Universidade Estadual Paulista

Câmpus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Corpos cujo condutor é potência de primo: caracterização e reticulados ideais associados

Eduardo Rogério Fávaro

Orientador: Prof. Dr. Antonio Aparecido de Andrade
Co-orientador: Prof. Dr. Trajano Pires da Nóbrega Neto

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

São José do Rio Preto

02 de Agosto de 2012

Eduardo Rogério Fávaro[1]

Corpos cujo condutor é potência de primo: caracterização e reticulados ideais associados

Orientador: ***Prof. Dr. Antonio Aparecido de Andrade***
Co-orientador: ***Prof. Dr. Trajano Pires da Nóbrega Neto***

Tese apresentada para obtenção do título de Doutor em Matemática, área de Matemática junto ao Programa de Pós-Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto.

Banca Examinadora

Prof. Dr. Antonio Aparecido de Andrade
UNESP - São José do Rio Preto
Orientador

Profa. Dra. Cleonice Fátima Bracciali
UNESP - São José do Rio Preto

Prof. Dr. Reginaldo Palazzo Jr.
UNICAMP - Campinas

Profa. Dra. Sueli Irene Rodrigues Costa
UNICAMP - Campinas

Prof. Dr. Carlile Campos Lavor
UNICAMP - Campinas

UNESP - São José do Rio Preto
02 de Agosto de 2012

[1]Bolsista Fapesp, processo 2007/07478-2

Aos meus pais, Anísio e Antônia,
com muito amor e carinho.

Ao desenvolvimento e à difusão das ciências.

Agradecimentos

Gostaria de lembrar aqui de, alguns, daqueles que tornaram possível a realização deste trabalho. Por mais que eu me esforçasse jamais conseguiria colocar aqui uma lista completa das pessoas que me ajudaram, direta ou indiretamente, para a obtenção deste título. Fica aqui meu profundo agradecimento a todos, porém gostaria de destacar algumas pessoas.

Gostaria de agradecer minha família, em especial meu pais Anísio Fávaro e Antônia Espalaor Fávaro, pelo apoio e suporte durante toda minha vida acadêmica, sem contar o amor e apoio incondicionais ao longo de toda a vida, sem os quais eu não estaria aqui.

Agradeco a todos os professores que me auxiliaram durante este trajeto, desde a graduação até o doutorado. Em especial, gostaria de agradecer ao Prof. Dr. Antonio Aparecido de Andrade, pela paciência, motivação, compreensão, pelas broncas nos momentos necessários, entre outras coisas, durante todo este periodo de orientação, ao Prof. Dr. Trajano Pires da Nóbrega Neto pelo apoio e sugestões durante o trabalho. À Profa. Dra. Grabiele Nebe, que me recebeu durente meu estágio na Alemanha, junto à RWTH, com muitas contribuições neste trabalho, introduzindo novos conceitos e ferramentas para abordar os temas que vinham sendo trabalhados ao longo do doutorado, além da paciência e o gentil acolhimento.

À Profa. Dra. Maria Gorete Carreira de Andrade e ao Prof. Dr. Adalberto Spezamiglio, pelo tempo que perticipei do PET, tendo somente agradecimentos para fazer.

A todos os colegas do Ibilce, em especial os colegas de doutorado da minha turma, Rafael, Pedro e Tiago, e também ao Oyran, Ruikson e Rodiak, desde as primeiras disciplinas cursadas no programa de pós graduação. Aos colegas que compartinharam meu caminho desde a graduação, Cintya, Júnior, Gustavo e Jucilene. Ao Agnaldo e à Grasiele, por serem os "irmãos mais velhos" nesta área de pesquisa, sendo um exemplo a ser seguido, e pela amizade. Aos amigos que repartiram a casa durante esses longos anos, Julio, Durval, Pedro, Deivid, Beethoven, Eliel, Guilherme e Fernando.

Agradecemos à Fapesp pelo apoio financeiro, através do processo 2007/07478-2, que possibilitou a realização deste doutorado, como também pelo apoio financeiro durante a graduação, com a bolsa de iniciação científica, processo 2006/02508-8.

Resumo

Este trabalho está relacionado com a Teoria Algébrica dos Números e aplicações em Reticulados Ideais. Descrevemos os corpos cujo condutor é potência de primo. Quando o primo é dois, descrevemos também o anel de inteiros. Quando o primo é ímpar calculamos o discriminante de um modo alternativo ao existente na literatura. Neste caso, e quando o corpo tem como grau o próprio primo ímpar, descrevemos o anel de inteiros com uma base integral e a forma traço associada, além do mínimo euclidiano. Com isso, obtemos uma família de reticulados ideais de dimensão prima ímpar.

Abstract

This work is relate to Algebric Number Theory and applications in Ideal Lattices. We describe number fields with power prime conductor. In the case prime two, we showed the ring of integers. For odd prime, we give a new proof for formula of discrimanate. In the case that the the degree of the field is the odd prime, we describe the ring of integers, the trace form associated and the Euclidean minimum. With this, we have a family of ideal lattices in odd prime dimension.

Sumário

Introdução

Este trabalho foi motivado pelas várias construções de reticulados e reticulados ideais utilizando ferramentas algébricas, em especial, corpos de números e ordens sobre corpos de números, [1], [4], [5], [10], [11], [12], [29], [36]. A grande maioria desses métodos são baseados em corpos ciclotômicos ou corpos maximais de corpos ciclotômicos. Nesta linha tem sido obtidos resultados significativos, envolvendo reticulados e reticulados ideais com bons parâmetros, seja para a densidade de centro de reticulados no $\mathbb{R}^n$ ou para distância produto mínima de reticulados ideais, utilizando esses corpos. Por outro lado, existem uma enorme quantidade de corpos abelianos que podem ser utilizados para gerar reticulados. Para isso, é necessário conhecer algumas características sobre esses corpos abelianos, tais como, elemento gerador, discriminante, anel de inteiros e forma traço. Como o discriminante para corpos abelianos já é conhecido, [13], [24] e [18], este trabalho inicia-se pela caracterização de corpos de números abelianos contidos em extensões ciclotômicas cíclicas. Encontramos um gerador para cada subcorpo cujo condutor é uma potência de primo. Para alguns casos particulares apresentamos também o anel de inteiros.

Entretanto, para gerar reticulados e reticulados ideais é necessário o conhecimento do anel de inteiros e da forma traço. Para cada corpo de números de grau p e condutor p^2, onde p é um primo impar, obtemos o anel de inteiros e a forma traço associada. Para estes corpos, obtivemos o ideal reticulado gerado pelo anel de inteiros. Com isso, foi possível calcular o mínimo euclidiano, sendo provado que esses corpos satisfazem a conjectura de Minkowski.

De um modo geral, apresentamos neste trabalho a descrição de corpos cujo condutor é potência de um primo e no mínimo euclidiano para corpos de grau primo impar p e condutor p^2.

Neste sentido, a seguir listamos nossas principais contribuições do presente trabalho.

1. No Teorema 3.9, apresentamos uma nova demonstração para a fórmula do discriminante de corpos cujo condutor é um potência de um primo ímpar.

2. No Teorema 5.2 descrevemos uma expressão para os corpos de condutor potência de um primo ímpar.

3. No Teorema 6.2, descrevemos todos os corpos cujo condutor é potência do primo 2. Existem três famílias de corpos cujo condutor é potência do primo 2. Duas destas famílias, uma consistindo de corpos ciclotômicos e a outra consistindo de subcorpos maximais reais de corpos ciclotômicos, já são bem conhecidos os anéis de inteiros algébricos. A Proposição 6.4, que fornece os anéis de inteiros para os corpos da outra família, onde eram desconhecidos os respectivos anéis de inteiros.

4. No Teorema 7.2, apresentamos uma base integral para os corpos de grau p e condutor p^2, que é o único corpo que possui essas características, sendo p um primo ímpar, e no Corolário 7.3, apresentamos a matriz da forma traço para estes corpos. O anel de inteiros destes corpos gera um reticulado ideal integral.

5. No Teorema 7.3, apresentamos um limitante superior para o mínimo euclidiano do corpo de grau p e condutor p^2, onde p é um primo ímpar. Tal corpo satisfaz a conjectura de Minkowski.

A seguir, descreveremos brevemente os resultados presentes na literatura e, de forma mais detalhada, os resultados frutos deste trabalho.

No Capítulo 1, apresentamos a Teoria Algébrica dos Números, onde são introduzidos, na Seção 1.1, as extensões de corpos, os números algébricos e os inteiros algébricos. O Teorema 1.4, conhecido como Teorema Fundamental da Teoria de Galois, é o resultado mais importante da seção. O Corolário 5.1, como resultado do Teorema 1.4, classifica quais extensões ciclotômicas são cíclicas. Também são apresentadas as extensões quadráticas e ciclotômicas, que são exemplos de extensões de Galois. Na Seção 1.2, apresentamos o Teorema de Kronecker-Weber, que afirma que toda extensão abeliana finita está contida num corpo ciclotômico e, em seguida, definimos o condutor de uma extensão abeliana. Na Seção 1.3, apresentamos os principais resultados sobre integralidade, em especial, definimos o anel de inteiros algébricos de um corpo de números e introduzimos o conceito de base integral. Também são definidos a norma e o traço numa extensão de Galois, assim como os conceitos de homomorfismo real e imaginário, e a assinatura de um corpo de números. Dedicamos a Seção 1.4 aos anéis e módulos noetherianos e aos anéis de Dedekind, que são anéis em que vale a unicidade da fatoração de ideais fracionários em ideais primos, conforme o Lema 1.1. Também é definida a norma de um ideal integral. Na Seção 1.5, tratamos sobre ramificação. Sendo $L|K$ uma extensão de corpos, apresentamos a decomposição de um ideal primo de $\mathcal{O}_K$ em ideais primos de $\mathcal{O}_L$. São definidos os principais fatos sobre essa decomposição e, também, a igualdade fundamental para uma extensão separável. O Teorema 1.16 fornece o Teorema de Kummer, um método computacional para fatorar um ideal primo numa extensão, do qual apresentamos alguns exemplos de decomposição.

No Capítulo 2, apresentamos os números p-ádicos, introduzidos no início do século XX, pelo matemático Kurt Hensel (1861-1941). Na Seção 2.1, são apresentados as localizações e os anéis de frações, em especial a localização de um anel em um ideal primo $\mathfrak{p}$. Também são definidos anel de valorização discreta e a função valorização. Na Seção 2.2, são introduzidos os inteiros p-ádicos e os números p-ádicos, resultando nos anéis de inteiros p-ádicos e nos corpos de números p-ádicos. Também apresentamos o conceito de extensão fracamente ramificada. Na Seção 2.3, definimos a valorização p-ádica sobre os corpos p-ádicos, dessa forma, finalizando o capítulo.

No Capítulo 3, apresentamos os resultados de diferente e discriminante, onde na Seção 3.1, apresentamos o conceito de discriminante e, em especial, o discriminante de uma extensão, o discriminante de um corpo de números e o discriminante absoluto de um corpo de números, assim como alguns fatos sobre o discriminante. A Proposição 3.4 apresenta uma condição necessária e suficiente para um conjunto ser uma base integral para uma extensão. Na Seção 3.2, apresentamos os principais resultados para o cálculo do discriminante conhecidos na literatura. Na Seção 3.3, a partir do $\mathcal{O}_L$-módulo dual, apresentamos o codiferente de uma extensão, que é um ideal fracionário. O inverso multiplicativo do codiferente é o diferente. Em seguida, apresentamos o conceito de ideal discriminante, que está diretamente relacionado com o diferente. Na Seção 3.4, utilizando os corpos de números p-ádicos, o ideal discriminante e o diferente, partindo da Proposição 3.5, provamos o Teorema 3.9, que fornece o discriminante absoluto de corpos de números cujo condutor é uma potência de um primo ímpar, de um modo alternativo à referência [24]. Ressaltamos que a demonstração para o Teorema 3.9, presente em [24], é baseada nos caracteres de Dirichlet. Neste trabalho apresentamos uma demonstração fazendo uso de corpos p-ádicos e do diferente. Também são apresentadas algumas consequências desse resultado.

No Capítulo 4, apresentamos os conceitos de reticulados e a Conjectura de Minkowski. Na Seção 4.1, apresentamos os reticulados no $\mathbb{R}^n$, que são subconjuntos discretos contidos no espaço euclidiano n-dimensional $\mathbb{R}^n$ que formam um grupo aditivo. Também apresentamos as matrizes geradora e de Gram de um reticulado, onde a matriz geradora caracteriza o reticulado. Também foram estabelecidos quando dois reticulados são equivalentes e congruentes. Na Seção 4.2, apresentamos o homomorfismo canônico ou de Minkowski, geradores de reticulados no $\mathbb{R}^n$ a partir de ideais fracionários de corpos de números. Definimos, na Seção 4.3, os reticulados ideais, inicialmente como uma generalização para os reticulados. Na Seção 4.4, apresentamos o homomorfismo torcido, que generaliza o homomorfismo de Minkowski apresentado na Seção 4.2, sendo o homomorfismo de Minkowski um caso particular do homomorfismo torcido. Também provamos que, em determinadas situações, reticulados ideais e reticulados no $\mathbb{R}^n$ são equivalentes. Na Seção 4.5, apresentamos o mínimo euclidiano, sendo este baseado no algoritmo de Euclides. De modo informal, o mínimo euclidiano mede o quanto distante está o corpo de números de ser um corpo euclidiano. Com isso, reunimos todas as definições necessárias para apresentar a conjectura de Minkowski, na Seção 4.6. A conjectura de Minkowski foi apresentada inicialmente para reticulados no $\mathbb{R}^n$ e, posteriormente,

foi estendida para corpos de números totalmente reais, utilizando o mínimo euclidiano. Finalmente, na Seção 4.7, apresentamos algumas cotas para o mínimo euclidiano conhecidas. Destacamos que, embora a conjectura de Minkowski seja para corpos de números totalmente reais, o limitante também vale para outros corpos. Em particular, apresentamos o resultado para corpos ciclotômicos.

Detalhamos, a seguir, as partes centrais deste trabalho. Os Capítulos 1, 2 e 4 são pré-requisitos para o presente trabalho e não apresentam nenhuma de nossas contribuições. Deste modo, nos Capítulos 3, 5, 6 e 7 apresentamos as contribuições sobre a obtenção de subcorpos de corpos ciclotômicos com seus respectivos anéis de inteiros e, também, aplicações na construção de reticulados ideais.

Capítulo 3

Seja K um corpo de números cujo condutor é p^n, onde p é um primo ímpar, e $L = \mathbb{Q}(\xi)$ o p^n-ésimo corpo ciclotômico, onde $\xi = \xi_{p^n}$. Para calcular o discriminante de K utilizamos os corpos p-ádicos e o diferente. Sejam $L_p = \mathbb{Q}_p(\xi_p) = L\mathbb{Q}_p$ e K_p o subcorpo de L_p de grau ep^{n-1}. Observamos que $K_p = K\mathbb{Q}_p$. Como $\mathfrak{d}_{L_p|\mathbb{Q}_p} = \mathfrak{d}_{L|\mathbb{Q}}$ e $\mathfrak{d}_{K_p|\mathbb{Q}_p} = \mathfrak{d}_{K|\mathbb{Q}}$, segue que é suficiente calcular $\mathfrak{d}_{K_p|\mathbb{Q}_p}$.

Com esta notação, apresentamos uma nova demonstração para a fórmula do discriminante de corpos de números cujo condutor é uma potência de um primo ímpar, que é sumarizada nos seguintes resultados.

Lema 3.2. O discriminante absoluto do corpo p-ádico K_p é dado por

$$|d_{K_p|\mathbb{Q}_p}| = p^a,$$

onde $a = e[(n+1)p^{n-1} - \dfrac{p^n - 1}{p-1}] - 1$.

Como consequência obtemos o seguinte teorema.

Teorema 3.9. Se K é o subcorpo de $\mathbb{Q}(\xi_{p^n})$ de grau ep^{n-1}, com p um primo ímpar e $e|p-1$, então

$$|d_{K|\mathbb{Q}}| = p^a,$$

onde $a = e[(n+1)p^{n-1} - \dfrac{p^n - 1}{p-1}] - 1$.

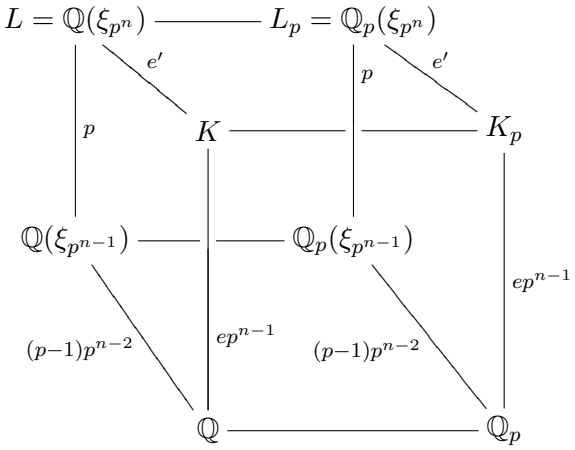

Figura 3.1: Relação entre corpos de números e corpos de números p-ádicos.

Corolário 3.1. Se K é o subcorpo de $\mathbb{Q}(\xi_p)$ de grau e, então

$$|d_K| = p^{e-1}.$$

Corolário 3.2. Se K é o subcorpo de $\mathbb{Q}(\xi_{p^2})$ de grau p, então

$$|d_K| = p^{2(p-1)}.$$

Capítulo 5

O objetivo deste é apresentar uma descrição para os corpos de números cujo condutor é p^r, onde p é um primo ímpar. Para isso, sejam $L = \mathbb{Q}(\xi_{p^r})$ o p^r-ésimo corpo ciclotômico e K um subcorpo de L com condutor p^r. Na Seção 5.1, são apresentados os principais resultados sobre extensões cíclicas conhecidos na literatura, tais como.

Proposição 5.1. Seja $L = \mathbb{Q}(\xi_n)$ o n-ésimo corpo ciclotômico, com $n \in \mathbb{Z}$ um inteiro positivo. O grupo de Galois $G = Gal(L|\mathbb{Q})$ da extensão $L|\mathbb{Q}$ é isomorfo ao grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$, dos inteiros inversíveis módulo n.

Proposição 5.2. O grupo multiplicativo de $\mathbb{Z}/4\mathbb{Z}$ é cíclico, gerado pela imagem canônica de $3 \in \mathbb{Z}$ em $\mathbb{Z}/4\mathbb{Z}$. Se $r \geqslant 3$, então $(\mathbb{Z}/2^r\mathbb{Z})^* = \langle \alpha, \beta \rangle$ não é um grupo multiplicativo cíclico, onde α possui ordem multiplicativa 2 e β possui ordem 2^{r-2} no grupo multiplicativo $(\mathbb{Z}/2^r\mathbb{Z})^*$.

O próximo teorema classifica para quais valores de n, onde n é um inteiro positivo, o grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$ é cíclico.

Teorema 5.1. O grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$ é cíclico se, e somente se,

$$n = 2, 4, p^r \ ou \ 2p^r,$$

onde $p > 2$ é um primo ímpar e $r \geqslant 1$ é um inteiro.

Pelo Teorema Fundamental da Teoria de Galois (Teorema 1.4), tem-se quais extensões ciclotômicas são cíclicas.

Corolário 5.1. As únicas extensões ciclotômicas cíclicas dos racionais são $\mathbb{Q}(i)$ e $\mathbb{Q}(\xi_{p^r}) = \mathbb{Q}(\xi_{2p^r})$, onde p é um primo ímpar e $r > 0$ um inteiro.

Tem-se também o seguinte resultado que será utilizado no Capítulo 6.

Corolário 5.2. O número de subgrupos de um grupo cíclico é o número de divisores da ordem do grupo.

Como a extensão $L|\mathbb{Q}$ é cíclica, segue que para cada divisor k do grau de L sobre $\mathbb{Q}$, existe exatamente um subcorpo K de L com $[K : \mathbb{Q}] = k$. Assim, para encontrar um subcorpo de L de um grau previamente fixado n é suficiente encontrar um elemento algébrico θ com o referido grau. Por outro lado, provar diretamente pela definição que θ tem n potências linearmente independentes sobre $\mathbb{Q}$ não é uma tarefa fácil. Uma idéia interessante é utilizar os conjugados de θ.

Baseado no Teorema 1.2, segue o nossa contribuição mais importante desta seção, que será utilizado para obter o gerador do subcorpo de L.

Proposição 5.6. Seja $\theta \in L = \mathbb{Q}(\xi_{p^r})$. Se θ possui exatamente n conjugados distintos em L então o corpo $K = \mathbb{Q}(\theta)$ possui grau n sobre $\mathbb{Q}$. Além disso, K é o único subcorpo de L que possui grau n sobre $\mathbb{Q}$.

Na Seção 5.2, descrevemos explicitamente o corpo K, que é dado por $\mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi_{p^r})$. Para isso, considere $\varphi(x) = \varphi_{p^r}(x) = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + x^{(p-1)p^{r-1}}$ o p^r-ésimo polinômio ciclotômico e $n = \phi(p^r) = (p-1)p^{r-1}$, onde ϕ é a função de Euler. Sejam σ um gerador de $Gal(L|\mathbb{Q})$ e $\alpha \in \mathbb{Z}$ um inteiro positivo com $0 < \alpha < p^r$ tal que $\sigma(\xi) = \xi^\alpha$. Desse modo, tem-se que

$$\begin{aligned} Gal(L|\mathbb{Q}) &= \{\sigma, \sigma^2, \ldots, \sigma^{(p-1)p^{r-1}} = Id_L\}, \\ Gal(K|\mathbb{Q}) &= \{\sigma_{|K}, \sigma_{|K}^2, \ldots, \sigma_{|K}^{ep^{r-1}} = Id_K\} \text{ e} \\ Gal(L|K) &= \{\sigma^{ep^{r-1}}, \sigma^{2ep^{r-1}}, \ldots, \sigma^{(p-1)p^{r-1}} = Id_L\}. \end{aligned}$$

A próxima proposição é utilizada diretamente na Proposição 5.10, onde é demonstrado que os conjugados de θ são distintos, o que, juntamente com a Proposição 5.6, resulta no Teorema 5.2, que fornece a descrição do subcorpo K, que pode ser expresso como $\mathbb{Q}(\theta)$.

Proposição 5.7. Seja $h \in \mathbb{Z}[x]$ um polinômio de grau $\leqslant p^r - 1$. Se $h(\xi) = 0$ então $h = \varphi g$, onde $g \in \mathbb{Z}[x]$ é um polinômio de grau $\leqslant p^{r-1} - 1$ e h tem lp termos não nulos, onde l é o número de termos não nulos de g.

