lado se $\chi$ pode ser visto como um caracter módulo $m$ temos: para todo $a$ tal que $(a, n) = 1$ e $a \equiv 1 (\mathrm{mod}\, m)$ tem-se $\chi(\overline{a}) = 1$. Assim o condutor de $\chi$ é $m$ se, e somente se, $m$ é o menor inteiro dividindo $n$ que satisfaz a seguinte condição: Para todo $a$ tal que $(a, n) = 1$ e $a \equiv 1 (\mathrm{mod}\, m)$ tem-se $\chi(\overline{a}) = 1$. ■

**Exemplo 2.1** *Considere* $\chi$ *definido* mod 12 *por* $\chi(1) = 1; \chi(5) = -1; \chi(7) = -1; \chi(11) = 1$ *e* $\psi$ *definido* mod 3 *por* $\psi(1) = 1; \psi(2) = -1$. *Então* $\chi\psi$ *em* $(\mathbb{Z}/12\mathbb{Z})^*$ *tem valores* $\chi\psi(1) = \chi(1)\psi(1) = 1; \chi\psi(5) = \chi(5)\psi(5) = 1$; $\chi\psi(7) = \chi(7)\psi(7) = -1$; $\chi\psi(11) = \chi(11)\psi(11) = -1$. *É fácil ver que* $\chi\psi$ *tem condutor* 4 *e* $\chi\psi(1) = 1$, $\chi\psi(3) = -1$. *Note que* $\chi\psi(3) = -1 \neq \chi(3)\psi(3)$.

Um fato também importante é que se $(f_\chi, f_\psi) = 1$ então $f_{\chi\psi} = f_\chi f_\psi$.

Seja $m = m_1 \cdots m_r$ uma decomposição de $m$ em um produto de inteiros dois a dois relativamente primos (por exemplo, se $m = \prod_{i=1}^{r} p_i^{e_i}$ é a decomposição de $m$ em produto de potências de primos) e seja

$$\theta : (\mathbb{Z}/m\mathbb{Z})^* \to \prod_{i=1}^{r} (\mathbb{Z}/m_i\mathbb{Z})^*$$

o isomorfismo de grupos dado por $\theta(x (\mathrm{mod}\, m)) = (x (\mathrm{mod}\, m_1), \ldots, x (\mathrm{mod}\, m_r))$. Dado

$$\begin{aligned} \chi \;&\in\; \textstyle\prod_{i=1}^{r} \widehat{(\mathbb{Z}/m_i\mathbb{Z})^*},\ \chi(x_1, \ldots, x_r) = \chi((x_1, \ldots, 1) \cdots (1, \ldots, x_r)) \\ &=\; \chi(x_1, \ldots, 1) \cdots \chi(1, \ldots, x_r). \end{aligned}$$

Seja $\chi_i \in \widehat{(\mathbb{Z}/m_i\mathbb{Z})^*}$ dado por $\chi_i(x_i) = \chi(1, \ldots, x_i, \ldots, 1)$. Assim, $\chi(x_1, \ldots, x_r) = \chi_1(x_1) \cdots \chi_r(x_r)$.

Temos então $\widehat{\theta} : \prod_{i=1}^{r} \widehat{(\mathbb{Z}/m_i\mathbb{Z})^*} \to \widehat{(\mathbb{Z}/m\mathbb{Z})^*}$ onde $\widehat{\theta} = (\chi_1, \ldots, \chi_r)$, onde $\chi_i \in \widehat{(\mathbb{Z}/m_i\mathbb{Z})^*}$.

$\widehat{\theta}(\chi) = \chi \circ \theta$, onde

$$(\chi \circ \theta)(x) = \chi(\theta(x)) = \chi(\overline{x}_1, \ldots, \overline{x}_r) = \chi_1(\overline{x}_1) \cdots \chi_r(\overline{x}_r)$$

Assim podemos fazer a identificação $\widehat{\theta} = (\chi_1, \ldots, \chi_r)$ onde $\chi_i \in \widehat{(\mathbb{Z}/m_i\mathbb{Z})^*}$. $\widehat{\theta}$ é isomorfismo e, portanto, todo caracter de $\psi \in (\mathbb{Z}/m\mathbb{Z})^*$ pode ser escrito na forma $\psi = \chi_1 \cdots \chi_r = \prod_{i=1}^{r} \chi_i$, onde $\chi_i$ é um caracter módulo $m_i$. Desta forma, para descrevermos os caracteres de $(\mathbb{Z}/m\mathbb{Z})^*$ basta conhecermos os caracteres de $(\mathbb{Z}/p^e\mathbb{Z})^*$ onde $p$ é um número primo. Se $p \neq 2$, $(\mathbb{Z}/p^e\mathbb{Z})^*$ é cíclico e $(\mathbb{Z}/p^e\mathbb{Z})^* = B \times C$, onde $B$ é um grupo multiplicativo cíclico de ordem $p-1$ com gerador $b \bmod p^e$ e $C$ é um grupo multiplicativo cíclico de ordem $p^{e-1}$ com gerador $(p+1) \bmod p^e$ e assim, para todo inteiro $a$, temos $a \equiv b^m(p+1)^n (\bmod p^e)$ com $0 \leq m < p-1$ e $0 \leq n < p^{e-1}$. Os caracteres de $(\mathbb{Z}/p^e\mathbb{Z})^*$ são do tipo $\chi_{il}$ onde $\chi_{il}(a) = \zeta_{p-1}^{mi} \cdot \zeta_{p^{e-1}}^{nl}$.

Da mesma forma, se $p = 2$ e $e \geq 2$, $(\mathbb{Z}/2^e\mathbb{Z})^* \cong \{1, -1\} \times C$, onde $C$ é um grupo multiplicativo cíclico de ordem $2^{e-2}$ gerado por $5 \bmod 2^e$ e assim, para todo inteiro $a$, temos $a \equiv (-1)^m 5^n \pmod{2^e}$ com $0 \leq m < 2$ e $0 \leq n < 2^{e-2}$. Os caracteres de $(\mathbb{Z}/2^e\mathbb{Z})^*$ são do tipo $\chi_{il}$, onde $\chi_{il}(a) = (-1)^{mi} \cdot \zeta_{2^{e-2}}^{nl}$.

Muitas vezes é interessante considerar os caracteres de Dirichlet como sendo caracteres no grupo de Galois de corpos ciclotômicos. Se identificamos $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ com $(\mathbb{Z}/n\mathbb{Z})^*$, um caracter de Dirichlet $\bmod n$ é dito ser um caracter de Galois. Um caracter $\chi \bmod n$ é portanto um caracter de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e se $K$ é o corpo fixo do núcleo de $\chi$ temos $K \subset \mathbb{Q}(\zeta_n)$ e, se $n$ é minimal, $n = f_\chi$. Em geral se $X$ é um grupo de caracteres de Dirichlet e $n$ é o mínimo múltiplo comum dos condutores dos caracteres de $X$ então $X$ é um subgrupo dos caracteres de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Se $H$ é a interseção dos núcleos destes caracteres e $K$ é o corpo fixo de $H$ então $X$ é precisamente o conjunto dos homomorfismos $Gal(K/\mathbb{Q}) \to \mathbb{C}^*$. Na realidade temos $X \cong Gal(K/\mathbb{Q})$.

Sejam $K$ um subcorpo de $\mathbb{Q}(\zeta_n)$, $H$ o subgrupo de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa $K$ e

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

O conjunto $X_K$ é chamado de grupo dos caracteres de Dirichlet associados a $K$, $[K : \mathbb{Q}] = |X_K|$ e a correspondência $K \longleftrightarrow X_K$ é bijetiva, preservando inclusões, entre os subgrupos de $X_K$ e os subcorpos de $K$.

### 2.1.2 A Fórmula do Condutor-Discriminante

O cálculo do discriminante de um Corpo de Números ganhou uma alternativa com a Fórmula do Condutor-Discriminante (Teorema de Hasse). Na essência para se determinar o discriminante de um Corpo de Números Abeliano $K$, deve-se primeiro encontrar o grupo dos caracteres numéricos associados a $K$ e em seguida calcular o condutor de cada um desses caracteres e a Fórmula do Condutor-Discriminante assegura que o discriminante de $K$ é, a menos de sinal, o produto desses condutores.

Seja $\chi$ um Caracter de Dirichlet de condutor $f$. A $L$-série associada a $\chi$ é definida por

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \mathrm{Re}(s) > 1$$

Para $\chi = 1$, temos a usual função zeta de Riemann. É conhecido que $L(s, \chi)$ pode ser estendida analiticamente a todo plano complexo, exceto para o polo simples em $s = 1$, quando $\chi = 1$.

Seja $\Gamma(s)$ a função Gamma, $\tau(\chi) = \sum_{a=1}^{f} \chi(a) e^{2\pi i a/f}$ uma soma de Gauss, e $\delta = 0$ se $\chi(-1) = 1, \delta = 1$ se $\chi(-1) = -1$. Então

$$\left(\frac{f}{\pi}\right)^{\frac{s}{2}} \Gamma\left(\frac{s+\delta}{2}\right) L(s, \chi) = W_\chi \left(\frac{f}{\pi}\right)^{\frac{1-s}{2}} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s, \overline{\chi}), \text{ onde } W_\chi = \frac{\tau(\chi)}{\sqrt{f} i^\delta}$$

Segue (cf. [Was, pag. 37, Lema 4.8]) que $|W_\chi| = 1$.

**Teorema 2.5 (Fórmula do Condutor-Discriminante)** *Seja $K$ um corpo de números associado ao grupo $X$ de caracteres de Dirichlet. Então o discriminante de $K$ é dado por*

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

**Prova.** É suficiente mostrar que $|\mathrm{Disc}(K)| = \prod_{\chi \in X} f_\chi$, pois o sinal do discriminante é, como sabemos, $(-1)^{r_2}$(cf. [Was, Lema 2.2, pag. 10]). É conhecido que $\zeta_K(s)$ satisfaz a equação funcional

$$A^s \Gamma(\frac{s}{2}) \Gamma(s)^{r_2} \zeta_K(s) = A^{1-s} \Gamma(\frac{1-s}{2})^{r_1} \Gamma(1-s)^{r_2} \zeta_K(1-s),$$

onde $A = 2^{-r_2} \pi^{-\frac{N}{2}} \sqrt{|\mathrm{Disc}(K)|}$ e $N = [K : \mathbb{Q}]$,(cf. [Lan, pag. 254])

Desde que $K/\mathbb{Q}$ é de Galois temos ou $r_1 = 0$ ou $r_2 = 0$.

i) Se $r_2 = 0$. Neste caso $N = r_1$, $K$ é totalmente real e $\chi(-1) = 1$ para todo $\chi$ e a equação funcional acima toma a forma

$$A^s \Gamma(\frac{s}{2})^{r_1} \zeta_K(s) = A^{1-s} \Gamma(\frac{1-s}{2})^{r_1} \zeta_K(1-s) \quad \text{(I)}$$

A equação funcional para $L$-séries é

$$\left(\frac{f_\chi}{\pi}\right)^{\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) L(s,\chi) = W_\chi \left(\frac{f_\chi}{\pi}\right)^{\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right) L(1-s,\overline{\chi})$$

Tomando o produto sobre todos os $\chi \in X$ temos:

$$\left(\frac{\prod_{\chi \in X} f_\chi}{\pi^{r_1}}\right)^{\frac{s}{2}} \Gamma\left(\frac{s}{2}\right)^{r_1} \prod_{\chi \in X} L(s,\chi) = \prod_\chi W_\chi \left(\frac{\prod_{\chi \in X} f_\chi}{\pi^{r_1}}\right)^{\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right)^{r_1} \prod_{\chi \in X} L(1-s,\overline{\chi})$$

Como $\zeta_K(s) = \prod_\chi L(s,\chi)$ (cf. [Was, Teorema 4.3, pag. 34]),temos:

$$\left(\frac{\prod_{\chi\in X} f_\chi}{\pi^{r_1}}\right)^{\frac{s}{2}} \Gamma\left(\frac{s}{2}\right)^{r_1} \zeta_K(s) = \prod_{\chi\in X} W_\chi \left(\frac{\prod_{\chi\in X} f_\chi}{\pi^{r_1}}\right)^{\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right)^{r_1} \zeta_K(s) \ (II)$$

Comparando (I) e (II),chegamos a $\prod_{\chi\in X} W_\chi = 1$ e

$$A = \left(\frac{\prod_{\chi\in X} f_\chi}{\pi^{r_1}}\right)^{\frac{1}{2}}$$

e daí

$$2^{-r_2}\pi^{-\frac{N}{2}}\sqrt{|\mathrm{Disc}(K)|} = \left(\frac{\prod_{\chi\in X} f_\chi}{\pi^{r_1}}\right)^{\frac{1}{2}}.$$

Conseqüentemente $|\mathrm{Disc}(K)| = \prod_{\chi\in X} f_\chi$.

ii) Se $r_1 = 0$ então $r_2 = \frac{N}{2}$. Neste caso metade dos caracteres são pares e a outra metade é ímpar. Usando a identidade $\Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2}) = 2^{1-s}\sqrt{\pi}\Gamma(s)$ chegamos também ao resultado $|\mathrm{Disc}(K)| = \prod_{\chi\in X} f_\chi$. ■

Usando este teorema, podemos calcular de forma bastante simples o discriminante de alguns Corpos de Números Abelianos. Por exemplo: considere $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ o subcorpo real maximal de $\mathbb{Q}(\zeta_p)$.O grupo dos caracteres associados consiste do caracter trivial e de $\frac{p-3}{2}$ outros caracteres, todos de condutor $p$. Como $r_2 = 0$, temos $\mathrm{Disc}(K) = p^{\frac{p-3}{2}}$.

O objetivo desta Tese é exatamente obter uma fórmula para calcular o discriminante dos Corpos Abelianos. Em geral a situação não é simples, mas a Fórmula do Condutor-Discriminante será fundamental para atingir tal objetivo.

# Capítulo 3

# Discriminantes dos Corpos de Números Abelianos

De acordo com o Teorema de Kronecker-Weber todo Corpo de Números Abeliano $K$, de grau finito, está contido em alguma extensão ciclotômica $\mathbb{Q}(\zeta_m)$ e, neste caso, podemos usar a Fórmula do Condutor-Discriminante para calcular o discriminante de $K$. Usamos dois caminhos na busca do nosso objetivo: no primeiro trabalhamos diretamente com os subgrupos do grupo de Galois de $K$ sobre $\mathbb{Q}$ e, a partir daí, explicitamos o grupo de caracteres associados a $K$, como também os condutores de seus elementos. No segundo damos atenção direta para o grupo dos caracteres associados ao corpo $K$, sem explicitá-lo mas calculando os possíveis valores dos condutores dos seus caracteres e a quantidade de caracteres para cada valor possível do condutor. Com o primeiro enfoque conseguimos obter resposta para os casos dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$ com $p$ primo e $r$ inteiro positivo. Com o segundo conseguimos uma fórmula geral para os subcorpos de $\mathbb{Q}(\zeta_m)$. A fórmula obtida para o discriminante dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$, $p$ primo ímpar, depende apenas do seu grau. Para o caso dos subcorpos de $\mathbb{Q}(\zeta_{2^r})$ a fórmula obtida depende do grau do subcorpo $K$ e do fato de $K$ ser ou não ciclotômico. Já no caso geral a fórmula obtida depende dos graus das interseções do subcorpo $K$ com alguns subcorpos particulares de $\mathbb{Q}(\zeta_m)$.

## 3.1 Os subcorpos de $\mathbb{Q}(\zeta_{p^r})$, $p$ primo ímpar

Dados um número primo ímpar $p$ e um inteiro positivo $r$, $\mathbb{Q}(\zeta_{p^r})$ é uma extensão Galoisiana de $\mathbb{Q}$ e seu grupo de Galois é isomorfo a $(\mathbb{Z}/p^r\mathbb{Z})^*$ o qual é um grupo cíclico multiplicativo de ordem $\phi(p^r) = (p-1)p^{r-1}$. O Teorema Fundamental da Teoria de Galois garante que existe uma correspondência um a um entre os subcorpos de $\mathbb{Q}(\zeta_{p^r})$ e os subgrupos de $(\mathbb{Z}/p^r\mathbb{Z})^*$. Tal correspondência associa a cada subcorpo $K$ de $\mathbb{Q}(\zeta_{p^r})$ o subgrupo $H$ de $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ formado pelos automorfismos de $\mathbb{Q}(\zeta_{p^r})$ que fixam $K$. O isomorfismo entre $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ e $(\mathbb{Z}/p^r\mathbb{Z})^*$ é determinado pela correspondência $\sigma_i \mapsto \bar{i}$ onde $\sigma_i(\zeta_{p^r}) = \zeta_{p^r}^i$ onde $0 < i < p^r$ e $(i,p) = 1$. Assim $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ é cíclico de ordem $\phi(p^r) = (p-1)p^{r-1}$, dado um divisor $s$ de $(p-1)p^{r-1}$ existe um único subcorpo $K$ de $\mathbb{Q}(\zeta_{p^r})$ de grau $s$. Tal corpo é fixado pelo único subgrupo $H$ de $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ de índice $s$.

Veremos, inicialmente, alguns resultados que serão importantes para os nossos propósitos.

**Lema 3.1** *Sejam $p$ um número primo ímpar, $r$ um inteiro positivo e $g$ um inteiro tal que $\overline{g} \equiv g(\mathrm{mod}\, p^r)$ é um gerador do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$. Então, para todo $j$ tal que $0 < j \leq r$, tem-se $g^k \equiv 1(\mathrm{mod}\, p^j)$ se, e somente se, $k \equiv 0(\mathrm{mod}(p-1)p^{j-1})$.*

**Prova.** Se $g^k = 1 + p^j t$, então $g^{kp} = 1 + p^{j+1}t_1$, onde $t$ e $t_1$ são inteiros. Repetindo o raciocínio tem-se $g^{kp^{r-j}} = 1 + p^r t_{r-j}$, onde $t_{r-j}$ é inteiro. Assim $g^k \equiv 1(\mathrm{mod}\, p^j)$ implica $g^{kp^{r-j}} \equiv 1(\mathrm{mod}\, p^r)$ e daí $(p-1)p^{r-1}$ divide $kp^{r-j}$ e, portanto, $k \equiv 0(\mathrm{mod}(p-1)p^{j-1})$. Reciprocamente, suponha $k \equiv 0(\mathrm{mod}(p-1)p^{j-1})$. Como $(\mathbb{Z}/p^j\mathbb{Z})^*$ tem ordem $(p-1)p^{j-1}$, tem-se $g^k \equiv 1(\mathrm{mod}\, p^j)$. ■

Vamos considerar um inteiro $g$ tal que $\overline{g} \equiv g(\mathrm{mod}\, p^r)$ é um gerador do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$ e $\chi : (\mathbb{Z}/p^r\mathbb{Z})^* \to \mathbb{C}^*$ um caracter de Dirichlet. Como existem exatamente $n$ caracteres definidos sobre um grupo abeliano de ordem $n$, existem $(p-1)p^{r-1}$ caracteres de Dirichlet $\chi$ definidos sobre $(\mathbb{Z}/p^r\mathbb{Z})^*$ e tais caracteres são completamente determinados

pela imagem de $\overline{g}$. Por outro lado,

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

e, assim, $\chi(\overline{g})$ é uma raiz $(p-1)p^{r-1}$-ésima da unidade. Com isso, dado um caracter $\chi$ módulo $p^r$ existe um inteiro $i$ onde $0 \leq i < (p-1)p^{r-1}$ tal que $\chi(\overline{g}) = \zeta^i_{(p-1)p^{r-1}}$. Considerando o número de caracteres e todas as possibilidades para o inteiro $i$ pode-se concluir que todos os caracteres definidos módulo $p^r$ são da forma

$$\chi_i(\overline{g}) = \zeta^i_{(p-1)p^{r-1}}, i = 0, \ldots, (p-1)p^{r-1} - 1.$$

**Lema 3.2** *Com a notação acima, seja $i$ um inteiro tal que $0 \leq i < (p-1)p^{r-1}$. Então $p^j = (i, p^r)$ se, e somente se, o condutor $f\chi_i$ de $\chi_i$ é $p^{r-j}$.*

**Prova.** Para $i = 0$ o resultado é imediato. Suponha que $i \neq 0$ e $p^j = (i, p^r)$. Assim $i = p^j t$, para algum inteiro positivo $t$. Seja $H = \{\overline{g}^a \in (\mathbb{Z}/p^r\mathbb{Z})^*; g^a \equiv 1 (\mathrm{mod}\, p^{r-j})\}$. Então $\chi_i$ pode ser definido módulo $p^{r-j}$ se, e somente se, $\chi_i(x) = 1, \forall x \in H$. Pelo Lema ??, $H = \left\langle g^{(p-1)p^{r-j-1}} \right\rangle$ e, como $\chi_i(g^a) = \zeta^{ai}_{(p-1)p^{r-1}}$, tem-se $\chi_i(g^{(p-1)p^{r-j-1}}) = 1$. Reciprocamente, suponha que $\chi_i$ pode ser definido módulo $p^{r-j}$. Então $\chi_i(x) = 1$, para todo $x$ em $H$ e, em particular, $\chi_i(g^{(p-1)p^{r-j-1}}) = 1$. Como