Para cada $n \in \mathbb{Z}$, denotamos por n' o representante da classe lateral $n + p^r\mathbb{Z}$ em $\mathbb{Z}/\mathbb{Z}_{p^r}$, onde n' é um inteiro positivo com $0 < n' \leqslant p^r$ e $\alpha'_{j,s} = (\alpha^{jep^{r-1}+s})'$. Com isso, obtemos uma outra expressão para os conjugados de θ.

Lema 5.2. Se $f_s(x) = x^{\alpha'_{1,s}} + x^{\alpha'_{2,s}} + \cdots + x^{\alpha'_{p-1,s}}$, então f_s é um polinômio de grau $\leqslant p^r - 1$ e $\sigma^s(\theta) = f_s(\xi)$.

Desse modo, tem-se na Proposição 5.10 que todos os conjugados de θ em K são distintos. O resultado mais importante do capítulo é dado pelo seguinte teorema.

Teorema 5.2. Seja K um subcorpo de $L = \mathbb{Q}(\xi)$ com $[L : K] = e'$, onde $e, e' > 1$ são inteiros com $ee' = p - 1$. Se $\theta = Tr_{L|K}(\xi)$ então K é o único subcorpo de L cujo grau é ep^{r-1}, $K = \mathbb{Q}(\theta)$ e o discriminante absoluto de K é dado por $|d_K| = p^a$, onde $a = e[(n+1)p^{n-1} - \dfrac{p^n - 1}{p - 1}] - 1$.

A figura abaixo apresente um diagrama dos subcorpos utilizados no Teorema 5.2.

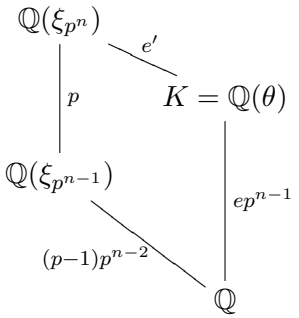

Figura 5.1: Subcorpo de $\mathbb{Q}(\xi_{p^r})$ e grau ep^{r-1}.

Apresentamos, na Seção 5.3, uma nova demonstração da descrição dos subcorpos K do p-ésimo corpo ciclotômico $\mathbb{Q}(\xi_p)$, conforme os seguintes resultados.

Lema 5.5. O subcorpo K do p-ésimo corpo ciclotômico $L = Q(\xi_p)$ é dado por $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi)$.

Teorema 5.3. O subcorpo K do p-ésimo corpo ciclotômico $L = \mathbb{Q}(\xi_p)$ é dado por $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi)$, os conjugados de θ em K formam uma base integral para o anel de inteiros $\mathcal{O}_K$ de K, e o discriminante absoluto de K é dado por $|d_K| = p^u$, onde $u = [K : \mathbb{Q}] - 1$.

A figura a seguir apresenta um diagrama dos subcorpos utilizados no Teorema 5.3.

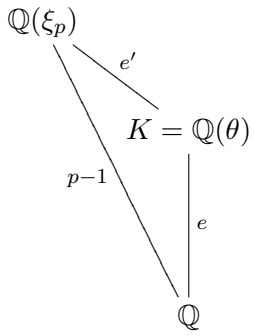

Figura 5.2: Subcorpo de $\mathbb{Q}(\xi_p)$ e grau e.

Na Seção 5.4, apresentamos os corpos de condutor potência de 3, onde provamos que apenas corpos ciclotômicos e corpos maximais reais de corpos ciclotômicos podem possuir condutor potência de 3, onde os corpos podem ser vistos na figura abaixo.

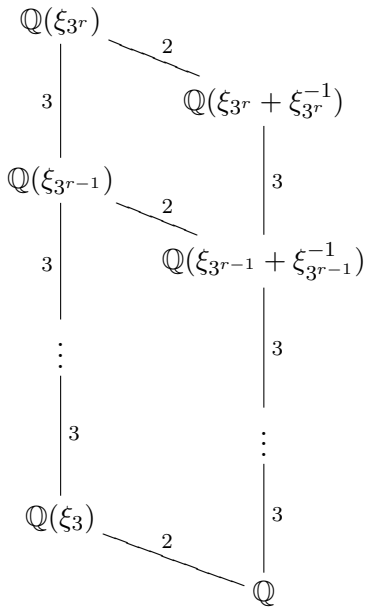

Figura 5.3: Subcorpos de $\mathbb{Q}(\xi_{3^r})$.

O próximo corolário é o principal resultado desta seção.

Corolário 5.3. Se K é um subcorpo de L, com $[K : \mathbb{Q}] \neq 1$, então existe um inteiro positivo s, com $s \leqslant r$, tal que $K = \mathbb{Q}(\xi_{3^s})$ ou $K = \mathbb{Q}(\xi_{3^s} + \xi_{3^s}^{-1})$. Se $K = \mathbb{Q}(\xi_{3^s})$ então o anel de inteiros de K é $\mathcal{O}_K = \mathbb{Z}[\xi_{3^s}]$, e o discriminante absoluto de K é $3^{2[(r+1)3^{r-1}-(3^r-1)/2]-1}$. Se $K = \mathbb{Q}(\xi_{3^s} + \xi_{3^s}^{-1})$, então o anel de inteiros de K é $\mathcal{O}_K = \mathbb{Z}[\xi_{3^s} + \xi_{3^s}^{-1}]$, e o discriminante absoluto é dado por 3^a, onde $a = [(r+1)3^{r-1} - (3^r - 1)/2] - 1$.

Capítulo 6

O Capítulo 6 é motivado pela conjectura apresentada no trabalho de Girald et al. [12], 1997, a saber, que o homomorfismo canônico do anel de inteiros de $\mathbb{Q}[\theta]$, onde $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2}}}$, pode ser utilizado para construir um reticulado $\mathbb{Z}^n$-rotacionado. Surgiu a ideia de provar que tal corpo é o subcorpo maximal de um 2^r-ésimo corpo ciclotômico $L = \mathbb{Q}(\xi)$, onde $\xi = \xi_{2^r}$ é uma raiz p^r-ésima primitiva da unidade e $r > 1$ é um inteiro positivo. Note que não existe um método na literatura que descreva a estrutura de um subcorpos K de $\mathbb{Q}(\xi_{2^r})$, exceto quando K é um subcorpo maximal. Pela Proposição 5.2, tem-se que a extensão $\mathbb{Q}(\xi)|\mathbb{Q}$ não é uma extensão cíclica, sendo que o grupo de Galois é gerado por dois elementos, um de ordem 2 e outro de ordem 2^{r-2}. A Seção 6.1, é destinada a obter a quantidade de subcorpos que L possui, sendo o resultado mais importante da seção dado pelo seguinte corolário.

Corolário 6.2. O número de subcorpos de L é $2 + 3(r - 2)$.

O objetivo da Seção 6.2 é encontrar todos os subcorpos que L possui, assim como os respectivos anéis de inteiros e o discriminante absoluto, onde consideramos $r > 2$.

Lema 6.3. Se $\gamma \in \mathbb{R}$, então $\cos(\gamma) = \pm\sqrt{\dfrac{1 + cos(2\gamma)}{2}}$.

Proposição 6.2. Se $\xi_{2^k} = e^{\frac{2\pi i}{2^k}}$ é uma raiz 2^k-ésima primitiva da unidade, então

$$\xi_{2^k} + \xi_{2^k}^{-1} = 2\cos(\frac{2\pi}{2^k}) = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}.$$

Introduzindo a notação $\theta_k = \xi_{2^k} + \xi_{2^k}^{-1} = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$, onde o algarismo 2 aparece $k - 2$ vezes, e $\theta_k' = -i(\xi_{2^k} - \xi_{2^k}^{-1}) = \sqrt{2 - \sqrt{2 + \cdots + \sqrt{2}}}$, onde o algarismo 2 aparece $k - 2$ vezes, obtém-se a relação

$$\xi_{2^k} = \frac{1}{2}(\theta_k + i\theta_k'),$$

sendo o seguinte teorema o resultado mais importante desta seção.

Teorema 6.2. Os subcorpos de $L = \mathbb{Q}(\xi_{2^r})$, onde $r \geqslant 3$ é um inteiro positivo, são $\mathbb{Q}$, $\mathbb{Q}(\xi_{2^j})$, para $j = 2, 3, \ldots, r$ e $\mathbb{Q}(\theta_k)$, $\mathbb{Q}(i\theta_k)$, para $k = 3, 4, \ldots, r$, com $\theta_k = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$,

onde o algarismo 2 aparece $k-2$ vezes.

Na Figura 6.1 temos um diagrama dos subcorpos do Teorema 6.2, onde, para deixar o gráfico mais claro, omitimos algumas inclusões.

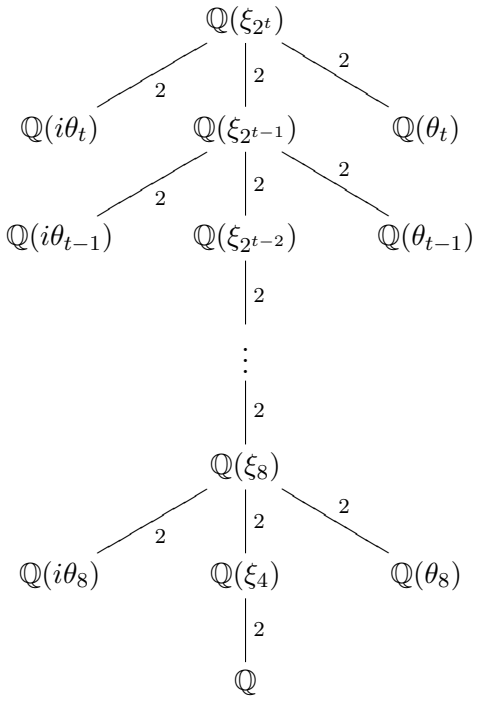

Figura 6.1: Subcorpos de $\mathbb{Q}(\xi_{2^r})$.

Uma vez que encontramos os subcorpos, é necessário encontrar o anel de inteiros de $\mathbb{Q}(i\theta)$, que é descrito nos seguintes resultados.

Proposição 6.4. Para todo $k > 2$ inteiro positivo, o anel de inteiros de $\mathbb{Q}(i\theta_k)$ é $\mathbb{Z}[i\theta_k]$.

Corolário 6.3. Para o subcorpo $\mathbb{Q}(\xi_{2^j})$ de $L = \mathbb{Q}(\xi_{2^r})$, como no Teorema 6.2, o discriminante absoluto é dado por 2^β, onde $\beta = (j-1)2^{j-1}$, e o anel de inteiros é $\mathbb{Z}[\xi_{2^r}]$. Se o subcorpo é $\mathbb{Q}(\theta_{k+1})$ ou $\mathbb{Q}(i\theta_{k+1})$ então o discriminante absoluto é dado por 2^β, onde $\beta = k2^{k-1} - 1$, e o anel de inteiros é dado por $\mathbb{Z}[\theta_{k+1}]$ ou $\mathbb{Z}[i\theta_{k+1}]$, respectivamente.

Na Seção 6.3, apresentamos a construção presente em [1] de reticulados $\mathbb{Z}^n$-rotacionados sobre o subcorpo maximal real $\mathbb{Q}(\theta)$ do 2^r-ésimo corpo ciclotômico $\mathbb{Q}(\xi_{2^r})$, onde, pela Seção 6.2, tem-se que $\theta = \xi_{2^r} + \xi_{2^r}^{-1} = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$. Uma construção similar pode ser encontrada em [29].

Proposição 6.5. Para todo p primo ímpar e r inteiro positivo, tem-se que

$$Tr_{\mathbb{Q}(\xi_{p^r})|\mathbb{Q}}(\xi_{p^r}^k) = \begin{cases} 0, & \text{se } \mathrm{mdc}(k,p^r) < p^{r-1}; \\ -p^{r-1}, & \text{se } \mathrm{mdc}(k,p^r) = p^{r-1}; \\ (p-1)p^{r-1}, & \text{se } \mathrm{mdc}(k,p^r) > p^{r-1}. \end{cases}$$

Quando $p = 2$, para o subcorpo maximal K de L tem-se o seguinte corolário.

Corolário 6.4. Se $K = \mathbb{Q}(\xi + \xi^{-1})$ então

$$Tr_{K|\mathbb{Q}}(\xi^k + \xi^{-k}) = \begin{cases} 0, & \text{se } \mathrm{mdc}(k,2^r) < 2^{r-1}; \\ -2^{r-1}, & \text{se } \mathrm{mdc}(k,2^r) = 2^{r-1}; \\ 2^{r-1}, & \text{se } \mathrm{mdc}(k,2^r) > 2^{r-1}. \end{cases}$$

Proposição 6.6. Considere $e_0 = 1$ e $e_j = \xi^j + \xi^{-j}$, para $j = 1, 2, \ldots, 2^{r-2} - 1$.

i) Se $j = 1, 2, \ldots, 2^{r-2} - 1$, então $Tr_{K|\mathbb{Q}}(e_j e_j) = \begin{cases} -2^{r-1}, & \text{se } j = 0; \\ 0, & \text{caso contrário.} \end{cases}$

ii) Se $j \neq 0$, então $Tr_{K|\mathbb{Q}}(e_j e_0) = \begin{cases} -2^{r-1}, & \text{se } j = 1; \\ 0, & \text{se } j \neq 1. \end{cases}$

iii) Se $j \neq 0$, $k \neq 0$ e $j \neq k$, então $Tr_{K|\mathbb{Q}}(e_j e_k) = \begin{cases} -2^{r-1}, & \text{se } |j-k| = 1; \\ 0, & \text{se } |j-k| \neq 1. \end{cases}$

Além disso, a construção de um reticulado $\mathbb{Z}^n$-rotacionado é dada pela seguinte proposição:

Proposição 6.7. Sejam $K = \mathbb{Q}(\xi + \xi^{-1})$ o subcorpo maximal real do 2^r-ésimo corpo ciclotômico $\mathbb{Q}(\xi_{2^r})$ e $\alpha = (1-\xi)(1+\xi) = 2 - (\xi + \xi^{-1})$. Considere $f_j = \sum_{k=0}^{2^{r-2}-1} e_k$. O conjunto $\{f_0, f_1, \ldots, f_{2^{r-1}-1}\}$ é uma base integral para $\mathcal{O}_K$ que satisfaz

$$\frac{1}{2^{r-1}} Tr_{K|\mathbb{Q}}(\alpha f_j f_k) = \delta_{jk},$$

onde δ_{jk} é o delta de Kronecker, isto é, $\delta_{jk} = 0$, se $j \neq k$, e $\delta_{jj} = 1$. Assim, o reticulado ideal integral $(\mathcal{O}_K, q_\alpha)$ é um reticulado $\mathbb{Z}^n$-rotacionado, onde $q_\alpha : \mathcal{O}_K \times \mathcal{O}_K \longrightarrow \mathbb{Z}$ é a forma bilinear simétrica dada por $q_\alpha(x,y) = \frac{1}{2^{r-1}} Tr_{K|\mathbb{Q}}(\alpha xy)$, para todo $x, y \in \mathcal{O}_K$ e $n = 2^{r-2}$.

A Proposição 6.7, juntamente com o Corolário 6.3, fornece a resposta da conjectura dada em [12].

Capítulo 7

No Capítulo 7, trabalhamos sobre o corpo de grau p e condutor p^2, onde p é um primo ímpar. Sejam $L = \mathbb{Q}(\xi)$ o p^2-ésimo corpo ciclotômico e K o subcorpo de L de grau p. O objetivo é encontrar o maior número possível de informações sobre K. Neste sentido, são obtidos o anel de inteiros de K, uma base integral, o discriminante absoluto, a forma traço e um limitante para o mínimo euclidiano de K, e também provamos que o corpo K satisfaz a conjectura de Minkowski. Tem-se também que $\mathcal{O}_K$ gera um reticulado ideal, através do homomorfismo de Minkowski, onde são utilizadas as técnicas presentes em [3] e [22].

Proposição 7.1. Se $L = \mathbb{Q}(\xi_{p^2})$ e K é um subcorpo de L, com grau p, então $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi_{p_2})$, e o discriminante absoluto de K é dado por $|d_K| = p^{2(p-1)}$.

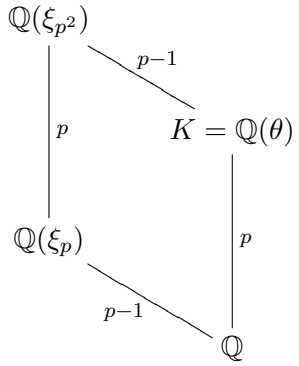

Figura 7.1: Subcorpo de $\mathbb{Q}(\xi_{p^2})$ e grau p.

Utilizando a descrição da forma traço dada em [22], segue a descrição para a forma traço sobre o corpo K, que é dado pelo seguinte corolário.

Corolário 7.1. Sejam $L = \mathbb{Q}(\xi_{p^2})$ o p^2-ésimo corpo ciclotômico e K é o subcorpo de L, com grau p. Se $\theta_j = Tr_{L|K}(\xi_{p^2})$ então

$$\begin{aligned}
Tr_{K|\mathbb{Q}}(\theta_p\theta_p) &= p; \\
Tr_{K|\mathbb{Q}}(\theta_p\theta_j) &= 0, && se\ \mathrm{mdc}(p,j) = 1; \\
Tr_{K|\mathbb{Q}}(\theta_i\theta_j) &= -p, && se\ \mathrm{mdc}(p,i) = \mathrm{mdc}(p,j) = 1, i \not\equiv j \pmod{p^2}; \\
Tr_{K|\mathbb{Q}}(\theta_j\theta_j) &= p(p-1), && se\ \mathrm{mdc}(p,j) = 1.
\end{aligned}$$

A seguir, definimos o reticulado $L_{b,n}$ e apresentamos o seu determinante, conforme [22].

Teorema 7.1. Sejam $n \in \mathbb{N}$ e $b \in \mathbb{R}$ com $b > n$. Se $L_{b,n}$ é um reticulado no $\mathbb{R}^n$ com

matriz de Gram dada por

$$A = bI_n - J_n = \begin{pmatrix} b-1 & -1 & \cdots & -1 \\ -1 & b-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & & b-1 \end{pmatrix},$$

onde I_n é a matriz identidade de ordem n e $J_n \in \{1\}^{n\times n}$ é uma matriz $n \times n$ com todas entradas 1, então $L_{b,n}$ é um reticulado definido positivo com determinante $(b-n)b^{n-1}$.

Como θ possui p conjugados, tomamos $p-1$ elementos no conjunto dos conjugados de θ, sendo esses elementos denotados por $\theta_{j_1}, \theta_{j_2}, \ldots, \theta_{j_{p-1}}$. Também denota-se $\theta_{j_0} = \theta_p$. Desse modo, tem-se o conjunto $\{\theta_{j_0}, \theta_{j_1}, \ldots, \theta_{j_{p-1}}\}$.

Lema 7.2. O conjunto $\{\theta_{j_0}, \theta_{j_1}, \ldots, \theta_{j_{p-1}}\}$ gera um reticulado com matriz de Gram dada por

$$p \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & p-1 & -1 & \cdots & -1 \\ 0 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & -1 & & p-1 \end{pmatrix}$$

e determinante $p^{2(p-1)}$.

No próximo teorema apresentamos o resultado mais importante deste capítulo, descrevendo uma base integral para $\mathcal{O}_K$ e a forma traço sobre K.

Teorema 7.2. Sejam K um subcorpo de $L = \mathbb{Q}(\xi_{p^2})$ de dado grau p, $\theta = Tr_{L|K}(\xi_{p^2})$ e $\theta_{j_0} = Tr_{L|K}(\xi_{p^2}^p) = Tr_{L|K}(\xi_p)$. O discriminante absoluto de K é $p^{2(p-1)}$. Se $\theta_{j_1}, \theta_{j_2}, \ldots, \theta_{j_{p-1}}$ são $p-1$ conjugados distintos de θ em K, então o conjunto $B = \{\theta_{j_0}, \theta_{j_1}, \ldots, \theta_{j_{p-1}}\}$ é uma base integral para o anel de inteiros $\mathcal{O}_K$ de K e a matriz de Gram do reticulado algébrico gerado a partir do anel de inteiros $\mathcal{O}_K$ de K, pelo homomorfismo canônico $\sigma : K \longrightarrow \mathbb{R}^p$, é a matriz A de ordem $p \times p$ dada por

$$A = p \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & p-1 & -1 & \cdots & -1 \\ 0 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & -1 & & p-1 \end{pmatrix}.$$

O reticulado ideal $(\mathcal{O}_K, Tr)$ é dado por:

Corolário 7.3. Sejam K um subcorpo de $L = \mathbb{Q}(\xi_{p^2})$ de dado grau p, $\theta = Tr_{L|K}(\xi_{p^2})$, $\theta_{j_0} = Tr_{L|K}(\xi_{p^2}^p) = Tr_{L|K}(\xi_p)$ e $B = \{\theta_{j_0}, \theta_{j_1}, \ldots, \theta_{j_{p-1}}\}$ uma base integral para K. A forma traço sobre K,

$$\begin{array}{rcl} Tr : K \times K & \longrightarrow & \mathbb{Q} \\ (x, y) & \longmapsto & Tr_{K|\mathbb{Q}}(xy), \end{array}$$

é caracterizada pela matriz

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & p-1 & -1 & \cdots & -1 \\ 0 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & -1 & & p-1 \end{pmatrix}.$$

Além disso, $(\mathcal{O}_K, Tr)$ é um reticulado ideal integral.

Finalmente, apresentamos na Seção 7.2 um método para calcular um limitante para o mínimo euclidiano de K, resultando que K satisfaz a conjectura de Minkowski, que é dado pelo seguinte teorema.

Teorema 7.3. O Mínimo Euclidiano do corpo K é dado por $M(K) \leqslant \dfrac{1}{2^p}\sqrt{|d_K|}$.

De modo geral, tem-se o seguinte corolário.

Corolário 7.4. Seja p um primo ímpar. Qualquer corpo de condutor p^2 e grau p satisfaz a conjectura de Minkowski.

Capítulo

1

Teoria Algébrica dos Números

Neste capítulo apresentamos os resultados básicos da teoria algébrica dos números que serão necessários para o desenvolvimento dos demais capítulos. Basicamente, todos os resultados contidos neste capítulo encontram-se no livro intitulado Algebraic Number Theory de J. Neukirch [23], Neste sentido, sempre que referimos a um inteiro primo ou um número primo estamos referindo a um inteiro positivo primo no anel dos inteiros $\mathbb{Z}$. Um corpo K está sempre contido nos números complexos. Além disso, neste e nos demais capítulos, salvo menção contrária, um anel é um domínio, isto é, um anel comutativo com unidade sem divisores próprios de zero. Usaremos indistintamente esses dois termos. Para cada $n \in \mathbb{Z}$ inteiro positivo, com $n > 2$, ξ_n é uma raiz n-ésima primitiva da unidade, que, quando não tiver ambiguidade, será denotada por ξ. O corpo $\mathbb{Q}(\xi_n)$ é o n-ésimo corpo ciclotômico.