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

existe um inteiro $t$ tal que $i(p-1)p^{r-j-1} = (p-1)p^{r-1}t$ o que implica $i = p^j t$. Em resumo, $i = p^j t$ se, e somente se, $\chi_i$ pode ser definido módulo $p^{r-j}$ e portanto o condutor de $\chi_i$ é $p^{r-j}$ se $p^j$ é a maior potência de $p$ que divide $i$, isto é, $p^j = (i, p^r)$. ■

### 3.1.1 O cálculo do discriminante

Sejam $p$ um primo ímpar, $r$ um número inteiro positivo e $K$ um subcorpo de $\mathbb{Q}(\zeta_{p^r})$. Desde que o grau de $K$ sobre $\mathbb{Q}$ é um divisor de $(p-1)p^{r-1}$, pode-se escrever $[K : \mathbb{Q}] = up^j$,

onde $u$ é um divisor de $p-1$ e $0 \leq j \leq r-1$. Sejam $H$ o subgrupo de

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})(\cong (\mathbb{Z}/p^r\mathbb{Z})^*)$$

que fixa $K$ e $X_K$ o grupo dos caracteres associados a $K$, isto é, o conjunto

$$\{\chi \in (\widehat{\mathbb{Z}/p^r\mathbb{Z}})^* \text{ tal que } \chi(i) = 1, \forall i \in H\}.$$

O discriminante de $K$, de acordo com a Fórmula do Condutor-Discriminante, é, a menos de sinal, o produto dos condutores dos caracteres de $X_K$.

**Teorema 3.1** *Sejam $p$ um primo ímpar, $r$ um número inteiro positivo e $K$ um subcorpo de $\mathbb{Q}(\zeta_{p^r})$, $[K:\mathbb{Q}] = up^j$, onde $u$ é um divisor de $p-1$ e $0 \leq j \leq r-1$. Então*

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

**Prova.** Observe que $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ é um grupo cíclico de ordem $(p-1)p^{r-1}$. Seja $g \in \mathbb{Z}$ tal que sua classe $\overline{g}$ é um gerador de $(\mathbb{Z}/p^r\mathbb{Z})^*$. Se $[K:\mathbb{Q}] = up^j$ o subgrupo $H$ de $G$ que fixa $K$ é cíclico de ordem

$$\frac{(p-1)p^{r-1}}{up^j} = \frac{p-1}{u} \cdot p^{r-j-1}.$$

Se $\sigma_a$ é um gerador de $H$, concluímos que um caracter $\chi$ definido módulo $p^r$ é associado a $K$ se, e somente se, $\chi(\sigma_a) = 1$. Desde que a ordem de $a$, módulo $p^r$, é igual a ordem de $H$, isto é, $(p-1)p^{r-j-1}/u$, podemos supor, sem perda de generalidade, que $a \equiv g^d (\mathrm{mod}\, p^r)$, onde $d = up^j$. Consequentemente, dado um caracter $\chi_i$ definido módulo $p^r$, temos $\chi_i(\overline{a}) = 1$ (isto é, $\chi_i$ é associado a $K$) se, e somente se, $di \equiv 0 (\mathrm{mod}(p-1)p^{r-1})$ ou, equivalentemente, se, e somente se, $i = (p-1)p^{r-1}t/d$ , $t = 0, \ldots, d-1$(lembre que $\chi_i(\overline{g}) = \zeta^i_{(p-1)p^{r-1}}$; e, portanto, $\chi_i(\overline{a}) = \zeta^{di}_{(p-1)p^{r-1}}$). Desde que $d = up^j$, $\chi_i(\overline{a}) = 1$ se, e somente se, $i = \frac{p-1}{u}p^{r-j-1}t$, onde $t = 0, \ldots, up^j - 1$. Se $t = 0$ então $i = 0$; e $f\chi_i = 1$.

Se $t \neq 0$, seja $t = p^l t_k$, onde $l$ é um inteiro em $[0,\ j]$, e $(t_k, p) = 1$. Note que para cada $l \in [0, j-1]$, existem $up^{j-l-1}(p-1)$ elementos $t_k$ nestas condições. Pelo Lema 3.3 os condutores dos correspondentes $\chi_i$ são todos iguais a $p^{j+1-l}$. Se $l = j$, existem $u-1$ números $t_k$ com $(t_k, p) = 1$, e os condutores dos correspondentes caracteres $\chi_i$ são iguais a $p$. A Tabela 3.1 resume esses resultados. Na primeira coluna temos os possíveis valores de $l$, na segunda temos o números de caracteres (não triviais) $\chi_i$ para os quais $i = \frac{p-1}{u} p^{r-j-1+l} t_k$, e $(t_k, p) = 1$ e na terceira coluna temos o condutor desses caracteres $\chi_i$. Note que, exceto para o caracter trivial, todos os caracteres associados a $K$ estão registrados na tabela abaixo.

| $l$ | Número de $\chi_i$ | $f_{\chi_{i,l}} = p^{j+1-l}$ |
|---|---|---|
| 0 | $up^{j-1}(p-1)$ | $p^{j+1}$ |
| 1 | $up^{j-2}(p-1)$ | $p^j$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $j-1$ | $up^0(p-1)$ | $p^2$ |
| $j$ | $u-1$ | $p$ |

Tabela 3.1: Tabela de caracteres

O discriminante de $K$ é, a menos do sinal, igual ao produto dos condutores dos caracteres $\chi_i$ que são associados a $K$. Usando este resultado e a Tabela 3.1, obtem-se:

$$|\mathrm{Disc}(K)| = \prod_{\chi_i \text{ associados a } K} f_{\chi_i} = p^\alpha$$

Onde $\alpha$ é computado como o somatório de cada elemento da segunda coluna multiplicado pelo $\log_p$ dos elementos correspondentes na terceira coluna. Daí,

$$\begin{aligned}
\alpha &= u\cdot(p-1)\cdot((j+1)p^{j-1}+jp^{j-2}+\cdots+2p^0)+u-1\\
&= \frac{u(p-1)}{p}\cdot\sum_{i=0}^{j}(i+1)p^i-\frac{u(p-1)}{p}+u-1\\
&= \frac{u(p-1)}{p}\cdot\left(\frac{(j+2)\cdot p^{j+1}\cdot(p-1)-(p^{j+2}-1)}{(p-1)^2}\right)+\frac{u}{p}-1\\
&= u\cdot\left((j+2)\cdot p^j-\frac{p^{j+2}-1}{p.(p-1)}+\frac{1}{p}\right)-1\\
&= u\cdot\left((j+2)\cdot p^j-\frac{p^{j+1}-1}{p-1}\right)-1.
\end{aligned}$$

■

**Corolário 3.1** *Dados inteiros positivos p e r, com p primo ímpar, o discriminante do corpo ciclotômico* $\mathbb{Q}(\zeta_{p^r})$ *é dado pela equação*

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

**Corolário 3.2** *Se p é um primo ímpar e* $K\subset\mathbb{Q}(\zeta_p)$*, então*

$$\mathrm{Disc}(K)=\pm p^{[K:\mathbb{Q}]-1}.$$

## 3.2 Os subcorpos de $\mathbb{Q}(\zeta_{2^r}), r\geq 3$

O Corpo Ciclotômico $\mathbb{Q}(\zeta_{2^r})$ é uma extensão Galoisiana de $\mathbb{Q}$ e seu grupo de Galois é isomorfo a $(\mathbb{Z}/2^r\mathbb{Z})^*$, que é um grupo multiplicativo de ordem $\phi(2^r)=2^{r-1}$. Com o objetivo de explicitar o discriminante dos subcorpos de $\mathbb{Q}(\zeta_{2^r})$, precisamos de alguns resultados semelhantes ao caso anterior, em que o objetivo era computar o discriminante dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$, onde p é um número primo ímpar.

**Lema 3.3** *Seja $t$ um número inteiro, $t \geq 3$. Então tem-se:*

$$5^{2^{t-3}} \equiv 1(\mathrm{mod}\, 2^{t-1}) \text{ e } 5^{2^{t-3}} \not\equiv 1(\mathrm{mod}\, 2^t), \text{ ou seja }, \mathrm{ord}_{2^t} 5 = 2^{t-2}.$$

**Prova.** Note que

$$5^{2^{t-3}} - 1 = (5^{2^{t-4}} + 1) \cdot (5^{2^{t-5}} + 1) \cdots (5^2 + 1) \cdot (5 + 1) \cdot (5 - 1) \equiv 0(\mathrm{mod}\, 4).$$

Como

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

temos $5^{2^{t-3}} - 1 = k2^{t-1}$, onde $k$ é ímpar. Logo $5^{2^{t-3}} \equiv 1(\mathrm{mod}\, 2^{t-1})$ e $5^{2^{t-3}} \not\equiv 1(\mathrm{mod}\, 2^t)$. Observe que $5^{2^{t-3}} \equiv 1(\mathrm{mod}\, 2^{t-1})$, $\forall t \geq 3$, implica que $5^{2^{t-2}} \equiv 1(\mathrm{mod}\, 2^t)$, $\forall t \geq 2$. Assim, para $t \geq 3$, tem-se $5^{2^{t-2}} \equiv 1(\mathrm{mod}\, 2^t)$ e $5^{2^{t-3}} \not\equiv 1(\mathrm{mod}\, 2^t)$, o que mostra que $\mathrm{ord}_{2^t} 5 = 2^{t-2}$. ■

**Lema 3.4** *Se $t \geq 2$ então $(-1)^a 5^b \equiv 1(\mathrm{mod}\, 2^t)$ se, e somente se, $b \equiv 0(\mathrm{mod}\, 2^{t-2})$ e $a$ é par.*

**Prova.** Suponha que $(-1)^a 5^b \equiv 1(\mathrm{mod}\, 2^t)$. Mostraremos, inicialmente, que $a$ é par. De fato, se $a$ fosse ímpar teríamos $-5^b \equiv 1(\mathrm{mod}\, 2^t)$, isto é, $5^b \equiv -1(\mathrm{mod}\, 2^t)$, o que não pode ocorrer pois $4 \nmid 5^b + 1$ já que

$$5^b + 1 \equiv 2(\mathrm{mod}\, 4).$$

Conseqüentemente nenhuma potência de 2, com expoente maior do que 1, divide $5^b + 1$, isto é, $5^b \not\equiv -1(\mathrm{mod}\, 2^t)$. Logo $a$ é par. Então

$$(-1)^a 5^b \equiv 1(\mathrm{mod}\, 2^t) \Longrightarrow 5^b \equiv 1(\mathrm{mod}\, 2^t) \Longrightarrow b \equiv 0(\mathrm{mod}\, 2^{t-2}).$$

Reciprocamente, se $b \equiv 0(\mathrm{mod}\, 2^{t-2})$ e $a$ é par, segue imediatamente que $(-1)^a 5^b \equiv 1(\mathrm{mod}\, 2^t)$, já que $\mathrm{ord}_{2^t}(-1) = 2$ e $\mathrm{ord}_{2^t} 5 = 2^{t-2}$. ■

Veremos agora como calcular o condutor de um caracter $\chi$ módulo $2^r$. O condutor de um tal caracter será um divisor de $2^r$.

Visto que

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

um caráter de $(\mathbb{Z}/2^r\mathbb{Z})^*$ ficará completamente determinado pelas imagens de $\overline{-1}$ e $\overline{5}$. Como $\text{ord}_{2^t} 5 = 2^{t-2}$ e $\text{ord}_{2^t}(-1) = 2$, dado $\chi \in \widehat{(\mathbb{Z}/2^r\mathbb{Z})^*}$ temos $\chi(\overline{-1}) = (-1)^i$ e $\chi(\overline{5}) = \xi_{2^{r-2}}^l$. Um tal caracter de $(\mathbb{Z}/2^r\mathbb{Z})^*$ será então denotado por $\chi_{i,l}$ onde $i \in \{1,2\}$ e $l \in \{1,2,\ldots,2^{r-2}\}$.

**Teorema 3.2** *Com a notação acima tem-se*:

$$f_{\chi_{i,l}} = \begin{cases} \frac{2^r}{(l,2^r)}, & \text{se } l \neq 2^{r-2} \\ 4, & \text{se } i = 1 \text{ e } l = 2^{r-2} \\ 1, & \text{se } i = 2 \text{ e } l = 2^{r-2}. \end{cases}$$

**Prova.** Seja $\chi_{i,l} \in \widehat{(\mathbb{Z}/2^r\mathbb{Z})^*}$. Dado $\overline{x} \in (\mathbb{Z}/2^r\mathbb{Z})^*$, tem-se $\overline{x} = \overline{(-1)}^a \overline{5}^b$. Assim, há dois casos a serem considerados: $l = 2^{r-2}$ e $l \neq 2^{r-2}$:

1º Caso $l = 2^{r-2}$.

Se $i = 2$, temos $\chi_{i,l}(\overline{x}) = \chi_{i,l}(\overline{(-1)}^a \overline{5}^b) = (-1)^{2a} \xi_{2^{r-2}}^{2^{r-2}} = 1$ e, portanto, o caracter $\chi_{i,l}$ é trivial e $f_{\chi_{i,l}} = 1$. Se $i = 1$, tem-se

$$\begin{aligned} \chi_{i,l}(\overline{x}) &= \chi_{i,l}(\overline{(-1)}^a \overline{5}^b) = (-1)^a \xi_{2^{r-2}}^{2^{r-2}} \\ &= (-1)^a = \begin{cases} 1 & \text{se } \overline{x} = \overline{5}^b \\ -1 & \text{se } \overline{x} = \overline{-1}.\overline{5}^b \end{cases} \end{aligned}$$

e, portanto, $\chi_{i,l}$ não é trivial. Se $x \equiv 1 (\text{mod}\, 4)$ temos $\overline{x} = \overline{5}^b$(pois $5^b \equiv 1 (\text{mod}\, 4)$ e $-5^b \equiv -1 (\text{mod}\, 4)$ ) e daí para todo $x$, satisfazendo $x \equiv 1 (\text{mod}\, 4)$, temos $\chi_{i,l}(\overline{x}) = 1$. Logo $f_{\chi_{i,l}} = 4$.

2º Caso $l \neq 2^{r-2}$.

Neste caso $\chi_{i,l}(\overline{5}) = \xi_{2^{r-2}}^{l} \neq 1$ e portanto $f_{\chi_{i,l}} > 4$, pois $5 \equiv 1(\mathrm{mod}\, 4)$. Temos então $f_{\chi_{i,l}} = 2^u$, onde $u > 2$. Dado $\overline{x} = \overline{(-1)}^{a}\overline{5}^{b} \in (\mathbb{Z}/2^r\mathbb{Z})^*$, $x \equiv 1(\mathrm{mod}\, 2^u)$ implica em $(-1)^a 5^b \equiv 1(\mathrm{mod}\, 2^u)$ se, e somente se, $b \equiv 0(\mathrm{mod}\, 2^{u-2})$ e $a = 2$ (Lema 3.4 ). Assim se $x \equiv 1(\mathrm{mod}\, 2^u)$ temos $\overline{x} = \overline{5}^{t.2^{u-2}}$, onde $t \in \{1, 2, \ldots, 2^{r-u}\}$. Como $f_{\chi_{i,l}} = 2^u$, se $x \equiv 1(\mathrm{mod}\, 2^u)$ devemos ter

$$\chi_{i,l}(\overline{x}) = \chi_{i,l}(\overline{5}^{2^{u-2}}) = \xi_{2^{r-2}}^{l.2^{u-2}} = 1$$

e daí $l.2^{u-2} \equiv 0(\mathrm{mod}\, 2^{r-2})$ e, portanto,

$$l \equiv 0 \,\mathrm{mod}\, 2^{r-u}. \tag{3.1}$$

Por outro lado, deveremos ter $\chi_{i,l}(\overline{5}^{2^{u-3}}) \neq 1$ pois se $\chi_{i,l}(\overline{5}^{2^{u-3}}) = 1$, dado $x \equiv 1(\mathrm{mod}\, 2^{u-1})$ temos, pelo Lema 3.4, $\overline{x} = \overline{5}^{t.2^{u-3}}$ e daí $\chi_{i,l}(\overline{x}) = (\chi_{i,l}(\overline{5}^{2^{u-3}}))^t = 1$, o que contradiz o fato de $2^u$ ser o condutor de $\chi_{i,l}$. Mas,

$$\chi_{i,l}(\overline{5}^{2^{u-3}}) \neq 1 \Longleftrightarrow \xi_{2^{r-2}}^{2^{u-3}l} \neq 1 \Longleftrightarrow l \not\equiv 0(\mathrm{mod}\, 2^{r-2-(u-3)}) \Longleftrightarrow l \not\equiv 0(\mathrm{mod}\, 2^{r-u+1}) \tag{3.2}$$

Das equações (3.1 e 3.2) temos $(l, 2^r) = 2^{r-u}$ e daí $2^u = \frac{2^r}{(l,2^r)}$, isto é, $f_{\chi_{i,l}} = \frac{2^r}{(l,2^r)}$. ■

### 3.2.1 O cálculo do discriminante

Para o cálculo do discriminante trabalharemos com o grupo dos caracteres de $(\mathbb{Z}/2^r\mathbb{Z})^*$. Dado um subcorpo $K$ de $\mathbb{Q}(\zeta_{2^r})$ consideraremos o subgrupo $H$, do grupo de Galois de $\mathbb{Q}(\zeta_{2^r})$ sobre $\mathbb{Q}$, que fixa $K$ e, a partir daí, tomaremos o subgrupo $X_K$ do grupo dos caracteres de $(\mathbb{Z}/2^r\mathbb{Z})^*$ cujo núcleo contém $H$. O discriminante de $K$, será o produto dos condutores desses caracteres.

Dado um subcorpo $K$ de $\mathbb{Q}(\xi_{2^r})$, de grau $2^{m-1}$, sabemos que o subgrupo $H$ de $G = \mathrm{Gal}(\mathbb{Q}(\xi_{2^r})/\mathbb{Q})$ que fixa $K$ tem ordem $2^{r-m}$ e tem uma das seguintes formas:

1. $H = \left\langle \overline{5}^{2^{m-2}} \right\rangle$;
2. $H = \left\langle -\overline{5}^{2^{m-2}} \right\rangle$;
3. $H = \left\langle \overline{-1}, \overline{5}^{2^{m-1}} \right\rangle$.

Se $X_K$ é o grupo dos caracteres de $(\mathbb{Z}/2^r\mathbb{Z})^*$ cujo núcleo contém $H$, de acordo com a Fórmula do Condutor-Discriminante, o discriminante de $K$ é, a menos de sinal, dado pelo produto dos condutores dos caracteres pertencentes a $X_K$.

**Lema 3.5** *Dado um número inteiro $m > 1$, então*

$$m \cdot 2^{m-2} + (m-1) \cdot 2^{m-3} + \cdots + 3 \cdot 2 + 2 \cdot 1 = 2^{m-1} \cdot (m-1).$$

**Prova.** O polinômio

$$f(x) = m.x^{m-1} + (m-1).x^{m-2} + \cdots + 3.x^2$$

é a derivada do polinômio

$$h(x) = x^m + x^{m-1} + \cdots + x^3 = \frac{x^{m+1} - x^3}{x-1}.$$

Mas a derivada de $h(x)$ é

$$\frac{m \cdot x^{m+1} - (m+1) \cdot x^m - 2 \cdot x^3 + 3 \cdot x^2}{(x-1)^2}.$$

Ou seja,

$$m \cdot x^{m-1} + (m-1) \cdot x^{m-2} + \cdots + 3 \cdot x^2 = \frac{m \cdot x^{m+1} - (m+1) \cdot x^m - 2 \cdot x^3 + 3 \cdot x^2}{(x-1)^2}$$

para todo $x \neq 1$. Logo, fazendo $x = 2$, concluímos a demonstração do Lema. ■

**Teorema 3.3** *Sejam $K$ um subcorpo de $\mathbb{Q}(\xi_{2^r})$, com $[K : \mathbb{Q}] = 2^{m-1}$ e $H$ o subgrupo de $G = \mathrm{Gal}(\mathbb{Q}(\xi_{2^r})/\mathbb{Q})$ que fixa $K$. Temos:*

1. *Se* $H = \left\langle \overline{5}^{2^{m-2}} \right\rangle$, *então* $K = \mathbb{Q}(\xi_{2^m})$ *e* $|\mathrm{Disc}(K)| = 2^{2^{m-1}(m-1)}$.