Introduzimos, na Seção 1.1, as extensões de corpos, os números algébricos e inteiros algébricos. O Teorema 1.4, conhecido como Teorema Fundamental da Teoria de Galois, é o resultado mais importante da seção. Utilizando-o, o Corolário 5.1 classifica quais extensões ciclotômicas são cíclicas. Também são apresentadas as extensões quadráticas e ciclotômicas, as quais são exemplos de extensões de Galois. Na Seção 1.2, apresentamos o Teorema de Kronecker-Weber, que afirma que toda extensão abeliana finita está contida num corpo ciclotômico e, em seguida, definimos o condutor de uma extensão abeliana. Na Seção 1.3, apresentamos os principais fatos sobre integralidade, em especial, o anel de inteiros algébricos de um corpo de números e o conceito de base integral. São definidas a norma e o traço numa extensão de Galois, assim como os homomorfismos reais e imaginários, e a assinatura de um corpo de números. Na Seção 1.4 apresentamos os anéis e módulos noetherianos, e os anéis de

Dedekind, que são anéis em que vale a unicidade da fatoração de ideais fracionários, em ideais primos, conforme o Lema 1.1. Também definimos a norma de um ideal integral. Na Seção 1.5 tratamos sobre ramificação. Sendo $L|K$ uma extensão de corpos, é estudado a decomposição de um ideal primo de $\mathcal{O}_K$ em ideais primos de $\mathcal{O}_L$. São definidos os principais elementos nesta decomposição, e também a igualdade fundamental para uma extensão separável. O Teorema 1.16 fornece o Teorema de Kummer, que é um método computacional para fatorar um ideal primo numa extensão. Através deste método, apresentamos alguns exemplos de decomposição.

1.1 Extensões de corpos

Nesta seção, descrevemos brevemente o conceito de extensões de corpos, com enfoque em extensões de Galois, resultando no Teorema 1.4, conhecido como Teorema Fundamental da Teoria de Galois. Os resultados desta seção podem ser encontrados em livros de Teoria de Galois ou de Teoria Algébrica dos Números, por exemplo, [28], Capítulo VI, ou [33].

Sejam K e L corpos. Se $K \subseteq L$ diz-se que L é uma **extensão** do corpo K, que K é um **subcorpo** de L, ou que $L|K$ é uma **extensão de corpos**. Quando $L|K$ é uma extensão, admitimos que $L \subseteq \mathbb{C}$. O corpo L pode ser visto como um espaço vetorial sobre K, que possui uma dimensão.

Definição 1.1. *Seja $L|K$ uma extensão de corpos. A dimensão do K-espaço vetorial L, denotado por $[L : K]$, é chamado o* **grau** *da extensão $L|K$.*

Introduzimos, agora, os elementos algébricos numa extensão de corpos, que serão utilizados para definir os números algébricos e os inteiros algébricos.

Definição 1.2. *Sejam $L|K$ uma extensão de corpos e $\alpha \in L$. Se existe um polinômio sobre K, tal que α é raiz, então α é dito um* **elemento algébrico** *sobre K. O polinômio sobre K de menor grau e coeficientes inteiros que possui α como raiz é dito* **polinômio minimal** *de α sobre K.*

Note que o polinômio minimal de um elemento algébrico sobre K é sempre irredutível sobre K.

Definição 1.3. *Um* **corpo de números algébricos***, ou simplesmente um* **corpo de números***, é uma extensão finita K dos racionais $\mathbb{Q}$, com $K \subseteq \mathbb{C}$. Os elementos de K são ditos* **números algébricos***. O grau da extensão $K|\mathbb{Q}$ é o* **grau** *de K.*

Proposição 1.1. [*34, pag.*23] *Sejam $L|K$ uma extensão de corpos e $\alpha \in L$. O elemento α é um elemento algébrico sobre K se, e somente se, $K(\alpha)$ é uma extensão finita de K. Neste caso, $[K(\alpha) : K] = grau(p)$, onde p é o polinômio minimal de α sobre K, e $K(\alpha) = K[\alpha]$.*

Tem-se que todo número algébrico é raiz de um polinômio com coeficientes inteiros.

Definição 1.4. *Um número algébrico é dito* **integral**, *ou um* **inteiro algébrico**, *se ele é raiz de um polinômio mônico, não nulo, com coeficientes inteiros.*

Definição 1.5. *Uma extensão de corpos de números $L|K$ é dita ser uma* **extensão quadrática** *se $[L : K] = 2$. Um corpo de números K é dito um* **corpo quadrático** *quando $[K : \mathbb{Q}] = 2$.*

Definição 1.6. *Sejam K um corpo, $x \in K$ e $n \in \mathbb{Z}$. O elemento x é dito ser uma raiz n-ésima da unidade se $x^n = 1$. Se x é um raiz n-ésima da unidade e $x^k \neq 1$ para todo número natural $k < n$, dizemos que x é uma raiz n-ésima primitiva da unidade.*

Definição 1.7. *Sejam K um corpo de característica zero, ξ_n uma raiz n-ésima primitiva de unidade em uma extensão de K e $L = K[\xi_n]$. O corpo L é dito uma* **extensão ciclotômica** *de K. Quando $K = \mathbb{Q}$, o corpo $\mathbb{Q}(\xi_n)$, obtido a partir de $\mathbb{Q}$, adjuntando um raiz n-ésima primitiva da unidade ξ_n, é chamado n-***ésimo corpo ciclotômico**.

Teorema 1.1. [*34, pag.*41] *Se K é um corpo de números, então existe um inteiro algébrico $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$.*

Assim, todo corpo de números possui um elemento inteiro que o gera sobre os racionais. Com isso, é interessante encontrar um elemento gerador para cada corpo de números. Embora o teorema afirme que tal elemento exista, o método exige um certo custo computacional para encontrar um elemento gerador para o corpo.

Teorema 1.2. [*28*] *Se K é um corpo de característica zero ou um corpo finito, L uma extensão de grau finito n sobre K e C um corpo algebricamente fechado contendo K, então existe exatamente n K-isomorfismos de L com imagem em C.*

Seja L um corpo. Tem-se que o conjunto de todos automorfismos de L é um grupo com a operação composição de funções. Tomando G um grupo de automorfismos de L, isto é, um subgrupo de todos os automorfismos de L, dizemos que o conjunto

$$\{x \in L : \sigma(x) = x \text{ para todo } \sigma \in G\} \subseteq L.$$

é o corpo fixo de G.

Teorema 1.3. [*28, pag.*86] *Sejam K um corpo finito ou de característica zero e L uma extensão de L com grau finito n. A seguintes afirmações são equivalentes:*

i) K é o corpo fixo do grupo G de todos os K-automorfismos de L.

ii) Para qualquer $x \in L$, o polinômio minimal de x sobre K possui todas as raízes em L.

iii) L é gerado por todas as raízes de um polinômio com coeficientes em K.

Nas condições acima, o grupo G de todos K-automorfismos de L possui ordem n.

Se as condições do Teorema 1.3 são válidas, então L é dito uma **extensão de Galois** de K e o grupo $G = Gal(L|K)$ de todos K-automorfismos de L é dito **grupo de Galois** de L sobre K. Se, além disso, tivermos G um grupo abeliano ou cíclico então a extensão é dita **abeliana** ou **cíclica**, respectivamente.

Sejam K um corpo finito ou de característica zero e L uma extensão de K de grau finito n. Se H é um grupo de automorfismos de L tal que K é o corpo fixo de H, então L é uma extensão de Galois de K e H é o grupo de Galois de L sobre K.

Quando temos uma torre de extensões $K \subseteq L \subseteq M$ dizemos que L é um **corpo intermediário** da extensão $M|K$. Podemos, agora, enunciar o Teorema Fundamental da Teoria de Galois, que relaciona os subcorpos de um corpo de característica finita ou zero com os subgrupos do grupo de automorfismos de L.

Teorema 1.4 (Teorema Fundamental da Teoria de Galois)**.** [*28, pag.*87] *Sejam K um corpo finito ou de característica zero, L uma extensão de Galois finita de K e G o grupo de Galois de L sobre K. Para cada subgrupo G' de G associamos o corpo fixo $k(G')$ de G' e, para cada subcorpo K' de L contendo K, associamos o subgrupo $g(K')$ de G formado pelos K'-automorfismos de L.*

i) As funções g e k são bijetoras e uma é inversa da outra. Ambas são decrescentes com relação à inclusão sobre G e sobre L, isto é, elas invertem inclusões.

ii) Para que o corpo intermediário K' seja uma extensão de Galois de K é necessário e suficiente que $g(K')$ seja um subgrupo normal em G. Neste caso, o grupo de Galois da extensão K' sobre K pode ser identificado com o grupo quociente $G/g(K')$.

Note que dizer que uma função f inverte inclusões significa que, se $A \subseteq B$ são conjuntos do domínio da função f, então $f(B) \subseteq f(A)$.

Como exemplos de extensão de Galois, temos que as extensões quadráticas são extensões de Galois. De fato, se K é um corpo de característica zero e L é uma extensão de grau dois sobre K, então $L = K[\alpha]$, com $\alpha \in L$ uma raiz de um polinômio em x da forma $x^2 - d \in K[x]$ e $d \in K$ livre de quadrados. Como as duas raízes de $x^2 - d$ são $\alpha, -\alpha \in L$, segue que L é uma extensão de Galois de K.

As extensões ciclotômicas também são extensões de Galois. De fato, sejam K um corpo de característica zero, ξ_n uma raiz n-ésima primitiva de unidade em uma extensão de K e $L = K[\xi_n]$. Como o polinômio minimal de ξ_n sobre K divide $x^n - 1$ em $K[x]$, segue que todas as raízes do polinômio minimal de ξ_n sobre K são raízes n-ésimas da unidade e, assim, potências de ξ_n. Logo, todas as raízes do polinômio minimal de ξ_n sobre K estão em L e, portanto, a extensão é de Galois.

Definição 1.8. *Uma corpo L é dito algebricamente fechado quando todo polinômio com coeficientes em K possui uma raiz em L. Dada um corpo K, o menor corpo algebricamente fechado L que contém K é dito fecho algébrico de K.*

Definição 1.9. *Sejam K um corpo, $f \in K[x]$ um polinômio sobre K e L o fechamento algébrico de K. Se todos as raízes de f em L são simples então f é dito um* **polinômio separável**.

Se K é um corpo com característica zero então todo polinômio sobre K é separável.

Definição 1.10. *Uma extensão $K|L$ é dita* **separável** *se todo elemento $\alpha \in L$ é raiz de um polinômio separável sobre K.*

Toda extensão finita de corpos de números é separável

1.2 Teorema de Kronecker-Weber

O Teorema de Kronecker-Weber (Teorema 1.5) afirma que qualquer extensão finita abeliana dos racionais esta contida em um corpo ciclotômico. A primeira afirmação é devida à Kronecker, em 1853, mas a prova era incompleta, tendo dificuldades em extensões de grau potência de 2. A primeira prova foi dada por Weber em 1886, entretanto, ainda havia algumas lacunas. Ambas as provas, a de Kronecker e a de Weber, utilizavam os resolventes de Lagrange. Em 1896, Hilbert apresentou outra demonstração utilizando análise e ramificação de grupos. Atualmente, esse teorema é dado como uma consequência da teoria dos corpos de classes. Uma demonstração do Teorema 1.5 pode ser encontrada em [37], onde o Capítulo 14 é dedicado a esse resultado.

Teorema 1.5 (Teorema de Kronecker-Weber)**.** *[37] Se $K|\mathbb{Q}$ é uma extensão abeliana finita, então*

$$K \subseteq \mathbb{Q}(\xi_n),$$

para algum $n \in \mathbb{Z}$ inteiro positivo e ξ_n uma raiz n-ésima primitiva da unidade.

Seja K um extensão abeliana finita dos racionais $\mathbb{Q}$. Como, pelo Teorema 1.5, toda extensão abeliana finita dos racionais está contida num corpo ciclotômico, podemos tomar o menor n tal que $K \subseteq \mathbb{Q}(\xi_n)$.

Definição 1.11. *O menor $n \in \mathbb{N}$ tal que $K \subseteq \mathbb{Q}(\xi_n)$ é denominado* **condutor do corpo** K.

Assim, sempre que falarmos de condutor de um corpo de números abeliano, estamos admitindo o Teorema de Kronecker-Weber que afirma que todo corpo de números abeliano está contido num corpo ciclotômico.

Exemplo 1.1. *Seja $K = \mathbb{Q}(\sqrt{2})$ um corpo quadrático. Temos que $K \subseteq \mathbb{Q}(\xi_8)$ e $K \not\subseteq \mathbb{Q}(\xi_4)$. O condutor de K é 8.*

Exemplo 1.2. *Seja $K = \mathbb{Q}(\xi_n + \xi_n^{-1})$ o corpo maximal real do n-ésimo corpo ciclotômico $\mathbb{Q}(\xi_n)$. O condutor de K é n.*

1.3 Integralidade e corpos de números

Apresentamos, nesta seção, os conceitos de elementos inteiros, anéis de inteiros e suas principais propriedades. Apresentamos também a norma e o traço numa extensão separável, homomorfismo real e homomorfismo imaginário.

Definição 1.12. *Seja $A \subseteq B$ uma extensão de anéis. Um elemento $b \in B$ é dito* **inteiro** *sobre A se satisfaz uma equação mônica*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0,$$

com coeficientes $a_i \in A$, para $i = 0, 1, \ldots, n-1$. O anel B é dito **inteiro** *sobre A se todos os elementos $b \in B$ são inteiros sobre A.*

Definição 1.13. *O conjunto*

$$\mathcal{O}_B = \{b \in B; b \text{ é inteiro sobre } A\},$$

na extensão de anéis $A \subseteq B$, é dito **fecho inteiro** *de A em B*

Proposição 1.2. [*23*] *O fecho inteiro $\mathcal{O}_B$ de A em B, onde $A \subseteq B$ são anéis, forma um anel, e é dito* **fecho inteiro**.

Definição 1.14. *O anel A é dito* **integralmente fechado** *em B se $A = \mathcal{O}_B$. Assim, $\mathcal{O}_B$ é integralmente fechado em B. Se K é o corpo de frações de A, o fecho inteiro $\mathcal{O}_K$ de A em K é dito a* **normalização** *de A, e A é* **integralmente fechado** *quando $A = \mathcal{O}_K$.*

Seja K um corpo de números. Conforme a Definição 1.4, os elementos de K que são inteiros sobre $\mathbb{Z}$ são os inteiros algébricos de K e, assim,

$$\mathcal{O}_K = \{x \in K;\ x \text{ é inteiro algébrico}\},$$

também chamado **anel de inteiros de** K.

Teorema 1.6. [*34, pag.*67], [*28, pag.*35] *Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados. Se $K = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático, então o anel de inteiros de K é dado por*

i) $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, *se* $d \not\equiv 1 \pmod 4$;

ii) $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, *se* $d \equiv 1 \pmod 4$.

Teorema 1.7. [*37, pag.*11] *O anel de inteiros do n-ésimo corpo ciclotômico $K = \mathbb{Q}(\xi_n)$ é $\mathcal{O}_K = \mathbb{Z}[\xi_n]$, onde $n > 1$ é um inteiro positivo.*

Proposição 1.3. [*37, pag.*16] *Sejam $L = \mathbb{Q}(\xi_n)$ e $K = \mathbb{Q}(\xi_n + \xi_n^{-1})$ o subcorpo maximal real de L. O anel de inteiros de K é dado por $\mathcal{O}_K = \mathbb{Z}[\xi_n + \xi_n^{-1}]$.*

Sejam $A \subseteq B$ uma extensão de anéis. Um conjunto de elementos $\omega_1, \omega_2, \ldots, \omega_n \in B$, tal que todo elemento $b \in B$ possui uma única representação como combinação linear desses elementos, isto é,

$$b = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n,$$

com coeficientes $a_i \in A$, para $i = 1, 2, \ldots, n$, é dita uma **base integral** de B sobre A. A existência de uma base integral implica que B é um A-módulo livre de posto n. Neste caso, sendo K e L os corpos de frações de A e B, respectivamente, toda base integral de B sobre A também é uma base de L sobre K

Quando A é um anel de domínios principais, segue que qualquer B-submódulo não nulo e finitamente gerado de L é um A-módulo livre. Em particular, B admite uma base integral sobre A.

Definição 1.15. *Seja $L|K$ uma extensão de Galois de grau n com grupo de Galois $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Definimos a* **norma** *e o* **traço** *de um elemento $x \in L$ na extensão $L|K$ por*

$$N_{L|K}(x) = \prod_{i=1}^{n} \sigma(x) \quad e \quad Tr_{L|K}(x) = \sum_{i=1}^{n} \sigma(x).$$

Ressaltamos que a norma e o traço podem ser definidos de outros modos, e obtermos a igualdade acima como resultado.

Sejam A um anel, K seu corpo de frações, L uma extensão finita e separável de K e B o fecho inteiro de A em L. Se $x \in B$, então

$$Tr_{L|K}(x), \quad N_{L|K}(x) \in A.$$

Se $K \subseteq L \subseteq M$ são extensões de Galois finitas tem-se que

$$Tr_{L|K} \circ Tr_{M|L} = Tr_{M|K} \quad e \quad N_{L|K} \circ N_{M|L} = N_{M|K}.$$

Seja K um corpo de números de grau n. Pelo Teorema 1.2, tem-se que existem n K-homomorfismos $\sigma : K \longrightarrow \mathbb{C}$.

Definição 1.16. *Seja K um corpo de números e $\sigma : K \longrightarrow \mathbb{C}$ um K-homomorfismo. O homomorfismo σ é dito* **real** *se $\sigma(K) \subseteq \mathbb{R}$, caso contrário, σ é dito ser um* **homomorfismo imaginário**.

Os homomorfismo imaginários aparecem ao pares, pois para cada homomorfismo imaginário σ, o homomorfismo conjugado, dado por $\overline{\sigma}(x) = \overline{\sigma(x)}$, para todo $x \in K$, é também um homomorfismo imaginário.

Definição 1.17. *Seja K um corpo de números de grau n. Denota-se por r_1 o número de homomorfismo reais e por r_2 o número de homomorfismo imaginários. Tem-se que $n = r_1 + 2r_2$, e o par (r_1, r_2) é dito* **assinatura** *de K. O corpo K é dito ser* **totalmente real** *quando $r_2 = 0$, isto é, quando todos os homomorfismos de K forem reais, e ser* **totalmente complexo** *quando $r_1 = 0$, isto é, quando todos os homomorfismos de K forem imaginários.*

1.4 Anéis noetherianos e anéis de Dedekind

Apresentamos, nessa seção, os anéis e módulos noetherianos, e os anéis de Dedekind, onde vale a unicidade da fatoração de ideais. Veremos também quando o anel de inteiros de um corpo de números é um anel de Dedekind.

Definição 1.18. [*35, pag.*6] *Sejam A um anel e M um módulo sobre A. O A-módulo M é chamado* **noetheriano** *se todo A-submódulo de M é finitamente gerado. Diz-se que o próprio anel A é noetheriano se A é um A-módulo noetheriano, ou seja, o anel A é um anel noetheriano quando A é um A-módulo noetheriano.*

Note que A ser um A-módulo noetheriano significa que todo ideal de A é finitamente gerado. Qualquer A-submódulo de um A-módulo noetheriano A é um A-módulo noetheriano.

Definição 1.19. [*35, pag.*6] *Sejam A um anel e M um A-módulo. Diz-se que M satisfaz a* **condição da cadeia ascentente** *se qualquer cadeia crescente*

$$M_1 \subseteq M_2 \subseteq \cdots$$

de A submódulos de M é estacionária, isto é, se a sequência é constante a partir de um M_{n_0}, ou seja, existe $n_0 \in N$ tal que $M_k = M_{n_0}$, para todo $k \geqslant n_0$.

Lema 1.1. [*35, pag.*6] *Sejam A um anel e M um módulo sobre A. As seguintes condições são equivalentes:*

i) M é noetheriano.

ii) M satisfaz a condição da cadeia ascendente.

iii) Qualquer família não vazia de A-submódulos de M contém um elemento maximal.

Teorema 1.8. [*35, pag.*7] *Seja A um A-módulo noetheriano. Um A-módulo B é noetheriano se, e somente se, B é um A-módulo finitamente gerado.*

Exemplo 1.3. *O anel dos inteiros $\mathbb{Z}$ é um anel noetheriano.*

Teorema 1.9 (Teorema da Base de Hilbert)**.** [*35, pag.*8] *Se A é um anel noetheriano e B um anel contendo A, que é finitamente gerado com um anel, então B é noetheriano.*

Teorema 1.10. [*34, pag.*115] *Seja $\mathcal{O}_K$ o anel de inteiros de um corpo de números K.*

i) O corpo de frações de $\mathcal{O}_K$ é K.

ii) O_K é um anel noetheriano.

iii) Se $\alpha \in K$ é raiz de um polinômio mônico com coeficientes em $\mathcal{O}_K$, então $\alpha \in \mathcal{O}_K$.

iv) Qualquer ideal primo de $\mathcal{O}_K$ é maximal.

Um módulo é dito ser de **tipo finito** se contém um conjunto gerador finito.

Definição 1.20. *Um* **anel de Dedekind** *é um anel (domínio) tal que:*

i) A é integralmente fechado no seu corpo de frações;

ii) A é um anel noetheriano;

iii) Qualquer ideal primo não nulo é maximal.

Lema 1.2. [*35, pag.*9] *Qualquer anel de ideais principais é um anel de Dedekind.*

Exemplo 1.4. *O anel dos inteiros $\mathbb{Z}$ e o anel dos inteiros de Jacobi $\mathbb{Z}[i]$ são anéis de Dedekind.*

Exemplo 1.5. *Como veremos no Teorema 1.14, o anel de inteiros de um corpo de números é um anel de Dedekind.*

Sejam A um anel e K o corpo de frações de A. Um **ideal fracionário** $\mathfrak{a}$ de A é um A-submódulo de K finitamente gerado. Para evitar ambiguidade, os ideais em A também são chamados de ideais integrais.

Teorema 1.11. [*35, pag.*10] *O conjunto dos ideais fracionários não nulos de um anel de Dedekind formam um grupo multiplicativo.*

Teorema 1.12. [*35, pag.*11] *Em um anel de Dedekind A qualquer ideal integral não nulo $\mathfrak{a}$ em A pode ser expresso como o produto*

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m,$$

onde os $\mathfrak{p}_j$ são ideais primos de A, e essa expressão é única, a menos de ordem nos fatores.