2. *Se* $H = \left\langle \overline{-5}^{2^{m-2}} \right\rangle$ *ou* $H = \left\langle \overline{-1}, \overline{5}^{2^{m-1}} \right\rangle$, *então* $|\mathrm{Disc}(K)| = 2^{m2^{m-1}-1}$.

**Prova.**1) Se $H = \left\langle \overline{5}^{2^{m-2}} \right\rangle$ temos: $\chi_{i,l}(\overline{x}) = 1$, $\forall \overline{x} \in H$ se, e somente se,

$$\begin{aligned} \chi_{i,l}(\overline{5}^{2^{m-2}}) &= 1 \Longleftrightarrow \xi_{2^{r-2}}^{l.2^{m-2}} = 1 \Longleftrightarrow l \cdot 2^{m-2} \equiv 0 (\mathrm{mod}\, 2^{r-2}) \\ &\Longleftrightarrow l \equiv 0 (\mathrm{mod}\, 2^{r-m}) \Longleftrightarrow l = k \cdot 2^{r-m}, \end{aligned}$$

onde $k \in \{1, 2, \ldots, 2^{m-2}\}$. Assim os caracteres associados a $K$ são os $\chi_{i,l}$ tais que $i \in \{1, 2\}$ e

$$l \in \{2^{r-m}, 2.2^{r-m}, 3.2^{r-m}, \ldots, 2^{m-2}.2^{r-m}\}.$$

Portanto, temos $2.2^{m-2} = 2^{m-1}$ caracteres associados a $K$. Para calcularmos o discriminante de $K$ usaremos a Tabela 3.2:

| $(l, 2^r)$ | Número de $\chi_{i,l}$ | $f_{\chi_{i,l}}$ |
|---|---|---|
| $2^{r-m}$ | $2 \cdot \frac{2^{m-2}}{2} = 2^{m-2}$ | $\frac{2^r}{2^{r-m}} = 2^m$ |
| $2^{r-m+1}$ | $2 \cdot \frac{2^{m-3}}{2} = 2^{m-3}$ | $\frac{2^r}{2^{r-m+1}} = 2^{m-1}$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $2^{r-3} = 2^{r-m+(m-3)}$ | $2.\frac{2^{m-(m-1)}}{2} = 2$ | $\frac{2^r}{2^{r-3}} = 2^3$ |
| $2^{r-2} = 2^{r-m+(m-2)}$ e $i = 1$ | 1 | $2^2$ |
| $2^{r-2}$ e $i = 2$ | 1 | 1 |

Tabela 3.2: Tabela de caracteres

Portanto, $|\mathrm{Disc}(K)| = 2^\alpha$, onde

$$\alpha = m \cdot 2^{m-2} + (m-1) \cdot 2^{m-3} + (m-2) \cdot 2^{m-4} + \cdots + 3 \cdot 2 + 2 \cdot 1.$$

Logo, pelo Lema 3.5, $\alpha = 2^{m-1}(m-1)$.

2) Se $H = \left\langle -\overline{5}^{2^{m-2}} \right\rangle$ temos:

$$\chi_{i,l}(\overline{x}) = 1 \forall \overline{x} \in H \Longleftrightarrow \chi_{i,l}(-\overline{5}^{2^{m-2}}) = 1$$

ou, equivalentemente,

$$(-1)^i \xi_{2^{r-2}}^{l2^{m-2}} = 1 \Longleftrightarrow \xi_{2^{r-2}}^{l2^{m-2}} = (-1)^i.$$

Se $i = 1$, temos $\xi_{2^{r-2}}^{l2^{m-2}} = -1$ e daí

$$l \in \{2^{r-m-1}, 3 \cdot 2^{r-m-1}, 5 \cdot 2^{r-m-1}, \ldots, (2^{m-1} - 1) \cdot 2^{r-m-1}\}.$$

Neste caso temos $\frac{2^{m-1}-1+1}{2} = 2^{m-2}$ caracteres. Se $i = 2$, temos $\xi_{2^{r-2}}^{l2^{m-2}} = 1$ e daí $l \equiv 0 (\mathrm{mod}\, 2^{r-m})$ e então

$$l \in \{2^{r-m}, 2 \cdot 2^{r-m}, 3 \cdot 2^{r-m}, \ldots, 2^{m-2} \cdot 2^{r-m}\}$$

Neste caso temos $2^{m-2}$ caracteres.

No total temos $2 \cdot 2^{m-2} = 2^{m-1}$ caracteres associados a $K$. Para calcularmos o discriminante de $K$ usaremos a Tabela 3.3

| $(l, 2^r)$ | Número de $\chi_{i,l}$ | $f_{\chi_{i,l}}$ |
|---|---|---|
| $2^{r-m-1}$ | $2^{m-2}$ | $\frac{2^r}{2^{r-m-1}} = 2^{m+1}$ |
| $2^{r-m}$ | $\frac{2^{m-2}}{2} = 2^{m-3}$ | $\frac{2^r}{2^{r-m}} = 2^m$ |
| $2^{r-m+1}$ | $\frac{2^{m-3}}{2} = 2^{m-4}$ | $\frac{2^r}{2^{r-m+1}} = 2^{m-1}$ |
| $2^{r-m+2}$ | $\frac{2^{m-4}}{2} = 2^{m-5}$ | $\frac{2^r}{2^{r-m+2}} = 2^{m-2}$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $2^{r-3}$ | $\frac{2^{m-(m-1)}}{2} = 1$ | $\frac{2^r}{2^{r-3}} = 2^3$ |

Tabela 3.3: Tabela de caracteres

Portanto, $|\mathrm{Disc}(K)| = 2^\alpha$, onde

$$\alpha = (m+1) \cdot 2^{m-2} + m \cdot 2^{m-3} + (m-1) \cdot 2^{m-4} + \ldots + 3 \cdot 1.$$

Logo, pelo Lema 3.5, $\alpha = m \cdot 2^{m-1} - 1$.

3) Se $H = \left\langle \overline{-1}, \overline{5}^{2^{m-1}} \right\rangle$ temos:

$$\chi_{i,l}(\overline{x}) = 1 \forall \overline{x} \in H \Longleftrightarrow \chi_{i,l}(\overline{-1}) = \chi_{i,l}(-\overline{5}^{2^{m-1}}) = 1,$$

ou seja,

$$(-1)^i = \xi_{2^{r-2}}^{l2^{m-1}} = 1 \Longleftrightarrow i = 2 \text{ e } l.2^{m-1} \equiv 0 (\mathrm{mod}\, 2^{r-2}) \Leftrightarrow i = 2 \text{ e } l \equiv 0 (\mathrm{mod}\, 2^{r-m-1}),$$

isto é,

$$i = 2 \text{ e } l \in \{2^{r-m-1}, 2.2^{r-m-1}, 3.2^{r-m-1}, \ldots, 2^{m-1}.2^{r-m-1}\}.$$

Neste caso temos um total de $2^{m-1}$ caracteres associados a $K$. Para calcularmos o discriminante de $K$ usaremos a Tabela 3.4

| $(l, 2^r)$ | Número de $\chi_{i,l}$ | $f_{\chi_{i,l}}$ |
|---|---|---|
| $2^{r-m-1}$ | $2^{m-2}$ | $2^{m+1}$ |
| $2^{r-m}$ | $2^{m-3}$ | $2^m$ |
| $2^{r-m+1}$ | $2^{m-4}$ | $2^{m-1}$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $2^{r-3}$ | 1 | $2^3$ |
| $2^{r-2}$ | 1 | 1 |

Tabela 3.4: Tabela de caracteres

Assim sendo, $|\mathrm{Disc}(K)| = 2^\alpha$ onde

$$\begin{aligned} \alpha &= (m+1) \cdot 2^{m-2} + m \cdot 2^{m-3} + (m-1) \cdot 2^{m-4} + \cdots + 3 \cdot 1 \\ &= m \cdot 2^{m-1} - 1 \end{aligned}$$

e temos a mesma situação do caso (2) e o teorema está demonstrado. ■

**Corolário 3.3** *Seja $K$ um subcorpo de $\mathbb{Q}(\xi_{2^r})$ tal que $[K : \mathbb{Q}] = 2^{m-1}$. Se $K = \mathbb{Q}(\xi_{2^m})$, então* $\mathrm{Disc}(K) = 2^{(m-1)\cdot 2^{m-1}}$. *Se $K \neq \mathbb{Q}(\xi_{2^m})$, então* $\mathrm{Disc}(K) = 2^{m2^{m-1}-1}$.

**Prova.** Seja $H$ o subgrupo de $G$ que fixa $K$. Como $K$ é um subcorpo de grau $2^{m-1}$ de

$\mathbb{Q}(\xi_{2^r})$ tem-se

$$H = \left\langle \overline{5}^{2^{m-2}} \right\rangle, H = \left\langle -\overline{5}^{2^{m-2}} \right\rangle \text{ ou } H = \left\langle \overline{-1}, \overline{5}^{2^{m-1}} \right\rangle.$$

Como $5^{2^{m-2}} \equiv 1 (\mathrm{mod}\, 2^m)$ tem-se $5^{2^{m-2}} = 1 + 2^m k$ e daí $\sigma_{5^{2^{m-2}}}(\xi_{2^m}) = (\xi_{2^m})^{1+2^m k} = \xi_{2^m}$. Portanto, o corpo fixo por $\left\langle \overline{5}^{2^{m-2}} \right\rangle$ é $\mathbb{Q}(\xi_{2^m})$. Assim, se $K = \mathbb{Q}(\xi_{2^m})$, temos, pelo Teorema 3.3,

$$\mathrm{Disc}(\mathbb{Q}(\xi_{2^m})) = \pm 2^{(m-1)\cdot 2^{m-1}}.$$

Se $K \neq \mathbb{Q}(\xi_{2^m})$, então $H = \left\langle -\overline{5}^{2^{m-2}} \right\rangle$ ou $H = \left\langle \overline{-1}, \overline{5}^{2^{m-1}} \right\rangle$ e, novamente pelo Teorema 3.3, $\mathrm{Disc}(K) = \pm 2^{m\cdot 2^{m-1}-1}$. ■

## 3.3 Os Corpos de Números Abelianos

Segundo o Teorema de Kronecker-Weber, se $K$ é um Corpo de Números Abeliano, então $K$ está contido em algum Corpo Ciclotômico $\mathbb{Q}(\zeta_m)$. Se $m$ é o menor inteiro tal que $K \subset \mathbb{Q}(\zeta_m)$, $m$ é chamado de condutor de $K$.

Seja $H_K$ o subgrupo do grupo de Galois de $\mathbb{Q}(\zeta_m)$ sobre $\mathbb{Q}$, que fixa $K$. Como

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$$

temos que $H_K$ pode ser visto como um subgrupo de $(\mathbb{Z}/m\mathbb{Z})^*$. Seja $X_K$ o grupo dos caracteres associados a $K$, isto é, o conjunto dos elementos de $\widehat{(\mathbb{Z}/m\mathbb{Z})^*}$, cujo núcleo contém $H_K$. Assim, $X_K$ é um subgrupo de $\widehat{(\mathbb{Z}/m\mathbb{Z})^*}$, isomorfo a $\mathrm{Gal}(K/\mathbb{Q})$ (portanto, $[K : \mathbb{Q}] = |X_K|$).

A idéia aqui utilizada é a de analisar os possíveis condutores dos caracteres de $X_K$ e, em seguida, fazer uma contagem de quantos caracteres existem para cada valor do condutor.

Como nas situações anteriores, precisamos de alguns resultados preliminares.

**Lema 3.6** *Se $K$ e $L$ são subcorpos $\mathbb{Q}(\zeta_m)$ então*

$$K \subset L \text{ se, e somente se, } X_K \subset X_L.$$

**Prova.** Da Teoria de Galois, sabemos que

$$K \subset L \Longleftrightarrow H_L \subset H_K.$$

Das definições de $H_K$ e $X_L$ temos imediatamente que

$$H_L \subset H_K \Longleftrightarrow X_K \subset X_L.$$

Logo

$$K \subset L \Longleftrightarrow H_L \subset H_K \Longleftrightarrow X_K \subset X_L.$$

■

**Lema 3.7** *Se $K$ e $L$ são subcorpos $\mathbb{Q}(\zeta_m)$, então $X_K \cap X_L = X_{K \cap L}$.*

**Prova.** De modo análogo ao Lema anterior, a demonstração deste Lema é uma conseqüência imediata da Teoria de Galois. ■

**Corolário 3.4** *Sejam $K$ um subcorpo de $\mathbb{Q}(\zeta_m)$, $s$ e $d$ divisores de $m$, então*

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

*onde $t$ é o máximo divisor comum de $d$ e $s$.*

**Prova.**

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

pois $\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_s) = \mathbb{Q}(\zeta_t)$. ■

**Lema 3.8** *Sejam $A_1, \ldots, A_n$ conjuntos e*

$$B_r = \sum_{\substack{i_k=1,\ldots,n \\ i_j<i_{j+1}}} |A_{i_1} \cap \cdots \cap A_{i_r}|, r = 1, \ldots, n.$$

*Então*

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

### 3.3.1 O cálculo do discriminante

Sejam $K$ um Corpo de Números Abeliano e $m$ o seu condutor. Assim, $X_K \subset X_{\mathbb{Q}(\zeta_m)}$ e, portanto, os condutores dos caracteres de $X_K$ são divisores de $m$. Para calcular o discriminante de $K$ devemos determinar o número de caracteres de $X_K$ cujo condutor é $d$, para cada divisor $d$ de $m$. O conjunto $X_{K\cap\mathbb{Q}(\zeta_d)}$ consiste exatamente de todos os caracteres de $X_K$ cujo condutor divide $d$. Portanto, os caracteres de $X_K$ de condutor $d$ pertencem a $X_{K\cap\mathbb{Q}(\zeta_d)}$, cuja ordem é $[K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}]$. Assim o número de caracteres de $K$ de condutor $d$ é igual a

$$[K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - n(d),$$

onde $n(d)$ é o número de caracteres de $X_K$ cujo condutor é um divisor de $d$, diferente de $d$. Neste caso, um caracter $\chi$ associado a $K$ tem um tal condutor $l$ se, e somente se,

$$\chi \in \bigcup_{\substack{p|d \\ p \text{ primo}}} X_{K\cap\mathbb{Q}(\zeta_{d/p})}.$$

Portanto,

$$n(d) = \left| \bigcup_{\substack{p|d \\ p \text{ primo}}} X_{K\cap\mathbb{Q}(\zeta_{d/p})} \right|$$

(onde $|Y|$ denota o número de elementos do conjunto $Y$). Daí o número de caracteres associados a $K$, de condutor $d$, é

$$[K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - \left| \bigcup_{\substack{p|d \\ p \text{ primo}}} X_{K\cap\mathbb{Q}(\zeta_{d/p})} \right| .$$

Portanto, podemos afirmar que, se $K$ é um Corpo de Números Abeliano de condutor $m$, então

$$|\text{Disc}(K)| = \prod_{d|m} d^{\left( [K\cap\mathbb{Q}(\zeta_d):\mathbb{Q}] - \left| \bigcup_{\substack{p|d \\ p \text{ primo}}} X_{K\cap\mathbb{Q}(\zeta_{d/p})} \right| \right)} .$$

A fórmula acima pode ser melhorada e este será o nosso objetivo.

**Lema 3.9** *Se* $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}$, *então*:

$$\left| \bigcup_{\substack{p|d \\ p \text{ primo}}} X_{K\cap\mathbb{Q}(\zeta_{d/p})} \right| = \sum_{i=1,\ldots,r} g_{d/p_i} - \sum_{\substack{i_1,i_2=1,\ldots,r \\ i_1<i_2}} g_{d/p_{i_1}\cdot p_{i_2}} + \cdots + (-1)^{r+1} g_{d/p_1 p_2 \cdots p_r} .$$

$$\text{onde } g_s = \begin{cases} \left|X_{K\cap\mathbb{Q}(\zeta_s)}\right| , & \text{se } s \text{ é um inteiro positivo} \\ 0 , & \text{se } s \text{ é um racional não inteiro} \end{cases}$$

**Prova**. Este resultado é uma conseqüência dos Lemas 3.7 e 3.8 e do Corolário 3.4. ■

**Teorema 3.4** *Sejam* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *e* $K$ *um Corpo de Números Abeliano de condutor* $m$. *Então*:

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

**Prova.** Sejam

$$d = p_1^{t_1} \cdot p_2^{t_2} \cdots p_k^{t_k},\ 0 \leq t_i \leq \alpha_i$$

e $f_d$ o número de caracteres, de condutor $d$, associados a $K$. Então:

$$\begin{aligned} f_d &= [K \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}] - \left| \bigcup_{p|d} X_{K \cap \mathbb{Q}(\zeta_{d/p})} \right| \\ &= g_d - \sum_{i=1,\ldots,k} g_{d/p_i} + \sum_{\substack{i_1,i_2=1,\ldots,k \\ i_1<i_2}} g_{d/p_{i_1} \cdot p_{i_2}} + \cdots + (-1)^k g_{d/p_1 p_2 \cdots p_k} \end{aligned}$$

e, portanto,

$$|\mathrm{Disc}(K)| = \prod_{d|m} d^{f_d} = \prod_{d|m} d^{g_d - g_{d/p_1} - g_{d/p_2} - \cdots + (-1)^k g_{d/p_1 p_2 \cdots p_k}} = \prod_{d|m} (h_d)^{g_d}.$$

Teremos as seguintes possibilidades para $h_d$ :

i) Se $d = p_1^{t_1} . p_2^{t_2} \ldots p_k^{t_k}$, onde $0 \leq t_i < \alpha_i$ para $i = 1, 2, \ldots, k$ e $k \geqslant 2$, temos:

$$\begin{aligned} h_d &= d \cdot \left( \prod_{i=1}^{k} p_i d \right)^{-1} \cdot \left( \prod_{1 \leq i < j \leq k} (p_i p_j d) \right) \cdots \left( \prod_{1 \leq i_1 < i_2 < \ldots < i_k \leq k} (p_{i_1} p_{i_2} \cdots p_{i_k} d) \right)^{(-1)^k} \\ &= d^{\sum_{i=0}^{k} (-1)^i \cdot \binom{k}{i}} \cdot \prod_{i=1}^{k} p_i^{\sum_{i=0}^{k-1} (-1)^i \cdot \binom{k-1}{i}} = 1. \end{aligned}$$

ii) Se $d = p_1^{t_1} . p_2^{t_2} \cdots p_k^{t_k}$, onde $t_{i_1} = \alpha_{i_1}$ para algum $i_1$ e $0 \leq t_i < \alpha_i$, para $i \neq i_1$ e $k \geqslant 3$,

temos:

$$h_d = d \cdot \left(\prod_{j=2}^{k} p_{i_j} d\right)^{-1} \cdot \left(\prod_{2\le i<j\le k} (p_i p_j d)\right) \cdots \left(\prod_{2\le i_1<i_2<\ldots<i_{k-1}\le k} \left(p_{i_1} p_{i_2} \ldots p_{i_{k-1}} d\right)\right)^{(-1)^k}$$

$$= d^{\sum_{i=0}^{k-1}(-1)^i \cdot \binom{k-1}{i}} \cdot \prod_{i=1}^{k} p_i^{\sum_{i=0}^{k-1}(-1)^i \cdot \binom{k-2}{i}} = 1$$

De forma análoga mostra-se que $h_d = 1$ se $t_{i_1} = \alpha_{i_1}$, $t_{i_2} = \alpha_{i_2}, \ldots, t_{i_s} = \alpha_{i_s}, 0 \le t_i < \alpha_i$ para $i \neq i_1, i_2, \ldots, i_s$ e $2 \le s \le k-2$.

iii) Se $t_{i_1} = \alpha_{i_1}, t_{i_2} = \alpha_{i_2}, \ldots, t_{i_s} = \alpha_{i_s}$, $0 \le t_i < \alpha_i$ para $i \neq i_1, i_2, \ldots, i_s$ e $s = k-1$, ou seja, $d = m/p_i^r$, $1 \le r \le \alpha_i$, $1 \le j \le k$ temos $h_d = d.\,(p_i d)^{-1} = p_i^{-1}$.

iv) Finalmente, se $t_i = \alpha_i$ para $i = 1, 2, \ldots, k$, ou seja, $d = m$ temos $h_d = m$. Em resumo,

$$h_d = \begin{cases} m, & \text{se } d = m. \\ p_i^{-1}, & \text{se } d = m/p_i^r,\ 1 \le r \le \alpha_i,\ 1 \le i \le k. \\ 1, & \text{se } d \neq m \text{ e } d \neq m/p_i^r,\ 1 \le r \le \alpha_i,\ 1 \le i \le k. \end{cases}$$

e, portanto,

$$\begin{aligned} |\mathrm{Disc}(K)| &= \prod_{d|m} (h_d)^{g_d} = h_m^{g_m} \cdot \prod_{i=1}^{k} \left(\prod_{r=1}^{\alpha_i} h_{m/p_i^r}^{g_{m/p_i^r}}\right) \\ &= m^{[K:\mathbb{Q}]} \cdot \prod_{i=1}^{k} \left(\prod_{r=1}^{\alpha_i} p_i^{-g_{m/p_i^r}}\right) \\ &= m^{[K:\mathbb{Q}]} \cdot \prod_{i=1}^{k} \left(p_i^{-\sum_{r=1}^{\alpha_i} g_{m/p_i^r}}\right) \\ &= \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\sum_{r=1}^{\alpha_i} [K \cap \mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]}}. \end{aligned}$$