Com o Teorema 1.12, em um anel de Dedekind, qualquer ideal integral não nulo $\mathfrak{a}$ pode ser expresso como

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

onde os $\mathfrak{p}_j$ são ideais primos de A, dois a dois distintos, $e_j > 0$ são inteiros positivos, para $j = 1, 2, \ldots, r$, e essa expressão é única, a menos de ordem dos fatores.

Corolário 1.1. [*35, pag.*11] *Sejam A um anel de Dedekind e K o seu corpo de frações. Um ideal fracionário não nulo $\mathfrak{a}$ em A pode ser expresso na forma*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

onde os $\mathfrak{p}_j$ são ideais primos de A, dois a dois distintos, $e_j \neq 0$ são inteiros, para $j = 1, 2, \ldots, r$, e essa expressão é única, a menos de ordem dos fatores.

Exemplo 1.6. *No anel dos inteiros $\mathbb{Z}$ a fatoração de ideais equivale a fatoração de um inteiro em primos. De fato, sejam $n \in \mathbb{Z}$ um inteiro não nulo, e $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ a decomposição de n em fatores primos p_j. Passando para ideais, tem-se que*

$$\langle n \rangle = \langle p_1 \rangle^{\alpha_1} \langle p_2 \rangle^{\alpha_2} \cdots \langle p_r \rangle^{\alpha_r},$$

onde os ideais $\langle p_j \rangle$ são ideais primos em $\mathbb{Z}$.

Sejam K um corpo de números, $\mathcal{O}_K$ o anel de inteiros de K e $\mathfrak{a}$ um ideal integral de $\mathcal{O}_K$. O anel quociente $\mathcal{O}_K/\mathfrak{a}$ é finito. O número de elementos de $\mathcal{O}_K/\mathfrak{a}$ é a **norma** de $\mathfrak{a}$, denotada por $N(\mathfrak{a})$, isto é

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|.$$

Por convenção, $N(0) = 0$. Se $\alpha \in \mathcal{O}_K$ então $N(\alpha\mathfrak{a}) = |N_{K|\mathbb{Q}}(\alpha)|N(\mathfrak{a})$. Em particular $N(\langle\alpha\rangle) = |N_{K|\mathbb{Q}}(\alpha)|$. [35, pag. 14] e [34, pag. 125-126].

Lema 1.3. [*35, pag.*14],[*34, pag.*127] *Se $\mathfrak{a}_1, \mathfrak{a}_2$ são ideais integrais de $\mathcal{O}_K$, então*

$$N(\mathfrak{a}_1\mathfrak{a}_2) = N(\mathfrak{a}_1)N(\mathfrak{a}_2).$$

Teorema 1.13. [*28, pag.*49] *Sejam A um anel de Dedekind, K seu corpo de frações, L uma extensão finita de K e $\mathcal{O}_L$ o fecho inteiro de A em L. Se K possui característica zero, então $\mathcal{O}_L$ é um anel de Dedekind e é um A-módulo de tipo finito.*

Como consequência do Teorema 1.13, tem-se o resultado a seguir, que também pode ser provado diretamente de um modo mais simples que o geralmente utilizado para provar o Teorema 1.13

Teorema 1.14. [*35, pag.*15] *Se $\mathcal{O}_K$ é o anel de inteiros de um corpo de números K, então $\mathcal{O}_K$ é um anel de Dedekind.*

1.5 Ramificação

Nesta seção, apresentamos as principais definições sobre a ramificação de ideais. Para isso, sejam A um anel de Dedekind, K seu corpo de frações, L uma extensão finita de K, $\mathcal{O}_K$ o fecho inteiro de A em K e $\mathcal{O}_L$ o fecho inteiro de A em L. Pelo Teorema 1.13, tem-se que $\mathcal{O}_L$ é um anel de Dedekind. Agora, pelo Corolário 1.1, um ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_K$ decompõe em $\mathcal{O}_L$ de modo único, a menos de ordem, como o produto de ideais primos de $\mathcal{O}_L$ da seguinte forma

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2} \cdots \mathfrak{B}_r^{e_r}.$$

Denotamos sempre $\mathfrak{p}\mathcal{O}_L$ por $\mathfrak{p}$.

Dizemos que um ideal $\mathfrak{B}$ de $\mathcal{O}_L$ esta **acima** do ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ quando

$$\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K.$$

Neste caso, denotamos $\mathfrak{B}|\mathfrak{p}$, e dizemos que $\mathfrak{B}$ é um **divisor** de $\mathfrak{p}$.

Proposição 1.4. [*28, pag.*71] *Os ideais primos* $\mathfrak{B}$ *ocorrendo na decomposição de* $\mathfrak{p}\mathcal{O}_L$ *são precisamente os ideais primos* $\mathfrak{B}$ *de* $\mathcal{O}_L$ *que estão acima de* $\mathfrak{p}$*, ou seja,*

$$\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K.$$

Os anéis $\mathcal{O}_K/\mathfrak{p}$ e $\mathcal{O}_L/\mathfrak{B}$ são corpos finitos e são chamados de **corpos residuais**. O anel $\mathcal{O}_K/\mathfrak{p}$ pode ser identificado como um subanel de $\mathcal{O}_L/\mathfrak{B}$.

Definição 1.21. *Seja*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\cdots\mathfrak{B}_r^{e_r}$$

a fatoração do ideal primo $\mathfrak{p}$ *de* $\mathcal{O}_K$ *como produto de ideais primos de* $\mathcal{O}_L$*. O expoente* e_i *é dito* **índice de ramificação** *de* $\mathfrak{B}_i$ *sobre* $\mathfrak{p}$*, e o grau da extensão de corpos residuais*

$$f_i = [\mathcal{O}_L/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}]$$

é dito **grau de inércia** *de* $\mathfrak{B}_i$ *sobre* $\mathfrak{p}$*.*

Teorema 1.15. [*28, pag.*71] *Se a extensão* $L|K$ *é separável e* $[L : K] = n$*, tem-se a* **igualdade fundamental**

$$\sum_{j=1}^{r} e_j f_j = n,$$

onde os e_j*'s são os índices de ramificação e os* f_i *são os graus de inércia, de* $\mathfrak{B}_j$ *sobre* $\mathfrak{p}$*.*

Um ideal primo p é dito **totalmente decomposto**, ou que **decompõe completamente** em L, se na decomposição

$$\mathfrak{p} = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\cdots\mathfrak{B}_r^{e_r}$$

tivermos $r = n = [L : K]$, a assim $e_i = f_i = 1$. Logo, a decomposição de um ideal primo $\mathfrak{p}$ totalmente decomposto fica

$$\mathfrak{p} = \mathfrak{B}_1\mathfrak{B}_2\cdots\mathfrak{B}_n.$$

Se $r = 1$, isto é, se existe apenas um único ideal acima de $\mathfrak{p}$, dizemos que $\mathfrak{p}$ é **inerte** ou **indecomponível**.

Da igualdade fundamental, $\sum_{i=1}^{r} e_i f_i = n$, obtém-se o significado do grau de inércia, isto é, quanto menor é o grau de inércia mais o ideal $\mathfrak{p}$ será fatorado em um número maior de ideais primos em L.

O ideal primo $\mathfrak{B}_i$ na decomposição $\mathfrak{p} = \prod_{i=2}^{r} \mathfrak{B}_i{}^{e_i}$ é dito **não ramificado** sobre $\mathcal{O}_K$ (ou sobre K) se $e_i = 1$ e a extensão dos corpos residuais $\mathcal{O}_L/\mathfrak{B}_i|\mathcal{O}_K/\mathfrak{p}$ é separável. Caso contrário, $\mathfrak{B}_i$ é dito **ramificado**. O ideal primo $\mathfrak{B}_i$ é dito **totalmente ramificado** se for ramificado e $f_i = 1$.

O ideal primo $\mathfrak{p}$ é dito **não ramificado** quando todos os ideais primos $\mathfrak{B}_i$ são não ramificados. Caso contrário, é dito **ramificado**. A extensão $L|K$ é dita **não ramificada** se todos os ideais primos de K são não ramificados em L.

Exemplo 1.7. [*28, pag.*77] *Seja $p \in \mathbb{Z}$ um primo ímpar. O ideal primo $\langle p \rangle$ de $\mathbb{Z}$ é o único ideal primo que se ramifica no p-ésimo corpo ciclotômico $\mathbb{Q}(\xi_p)$.*

Se a extensão $L|K$ é separável, então apenas um número finito de ideais primos de K ramificam em L.

Seja $L|K$ extensão de Galois, com grupo de Galois $G = Gal(L|K)$. Se $\mathfrak{B}$ é um ideal primo de $\mathcal{O}_L$ e $\sigma \in G$ então $\sigma(\mathfrak{B})$ também é um ideal primo de $\mathcal{O}_L$. Neste caso, $\mathfrak{B}$ e $\sigma(\mathfrak{B})$ são ditos ideais primos **conjugados**.

Proposição 1.5. [*28, pag.*89] *Se a extensão $L|K$ é de Galois e $\mathfrak{p}$ é um ideal primo de $\mathcal{O}_K$ então os ideais primos $\mathfrak{B}$ de $\mathcal{O}_L$ que aparecem na decomposição de $\mathfrak{p}$ como produto de ideais primos de $\mathcal{O}_L$, $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\cdots\mathfrak{B}_r^{e_r}$, são todos conjugados. Neste caso, os graus de inércia, $f_1, f_2, \ldots, f_r$, e os índices de ramificação, $e_1, e_2, \ldots, e_r$, são ambos independentes de i, isto é,*

$$f_1 = f_2 = \cdots = f_r = f, \quad e_1 = e_2 = \cdots = e_r = e.$$

Assim, quando a extensão $L|K$ é de Galois,

$$\mathfrak{p} = (\mathfrak{B}_1\mathfrak{B}_2\cdots\mathfrak{B}_r)^e,$$

e a igualdade fundamental é dada por

$$n = efr.$$

Teorema 1.16 (Teorema de Kummer)**.** [*16, pag.*27] *Sejam A um anel de Dedekind, K o corpo de frações de A, L um extensão separável de K de grau n, $\mathcal{O}_L$ o anel de inteiros de L sobre A, $\beta \in \mathcal{O}_L$ tal que $\mathcal{O}_L = A[\beta]$ e $\mathfrak{p}$ um ideal primo não nulo de A. Sejam ainda $f \in A[x]$ o polinômio minimal de β sobre A, $f_1, f_2, \ldots, f_r \in A$ polinômios mônicos tais que cada $\overline{f_j} \in A/\mathfrak{p}[x]$, a projeção canônica de f_j em $A/\mathfrak{p}[x]$, é irredutível, de modo que a fatoração do polinômio $\overline{f}$, a projeção canônica de f em $A/\mathfrak{p}[x]$, é dada por*

$$\overline{f} = \overline{f_1}^{e_1}\overline{f_2}^{e_2}\cdots\overline{f_r}^{e_r}.$$

Nestas condições, a fatoração de $\mathfrak{p}$ em ideais primos de $\mathcal{O}_L$ é dada por

$$p = \mathfrak{p} = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\cdots\mathfrak{B}_r^{e_r},$$

onde $\mathfrak{B}_j = p\mathcal{O}_L + f_j(\beta)\mathcal{O}_L$ é um ideal primo de $\mathcal{O}_L$ acima de $\mathfrak{p}$, o índice de ramificação de $\mathfrak{B}$ sobre $\mathfrak{p}$ é e_j, e o grau de inércia f_j de $\mathfrak{B}$ sobre $\mathfrak{p}$ é $f_j = grau(f_j)$, para $j = 1, 2 \ldots, n$.

Note que quando $A = \mathbb{Z}$, L é um corpo de números e $\mathcal{O}_L$ o anel de inteiros de L, se $\mathcal{O}_L = \mathbb{Z}[\beta]$, para algum $\beta \in L$, então as hipóteses do Teorema de Kummer são satisfeitas.

Exemplo 1.8. *Consideramos a fatoração do ideal gerado por 3 no corpo quadrático $\mathbb{Q}(\sqrt{7})$. Tem-se que o anel de inteiros de $L = \mathbb{Q}(\sqrt{7})$ é $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$ e o polinômio minimal de $\sqrt{7}$*

sobre $\mathbb{Z}$ *é* x^2-7. *Tomando o ideal primo* $\mathfrak{p}=\langle 3\rangle$, *a fatoração de* $\overline{f}$ *em polinômios irredutíveis sobre* $\mathcal{O}_L$ *é dada por*

$$f \equiv (x+1)(x+2) \pmod{3\mathbb{Z}[x]}.$$

Pelo Teorema 1.16, tem-se que

$$3\mathbb{Z}[\sqrt{3}] = \langle 3, \sqrt{7}+1\rangle\langle 3\sqrt{7}+2\rangle$$

é a decomposição do ideal $3\mathcal{O}_L$ *em ideais primos de* $\mathcal{O}_L$.

Exemplo 1.9. *Sejam* ξ_{24} *uma raiz vigésima quarta primitiva da unidade,* $L=\mathbb{Q}(\xi_{24})$ *o vigésimo quarto corpo ciclotômico e* $O_L=\mathbb{Z}[\xi_{24}]$ *o anel de inteiros de* L. *O polinômio minimal de* ξ *é* $\phi_{24}=x^8-x^4+1$. *Tomando os ideais primos* $\langle 2\rangle$ *e* $\langle 3\rangle$ *de* $\mathbb{Z}$, *tem-se que*

$$\begin{aligned}\phi_{24}(x) &\equiv (x^2+x+1)^4 \pmod{2\mathbb{Z}[x]} \text{ e}\\ \phi_{24}(x) &\equiv (x^2+x+2)(x^2+2x+2) \pmod{3\mathbb{Z}[x]}.\end{aligned}$$

Pelo Teorema de Kummer, tem-se que

$$\begin{aligned}2\mathcal{O}_L &= \langle 2, 1+\xi_{24}+\xi_{24}^2\rangle^2 \text{ e}\\ 3\mathcal{O}_L &= \langle 3, 2+\xi_{24}+\xi_{24}^2\rangle\langle 3, 2+2\xi_{24}+\xi_{24}^2\rangle,\end{aligned}$$

é a fatoração dos ideais gerados por 2 *e* 3 *em ideais primos de* $\mathcal{O}_L$, *respectivamente.*

Exemplo 1.10. *Sejam* $p\in\mathbb{Z}$ *um primo ímpar,* ξ_p *uma raiz p-ésima primitiva da unidade,* $\mathbb{Q}(\xi_p)$ *o p-ésimo corpo ciclotômico,* $\mathcal{O}_L=\mathbb{Z}[\xi_p]$ *o anel de inteiros de* $\mathbb{Q}(\xi_p)$ *e* $\phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ *o polinômio minimal de* ξ_p. *Como*

$$\phi_p \equiv (x-1)^{p-1} \pmod{p\mathbb{Z}[x]},$$

segue, pelo Teorema 1.16, que

$$p\mathcal{O}_L = \langle p, 1-\xi_p\rangle^{p-1}$$

é a fatoração do ideal $p\mathcal{O}_L$ *em ideais primos de* $\mathcal{O}_L$.

1.6 Conclusões

Neste capítulo foram apresentados os fundamentos da Teoria Algébrica dos Números, que são um dos pilares para o desenvolvimento deste trabalho. Os principais resultados do capítulo são o Teorema Fundamental da Teoria de Galois, apresentado no Teorema 1.4, e o Teorema de Kronecker-Weber, apresentado no Teorema 1.5, a partir do qual faz sentido falar em condutor de um corpo abeliano. Neste sentido, neste capítulo forma apresentados os principais resultados da teoria algébrica dos números necessários para o entendimento dos demais capítulos.

Capítulo

2

Teoria das Valorizações

Dedicamos este capítulo aos números p-ádicos, que foram introduzidos, no início do século XX, pelo matemático Kurt Hensel (1861-1941). Deste modo, na Seção 2.1, são apresentados os conceitos de localização e anéis de frações, em especial a localização de um anel em um ideal primo $\mathfrak{p}$. Também é definido anel de valorização discreta, e a função valorização. Na Seção 2.2, introduzimos os inteiros p-ádicos e o números p-ádicos, resultando nos anéis de inteiros p-ádicos e nos corpos de números p-ádicos. O conceito de fracamente ramificado, apresentado na Seção 2.2, será importante para obter uma nova demonstração para a fórmula do discriminante de corpos de números cujo condutor é uma potência de primo ímpar presente em [13]. Na Seção 2.3 apresentamos o conceito de valorização p-ádica sobre os corpos p-ádicos, finalizando o capítulo. A referência básica para este capítulo é o livro Algebraic Number Theory de J. Neukirch [23].

2.1 Localizações

Sejam A um anel e K seu corpo de frações. Tomando um subconjunto não vazio $S \subseteq A\backslash\{0\}$, multiplicativamente fechado, obtém-se o conjunto

$$S^{-1}A = \{\frac{a}{s} \in K : a \in A, s \in S\},$$

que munido com as operações de soma e adição, dadas por

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \text{ e } \frac{a}{s}\frac{b}{t} = \frac{ab}{st} \text{ para todos } a, b \in A \text{ e } s, t \in S,$$

formam um anel, chamado **anel de frações de A com relação a S.**

O caso mais importante é quando o conjunto multiplicativamente fechado é dado por $S = A\backslash\mathfrak{p}$, o complemento de um ideal primo $\mathfrak{p}$ de A. Neste caso, escrevemos $A_\mathfrak{p} = S^{-1}A$ e o anel $A_\mathfrak{p}$ é dito a **localização** de A em $\mathfrak{p}$.

Teorema 2.1. [*23*], *pag.*44] *Se $\mathfrak{p}$ é um ideal primo de A, então o anel $A_\mathfrak{p}$ é um anel local, isto é, possui um único ideal maximal, dado por $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$.*

Definição 2.1. *Um* **domínio de valorização discreta** *é um anel de ideais principais $\mathcal{O}$ que possui um único ideal maximal $\mathfrak{p} \neq 0$.*

Em um domínio de valorização discreta $\mathcal{O}$, o ideal principal é da forma $\mathfrak{p} = (\pi) = \pi\mathcal{O}$, para algum elemento primo π. Como todo elemento que não pertença ao ideal $\mathfrak{p}$ é uma unidade, segue que, a menos de associados, π é o único elemento primo de $\mathcal{O}$. Logo, todo elemento de $\mathcal{O}$ pode ser expresso como $\varepsilon\pi^n$, para alguma unidade $\varepsilon \in \mathcal{O}$ e algum $n \geqslant 0$ inteiro. De modo geral, qualquer elemento não nulo $a \neq 0$ do corpo de frações K de $\mathcal{O}$ pode ser escrito como

$$a = \varepsilon\pi^n, \quad \textit{onde } \varepsilon \in \mathcal{O} \text{ é uma unidade e } n \in \mathbb{Z}.$$

Definição 2.2. *Sejam $\mathcal{O}$ um domínio de valorização discreta e π um elemento primo de A. O inteiro $n \in \mathbb{Z}$ que aparece em $a = \varepsilon\pi^n$, com $\varepsilon \in \mathcal{O}$ uma unidade, é chamado* **valorização** *de a, denotado por $v(a)$, onde $a \in \mathcal{O}$ é um elemento não nulo.*

A valorização $v(a)$ é caracterizada pela equação

$$(a) = \mathfrak{p}^{v(a)},$$

onde $\mathfrak{p} = \langle\pi\rangle$ é o ideal maximal de $\mathcal{O}$. Além disso, uma valorização pode ser vista com uma função

$$v : K^* \longrightarrow \mathbb{Z},$$

onde $K^* = K\backslash\{0\}$, que pode ser entendida para K convencionando-se que $v(0) = \infty$.

Proposição 2.1. [*23*, *pags.*$67 - 68$] *Uma valorização tem as seguintes propriedades:*

i) $v(ab) = v(a) + v(b)$, *para todos* $a, b \in K$.

ii) $v(a + b) \geqslant \min\{v(a), v(b)\}$, *para todos* $a, b \in K$.

Proposição 2.2. [*23*, *pag.*68] *Se $\mathcal{O}$ é um anel de Dedekind então, para qualquer subconjunto não vazio $S \subseteq \mathcal{O}\backslash\{0\}$ multiplicativamente fechado, o anel $S^{-1}\mathcal{O}$ é um anel de Dedekind.*

Proposição 2.3. [*23*, *pag.*68] *Uma condição necessária e suficiente para que um anel noetheriano $\mathcal{O}$ seja um anel de Dedekind é que, para todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}$, a localização $\mathcal{O}_\mathfrak{p}$ seja um anel de valorização discreta.*

Assim, em um anel de Dedekind $\mathcal{O}$, para cada ideal primo não nulo $\mathfrak{p}$, tem-se o anel de valorização discreta $\mathcal{O}_\mathfrak{p}$ e a correspondente valorização

$$v_p : K^* \longrightarrow \mathbb{Z},$$

onde K é o corpo de frações de $\mathcal{O}$ e $K^* = K\backslash\{0\}$ Além disso, para cada $x \in K^*$, tem-se que a fatoração do ideal principal (x) é dada por

$$(x) = \prod_\mathfrak{p} \mathfrak{p}^{v_p},$$

onde, para cada ideal primo $\mathfrak{p}$, denotamos $v_\mathfrak{p} = v_\mathfrak{p}(x)$. Devido a essa relação, a valorização $v_\mathfrak{p}$ também é dita **valorização exponencial**.

A localização do anel de inteiros $\mathbb{Z}$ em um ideal primo $(p) = p\mathbb{Z}$ é dada por

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} | a, b \in \mathbb{Z} : p \not| b\}.$$

O ideal maximal $p\mathbb{Z}_{(p)}$ consiste de todas as frações a/b, com $p|a$ e $p \not| b$, e o grupo das unidades consiste de todas as frações a/b, com $p \not| ab$. A valorização associada a $\mathbb{Q}$,

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\},$$

é dita **valorização p-ádica** de $\mathbb{Q}$. A valorização $v_p(x)$, de um elemento $x \in \mathbb{Q}^*$, é dada por

$$v_p(x) = v,$$

onde $x = p^v a/b$, com os inteiros a e b relativamente primos com p.

2.2 Inteiros e números p-ádicos

Nesta seção, apresentamos os inteiros e números p-ádicos, Existe mais de um modo de definir os números p-ádicos, que são equivalentes, mas com enfoques ou pontos de vistas ligeiramentes diferentes.