■

**Corolário 3.5** *Seja $K$ um subcorpo de $\mathbb{Q}(\zeta_{p^n})$ de grau $up^j$, onde $u$ e $p$ são relativamente primos e $p$ é um primo ímpar, então:*

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

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

$$\begin{aligned} |\mathrm{Disc}(K)| &= \frac{m^{[K:\mathbb{Q}]}}{p^{\sum_{r=1}^{j+1}[K\cap\mathbb{Q}(\zeta_{m/p^r}):\mathbb{Q}]}} \\ &= \frac{\left(p^{j+1}\right)^{up^j}}{p^{\sum_{r=1}^{j+1}[K\cap\mathbb{Q}(\zeta_{p^{j+1}/p^r}):\mathbb{Q}]}} \\ &= \frac{\left(p^{j+1}\right)^{up^j}}{p^{\sum_{r=0}^{j}[K\cap\mathbb{Q}(\zeta_{p^r}):\mathbb{Q}]}}. \end{aligned}$$

Como $[K \cap \mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = up^{r-1}$ para $r \geq 1$ e $[K \cap \mathbb{Q}(\zeta_{p^0}) : \mathbb{Q}] = 1$ temos:

$$
\begin{aligned}
|\mathrm{Disc}(K)| &= \frac{(p^{j+1})^{up^j}}{p^{up^{j-1}+up^{j-2}+\cdots+up+u+1}} \\
&= \frac{(p^{j+1})^{up^j}}{p^{u(p^{j-1}+p^{j-2}+\cdots+p+1)+1}} \\
&= \frac{p^{(j+1)up^j}}{p^{u(\frac{p^j-1}{p-1})+1}} \\
&= p^{(j+1)up^j-u(\frac{p^j-1}{p-1})-1} \\
&= p^{u((j+1)p^j-\frac{p^j-1}{p-1})-1} \\
&= p^{u((j+1)p^j-\frac{p^j-1}{p-1}+p^j-p^j)-1} \\
&= p^{u[(j+2)p^j-(\frac{p^j-1}{p-1}+p^j)]-1} \\
&= p^{u[(j+2)p^j-(\frac{p^{j+1}-1}{p-1})]-1}
\end{aligned}
$$

■

**Corolário 3.6** *Seja $K$ um subcorpo de $\mathbb{Q}(\zeta_{2^n})$ de grau $2^{m-1}$. Se $K = \mathbb{Q}(\zeta_{2^m})$, $\mathrm{Disc}(K) = 2^{(m-1)2^{m-1}}$, caso contrário, $\mathrm{Disc}(K) = 2^{m2^{m-1}-1}$.*

**Prova**. Visto que

$$[K \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^m}) \cap \mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^i}) : \mathbb{Q}] = 2^{i-1}, i \geq 1$$

e $[\mathbb{Q}(\zeta_{2^0}):\mathbb{Q}]=1$; se $K=\mathbb{Q}(\zeta_{2^m})$, temos:

$$\begin{aligned}\mathrm{Disc}(K) &= \frac{2^{m[K:\mathbb{Q}]}}{2^{\sum_{r=1}^{m}[K\cap\mathbb{Q}(\zeta_{2^m/2^r}):\mathbb{Q}]}}\\ &= \frac{2^{m2^{m-1}}}{2^{\sum_{r=0}^{m-1}[K\cap\mathbb{Q}(\zeta_{2^r}):\mathbb{Q}]}}\\ &= \frac{2^{m2^{m-1}}}{2^{2^{m-2}+2^{m-3}+\cdots+2+1+1}}\\ &= \frac{2^{m2^{m-1}}}{2^{2^{m-1}-2+2}}=\frac{2^{m2^{m-1}}}{2^{2^{m-1}}}=2^{(m-1)2^{(m-1)}}.\end{aligned}$$

Se $K\neq\mathbb{Q}(\zeta_{2^m})$, então $K\subset\mathbb{Q}(\zeta_{2^{m+1}})$ e $[\mathbb{Q}(\zeta_{2^{m+1}}):K]=2$, logo $[\mathbb{Q}(\zeta_{2^i}):K\cap\mathbb{Q}(\zeta_{2^i})]=2$, para todo $i\in\{2,\ldots,m\}$ e, portanto,

$$\begin{aligned}[K\cap\mathbb{Q}(\zeta_{2^i}) &: \mathbb{Q}]=[\mathbb{Q}(\zeta_{2^i}):\mathbb{Q}]/2=2^{i-2}, i\geq 2\\ [K\cap\mathbb{Q}(\zeta_2);\mathbb{Q}] &= [K\cap\mathbb{Q}(\zeta_{2^0}):\mathbb{Q}]=1.\end{aligned}$$

Logo,

$$\begin{aligned}\mathrm{Disc}(K) &= \frac{2^{(m+1)[K:\mathbb{Q}]}}{2^{\sum_{r=1}^{m+1}[K\cap\mathbb{Q}(\zeta_{2^m/2^r}):\mathbb{Q}]}}\\ &= \frac{2^{(m+1)2^{m-1}}}{2^{\sum_{r=0}^{m}[K\cap\mathbb{Q}(\zeta_{2^r}):\mathbb{Q}]}}\\ &= \frac{2^{(m+1)[K:\mathbb{Q}]}}{2^{2^{m-2}+2^{m-3}+\cdots+2+1+1+1}}=\frac{2^{(m+1)2^{m-1}}}{2^{2^{m-1}+1}}=2^{m2^{m-1}-1}.\end{aligned}$$

■

**Corolário 3.7** *(cf. [Was, Proposição 2.7, pag. 12])Se $K=\mathbb{Q}(\zeta_m)$, então*

$$|\mathrm{Disc}(K)|=\frac{m^{\phi(m)}}{\prod_{p|m}p^{\frac{\phi(m)}{p-1}}}.$$

**Prova**. Temos $K \cap \mathbb{Q}(\zeta_{m/p_i^j}) = \mathbb{Q}(\zeta_{m/p_i^j})$ e daí $[K \cap \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}] = \phi(m/p_i^j)$. Temos, também, que $[K : \mathbb{Q}] = \phi(m)$. Logo,

$$
\begin{aligned}
|\mathrm{Disc}(K)| &= \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\sum_{j=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^j}):\mathbb{Q}]}} \\
&= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{\sum_{j=1}^{\alpha_i}\phi(m/p_i^j)}} \\
&= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{\phi(m/p_i)+\phi(m/p_i^2)+\cdots+\phi(m/p_i^{\alpha_i})}} \\
&= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_i^{\alpha_i-1}\cdots p_k^{\alpha_k})+\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_i^{\alpha_i-2}\cdots p_k^{\alpha_k})+\cdots+\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_i^{\alpha_i-\alpha_i}\cdots p_k^{\alpha_k})}} \\
&= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{\sum_{j=0}^{\alpha_i-1}\phi(p_i^j)\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{i-1}^{\alpha_{i-1}}\cdot p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}} \\
&= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{i-1}^{\alpha_{i-1}}\cdot p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})\sum_{j=0}^{\alpha_i-1}\phi(p_i^j)}} \\
&= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{(1+(p_i-1)+(p_i-1)p_i+(p_i-1)p_i^2+\cdots+(p_i-1)p_i^{\alpha_i-2})\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{i-1}^{\alpha_{i-1}}\cdot p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}}
\end{aligned}
$$

$$= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{(1+(p_i-1)(\frac{p_i^{\alpha_i-1}-1}{p_i-1}))\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{i-1}^{\alpha_{i-1}}\cdot p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}}$$

$$= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{(1+p_i^{\alpha_i-1}-1))\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{i-1}^{\alpha_{i-1}}\cdot p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}}$$

$$= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{(p_i^{\alpha_i-1})\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{i-1}^{\alpha_{i-1}}\cdot p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}}$$

$$= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{\frac{\phi(p_i^{\alpha_i})}{(p_i-1)}\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{i-1}^{\alpha_{i-1}}\cdot p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}}$$

$$= \frac{m^{\phi(m)}}{\prod_{i=1}^{k} p_i^{\frac{\phi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{i-1}^{\alpha_{i-1}}\cdot p_i^{\alpha_i}\cdot p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k})}{(p_i-1)}}}$$

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

■

**Corolário 3.8** *Seja $K$ um Corpo de Números de Condutor $m$. Se $K \cap \mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$, para todo divisor primo $p$ de $m$, então $|\mathrm{Disc}(K)| = m^{[K:\mathbb{Q}]-1}$.*

**Prova.** De fato, como $K \cap \mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$, para todo divisor primo $p$ de $m$, temos $\sum_{r=1}^{\alpha_i}[K \cap \mathbb{Q}(\zeta_{m/p_i^r}) : \mathbb{Q}] = \alpha_i$ e então

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

$$= \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i}} = \frac{m^{[K:\mathbb{Q}]}}{m} = m^{[K:\mathbb{Q}]-1}$$

■

**Corolário 3.9** *Seja $K$ um Corpo de Números Abeliano de grau primo $p$ (isto é, $[K : \mathbb{Q}] = p$) e condutor $m$. Então $|\mathrm{Disc}(K)| = m^{p-1}$.*

**Prova.** De fato, neste caso temos $K \cap \mathbb{Q}(\zeta_{m/p}) = \mathbb{Q}$ para todo divisor primo $p$ de $m$ pois, $K \cap \mathbb{Q}(\zeta_{m/p})$ é subcorpo de $K$, diferente de $K$ ( pois, se $K \cap \mathbb{Q}(\zeta_{m/p}) = K$ teríamos $K \subset \mathbb{Q}(\zeta_{m/p})$, que contrariaria a minimalidade de $m$) e que não pode conter estritamente $\mathbb{Q}$, devido ao grau de $K$ ser primo. Assim, pelo Teorema 3.4, $|\mathrm{Disc}(K)| = m^{[K:\mathbb{Q}]-1} = m^{p-1}$. ■