Seja p um número primo ímpar. Cada número natural não nulo $f \in \mathbb{N}$ admite uma **expansão p-ádica**

$$f = a_0 + a_1 p + \cdots + a_n p^n,$$

onde $0 \leqslant a_i \leqslant p-1$ são inteiros, para $i = 0, 1, \ldots, n$. Os inteiros p-ádicos generalizam esse conceito.

Definição 2.3. *Seja p um primo ímpar. Um* **inteiro p-ádico** *é uma série formal infinita*

$$a_0 + a_1 p + a_2 p^2 + \cdots = \sum_{v=0}^{\infty} a_v p^v,$$

onde $0 \leqslant a_v \leqslant p-1$ são inteiros, para $v = 0, 1, \ldots$. O conjunto de todos os números p-ádicos é denotado por $\mathbb{Z}_p$.

O conjunto dos inteiros p-ádicos $\mathbb{Z}_p$ forma um anel, chamado **anel dos inteiros p-ádicos**.

Exemplo 2.1. *O anel dos inteiros 3-ádicos é o conjunto*

$$\mathbb{Z}_3 = \left\{ a_0 + a_1 3 + a_2 3^2 + \cdots = \sum_{v=0}^{\infty} a_v 3^v;\ a_v \in \mathbb{Z},\ 0 \leqslant a_v \leqslant 2,\ v = 0, 1, \ldots \right\}.$$

Definição 2.4. *As séries formais infinitas*

$$\sum_{v=-m}^{\infty} a_v p^v = a_{-m} p^{-m} + \cdots + a_{-1} p^{-1} a_0 + a_1 p + \cdots,$$

onde $m \in \mathbb{Z}$ e $0 \leqslant a_v \leqslant p-1$ são inteiros, para todo $v = -m, -(m-1), \ldots$, são chamadas de **números p-ádicos** *e o conjunto de todos números p-ádicos é denotado $\mathbb{Q}_p$.*

O conjunto dos números p-ádicos $\mathbb{Q}_p$ forma um corpo, chamado **corpo de números p-ádicos**.

Exemplo 2.2. *O corpo dos números 7-ádicos é o conjunto*

$$\mathbb{Q}_7 = \left\{ \sum_{v=-m}^{\infty} a_v 7^v;\ a_v \in \mathbb{Z},\ m \in \mathbb{Z},\ 0 \leqslant a_v \leqslant 7,\ v = -m, -(m-1), \ldots \right\}.$$

Definição 2.5. *Sejam $L|K$ uma extensão algébrica finita de corpos p-ádicos e p a característica do corpo residual de K. Se a extensão dos corpos residuais for separável e $\mathrm{mdc}([L:K], p) = 1$, diremos que a extensão é* **fracamente ramificada** *(tamely ramified).*

2.3 Valor absoluto p-ádico

Nessa seção, apresentamos o conceito de valor absoluto p-ádico, indiciando definindo valorização p-ádica e valor absoluto p-ádico sobre o corpo dos racionais $\mathbb{Q}$ e, em seguida, estenderemos esses conceitos para os corpos p-ádicos $\mathbb{Q}_p$.

Seja $a \in \mathbb{Q}$ um número racional não nulo. Representando a na base p, tem-se

$$a = \sum_{v=-m}^{s} a_v p^v = a_{-m} p^{-m} + \cdots + a_{-1} p^{-1} a_0 + a_1 p + \cdots + a_s p^s,$$

onde $m \in \mathbb{Z}$ e $0 \leqslant a_v \leqslant p-1$ são inteiros, para todo $v = -m, -(m-1), \ldots, s$, e a_s é não nulo. Seja $v_p(a) = s$. Se $a = 0$ então definimos $v_p(0) = \infty$. Temos assim a função

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\},$$

que satisfaz as seguintes propriedades:

i) $v_p(a) = \infty$ se, e somente se, $a = 0$,

ii) $v_p(ab) = v_p(a) + v_p(b)$,

iii) $v_p(a+b) \geqslant \min\{v_p(a), v_p(b)\}$,

onde $x + \infty = \infty$, $\infty + \infty = \infty$ e $\infty > x$, para todo $x \in \mathbb{Z}$. A função v_p é uma valorização.

Definição 2.6. *A função v_p é dita a* **valorização p-ádica** *de $\mathbb{Q}$. O* **valor absoluto p-ádico** *é definido por*

$$\begin{aligned} |\,.\,|_p : \mathbb{Q} &\longrightarrow \mathbb{R}, \\ a &\longmapsto |a|_p = p^{-v_p(a)}. \end{aligned}$$

Proposição 2.4. [*23, pag.*107] *O valor absoluto p-ádico é uma norma sobre $\mathbb{Q}$.*

Estendendo esses conceitos para um corpo p-ádico, dado um número p-ádico não nulo

$$a = \sum_{v=-m}^{\infty} a_v p^v = a_{-m}p^{-m} + \cdots + a_{-1}p^{-1}a_0 + a_1 p + \cdots,$$

onde $m \in \mathbb{Z}$ e $0 \leqslant a_v \leqslant p-1$ são inteiros, para todo $v = -m, -(m-1), \ldots, s$, seja s o menor natural tal que a_s é não nulo e que todos os a_i's posteriores são nulos. Seja $v_p(a) = v$. Do mesmo modo, se $a = 0$, então definimos $v_p(0) = \infty$. Assim, temos uma função $v_p : \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}$, que satisfaz as propriedades de valorização, dadas anteriormente, e v_p é dita **valorização p-ádica** de $\mathbb{Q}_p$. O **valor absoluto p-ádico** sobre $\mathbb{Q}_p$ é definido por

$$\begin{aligned} |\,.\,|_p : \mathbb{Q}_p &\longrightarrow \mathbb{R}, \\ a &\longmapsto |a|_p = p^{-v_p(a)}, \end{aligned}$$

que é uma norma sobre $\mathbb{Q}_p$.

2.4 Conclusões

Neste capítulo foram introduzidos os conceitos de localização, inteiros e números p-ádicos e valor absoluto p-ádico, que serão úteis nos próximos capítulos, em particular no Capítulo 3 para auxiliar nas demonstrações de alguns resultados envolvendo o discriminante.

Capítulo

3

Diferente e Discriminante

Introduzimos, neste capítulo, os conceitos de discriminante, ideal discriminante e diferente, o que proverá uma ferramenta alternativa para o cálculo do discriminante absoluto de um corpo de números abelianos. Deste modo, na Seção 3.1, apresentamos o conceito de discriminante, enfocando o discriminante de uma extensão, o discriminante de um corpo de números e o discriminante absoluto de um corpo de números, assim como alguns fatos sobre o discriminante. Neste sentido, a Proposição 3.4 apresenta uma condição necessária e suficiente para um conjunto ser uma base integral para uma extensão. Na Seção 3.2 é apresentamos um apanhado sobre os principais resultados para o cálculo do discriminante. Na Seção 3.3, a partir do $\mathcal{O}_L$-módulo dual, definimos o codiferente de uma extensão, que é um ideal fracionário. O inverso multiplicativo do codiferente é o diferente. Em seguida definimos o ideal discriminante, que está diretamente relacionado com o diferente. Na Seção 3.4, utilizando os corpos de números p-ádicos, o ideal discriminante e o diferente, partindo da Proposição 3.5, provamos o Teorema 3.9, que fornece o discriminante absoluto de corpos de números de condutor potência de primo ímpar, de um modo alternativo à referência existente na literatura [24]. Finalizamos o capítulo apresentando algumas consequências desse resultado.

3.1 Discriminante

Apresentamos, nesta seção, o conceito de discriminante juntamente com algumas de suas principais propriedades e alguns fatos sobre integralidade. Posteriormente, na Seção 3.3,

introduzimos a definição do ideal discriminante utilizando o diferente, o que permitirá obter o discriminante de corpos números de condutor potência de primo, de um modo diferente dos conhecidos na literatura.

Sejam $L|K$ uma extensão separável de grau n e σ_i, para $i = 1, 2, \ldots, n$, os K-homomorfismos. O **discriminante** de um conjunto de elementos $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq L$ de $L|K$ é definido por

$$d(\alpha_1, \alpha_2, \ldots, \alpha_n) = det(\sigma_i(\alpha_j))^2.$$

Assim,

$$d(\alpha_1, \alpha_2, \ldots, \alpha_n) = det(Tr_{L|K}(\alpha_i\alpha_j)).$$

Proposição 3.1. [*28, pag.*39] *O discriminante* $d(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *é não nulo se, e somente se,* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *é uma base de* $L|K$

Proposição 3.2. [*19, pag.*26] *Se o conjunto é da forma* $\{1, \theta, \ldots, \theta^{n-1}\}$ *tem-se que*

$$d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j}(\sigma_i(\theta) - \sigma_j(\theta))^2 = \pm N_{L|K}(f'(\theta)),$$

onde f' *é a derivada formal do polinômio minimal de* θ *sobre* K.

O discriminante de uma base é um elemento não nulo de K e a forma bilinear dada por

$$\begin{array}{rcl} Tr : L \times L & \longrightarrow & K \\ (x, y) & \longmapsto & Tr(x, y) = Tr_{L|K}(xy) \end{array}$$

é uma forma bilinear não degenerada sobre o K-espaço vetorial L.

Sejam $\mathcal{O}_K$ e $\mathcal{O}_L$ os anéis de inteiros de K e L, respectivamente. Se $\{\omega_1, \omega_2, \ldots, \omega_n\}$ é uma base integral de $\mathcal{O}_L$ sobre $\mathcal{O}_K$ então o **discriminante de** L **sobre** K é definido por

$$d_{L|K} = d(\omega_1, \omega_2, \ldots, \omega_n) = det(\sigma_i(\omega_j))^2, \tag{3.1}$$

que independe da escolha da base $\{\omega_1, \omega_2, \ldots, \omega_n\}$.

Sejam K um corpo de números e $\mathcal{O}_K \subseteq K$ o anel de inteiros de K. Tem-se que $\mathcal{O}_K$ admite uma $\mathbb{Z}$-base e que o discriminante de qualquer base integral é o mesmo, chamado **discriminante do corpo de número** K, e denotado por d_K. Sendo $\{\omega_1, \omega_2, \ldots, \omega_n\}$ uma base integral de $\mathcal{O}_K$, segue que o discriminante do corpo de números K é dado por

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \omega_2, \ldots, \omega_n).$$

Geralmente estamos interessados apenas no valor absoluto do discriminante de um corpo de números, chamado **discriminante absoluto do corpo de números K**, e denotado por $|d_K|$. O próximo lema justifica o motivo pelo qual é importante apenas o valor absoluto do discriminante.

Lema 3.1. [*37, pag.*10] *Se K é um corpo de números e r_2 o número de pares de homomorfismos complexos de K, então o discriminante d_K de K possui sinal $(-1)^{r_2}$.*

Teorema 3.1. [*35, pag.*5] *O discrimanate de um corpo de números K satisfaz*

$$d_K \equiv 0 \text{ ou } 1 \pmod 4.$$

Teorema 3.2. [*34, pag.*126] *Sejam K um corpo de números de grau $n > 1$, $\mathcal{O}_K$ o anel de inteiros de K e $\mathfrak{a}$ um ideal integral de $\mathcal{O}_K$.*

i) Se $\mathfrak{a}$ é não nulo, então $\mathfrak{a}$ possui uma $\mathbb{Z}$-base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

ii) A norma do ideal $\mathfrak{a}$ é dada por

$$N(\mathfrak{a}) = \left| \frac{d(\alpha_1, \alpha_2, \ldots, \alpha_n)}{|d_K|} \right|^{1/2},$$

onde $|d_K|$ é o discriminante absoluto de K.

Proposição 3.3. [*6, pag.*166] *Se $K = \mathbb{Q}(\theta)$ é um corpo de números de grau n, com $\theta \in \mathcal{O}_K$, então*

$$d(1, \theta, \ldots, \theta^{n-1}) = [\mathcal{O}_K : \mathbb{Z}[\theta]] d_K,$$

onde $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ é o grau da extensão de anéis $\mathcal{O}_K | \mathbb{Z}[\theta]$, chamado **índice** *de θ em $\mathcal{O}_K$.*

Proposição 3.4. [*6, pag.*167] *Seja K um corpo de números de grau n. Os números algébricos $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ formam um base integral de K se, e somente se, cada α_j é um inteiro algébrico e*

$$d(\alpha_1, \alpha_2, \ldots, \alpha_n) = d_K.$$

.

3.2 Fórmulas conhecidas para o discriminante absoluto

Apresentamos, nessa seção, alguns resultados conhecidos envolvendo o cálculo do discriminante de corpos abelianos.

Teorema 3.3. [*34, pag.*68] *Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados. Se $K = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático, então o discriminante d_K de K é dado por*

i) $d_K = 4d$, se $d \not\equiv 1 \pmod 4$;

ii) $d_K = d$, se $d \equiv 1 \pmod 4$.

Teorema 3.4. [*34, pag.*74] *Sejam p um primo ímpar e $\xi = \xi_p$ uma raiz p-ésima da unidade. O discriminante do p-ésimo corpo ciclotômico $K = \mathbb{Q}(\xi_p)$ é dado por*

$$d_K = (-1)^{(p-1)/2} p^{p-2}.$$

Teorema 3.5. [*37, pag.9*] *Seja p um primo e $r \in \mathbb{Z}$ um inteiro positivo. O discriminante absoluto do p^r-ésimo corpo ciclotômico é dado por*

$$|d_K| = p^{p^{r-1}(pr-r-1)}.$$

Teorema 3.6. [*24, pag.322*] *Se K é um subcorpo de $\mathbb{Q}(\xi_{p^n})$ de grau ep^{n-1}, com p um primo ímpar e $e|p-1$, então*

$$|d_K| = p^a,$$

onde $a = e[(n+1)p^{n-1} - \dfrac{p^n-1}{p-1}] - 1$.

Na Seção 3.4 apresentaremos uma nova demonstração para o Teorema 3.6 fazendo uso de corpos p-ádicos e do diferente.

Teorema 3.7. [*37, pag.12*] *Seja $n \in \mathbb{Z}$, onde $n > 1$ um inteiro positivo. O discriminante do n-ésimo corpo ciclotômico é dado por*

$$d_K = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}},$$

onde o produto é tomado sobre todos os $p \in \mathbb{Z}$, onde $p > 1$, que são inteiros primos divisores de n.

Teorema 3.8. [*13*] *Seja $m = \prod_{j=1}^{k} p_j^{\alpha_j}$ a decomposição do inteiro positivo $m \in \mathbb{Z}$ em fatores primos $p_j \in \mathbb{Z}$. Se K é um corpo abeliano de condutor m, então o discriminante absoluto $|d_K|$ de K é*

$$|d_K| = \begin{cases} \left(\dfrac{m}{\prod_{j=1}^{k} \frac{p_j^{\alpha_j - 1 - 1 + \frac{p_j - 1}{u_j}}}{p_j^{\alpha_j - 1}(p_j - 1)}} \right)^{[K:\mathbb{Q}]}, & \text{se } m \neq 2^n \text{ para todo } n \in \mathbb{N}; \\ 2^{(n-1)2^{n-1}}, & \text{se } K = \mathbb{Q}(\xi_{2^n}) \text{ para algum } n \in \mathbb{N}; \\ 2^{n2^{n-1}-1}, & \text{se } m = 2^n \text{ para algum } n \in \mathbb{N} \text{ e } K \neq \mathbb{Q}(\xi_{2^n}); \end{cases}$$

onde $u_j = [K\mathbb{Q}(\xi_{m/p_j^{\alpha_j}}) : \mathbb{Q}(\xi_{m/p_j^{\alpha_j}})]/p_j^{\alpha_j - 1}$.

3.3 Diferente e ideal discriminante

Nesta seção, apresentamos os con de diferente e ideal discriminante, que juntamente com os números p-ádicos serão importantes para nossa contribuição nos resultados envolvendo discriminantes. Sejam A um anel de Dedekind, K seu corpo de frações, L uma extensão finita e separável de K, $\mathcal{O}_K$ o fecho inteiro de K em A e $\mathcal{O}_L$ o fecho inteiro de $\mathcal{O}_K$ em L.

Assumimos que a extensão dos corpos residuais é separável. Considere a forma canônica bilinear simétrica e não degenerada [23, pag. 194], dada pela **forma traço**

$$\begin{aligned} Tr : L \times L &\longrightarrow K \\ (x, y) &\longmapsto Tr(x, y) = Tr_{L|K}(xy). \end{aligned}$$

Para cada ideal $\mathfrak{U}$ de L, seja o $\mathcal{O}_L$-módulo **dual** definido por

$$\mathfrak{U}^* = \{x \in L | Tr_{L|K}(x\mathfrak{U}) \subseteq \mathcal{O}_K\}.$$

A noção de dualidade é justificada pelo isomorfismo

$$\begin{aligned} \mathfrak{U}^* &\longrightarrow Hom_{\mathcal{O}_K}(\mathfrak{U}, \mathcal{O}_K), \\ x &\longmapsto T_x, \end{aligned}$$

onde a aplicação $T_x : \mathfrak{U} \longrightarrow \mathcal{O}_K$ é definida por $T_x(y) = Tr_{L|K}(x, y)$. Além disso,

$$\mathcal{O}_L^* \cong Hom_{\mathcal{O}_K}(\mathcal{O}_L, O_K).$$

O ideal

$$\mathfrak{C}_{\mathcal{O}_L|\mathcal{O}_K} = \mathcal{O}_L^* = \{x \in L | Tr_{L|K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\}$$

é denominado **módulo complementar de Dedekind**, **inverso do diferente** ou **codiferente**. Seu inverso,

$$\mathfrak{D}_{\mathcal{O}_L|\mathcal{O}_K} = \mathfrak{C}_{\mathcal{O}_L|\mathcal{O}_K}^{-1},$$

também denotado por $\mathfrak{D}_{L|K}$, é denominado **diferente** de $\mathcal{O}_L|\mathcal{O}_K$. [23, pag. 194-195].

Como $\mathcal{O}_L \subseteq \mathfrak{C}_{\mathcal{O}_L|\mathcal{O}_K}$, segue que o ideal $\mathfrak{D}_{L|K} \subseteq \mathcal{O}_L$ é um ideal inteiro. Além disso, se $K \subseteq L \subseteq M$ são extensões de corpos, [23, pag. 195] tem-se que

$$\mathfrak{D}_{M|K} = \mathfrak{D}_{M|L}\mathfrak{D}_{L|K}. \tag{3.2}$$

O **ideal discriminante** $\mathfrak{d}_{\mathcal{O}_L|\mathcal{O}_K}$, também denotado por $\mathfrak{d}_{L|K}$, é um ideal de $\mathcal{O}_K$ gerado pelo discriminante $d(\alpha_1, \alpha_2, \ldots, \alpha_n)$ de todas as bases $\alpha_1, \alpha_2, \ldots, \alpha_n$ de L sobre K que estão contidas em $\mathcal{O}_L$. O ideal discriminante é um ideal principal, gerado pelo discriminante [23, pag. 197-198], isto é

$$\mathfrak{d}_{L|K} = \langle d_{L|K} \rangle.$$

O ideal discriminante e o diferente estão relacionados, por [23, pag. 201], do seguinte modo:

$$\mathfrak{d}_{L|K} = N_{L|K}(\mathfrak{D}_{L|K}).$$

Finalmente, se $L|K$ é uma extensão fracamente ramificada de grau e então

$$\mathfrak{D}_{L|K} = \pi_L^{e-1}, \tag{3.3}$$

onde π_L é um elemento primo de $\mathcal{O}_L$.

3.4 Discriminante de subcorpos de $\mathbb{Q}(\xi_{p^r})$, onde p é um primo ímpar

Nesta seção, apresentamos uma nova demonstração para a formula do discriminante de corpos de números cujo condutor é uma potência de um primo ímpar. Pelo Teorema de Kronecker-Weber (Teorema 1.5) tem-se que toda extensão abeliana finita está contida em um corpo ciclotômico. Logo, corpos de números cujo condutor é uma potência de um primo ímpar são exatamente subcorpos de corpos ciclotômicos $\mathbb{Q}(\xi_{p^n})$, onde $n > 0$ é número inteiro e $p > 0$ um primo ímpar.

Deste modo, se K é um corpo de números, cujo condutor é uma potência de um primo ímpar, então K um corpo ciclotômico, ou é um subcorpo de um corpo ciclotômico. Para o primeiro caso, o discriminante absoluto é dado pelo Teorema 3.5. Assim, o discriminante absoluto do p^r-ésimo corpo ciclotômico $L = \mathbb{Q}(\xi_p)$ é dado por

$$|d_{L|\mathbb{Q}}| = p^{p^{p-1}(pn-n-1)}.$$

Agora, seja K um corpo de números cujo condutor é p^n, com p um primo ímpar. Logo, K é um subcorpo de $L = \mathbb{Q}(\xi)$ de grau ep^{n-1} sobre os racionais, onde $\xi = \xi_{p^n}$ é uma raiz p^n-ésima da unidade, com $e, e' \in \mathbb{Z}$ inteiros positivos satisfazendo $ee' = p - 1$. Note que $[L : K] = e'$.

Para calcular o discriminante de K utilizamos os corpos p-ádicos e o diferente. Sejam $L_p = \mathbb{Q}_p(\xi_p) = L\mathbb{Q}_p$ e K_p o subcorpo de L_p de grau ep^{n-1}. Observe que $K_p = K\mathbb{Q}_p$. Como $\mathfrak{d}_{L_p|\mathbb{Q}_p} = \mathfrak{d}_{L|\mathbb{Q}}$ e $\mathfrak{d}_{K_p|\mathbb{Q}_p} = \mathfrak{d}_{K|\mathbb{Q}}$ segue que é suficiente calcular $\mathfrak{d}_{K_p|\mathbb{Q}_p}$. A figura 3.1 apresenta uma relação entre corpos de números e corpos de números p-ádicos, onde os números ao lado das linhas significa o grau da extensão.

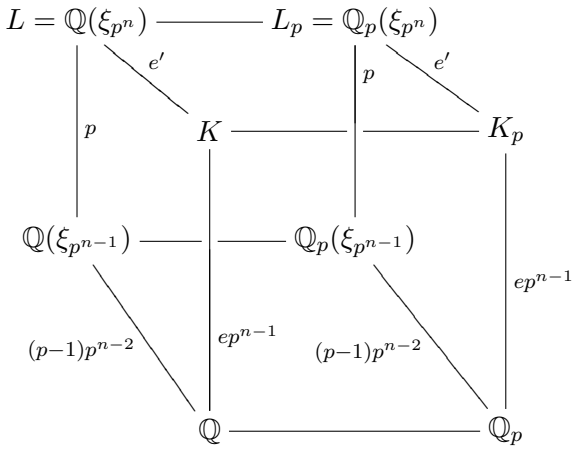

Figura 3.1: Relação entre corpos de números e corpos de números p-ádicos.

Lema 3.2. *O discriminante absoluto do corpo p-ádico K_p é dado por*

$$|d_{K_p|\mathbb{Q}_p}| = p^a, \tag{3.4}$$

onde $a = e[(n+1)p^{n-1} - \dfrac{p^n-1}{p-1}] - 1$.

Demonstração. Pela Proposição 3.5, tem-se que

$$|d_{L_p|\mathbb{Q}_p}| = p^{p^{p-1}(pn-n-1)},$$

isto é,

$$\mathfrak{D}_{L_p|\mathbb{Q}_p} = \pi_{L_p}^{p^{p-1}(pn-n-1)}.$$

Da Equação (3.2) segue que $\mathfrak{D}_{L_p|\mathbb{Q}_p} = \mathfrak{D}_{L_p|K_p}\mathfrak{D}_{K_p|\mathbb{Q}_p}$. Como a extensão $L_p|K_p$ é fracamente ramificada, segue, pela Equação (3.3), que

$$\mathfrak{D}_{L_p|K_p} = \pi_{L_p}^{e'-1}.$$

Assim,

$$\begin{aligned}
(\pi_{L_p})^{p^{n-1}(pn-n-1)} &= \mathfrak{D}_{L_p|\mathbb{Q}_p} \\
&= \mathfrak{D}_{L_p|K_p}\mathfrak{D}_{K_p|\mathbb{Q}_p} \\
&= (\pi_{L_p})^{e'-1}(\pi_{K_p})^a \\
&= (\pi_{L_p})^{e'-1}(\pi_{L_p}^{e'})^a \\
&= (\pi_{L_p})^{e'-1}(\pi_{L_p})^{e'a} \\
&= (\pi_{L_p})^{'-1+e'a},
\end{aligned}$$

e igualando os expoentes, tem-se que

$$p^{n-1}(pn-n-1) = (e'-1) + e'a.$$

Logo,

$$\begin{aligned}
e'a &= p^{n-1}[(p-1)n-1] + e' + 1 \\
&= (p-1)p^{n-1}n - e' - (p^{n-1}-1).
\end{aligned}$$

Desta forma,

$$\begin{aligned}
a &= ep^{n-1}n - e\frac{p^{n-1}-1}{p-1} - 1 \\
&= e[np^{n-1} - p^{n-2} - (p^{n-3} + \cdots + 1)] - 1 \\
&= e[(n+1)p^{n-1} - p^{n-1} - p^{n-2} - p^{n-3} - \cdots - 1] - 1 \\
&= e[(n+1)p^{n-1} - \frac{p^n-1}{p-1}] - 1.
\end{aligned}$$

Portanto, $\mathfrak{D}_{K_p/\mathbb{Q}_p} = (\pi_K)^a$, onde $a = e[(n+1)p^{n-1} - \dfrac{p^n-1}{p-1}] - 1$. Agora, pela definição de discriminante, tem-se que

$$\mathfrak{d}_{K_p|\mathbb{Q}_p} = N_{K_p|\mathbb{Q}_p}(\mathfrak{D}_{K_p|\mathbb{Q}_p}) = N_{K|\mathbb{Q}}(\pi_{K_p}^a) = N_{K_p|\mathbb{Q}_p}(\pi_K)^a = \langle p^a \rangle,$$

onde $a = e[(n+1)p^{n-1} - \dfrac{p^n-1}{p-1}] - 1$. Logo, como $\mathfrak{d}_{K_p|\mathbb{Q}_p} = \langle d_{K_p|\mathbb{Q}_p} \rangle$, segue que $|d_{K_P|\mathbb{Q}_P}| = p^a$, com $a = e[(n+1)p^{n-1} - \dfrac{p^n-1}{p-1}] - 1$, o que prova o lema. □

Teorema 3.9. *Se K é o subcorpo de $\mathbb{Q}(\xi_{p^n})$ de grau ep^{n-1}, com p um primo ímpar e $e|p-1$, então*

$$|d_{K|\mathbb{Q}}| = p^a, \tag{3.5}$$

onde $a = e[(n+1)p^{n-1} - \dfrac{p^n-1}{p-1}] - 1$.

Demonstração. Segue diretamente do Lema 3.2 e das igualdades $\mathfrak{d}_{K|\mathbb{Q}} = \mathfrak{d}_{K_p|\mathbb{Q}_p}$ e $\mathfrak{d}_{K|\mathbb{Q}} = \langle d_{K|\mathbb{Q}} \rangle$. □

Corolário 3.1. *Se K é um subcorpo de $\mathbb{Q}(\xi_p)$, de grau e, então*

$$|d_K| = p^{e-1}.$$

Demonstração. É suficiente provar que, no Teorema 3.9, $a = e - 1$ quando $n = 1$. Para isto, tem-se que

$$\begin{aligned} a &= e[(n+1)p^{n-1} - \frac{p^n-1}{p-1}] - 1 \\ &= e[2p^0 - \frac{p-1}{p-1}] - 1 \\ &= e[2-1] - 1 \\ &= e - 1, \end{aligned}$$

o que prova o corolário. □

Corolário 3.2. *Se K é um subcorpo de $\mathbb{Q}(\xi_{p^2})$ de grau p então*

$$d_K = p^{2(p-1)}.$$

Demonstração. Pelo Teorema 3.9, é suficiente provar que $a = 2(p-1)$ quando $e = 1$ e $n = 2$. Assim,

$$\begin{aligned} a &= e[(n+1)p^{n-1} - \frac{p^n-1}{p-1}] - 1 \\ &= [(3)p^1 - \frac{p^2-1}{p-1}] - 1 \\ &= [3p - p - 1] - 1 \\ &= 2p - 2 \\ &= 2(p-1), \end{aligned}$$

o que prova o corolário. □

3.5 Conclusões

Neste capítulo foram apresentados os principais resultados conhecidos na literatura sobre discriminante de corpos de números abelianos. Nota-se que esses resultados, embora se mostrando muito úteis, como ferramenta de análise durante a geração de reticulados via corpos de números, ainda não são tão amplamente utilizados nas pesquisas. Fazendo uso desses resultados, apresentamos, na Seção 3.4 uma nova demonstração para a fórmula do discriminante para corpos de números abelianos cujo condutor é uma potência de primo ímpar. Esse resultado, juntamente com os corolários, são a nossa principal contribuição deste capítulo. Os resultados obtidos neste capítulo auxiliam na pesquisa da obtenção de reticulados algébricos com enfoque em seus principais parâmetros.

Capítulo

4

Reticulados e Conjectura de Minkowski

Neste capítulo apresentamos o conceito de reticulados e a conjectura de Minkowski. Um reticulado no $\mathbb{R}^n$ é um subconjunto discreto que forma um grupo aditivo. Relacionado a um reticulado, existem as matrizes geradora e de Gram deste reticulado. A matriz geradora de um reticulado caracteriza completamente o reticulado. Para gerar um reticulado no $\mathbb{R}^n$, utilizando a teoria algébrica dos números, em particular, um ideal fracionário de um corpo de números, existem o homomorfismo canônico, também conhecido como homomorfismo de Minkowski, e o homomorfismo torcido. Também existe a noção de reticulado ideal, que é dado de modo mais abstrato do que um reticulado no $\mathbb{R}^n$, mas prova-se que os dois conceitos são equivalentes. Em seguida, apresentamos o mínimo euclidiano para corpos de números, que, de modo informal, mede o quão distante está o corpo de números de ser euclidiano. Apresentamos também algumas cotas conhecidas para o mínimo euclidiano, e a conjectura de Minkowski, que é estabelecida para reticulados em geral e para corpos de números.

4.1 Reticulados

Nesta seção, apresentamos o conceito de reticulado, juntamente com suas principais propriedades. Seja $n \in \mathbb{Z}$ um inteiro positivo. Um conjunto $\Lambda \subseteq \mathbb{R}^n$ é um **reticulado** no $\mathbb{R}^n$ quando Λ é um grupo aditivo discreto. Tem-se que um conjunto $\Lambda \subseteq \mathbb{R}^n$ é um reticulado no $\mathbb{R}^n$ se, e somente se, existe um conjunto de vetores $\{v_1, v_2, \ldots, v_m\}$, com $m \leqslant n$, linearmente

independentes tal que

$$\Lambda = \left\{ \sum_{j=1}^{m} \lambda_j v_j; \quad \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, 2, \ldots, m \right\},$$

ou seja, Λ é um $\mathbb{Z}$-módulo livre de posto m e $\{v_1, v_2, \ldots, v_m\}$ é uma base de Λ. Neste caso, Λ é dito um reticulado de **posto** m e $\{v_1, v_2, \ldots, v_m\}$ é dita uma **base** do reticulado ([7, pags. 3-4]).

Definimos, agora, as matrizes geradora e de Gram de um reticulado.

Definição 4.1. [7, *pag.*4] *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto $m \leqslant n$ e $\{v_1, v_2, \ldots, v_m\}$ uma base de Λ. Seja $v_j = (v_{j1}, v_{j2}, \ldots, v_{jn})$ a representação do vetor v_j na base canônica do $\mathbb{R}^n$, para $j = 1, 2, \ldots m$. A matriz*

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

é chamada **matriz geradora** *do reticulado Λ e os vetores do reticulado Λ são todos os vetores da forma*

$$xM,$$

onde $x = (x_1, x_2, \ldots, x_m) \in \mathbb{Z}^m$ é um vetor arbitrário com entradas x_j inteiras. A matriz

$$G = MM^t,$$

onde M^t denota a matriz transposta de M, é chamada **matriz de Gram** *de Λ. As entradas da matriz G são $\langle v_j, v_k \rangle$, para $j, k = 1, 2 \ldots, m$, ou seja, cada entrada da matriz G é o produto interno de elementos da base de Λ.*

Embora para cada base do reticulado Λ temos uma matriz geradora diferente e uma matriz de Gram diferente, o determinante da matriz de Gram independe da escolha da base. Tal valor é o **determinante do reticulado** Λ e é denotado por $\det(\Lambda)$. .

Definição 4.2. *Diz-se que um subconjunto $\Lambda' \subseteq \Lambda$ de um reticulado Λ é um* **subreticulado** *se Λ' for um reticulado. A cardinalidade do grupo quociente Λ/Λ' é chamado* **índice** *de Λ/Λ'.*

Definição 4.3. [7, *pag.*10] *Dado um reticulado n-dimensional $\Lambda \subseteq \mathbb{R}^n$, o* **reticulado dual** *de Λ é definido por*

$$\Lambda^* = \{x \in \mathbb{R}^n; \langle x, z \rangle \in \mathbb{Z} \text{ para todo } z \in \Lambda\}.$$

O reticulado dual é um reticulado e, se M é a matriz geradora de um reticulado n-dimensional Λ, então $(M^{-1})^t$ é a matriz geradora do reticulado dual Λ^*.

Definição 4.4. [7, *pag.*4] *Dado um reticulado* $\Lambda \subseteq \mathbb{R}^n$ *com base* $\{v_1, v_2, \ldots, v_n\}$*, o conjunto*

$$\left\{ \sum_{j=1}^{n} a_j v_j;\ 0 \leqslant a_j \leqslant 1,\ \textit{para } i = 1, 2, \ldots n \right\}$$

é chamado **politopo fundamental** *de* Λ *ou* **paralepípedo fundamental** *de* λ*.*

Definição 4.5. [7, *pag.*4] *Dado um reticulado n-dimensional* $\Lambda \subseteq \mathbb{R}^n$*, um subconjunto* $F \subseteq \mathbb{R}^n$ *é uma* **região fundamental** *do reticulado* Λ *se* F *ladrilha o espaço* $\mathbb{R}^n$ *por translações* $v+F$*, com* $v \in \Lambda$*, isto é,* $R^n = \bigcup_{v\in\Lambda} v+F$*, e dois ladrilhos ou são distintos ou se interceptam apenas nos bordos, onde, para cada* $v \in \Lambda$*,* $v + F$ *é chamado* **ladrilho***.*

O volume de qualquer região fundamental de um reticulado Λ é o mesmo e tal valor é denominado **volume do reticulado** Λ e denotado portanto $vol(\Lambda)$. O politopo fundamental de Λ é uma região fundamental para Λ.

Proposição 4.1. *O volume da região fundamental é dado por*

$$vol(\Lambda) = det(\Lambda)^{1/2}.$$

Definição 4.6. [7, *pag.*10] *Se dois reticulados podem ser obtidos, um do outro, por uma rotação, reflexão e multiplicação por escalar, então eles são ditos* **equivalentes** *ou* **isomorfos***.*

Duas matrizes geradoras M e M' definem reticulados equivalentes se, e somente se, elas estão relacionadas por

$$M' = cUMB,$$

onde $c \in \mathbb{R}$ é uma constante não nula, U é uma matriz com entradas inteiras e determinante ± 1, e B é uma matriz real ortogonal (isto é, $BB^t = Id$ é a matriz identidade). As correspondentes matriz de Gram são relacionadas por

$$M'(M')^t = c^2 UMM^t U^T.$$

Se $c = 1$, então os reticulados M e M' são ditos reticulados **congruentes**.

Um reticulado é dito **integral** se sua matriz de Gram possui entradas inteiras . Tem-se que um reticulado Λ é integral se, e somente se,

$$\Lambda \subseteq \Lambda^*.$$

Um reticulado integral Λ é dito **par** se $\langle x, x\rangle$ é um inteiro par, para todo $x \in \Lambda$; caso contrário, Λ é dito um reticulado ímpar. Para todo reticulado integral Λ, tem-se que

$$\Lambda \subseteq \Lambda^* \subseteq \frac{1}{\det(\Lambda)}\Lambda.$$

Um reticulado integral Λ é dito **auto-dual** ou **unimodular** quando $|\det(\Lambda)| = 1$, ou, equivalentemente, $\Lambda = \Lambda^*$.

Os reticulados E_8 e Λ_{24} são exemplos de reticulados unimodulares pares, e os reticulados $\mathbb{Z}^n$, para $n = 1, 2, \ldots$, são reticulados unimodulares ímpares.

4.2 Homomorfismo de Minkowski

Neste capítulo apresentamos o homomorfismos de Minkowski, sendo uma ferramenta importante na geração de reticulados no $\mathbb{R}^n$.utilizado para gerar reticulados a partir de corpos de números Seja K um corpo de números de grau n e assinatura (r_1, r_2), isto é, r_1 é o número de homomorfismo reais e $2r_2$ é o número de homomorfismo imaginários (Definição 1.17). Tem-se que $n = r_1 + 2r_2$.

Definição 4.7. [*28, pag.*56] *Sejam K um corpo de números de grau n e assinatura (r_1, r_2). A aplicação*

$$\begin{aligned} \sigma_K : K &\longrightarrow \mathbb{R}^n \\ x &\longrightarrow \sigma_K(x), \end{aligned}$$

dada por

$$\begin{aligned} \sigma_K(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \\ \Re(\sigma_{r_1+2}(x)), \Im(\sigma_{r_1+2}(x)), \ldots, \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))), \end{aligned}$$

onde $\Re$ e $\Im$ representam a parte real e imaginária, respectivamente, de um número complexo, é chamado **homomorfismo canônico** *ou* **homomorfismo de Minkowski** *de K em $\mathbb{R}^n$.*

O homomorfismo de Minkowski é um homomorfismo injetor de grupos aditivos.

Proposição 4.2. [*28, pag.*56] *Se $M \subseteq K$ é um $\mathbb{Z}$-submódulo livre de posto n de K, com base $\{x_1, x_2, \ldots, x_n\}$, então $\sigma_K(M)$ é um reticulado n-dimensional no $\mathbb{R}^n$ com base $\{\sigma_K(x_1), \sigma_K(x_2), \ldots, \sigma_K(x_2)\}$. Além disso,*

$$vol(\sigma_K(M) = \det(\sigma_K(M))^{1/2} = 2^{-r_2}|det(\sigma_j(x_k)| = 2^{-r_2}|det(Tr_{K|\mathbb{Q}}(x_j x_k))|^{1/2}.$$

Suponha, agora, que K é um corpo de números totalmente real de grau n. O homomorfismo canônico é dado por

$$\sigma_K(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)).$$

Se $M \subseteq K$ é um $\mathbb{Z}$-submódulo livre de posto n de K, com base $\{x_1, x_2, \ldots, x_n\}$, então a matriz geradora do reticulado $\sigma_K(M)$ é dada por

$$\begin{pmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \cdots & \sigma_1(x_n) \\ \sigma_2(x_1) & \sigma_2(x_2) & \cdots & \sigma_2(x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(x_1) & \sigma_n(x_2) & \cdots & \sigma_n(x_n) \end{pmatrix}$$

e a matriz de Gram é dada por

$$G = (Tr_{K|\mathbb{Q}}(x_j x_k)) = \begin{pmatrix} Tr_{K|\mathbb{Q}}(x_1x_1) & Tr_{K|\mathbb{Q}}(x_1x_2) & \cdots & Tr_{K|\mathbb{Q}}(x_1x_n) \\ Tr_{K|\mathbb{Q}}(x_2x_1) & Tr_{K|\mathbb{Q}}(x_2x_2) & \cdots & Tr_{K|\mathbb{Q}}(x_2x_n) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{K|\mathbb{Q}}(x_nx_1) & Tr_{K|\mathbb{Q}}(x_nx_2) & \cdots & Tr_{K|\mathbb{Q}}(x_nx_n) \end{pmatrix}.$$

Proposição 4.3. [*28, pag.*57] *Sejam K um corpo de números e $\mathcal{O}_K$ o anel de inteiros de K. Se $I \subseteq \mathcal{O}_K$ é um ideal não nulo de $\mathcal{O}_K$ então $\sigma_K(I)$ é um reticulado com volume*

$$vol(\sigma_K(I)) = det(\sigma_K(I))^{1/2} = 2^{-r_2}|d_K|^{1/2}N(I),$$

onde r_2 é o número de pares de homomorfismos imaginários de K, $N(I)$ é a norma do ideal I e $|d_K|$ é o discriminante absoluto de K. Se K é um corpo totalmente real então $\sigma_K(\mathcal{O}_K)$ é um reticulado com volume

$$vol(\sigma_K(\mathcal{O}_K)) = |d_K|^{1/2}.$$

Com isso, tem-se que cada corpo de números totalmente real de grau n gera um reticulado $\sigma_K(\mathcal{O}_K) \subseteq \mathbb{R}^n$, com determinante $det(\sigma_K(\mathcal{O}_K)) = |d_K|$.

4.3 Reticulados ideais

Utilizamos, nesta seção, as notações e a terminologia presente em [5] e [4]. Definimos, aqui, os reticulados de um modo mais genérico do que o apresentado na Seção 4.1, entretanto, usaremos indistintamente os dois conceitos.

Definição 4.8. *Sejam K um corpo de números e $\mathcal{O}_K$ o anel de inteiros de K. Um* **reticulado** *é um par $(\mathfrak{a}, b)$, onde $\mathfrak{a}$ é um ideal fracionário de K, e $b : \mathfrak{a} \times \mathfrak{a} :\longrightarrow \mathbb{R}$ é uma forma bilinear simétrica tal que*

$$b(\lambda x, y) = b(x, \overline{\lambda} y,)$$

para todos $x, y \in \mathfrak{a}$ e todo $\lambda \in \mathcal{O}_K$.

Quando $b(x, y) \in \mathbb{Z}$, para todo $x, y \in \mathfrak{a}$, diz-se que $(\mathfrak{a}, b)$ é um reticulado integral. Um reticulado integral $(\mathfrak{a}, b)$ é dito ser par, se $b(x, x) \in 2\mathbb{Z}$, para todo $x \in \mathfrak{a}$.

Proposição 4.4. [*5, pag.*169] *Sejam K um corpo de números e $\mathcal{O}_K$ o anel de inteiros de K. Se $(\mathfrak{a}, b)$ é um reticulado, onde $\mathfrak{a}$ é um ideal fracionário de K e $b : \mathfrak{a} \times \mathfrak{a} :\longrightarrow \mathbb{R}$, então as seguintes afirmações são equivalentes:*

i) $(\mathfrak{a}, b)$ *é um reticulado ideal;*

ii) existe um elemento $\alpha \in K$, com $\overline{\alpha} = \alpha$, tal que

$$b(x, y) = Tr_{K|\mathbb{Q}}(\alpha x \overline{y}).$$

O **posto** do reticulado ideal é o grau do corpo de números K.

Apresentamos, na Seção 3.3, o codiferente, que é dado por

$$\mathfrak{C}_{\mathcal{O}_L|\mathcal{O}_K} = \{x \in L | Tr_{L|K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\},$$

referente a extensão de corpos de números $L|K$. Tomando a extensão $K|\mathbb{Q}$, tem-se o que codiferente de K é dado por

$$\mathfrak{C}_K = \{x \in K | Tr_{K|\mathbb{Q}}(xy) \in \mathbb{Z}, \text{ para todo } y \in \mathcal{O}_K\}.$$

Proposição 4.5. *Seja K um corpo de números, $\mathfrak{a}$ um ideal de $\mathcal{O}_K$, $\alpha \in K$ e $b : \mathfrak{a} \times \mathfrak{a} \longrightarrow \mathbb{R}$ a forma $\mathbb{Z}$-bilinear dada por*

$$b(x, y) = TrK|\mathbb{Q}(\alpha x\overline{y}).$$

O reticulado ideal $(\mathfrak{a}, b)$ é um reticulado ideal integral se, e somente se,

$$\alpha\mathfrak{a}\overline{\mathfrak{a}} \subseteq \mathfrak{C}_K.$$

4.4 Homomorfismo torcido

Nesta seção, apresentamos uma variante do homomorfismo canônico, onde o homomorfismo canônico torna-se um caso particular do homomorfismo torcido. Este homomorfismo gera reticulados no $\mathbb{R}^n$. Sejam K um corpo de números de grau n e assinatura (r_1, r_2), isto é, r_1 é o número de homomorfismo reais e $2r_2$ é o número de homomorfismo imaginários. Se $\sigma : K \longrightarrow \mathbb{R}^n$ é o homomorfismo de Minkowski, conforme Definição 4.7, tem-se que para cada ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, o par $(\mathfrak{a}, b)$, onde b é a forma bilinear simétrica dada por $b(x, y) = Tr_{K|\mathbb{Q}}(x\overline{y})$, é um reticulado ideal integral.