**Corolário 3.10** *O menor valor possível para o valor absoluto dos discriminantes das extensões de grau primo $p$ é o menor valor entre $p^{2(p-1)}$ e $(kp+1)^{(p-1)}$, onde $k$ é inteiro positivo e $kp+1$ é primo.*

**Prova.** Temos $|\mathrm{Disc}(K)| = m^{p-1}$ onde $m$ é o condutor de $K$. Vamos procurar o menor inteiro possível para o condutor $m$. Se $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, então

$$\phi(m) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdot (p_2 - 1)p_2^{\alpha_2 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}$$

e temos

$$p \mid \phi(m) \Longleftrightarrow p \mid (p_i - 1),$$

para algum $i$ ou $p \mid p_j^{\alpha_j - 1}$, para algum $j$. Para que $m$ seja mínimo devemos ter $m = p^2$ ou $m = kp + 1$, $kp + 1$ primo. Como as extensões $\mathbb{Q}(\zeta_{kp+1})$ e $\mathbb{Q}(\zeta_{p^2})$ são cíclicas (pois $kp + 1$ e $p$ são primos) elas contêm subcorpos de grau $p$ (pois $p \mid \phi(kp + 1)$ e $p \mid \phi(p^2)$) e daí o resultado segue. ■

**Corolário 3.11** *O menor valor possível para o discriminante de uma cúbica galoisiana é* 49.

**Prova.** O menor valor possível para o discriminante de uma cúbica é o menor elemento do conjunto

$$\{3^{2(3-1)}, (3.2+1)^{(3-1)}\} = \{81, 49\}.$$

Daí o menor valor possível para o discriminante de uma cúbica é 49. ■

Usando a idéia de contar os elementos do grupo de caracteres associados ao corpo $K$ podemos demonstrar o seguinte resultado:

**Proposição 3.1** *Sejam $K$ e $L$ Corpos de Números Abelianos linearmente disjuntos sobre $\mathbb{Q}$ (isto é, tais que $[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$ e $\mathrm{Disc}(K)$ e $\mathrm{Disc}(L)$ são relativamente primos). Então*

$$|\mathrm{Disc}(K \cdot L)| = |\mathrm{Disc}(K)|^{[L:\mathbb{Q}]} \cdot |\mathrm{Disc}(L)|^{[K:\mathbb{Q}]}.$$

**Prova.** De fato, sejam $X_K$ e $X_L$ os grupos de caracteres associados a $K$ e a $L$, respectivamente. O grupo de caracteres associados ao compósito $KL$, que denotaremos por $X_{KL}$, é o grupo gerado por $X_K$ e $X_L$ que é, neste caso, $X_K.X_L$ (pois os grupos são abelianos).

Sejam $r = [K : \mathbb{Q}]$, $s = [L : \mathbb{Q}]$ , $X_K = \{\chi_0, \chi_1, \ldots, \chi_{r-1}\}$ e $X_L = \{\psi_0, \psi_2, \ldots, \psi_{s-1}\}$. Desta forma

$$|\mathrm{Disc}(K)| = f_{\chi_0} \cdot f_{\chi_0} \cdots f_{\chi_{r-1}} \text{ e } |\mathrm{Disc}(L)| = f_{\psi_0} \cdot f_{\psi_0} \cdots f_{\psi_{s-1}}.$$

Por outro lado, $\chi_0 = \psi_0$, $\chi_i \neq \psi_j$ para $i \neq j$ (já que $\mathrm{Disc}(K)$ e $\mathrm{Disc}(L)$ são relativamente primos) e $\chi_i.\psi_j \neq \chi_l.\psi_m$ para $i \neq j$ ou $l \neq m$ pois, a ordem de $X_K \cdot X_L$ é $rs$ já que $[K \cdot L : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$. Como

$$X_{KL} = X_K \cdot X_L = \{\chi_i.\psi_j; 0 \leq i \leq r-1 \text{ e } 0 \leq j \leq s-1\}$$

temos:

$$\begin{aligned} |\mathrm{Disc}(K\cdot L)| &= \prod_{\substack{0\le i\le r-1\\ 0\le j\le s-1}} f_{\chi_i\chi_j} = \prod_{\substack{0\le i\le r-1\\ 0\le j\le s-1}} f_{\chi_i} f_{\psi_j} \\ &= (f_{\chi_0}\cdot f_{\chi_1}\cdots f_{\chi_{r-1}})^{[L:\mathbb{Q}]}(f_{\psi_0}\cdot f_{\psi_1}\cdots f_{\psi_{s-1}})^{[K:\mathbb{Q}]} \\ &= |\mathrm{Disc}(K)|^{[L:\mathbb{Q}]}\cdot|\mathrm{Disc}(L)|^{[K:\mathbb{Q}]} \end{aligned}$$

($f_{\chi_i\chi_j} = f_{\chi_i}f_{\psi_j}$, pois $f_{\chi_i}$ e $f_{\psi_j}$ são relativamente primos, já que $\mathrm{Disc}(K)$ e $\mathrm{Disc}(L)$ são relativamente primos) ■

**Corolário 3.12** *Se $m$ e $n$ são relativamente primos, então*

$$|\mathrm{Disc}(\mathbb{Q}(\zeta_{mn}))| = |\mathrm{Disc}(\mathbb{Q}(\zeta_m))|^{\phi(n)}\,|\mathrm{Disc}(\mathbb{Q}(\zeta_n))|^{\phi(m)}.$$

**Prova.** Sejam $X_m$, $X_n$ e $X_{mn}$ os grupos de caracteres associados, respectivamente, a $\mathbb{Q}(\zeta_m)$, $\mathbb{Q}(\zeta_n)$ e $\mathbb{Q}(\zeta_{mn})$. Como $m$ e $n$ são relativamente primos, $X_m\cap X_n = \{\chi_0\}$. Por outro lado, o grupo gerado por $X_m$ e $X_n$ é $X_{mn}$. Assim os corpos $\mathbb{Q}(\zeta_m)$ e $\mathbb{Q}(\zeta_n)$ são linearmente disjuntos e $\mathbb{Q}(\zeta_m)\cdot\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$. O resultado segue aplicando o Corolário anterior. ■

**Teorema 3.5** *Seja $K$ um Corpo de Números Abeliano de Condutor $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ e $p$ o menor número primo que divide $[K:\mathbb{Q}]$. Então*

$$\max\left\{\frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\frac{\phi(m)}{p_i-1}}}, m^{(1-\frac{1}{p})[K:\mathbb{Q}]}\right\} \le |\mathrm{Disc}(K)| \le m^{[K:\mathbb{Q}]-1}.$$

**Prova.** Temos:

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

Por outro lado, temos:

$$\begin{aligned}\alpha_i &\leq \sum_{r=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]\\ &\leq \sum_{r=1}^{\alpha_i}[\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]\\ &\leq \sum_{r=1}^{\alpha_i}\phi(m/p_i^r)=\frac{\phi(m)}{p_i-1}.\end{aligned}$$

Daí,

$$\begin{aligned}\frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k}p_i^{\frac{\phi(m)}{p_i-1}}} &\leq \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k}p_i^{\sum_{r=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]}}\leq\frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k}p_i^{\alpha_i}}\\ \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k}p_i^{\frac{\phi(m)}{p_i-1}}} &\leq \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k}p_i^{\sum_{r=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]}}\leq\frac{m^{[K:\mathbb{Q}]}}{m}=m^{[K:\mathbb{Q}]-1},\end{aligned}$$

isto é,

$$\frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k}p_i^{\frac{\phi(m)}{p_i-1}}}\leq|\mathrm{Disc}(K)|\leq m^{[K:\mathbb{Q}]-1} \tag{3.3}$$

Temos também:

$$\alpha_i\leq\sum_{r=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]\leq\sum_{r=1}^{\alpha_i}[K:\mathbb{Q}]/p=\alpha_i[K:\mathbb{Q}]/p,$$

onde $p$ é o menor número primo que divide $[K:\mathbb{Q}]$.

Logo,

$$\begin{aligned}
\frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i[\mathbb{K}:\mathbb{Q}]/p}} &\leq \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\sum_{r=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]}} \leq \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\alpha_i}} \qquad (3.4)\\
\frac{m^{[K:\mathbb{Q}]}}{m^{[\mathbb{K}\,\mathbb{Q}]/p}} &\leq \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\sum_{r=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]}} \leq \frac{m^{[K:\mathbb{Q}]}}{m} = m^{[K:\mathbb{Q}]-1}\\
m^{[K:\mathbb{Q}]-[K:\mathbb{Q}]/p} &\leq |\mathrm{Disc}(K)| \leq m^{[K:\mathbb{Q}]-1}\\
m^{(1-\frac{1}{p})[K:\mathbb{Q}]} &\leq |\mathrm{Disc}(K)| \leq m^{[K:\mathbb{Q}]-1}
\end{aligned}$$

O Teorema é uma conseqüência das desigualdades (3.3 e 3.4). ■

# Referências Bibliográficas


[Bor] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[Con] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 2nd. ed., Springer-Verlag, New York, 1998.

[Cas] A. Cassels, *An Introduction to Geometry of Numbers*. Springer-Verlag, 1971

[Cra] M. Craig, "A cyclotomic construction for Leech´s lattice" *Mathematika*, vol 25, pp 236-241.

[Lan] S. Lang, *Algebraic Number Theory*, Addison-Wesley; Reading, Massachusetts, 1970.

[Oth] J .O. D. Lopes, "Discriminants of subfields of $\mathbb{Q}(\zeta_{2^r})$," a aparecer em *Journal of Algebra and Its Applications*.

[Mar] D. A. Marcos, *Numbers Fields*. Springer-Verlag, New York, 1977.

[Mol] R. A. Mollin, *Algebraic Number Theory*, Chapman & Hall/CRC, Boca Raton, FL, 1999.

[Tra] T. P. da Nóbrega Neto, J. C. Interlando and J. O. D. Lopes, "On computing discriminants of subfields of $\mathbb{Q}(\zeta_{p^r})$," *Journal of Number Theory* 96, 319-325 (2002).

[Rot] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th ed., Springer-Verlag, New York, 1995.

[Rib] P. Ribenboin, *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.

[Sam] P. Samuel, *Algebraic Theory of Numbers*, Hermann, Paris, 1970.

[Ste1] I. N. Stewart, *Galois Theory*, 2nd. ed., Chapman & Hall/CRC, London, 1990.

[Ste2] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*, 2nd. ed., Chapman & Hall, London, 1992.

[Was] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd. ed., Springer-Verlag, New York, 1997.