Seja $\alpha \in K$ totalmente positivo, isto é $\sigma_j(\alpha) \in \mathbb{R}$ e $\sigma_j(\alpha) > 0$, para todo $j = 1, 2, \ldots, n$. O homomorfismo

$$\begin{aligned}\sigma_\alpha(x) = (&\sqrt{\alpha_1}x_1, \sqrt{\alpha_2}x_2, \ldots, \sqrt{\alpha_{r_1}}x_{r_1}, \sqrt{2\alpha_{r_1+1}}\Re(x_{r_1+1}), \sqrt{2\alpha_{r_1+1}}\Im(x_{r_1+1}),\\ &\sqrt{2\alpha_{r_1+2}}\Re(x_{r_1+2}), \sqrt{2\alpha_{r_1+2}}\Im(x_{r_1+2}), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Re(x_{r_1+r_2}), \sqrt{2\alpha_{r_1+r_2}}\Im(x_{r_1+r_2})),\end{aligned}$$

onde $x_j = \sigma_j(x)$, $\alpha_j = \sigma_j(\alpha)$ e $\Re(x)$ e $\Im(x)$ denotam a parte real e imaginária de x, respectivamente, é chamado **homomorfismo torcido**.

Proposição 4.6. [5, *pag.*179] *Para cada ideal integral $\mathfrak{a}$ de K e para cada elemento $\alpha \in K$ totalmente positivo, o reticulado $\sigma_\alpha(\mathfrak{a}) \subseteq \mathbb{R}^n$ é um reticulado ideal. Reciprocamente, para cada reticulado ideal $(\mathfrak{a}, b)$, existe $\alpha \in K$ tal que o reticulado ideal $\sigma_\alpha(\mathfrak{a})$ é isomorfo ao reticulado ideal $(\mathfrak{a}, b)$.*

A Proposição 4.6 relaciona as definições de reticulados apresentadas nas Seções 4.1 e 4.3, provando que as duas definições são equivalentes.

4.5 Mínimo euclidiano

Nesta seção, apresentamos o conceito de mínimo euclidiano com o objetivo de de introduzir a conjectura de Minkowski, mas antes de introduzirmos o mínimo euclidiano é necessário definirmos o algoritmo de Euclides e os anéis euclidianos. O algoritmo de Euclides consiste no fato que, dados dois elementos inteiros $a, b \in \mathbb{Z}$, podemos fazer a divisão de a por b, obtendo um resto "pequeno", no sentido que o valor absoluto do resto é estritamente menor que o valor absoluto de b. Generalizando esse fato, tem-se um anel euclidiano.

Considere, nessa seção, K um corpo de números e $\mathcal{O}_K$ o anel de inteiros de K.

Definição 4.9. [*9, pag.*22] *Um* **anel euclidiano** *é um anel A munido de uma função*

$$\varphi : A\backslash\{0\} \longrightarrow \mathbb{Z}^+,$$

onde $\mathbb{Z}^+ = \{0, 1, 2, \ldots\}$ é o conjunto dos inteiros maiores ou iguais a zero, de modo que, dado quaisquer elementos $a, b \in A$, com b não nulo, existem $q, r \in A$ tais que

$$a = bq + r \text{ com } \varphi(r) < \varphi(b) \text{ ou } r = 0,$$

e que para todos $a, b \in A\backslash\{0\}$ tem-se que

$$\varphi(a) \leqslant \varphi(ab).$$

Definição 4.10. *Um corpo de números K é dito ser um* **corpo euclidiano** *se o anel de inteiros $\mathcal{O}_K$ de K é um anel euclidiano com respeito a norma do valor absoluto.*

Teorema 4.1. [*30, pag.*11] *O seu anel de inteiros $\mathcal{O}_K$ é euclidiano se, e somente se, para cada $y \in K$, existe um inteiro algébrico $x \in \mathcal{O}_K$, tal que $N(y - x) < 1$, onde N é a norma do valor absoluto.*

Definição 4.11. *Seja $x \in K$. O número real $m_K(x)$, definido por*

$$m_K(x) = \inf\{|N_{K|Q}(x - y)|;\ y \in \mathcal{O}_K\},$$

é chamado **mínimo euclidiano de x em K.**

Proposição 4.7. [*30, pag.*26] *O mínimo Euclidiano m_K possui as seguintes propriedades:*

i) $m_K(\alpha x - \beta) = m_K(x)$, para todo $x \in K$ e $\alpha, \beta \in \mathcal{O}_K$, com $\alpha \neq 0$.

ii) Para todo $x \in K$, existe $\alpha \in \mathcal{O}_K$ tal que $m_k(x) = |N_{K|\mathbb{Q}}(x - \alpha)|$.

iii) $m_K \in \mathbb{Q}$.

iv) $m_k(x) = 0$ se, e somente se, $x \in \mathcal{O}_K$.

Definição 4.12. *O número real positivo $M(K)$, definido por*

$$M(K) = \sup\{m_K(x);\ x \in K\},$$

é chamado o **mínimo euclidiano** *de K.*

O mínimo euclidiano também pode ser definido por

$$M(K) = \inf\{k \in \mathbb{R}; k > 0; \forall x \in K, \text{ existe } \alpha \in \mathcal{O}_K \text{ com } N_{K|\mathbb{Q}}(x - \alpha) < k\},$$

isto é, essas duas definições são equivalentes.

Quando $M(K) > 1$, segue que existem $a, b \in \mathcal{O}_K\backslash\{0\}$ tais que, para todo $q \in \mathcal{O}_K$ não nulo, $|N_{K|\mathbb{Q}}(a - bq)| > |N_{K|\mathbb{Q}}(b)|$, e assim $\mathcal{O}_K$ não é um anel euclidiano com a função norma $|N_{K|\mathbb{Q}}|$. Quando $M(K) < 1$, para todos $a, b \in \mathcal{O}_K\backslash\{0\}$, existe $q \in \mathcal{O}_K$ não nulo tal que $|N_{K|\mathbb{Q}}(a - bq)| < |N_{K|\mathbb{Q}}(b)|$, e assim $\mathcal{O}_K$ é um anel euclidiano com a função norma $|N_{K|\mathbb{Q}}|$. Entretanto, quando $M(K) = 1$ tem-se que $\mathcal{O}_K$ pode ser euclidiano ou não.

Definição 4.13. *Seja L um reticulado n-dimensional no $\mathbb{R}^n$. O* **mínimo** *de L é definido por*

$$\min(L) = min\{\langle l, l\rangle; l \in L, l \neq 0\},$$

que é o quadrado da distância mínima entre dois pontos em L, e o **máximo** *de L é definido por*

$$\max(L) = \sup\{\min\{\langle x - l, x - l\rangle; l \in L\}; x \in \mathbb{R}\},$$

que é a máxima distância de um ponto do $\mathbb{R}^n$ até L.

4.6 Conjectura de Minkowski

Nesta seção apresentamos a conjectura de Minkowski, devida à Minkowski, que aparece em *Diophantische Approximationen*, 1907 de H. Minkowski [20]. Em 1936, no trabalho de J. K. Koksma, [15], já era conhecida como Conjectura de Minkowski. Deste modo, apresentamos a conjectura de Minkowski para reticulados e, a partir do fato que a partir de um corpo de números totalmente real obtém-se um reticulado no $\mathbb{R}^n$, que é a conjectura de Minkowski para corpos de números totalmente reais. No Capítulo 7, Seção 7.2, apresentamos uma demonstração que a conjectura de Minkowski é válida para corpos de grau p e de condutor p^2, com p um primo ímpar. Para tal, é essencial o conhecimento do anel de inteiros deste corpo e a da forma traço sobre o mesmo, que é dada pelo Teorema 7.2.

Seja $n > 0$ um inteiro. Considere a função $N : \mathbb{R}^n \longrightarrow \mathbb{R}$ definida por $N(x) = |x_1 x_2 \cdots x_n|$, onde $x = (x_1, x_2, \ldots, x_n)$.

Conjectura 4.1. [*30, pag.*63] *Para qualquer reticulado $\Lambda \subseteq \mathbb{R}^n$ tem-se que*

$$\sup_{x \in \mathbb{R}^n} \inf_{y \in \Lambda} N(x - y) \leqslant 2^{-n}|det(\Lambda)|.$$

Este conjectura é válida para $n = 2, 3, 4$ e 5 através dos trabalhos de Minkowski, Remak, Dysib e Skubenko em [20], [25], [8], [32] e [31], respectivamente. Recentemente, foi apresentada por R. J. Hans-Gill et al, o trabalho *A unified simple proof of a conjecture of Woods for* $n \leqslant 6$ [38], que contém uma demonstração unificada para a conjectura de Woods para $n \leqslant 6$, o que implica que a conjectura de Minkowski é válida para $n \leqslant 6$. Seguindo a mesma construção, tem-se o trabalho *On conjectures of Minkowski and Woods for* $n = 7$, [39], que estende o resultado para $n = 7$.

Motivado pelo estudo de inteiros algébricos, tem-se a seguinte conjectura em teoria dos números:

Conjectura 4.2. [*3, pag.*306] *Seja K um corpo de números totalmente real de grau n e discriminante d_K. Para cada $x \in K$, existe um inteiro algébrico $y \in K$ tal que*

$$|N_{K|\mathbb{Q}}(x - y)| \leqslant 2^{-n}\sqrt{|d_K|}.$$

Conjectura 4.3. [*30, pag.*63] *Para todo corpo de números totalmente real K de grau n e discriminante d_K tem-se a seguinte cota superior para o mínimo euclidiano:*

$$M(K) \leqslant 2^{-n}\sqrt{|d_K|}.$$

4.7 Algumas cotas conhecidas para o mínimo euclidiano

Apresentamos, nessa seção, alguns resultados presentes em [22], 2005, e em [3], 2006, sobre o mínimo euclidiano, onde são encontrados limitantes para o mínimo euclidiano em corpos quadráticos, em certos corpos ciclotômicos e em determinados subcorpos maximais reais de corpos ciclotômicos.

Proposição 4.8. [*22, pag.*443] *Sejam $d > 1$ um inteiro positivo livre de quadrados, $K = \mathbb{Q}(\sqrt{d})$ um corpo quadrático e $\mathcal{O}_K$ o anel de inteiros de K. Se $\mathfrak{a} \subseteq K$ é um ideal fracionário de K, então*

$$M(\mathfrak{a}) \leqslant \frac{1}{4}\sqrt{|d_K|},$$

onde $|d_K|$ representa o discriminante absoluto de K. Em particular, a Conjectura 4.3 de Minkowski é válida para K.

Proposição 4.9. [*22, pag.*445] *Sejam $d > 1$ um inteiro positivo livre de quadrados e $K = \mathbb{Q}(\sqrt{d})$ um corpo quadrático com discriminante absoluto $|d_K|$. Se $|d_K| \neq 4(t^2 + 1)$ e $|d_K| \neq (2t - 1)^2 + 4$, para todo $t \in \mathbb{N}$ natural, então*

$$M(K) < \frac{1}{4}\sqrt{|d_K|}.$$

Sejam $U_p = pI_{p-1} - J_{p-1}$ a matriz de Gram de $L_{p,p-1}$ e $T_p = pI_{(p-1)/2} - 2J_{(p-1)/2}$ tal que $\frac{1}{2}T_p$ é a matriz de Gram de $L_{p/2,(p-1)/2}$, onde $L_{b,n}$ é um reticulado no $\mathbb{R}^n$ com matriz de

Gram

$$A = \begin{pmatrix} b-1 & -1 & \cdots & -1 \\ -1 & b-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & & b-1 \end{pmatrix}. \tag{4.1}$$

Mais detalhes sobre o reticulado $L_{b,n}$ podem ser obtidas no Teorema 7.1.

Proposição 4.10. [*22, pag.*450] *Sejam p um primo, $r \geqslant 1$ um inteiro positivo e $\xi = \xi_{p^r}$ uma raiz p^r-ésima primitiva da unidade em $\mathbb{C}$. Seja ainda $K = \mathbb{Q}(\xi + \xi^{-1})$ o subcorpo maximal real do p^r-ésimo corpo ciclotômico $\mathbb{Q}(\xi_{p^r})$ e $\mathcal{O}_K = \mathbb{Z}[\xi + \xi^{-1}]$ o anel de inteiros de K.*

i) Se $p > 2$ é ímpar, então o ideal reticulado $(\mathcal{O}_K, Tr(1))$ é isométrico ao reticulado ideal com matriz de Gram

$$\perp^{\frac{p^r-1}{2}} p^{r-1}U_p \perp p^{r-1}T_p.$$

ii) Se $p = 2$, então para $\alpha = 2+\xi+\xi^{-1} \in \mathcal{O}_K$ o ideal reticulado $(\mathcal{O}_K, 2^{1-r}Tr(\alpha)$ é isométrico ao reticulado $\mathbb{Z}^{2^{r-2}}$.

Corolário 4.1. [*22, pag.*451] *Sejam K e $\mathcal{O}_K$ como na Proposição 4.10. Se p é ímpar então*

$$\max(\mathcal{O}_K, Tr(1)) \leqslant \frac{p^{r-2}}{24}(p^{r+2} - p^r - 3p + 3).$$

Corolário 4.2. [*22, pag.*451] *Sejam p um primo ímpar, $r \geqslant 1$ um inteiro positivo (se $p = 3$ então suponha $r \geqslant 2$), $\xi = \xi_{p^r}$ uma raiz p^r-ésima primitiva da unidade em $\mathbb{C}$, $K = \mathbb{Q}(\xi+\xi^{-1})$ o subcorpo maximal real do p^r-ésimo corpo ciclotômico $\mathbb{Q}(\xi_{p^r})$ e $\mathcal{O}_K = \mathbb{Z}[\xi + \xi^{-1}]$ o anel de inteiros de K. O mínimo euclidiano de K satisfaz*

$$M(K) \leqslant (\frac{\max(\mathcal{O}_K, Tr(1))}{n})^{n/2} \leqslant (\frac{p^r(p+1)-3}{12p})^{n/2} = z^n\sqrt{|d_K|},$$

onde

$$z = \frac{1}{2\sqrt{3}}(\frac{p^{r+2}+p^r-3}{p})^{1/2}p^{-r/2}p^{\frac{1+p^{1-r}}{2(p-1)}} < \frac{1}{2\sqrt{3}}1.6 < \frac{1}{2}.$$

Se $p = 2$ então

$$M(K) \leqslant 2^{-n}\sqrt{|d_K|}.$$

Embora a conjectura de Minkowski seja feita sobre corpos totalmente reais e o limitante $M(K) \leqslant 2^n\sqrt{|d_K|}$ não seja válido para todo corpo de números K de grau n, esse limitante vale para algumas famílias. Para corpos ciclotômicos tem-se o seguinte teorema.

Teorema 4.2. [*3, pag.*306, 318] *Se K é um corpo ciclotômico de grau n e discriminante absoluto $|d_K|$, então*

$$M(K) \leqslant 2^{-n}\sqrt{|d_K|}.$$

Para certas famílias de corpos ciclotômicos existem limitantes melhores para o mínimo euclidiano.

Proposição 4.11. [*3, pag.*319] *Seja $K = \mathbb{Q}(\xi_m)$ o m-ésimo corpo ciclotômico de grau n. Se m é da forma $m = 2^r 3^s 5^t$, com $r \leqslant 0$, $s \leqslant 1$ e $t \leqslant 1$, $m = 2^r 5^s$, com $r \leqslant 2$ e $s \leqslant 1$, ou $m = 2^r 3^s$, com $r \leqslant 3$ e $s \leqslant 1$, onde $r, s, t \in \mathbb{Z}$ são inteiros, então*

$$M(K) \leqslant 8^{-n/2}\sqrt{|d_K|}.$$

Se m é da forma $m = 2^r 5^s 7^t$ com $r \leqslant 0$, $s \leqslant 1$ e $t \leqslant 1$, $m = 2^r 3^s 5^t$ com $r \leqslant 0$, $s \leqslant 2$ e $t \leqslant 1$ ou $m = 2^r 3^s 7^t$ com $r \leqslant 2$, $s \leqslant 1$ e $t \leqslant 1$, onde $r, s, t \in \mathbb{Z}$ são inteiros, então

$$M(K) \leqslant 12^{-n/2}\sqrt{|d_K|}.$$

4.8 Conclusões

Nesta capítulo, o objetivo foi apresentar a conjectura de Minkowski. Além disso, foram definidos os reticulados no $\mathbb{R}^n$ e os reticulados ideais, assim como dois métodos para obter reticulados algébricos a partir de corpos de números. A conjectura de Minkowski para reticulados utiliza tais conceitos, sendo que para a conjectura de Minkowski para corpos de números, motivada pelo homomorfismo de Minkowski, é necessário o conhecimento do mínimo euclidiano. Também apresentamos algumas cotas conhecidas para o mínimo euclidiano, sendo estes resultados motivadores da Seção 7.2.

Em especial, destacamos os trabalhos [38] e [39], que trabalham com a conjectura de Woods, que por sua vez implica na conjectura de Minkowski. Acreditamos que o raciocínio apresentado por esses trabalhos possa ser entendido para dimensões superiores. Entretanto, fazer tal extensão exigirá uma quantidade cada vez maior de cálculos. Para $n = 7$ é necessário analisar 64 casos e para $n = 8$ é necessário analisar 128 casos, o que impossibilita extender este raciocínio para dimensões n muito maiores, a menos que seja possível utilizar modelos computacionais para isto.

$K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi)$. Apresentamos, na Seção 5.3, uma nova demonstração da descrição dos subcorpos K do p-ésimo corpo ciclotômico $\mathbb{Q}(\xi_p)$. Ainda na Seção 5.3, o Lema 5.6 apresenta uma base integral para K e tal base integral é formada pelos conjugados de θ. O Teorema 5.3 resume os resultados da seção, assim como fornece a formula do discriminante absoluto para o subcorpo K. Na Seção 5.4, descrevemos explicitamente os corpos de condutor potência de 3, onde provamos que apenas corpos ciclotômicos e corpos maximais reais de corpos ciclotômicos podem possuir condutor potência de 3. Apresentamos, no Corolário 5.3, os anel de inteiros e o discriminante absoluto para cada um destes subcorpos.

5.1 Extensões cíclicas e conjugados

Apresentamos, nesta seção, alguns resultados presentes na literatura que serão utilizados nas seções seguintes para obtenção dos subcorpos do p^r-ésimo corpo ciclotômico $L = \mathbb{Q}(\xi_{p^r})$, onde p é um primo ímpar e $r > 0$ é um inteiro positivo.

Proposição 5.1. [*28, pag.*88] *Seja $L = \mathbb{Q}(\xi_n)$ o n-ésimo corpo ciclotômico, com $n \in \mathbb{Z}$ um inteiro positivo. O grupo de Galois $G = Gal(L|\mathbb{Q})$ da extensão $L|\mathbb{Q}$ é isomorfo ao grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$, dos inteiros inversíveis módulo n.*

Proposição 5.2. [*21, pag.*127],[*26, pag.*43] *O grupo multiplicativo de $\mathbb{Z}/4\mathbb{Z}$ é cíclico, gerado pela imagem canônica de $3 \in \mathbb{Z}$ em $\mathbb{Z}/4\mathbb{Z}$. Se $r \geqslant 3$, então $(\mathbb{Z}/2^r\mathbb{Z})^* = \langle \alpha, \beta \rangle$ não é um grupo multiplicativo cíclico, onde α é a imagem de -1 em $(\mathbb{Z}/2^r\mathbb{Z})^*$, pelo projeção canônica, que possui ordem multiplicativa 2, e β é a imagem de 5 em $(\mathbb{Z}/2^r\mathbb{Z})^*$, pela projeção canônica, que possui ordem 2^{r-2} no grupo multiplicativo $(\mathbb{Z}/2^r\mathbb{Z})^*$.*

O próximo teorema classifica para quais valores de n, um inteiro positivo, o grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$ é cíclico. Pelo Teorema Fundamental da Teoria de Galois (Teorema 1.4), tem-se quais extensões ciclotômicas são cíclicas. A partir deste resultado, passamos à descrição dos subcorpos das extensões ciclotômicas cíclicas.

Teorema 5.1. [*21*], [*26, pag.*44] *O grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$ é cíclico se, e somente se,*

$$n = 2, 4, p^r \text{ ou } 2p^r,$$

onde $p \in \mathbb{Z}$ é um primo ímpar e $r \geqslant 1$ é um inteiro.

Corolário 5.1. *As únicas extensões ciclotômicas cíclicas dos racionais são $\mathbb{Q}(i)$ e $\mathbb{Q}(\xi_{p^r}) = \mathbb{Q}(\xi_{2p^r})$, onde p é um primo ímpar e $r > 0$ um inteiro.*

Demonstração. Segue diretamente da Proposição 5.1 e do Teorema 5.1. □

Com a próxima proposição, tem-se que para cada grau divisor da ordem de um grupo cíclico, existe apenas um único subcorpo deste grau.

Proposição 5.3. [*27, pag.*12] *Se G é um grupo cíclico de ordem n gerado por x então x^k possui ordem $n/\text{mdc}(n,k)$, onde* mdc *denota o máximo divisor comum e k é um inteiro positivo.*

Proposição 5.4. [*27, pag.*13] *Seja G um grupo cíclico de ordem n e gerado por x. Para cada inteiro positivo d, divisor de n, existe exatamente um subgrupo de ordem d, e esse subgrupo é gerado por $x^{n/d}$.*

Demonstração. Se d divide n então o grupo gerado por $x^{n/d}$ possui ordem d. Para a unicidade, se $\langle x^k \rangle$ é um subgrupo de ordem d então $x^{kd} = 1$ e, portanto, n divide kd. Pela Proposição 5.3, segue que n/k divide d e, assim, $\langle x^k \rangle$ é um subgrupo de $\langle x^{n/d} \rangle$. Como esses dois grupos possuem a mesma ordem d, isto é, possuem o mesmo número de elementos, segue que eles são iguais, o que prova a proposição. □

Corolário 5.2. *O número de subgrupos de um grupo cíclico é o número de divisores da ordem do grupo.*

Demonstração. Seja G um grupo cíclico. Pela Proposição 5.4, tem-se que para cada divisor d da ordem do grupo G existe um subgrupo de ordem d. Portanto, o número de subgrupos do grupo G é o número de divisores da ordem do grupo G, o que prova o corolário. □

Sejam $L = \mathbb{Q}(\xi)$ o p^r-ésimo corpo ciclotômico e $G = Gal(L|\mathbb{Q})$ o grupo de Galois da extensão $L|\mathbb{Q}$. Pela Proposição 5.1, tem-se que G é um grupo cíclico finito e, pela Proposição 5.4, tem-se que G possui apenas um subgrupo para cada ordem dada. Pelo Teorema de Lagrange, tem-se que a ordem do subgrupo divide a ordem do grupo. Utilizando o Teorema Fundamental da Teoria de Galois (Teorema 1.4), se $H \subseteq G$ é um subgrupo de ordem m, então existe exatamente um subcorpo K de L que é o corpo fixo de H, e este corpo satisfaz $[L : K] = m$. Logo, para cada divisor k do grau de L sobre $\mathbb{Q}$, existe exatamente um subcorpo K de L com $[K : \mathbb{Q}] = k$. Com isso, podemos enunciar a seguinte proposição.

Proposição 5.5. *Sejam $L = \mathbb{Q}(\xi_{p^r})$ o p^r-ésimo corpo ciclotômico, onde p é um primo impar e $r > 0$ é um inteiro. Para cada inteiro $n > 0$, divisor de $[L : \mathbb{Q}]$, existe exatamente um subcorpo de L com $[K : \mathbb{Q}] = n$.*

Deste modo, o objetivo, deste capítulo, é encontrar uma descrição para o corpo K.

Para encontrar um subcorpo de L de um grau previamente fixado n é suficiente encontrar um elemento algébrico θ com o referido grau. Por outro lado, provar diretamente pela definição que θ tem n potências linearmente independentes sobre $\mathbb{Q}$ não é uma tarefa fácil. Uma idéia interessante é utilizar os conjugados de θ.

Baseado no Teorema 1.2, segue o resultado mais importante desta seção, que será utilizado para obter o gerador do subcorpo de L.

Proposição 5.6. *Seja $\theta \in L = \mathbb{Q}(\xi_{p^r})$ um elemento de L. Se θ possui exatamente n conjugados distintos em L então o corpo $K = \mathbb{Q}(\theta)$ possui grau n sobre $\mathbb{Q}$. Além disso, K é o único subcorpo de L que possui grau n sobre $\mathbb{Q}$.*

Demonstração. A unicidade segue da Proposição 5.5. Como cada homomorfismo $\sigma : \mathbb{Q}(\theta) \longrightarrow \mathbb{C}$ é unicamente determinado pelo valor que σ assume em θ, segue que o número de conjugados distintos que θ possui representa o número de $\mathbb{Q}$-homomorfismos distintos de $\mathbb{Q}(\theta)$. Pelo Teorema 1.2, segue o resultado. □

5.2 Subcorpos de $\mathbb{Q}(\xi_{p^r})$

Apresentamos, nesta seção, resultados que permitirão obter novas contribuições sobre subcorpos de $L = \mathbb{Q}(\xi)$, onde $\xi = \xi_{p^r}$ é uma raiz p^r-ésima da unidade. Podemos supor, sem perda de generalidade, que L é o menor corpo ciclotômico contendo o subcorpo K desejado, isto é, o condutor de K é p^r. Desconsiderando o caso trivial, onde K é $\mathbb{Q}$ ou L, existem $e, e' \in \mathbb{Z}$ inteiros positivos divisores de $p-1$ tais que $ee' = p-1$ e que o grau de K sobre $\mathbb{Q}$ é ep^{r-1}. O objetivo, desta seção, é provar que $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi)$.

Sejam σ um gerador de $Gal(L|\mathbb{Q})$ e $\alpha \in \mathbb{Z}$ um inteiro positivo com $0 < \alpha < p^r$ tal que $\sigma(\xi) = \xi^\alpha$. Assim, $\overline{\alpha}$ é um gerador de $(\mathbb{Z}/p^r\mathbb{Z})^*$, onde $\overline{\alpha}$ representa a projeção canônica de α em $\mathbb{Z}/p^r\mathbb{Z}$. Seja $\varphi(x) = \varphi_{p^r}(x) = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + x^{(p-1)p^{r-1}}$ é o p^r-ésimo polinômio ciclotômico e $n = \phi(p^r) = (p-1)p^{r-1}$, onde ϕ é a função de Euler.

A próxima proposição será utilizada diretamente na Proposição 5.10, onde será demonstrado que os conjugados de θ são distintos, o que, juntamente com a Proposição 5.6, resultará no Teorema 5.2, que fornece a descrição do subcorpo K, que pode ser expresso como $\mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi)$.

Proposição 5.7. *Seja $h \in \mathbb{Z}[x]$ um polinômio de grau no máximo $p^r - 1$. Se $h(\xi) = 0$ então $h = \varphi g$, onde $g \in \mathbb{Z}[x]$ é um polinômio de grau no máximo $p^{r-1} - 1$ e h tem lp termos não nulos, onde l é o número de termos não nulos de g.*

Demonstração. Seja $h \in \mathbb{Z}[x]$ um polinômio de grau no máximo $p^r - 1$ com $h(\xi) = 0$. Como φ é o polinômio minimal de ξ sobre $\mathbb{Z}$, segue que φ divide h. Portando, $h = \varphi g$ para algum $g \in \mathbb{Z}[x]$. Agora, para encontrar o grau de g, usando a propriedade do grau na multiplicação de polinômios em $h = \varphi g$, obtém-se que $\mathrm{gr}(h) = \mathrm{gr}(\varphi) + \mathrm{gr}(g)$, onde $\mathrm{gr}(.)$ denota o grau do polinômio. Deste modo, $\mathrm{gr}(g) = \mathrm{gr}(h) - \mathrm{gr}(\varphi)$. Como $\mathrm{gr}(h) \leqslant p^r - 1$ e $\mathrm{gr}(\varphi) = (p-1)p^{r-1} = p^r - p^{r-1}$, segue que $\mathrm{gr}(g) \leqslant p^r - 1 - (p^r - p^{r-1}) = p^{r-1} - 1$. Como g é um polinômio de grau no máximo $p^{r-1} - 1$, tem-se que g pode ser expresso como $g(x) = g_0 + g_1 x + \cdots + g_{p^{r-1}-1}x^{p-1}$, com os coeficientes $g_j \in \mathbb{Z}$, para $j = 0, 1, \ldots, p^{r-1} - 1$. Assim, de $h = \varphi g$, tem-se que

$$\begin{aligned} h &= \varphi g \\ &= \varphi(g_0 + g_1 x + g_2 x^2 + \cdots + g_{p^{r-1}-1}x^{p-1}) \\ &= g_0\varphi + g_1 x\varphi + \cdots + g_{p^{r-1}-1}x^{p^{r-1}-1}\varphi. \end{aligned}$$

De onde,

$$h = g_0(1 + x^{p^{r-1}} + x^{2p^{r-1}} + x^{(p-1)p^{r-1}}) + g_1x(1 + x^{p^{r-1}} + x^{2p^{r-1}} + x^{(p-1)p^{r-1}}) + \cdots$$
$$\cdots + g_{p^{r-1}-1}x^{p^{r-1}-1}(1 + x^{p^{r-1}} + x^{2p^{r-1}} + x^{(p-1)p^{r-1}}).$$

Logo,

$$h = g_0+g_1x+\cdots+g_{p^{r-1}-1}x^{p^{r-1}-1}+g_0x^{p^{r-1}}+g_1x^{p^{r-1}+1}+\cdots+g_{p^{r-1}-1}x^{p^{r-1}+p^{r-1}-1}+\cdots$$
$$\cdots + g_0x^{(p-1)p^{r-1}} + g_1x^{(p-1)p^{r-1}+1} + \cdots + g_{p^{r-1}-1}x^{(p-1)p^{r-1}+p^{r-1}-1},$$

e, portanto, $h = \varphi h$ tem lp termos não nulos. □

Agora, se K é o corpo fixo de $\langle\sigma^{ep^{r-1}}\rangle$ então

$$\begin{aligned} Gal(L|\mathbb{Q}) &= \{\sigma, \sigma^2, \ldots, \sigma^{(p-1)p^{r-1}} = Id_L\}, \\ Gal(K|\mathbb{Q}) &= \{\sigma_{|K}, \sigma^2_{|K}, \ldots, \sigma^{ep^{r-1}}_{|K} = Id_K\}, \\ Gal(L|K) &= \{\sigma^{ep^{r-1}}, \sigma^{2ep^{r-1}}, \ldots, \sigma^{(p-1)p^{r-1}} = Id_L\} \text{ e} \end{aligned}$$

K é um corpo de grau ep^{r-1} sobre $\mathbb{Q}$. Além disso, se K' é um outro subcorpo de L com o mesmo grau ep^{r-1}, pelo fato da extensão $L|\mathbb{Q}$ ser cíclica, segue que $K' = K$.

Proposição 5.8. *Para todo $j = 1, 2, \cdots, n-1$ tem-se que $\sigma^j(\xi) = \xi^{\alpha^j}$ e $\sigma^n(\xi) = \xi$.*

Demonstração. Como $\sigma(\xi) = \xi^\alpha$ segue que $\sigma^2(\xi) = \sigma(\xi^\alpha) = (\xi^\alpha)^\alpha = \xi^{\alpha^2}$. Similarmente, tem-se que $\sigma^3(\xi) = \xi^{\alpha^3}$. Assim, para $j = 1, 2, \ldots, n$, tem-se que $\sigma^j(\xi) = \xi^{\alpha^j}$. Finalmente, $\sigma^n(\xi) = \xi^{\alpha^n} = \xi$, o que conclui a demonstração. □

Na Proposição 5.8 obtém-se os conjugados de ξ. Agora, descrevemos explicitamente os conjugados de θ.

Proposição 5.9. *Se $\theta = Tr_{L|K}(\xi)$, então*

$$\begin{aligned}
\theta &= \xi^{\alpha^{ep^{r-1}}} + \xi^{\alpha^{2ep^{r-1}}} + \cdots + \xi^{\alpha^{lp^{r-1}}} + \cdots + \xi^{\alpha^{(p-1)p^{r-1}}}, \\
\sigma(\theta) &= \xi^{\alpha^{ep^{r-1}+1}} + \xi^{\alpha^{2ep^{r-1}+1}} + \cdots + \xi^{\alpha^{lep^{r-1}+1}} + \cdots + \xi^{\alpha^{(p-1)p^{r-1}+1}}, \\
\sigma^2(\theta) &= \xi^{\alpha^{ep^{r-1}+2}} + \xi^{\alpha^{2ep^{r-1}+2}} + \cdots + \xi^{\alpha^{lep^{r-1}+2}} + \cdots + \xi^{\alpha^{(p-1)p^{r-1}+2}}, \\
&\vdots \quad \vdots \\
\sigma^j(\theta) &= \xi^{\alpha^{ep^{r-1}+j}} + \xi^{\alpha^{2ep^{r-1}+j}} + \cdots + \xi^{\alpha^{lep^{r-1}+j}} + \cdots + \xi^{\alpha^{(p-1)p^{r-1}+j}}, \\
&\vdots \quad \vdots \\
\sigma^{ep^{r-1}}(\theta) &= \xi^{\alpha^{ep^{r-1}+ep^{r-1}}} + \xi^{\alpha^{2ep^{r-1}+ep^{r-1}}} + \cdots + \xi^{\alpha^{lep^{r-1}+ep^{r-1}}} + \cdots + \xi^{\alpha^{ee'p^{r-1}+ep^{r-1}}} \\
&= \theta.
\end{aligned}$$

Demonstração. Tem-se que

$$\begin{aligned}\theta &= Tr_{L|K}(\xi)\\ &= \sigma^{ep^{r-1}}(\xi)+\sigma^{2ep^{r-1}}(\xi)+\cdots+\sigma^{lep^{r-1}}(\xi)+\cdots+\sigma^{ee'p^{r-1}}(\xi).\end{aligned}$$

Pela Proposição 5.8, segue que

$$\theta = \xi^{\alpha^{ep^{r-1}}}+\xi^{\alpha^{2ep^{r-1}}}+\cdots+\xi^{\alpha^{lp^{r-1}}}+\cdots+\xi^{\alpha^{(p-1)p^{r-1}}}.$$

De modo análogo, para $\sigma(\theta)$ tem-se que

$$\begin{aligned}\sigma(\theta) &= \sigma(\sigma^{ep^{r-1}}(\xi)+\sigma^{2ep^{r-1}}(\xi)+\cdots+\sigma^{lep^{r-1}}(\xi)+\cdots\sigma^{(p-1)p^{r-1}}(\xi))\\ &= \sigma^{ep^{r-1}+1}(\xi)+\sigma^{2ep^{r-1}+1}(\xi)+\cdots+\sigma^{lep^{r-1}+1}(\xi)+\cdots+\sigma^{(p-1)p^{r-1}+1}(\xi)\\ &= \xi^{\alpha^{ep^{r-1}+1}}+\xi^{\alpha^{2ep^{r-1}+1}}+\cdots+\xi^{\alpha^{lep^{r-1}+1}}+\cdots+\xi^{\alpha^{(p-1)p^{r-1}+1}}.\end{aligned}$$

Para $\sigma^2(\theta)$ obtém-se que

$$\begin{aligned}\sigma^2(\theta) &= \sigma^2(\sigma^{ep^{r-1}}(\xi)+\sigma^{2ep^{r-1}}(\xi)+\cdots+\sigma^{lep^{r-1}}(\xi)+\cdots+\sigma^{(p-1)p^{r-1}}(\xi))\\ &= \sigma^{ep^{r-1}+2}(\xi)+\sigma^{2ep^{r-1}+2}(\xi)+\cdots+\sigma^{lep^{r-1}+2}(\xi)+\cdots+\sigma^{(p-1)p^{r-1}+2}(\xi)\\ &= \xi^{\alpha^{ep^{r-1}+2}}+\xi^{\alpha^{2ep^{r-1}+2}}+\cdots+\xi^{\alpha^{lep^{r-1}+2}}+\cdots+\xi^{\alpha^{(p-1)p^{r-1}+2}}.\end{aligned}$$

De modo geral, para $j=1,2,\ldots,ep^{r-1}$, segue que

$$\begin{aligned}\sigma^j(\theta) &= \sigma^j(\sigma^{ep^{r-1}}(\xi)+\sigma^{2ep^{r-1}}(\xi)+\cdots+\sigma^{lep^{r-1}}(\xi)+\cdots\sigma^{(p-1)p^{r-1}}(\xi))\\ &= \sigma^{ep^{r-1}+j}(\xi)+\sigma^{2ep^{r-1}+j}(\xi)+\cdots+\sigma^{lep^{r-1}+j}(\xi)+\cdots+\sigma^{(p-1)p^{r-1}+j}(\xi)\\ &= \xi^{\alpha^{ep^{r-1}+j}}+\xi^{\alpha^{2ep^{r-1}+j}}+\cdots+\xi^{\alpha^{lep^{r-1}+j}}+\cdots+\xi^{\alpha^{(p-1)p^{r-1}+j}}.\end{aligned}$$

Finalmente, para $\sigma^{ep^{r-1}}(\theta)$ obtém-se que

$$\begin{aligned}\sigma^{ep^{r-1}}(\theta) &= \sigma^{ep^{r-1}}(\sigma^{ep^{r-1}}(\xi)+\sigma^{2ep^{r-1}}(\xi)+\cdots+\sigma^{(p-1)p^{r-1}}(\xi))\\ &= \sigma^{ep^{r-1}+ep^{r-1}}(\xi)+\sigma^{2ep^{r-1}+ep^{r-1}}(\xi)+\cdots+\sigma^{(p-1)p^{r-1}+ep^{r-1}}(\xi)\\ &= \xi^{\alpha^{ep^{r-1}+ep^{r-1}}}+\xi^{\alpha^{2ep^{r-1}+ep^{r-1}}}+\cdots+\xi^{\alpha^{(p-1)p^{r-1}+ep^{r-1}}}\\ &= \xi^{\alpha^{ep^{r-1}}}+\xi^{\alpha^{2ep^{r-1}}}+\cdots+\xi^{\alpha^{(p-1)p^{r-1}}}\\ &= \theta,\end{aligned}$$

o que conclui a demonstração. □

Fixamos, agora, uma notação para facilitar a descrição dos próximos resultados. Para cada $n\in\mathbb{Z}$, denotamos n' o representante da classe lateral $n+p^r\mathbb{Z}$ em $\mathbb{Z}/\mathbb{Z}_{p^r}$, onde n' é um inteiro positivo com $0<n'\leqslant p^r$. Deste modo, se $\mathrm{mdc}(n,p^r)=1$ então $0<n'<p^r$ e $\mathrm{mcd}(n',p^r)=1$. Denotamos, ainda, $\alpha'_{j,s}=(\alpha^{jep^{r-1}+s})'$.

Lema 5.1. *Se $j=1,2,\ldots,e'$ e $s=1,2,\ldots,ep^{r-1}$, então os elementos $\alpha'_{j,s}$ são todos distintos. Além do mais, os elementos $\xi^{\alpha'_{i,j}}$ são distintos.*

Demonstração. Note que

$$\begin{aligned}\alpha'_{j,s} &= (\alpha^{jep^{r-1}+s})' \\ &= (\alpha^{jep^{r-1}+(p-1)p^{r-1}+s})' \\ &= (\alpha^{(j+(p-1))ep^{r-1}+s})' \\ &= \alpha'_{j+(p-1),s},\end{aligned}$$

onde $\alpha_{0,s} = \alpha_{p-1,s}$. Desse modo, é suficiente provar o resultado para $j = 0, 1, \ldots, e' - 1$. Os elementos $jep^{r-1} + s$ percorrem todos os inteiros de 1 a $(p-1)p^{r-1}$, sem repetição quando $j = 0, 1, \ldots, e' - 2$ e $s = 1, 2, \ldots, ep^{r-1}$. Por outro lado, $\overline{\alpha}$ tem ordem $(p-1)p^{r-1}$ no grupo multiplicativo de $\mathbb{Z}/p^r\mathbb{Z}$. Logo, todos os elementos $\alpha'_{j,s}$ são distintos. Para a segunda afirmação é suficiente observar que existe uma bijeção entre os elementos $\alpha'_{j,s}$ e as raízes da unidade $\xi^{\alpha'_{i,j}}$, o que prova o lema. □

Lema 5.2. *Se $f_s(x) = x^{\alpha'_{1,s}} + x^{\alpha'_{2,s}} + \cdots + x^{\alpha'_{p-1,s}}$, então f_s é um polinômio de grau no máximo $p^r - 1$ e $\sigma^s(\theta) = f_s(\xi)$.*

Demonstração. Pela definição de $\alpha'_{j,s}$ segue que $0 < \alpha'_{j,s} < p^r$ e, portanto, f_s é um polinômio de grau no máximo $p^r - 1$. Finalmente

$$\begin{aligned}\sigma^s(\theta) &= \xi^{\alpha^{ep^{r-1}+s}} + \xi^{\alpha^{2ep^{r-1}+s}} + \cdots + \xi^{\alpha^{lep^{r-1}+s}} + \cdots + \xi^{\alpha^{(p-1)ep^{r-1}+s}} \\ &= \xi^{\alpha'_{1,s}} + \xi^{\alpha'_{2,s}} + \cdots + \xi^{\alpha'_{p-1,s}} \\ &= f_s(\xi),\end{aligned}$$

o que conclui a prova. □

O Lema 5.2 fornece uma ligação entre os polinômios f_s e os conjugados de θ. Temos, agora, as ferramentas necessárias para provar a seguinte proposição.

Proposição 5.10. *Todos os conjugados de θ em K são distintos.*

Demonstração. Suponha que θ possui dois conjugados iguais, ou seja, suponha que existam $a, b \in \mathbb{N}$ distintos, de modo que $\sigma^a(\theta) = \sigma^b(\theta)$. Assuma, sem perca de generalidade, que $a \geqslant b$ e $a, b \in \{1, 2, \ldots, p^{r-1}\}$. Assim, tem-se que $\sigma^a(\theta) - \sigma^b(\theta) = 0$. Pelo Lema 5.2, segue que $f_a(\xi) - f_b(\xi) = 0$ e, pelo Lema 5.1, tem-se que todos os $\alpha'_{j,s}$ são distintos. Como todos as potências $x^{\alpha'_{j,s}}$ são distintas segue que $(f_a - f_b)(x) \in \mathbb{Z}[x]$ possui $2(p-1)$ termos não nulos e grau $\leqslant p^r - 1$, o que contradiz a Proposição 5.7. Logo, $(f_a - f_b)(\xi) \neq 0$ e consequentemente, $\sigma^a(\theta) \neq \sigma^b(\theta)$. Portanto, todos os ep^{r-1} conjugados de θ são distintos. □

Pela Proposição 5.7, segue que todos os ep^{r-1} conjugados de θ em K são distintos, onde $\theta = Tr_{L|K}(\xi)$. Como o grau de K é ep^{r-1}, segue que θ tem ep^{r-1} conjugados em L. Pela Proposição 5.6, tem-se que $\mathbb{Q}(\theta)$ é o único subcorpo de L que tem grau ep^{r-1}, o que implica que $K = \mathbb{Q}(\theta)$. O Teorema 3.9 fornece o valor do discriminante absoluto de K. A unicidade

é dada pela Proposição 5.6. A Figura 5.1 apresenta um diagrama desses subcorpos, onde os números ao lado das linhas significa o grau da extensão. Com base nestes fatos, segue diretamente o próximo teorema.

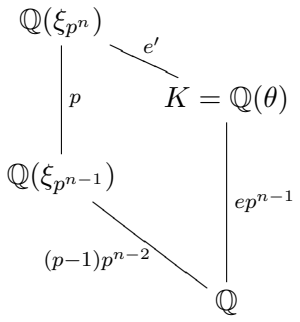

Figura 5.1: Subcorpo de $\mathbb{Q}(\xi_{p^r})$ e grau ep^{r-1}.

Teorema 5.2. *Seja K um subcorpo de $L = \mathbb{Q}(\xi)$ com $[L : K] = e'$, onde $e, e' > 1$ são inteiros com $ee' = p-1$. Se $\theta = Tr_{L|K}(\xi)$ então $K = \mathbb{Q}(\theta)$ é o único subcorpo de L cujo grau é ep^{r-1}, e o discriminante absoluto de K é dado por $|d_K| = p^a$, onde $a = e[(n+1)p^{n-1} - \dfrac{p^n - 1}{p-1}] - 1$.*

5.3 Subcorpos de $\mathbb{Q}(\xi_p)$

Apresentamos, nessa seção, resultados que permitirão obter os subcorpos do p-ésimo corpo ciclotômico $\mathbb{Q}(\xi_p)$, onde p é um primo ímpar, de um modo distinto do apresentado em [37]. Além do mais, essa construção permite a obtenção de uma base integral para o anel de inteiros para os subcorpos de $\mathbb{Q}(\xi_p)$.

Seja $p \in \mathbb{Z}$ um primo ímpar, $\xi = \xi_p$ uma raiz p-ésima primitiva da unidade, $L = \mathbb{Q}(\xi_p)$ o p-ésimo corpo ciclotômico e $K \subseteq L$ um subcorpo de K.

Lema 5.3. *Se p é um número primo ímpar e $L = \mathbb{Q}(\xi_p)$ o p-ésimo corpo ciclotômico, com $\xi = \xi_p$ uma raiz p-ésima primitiva da unidade, então os conjugados de ξ são $\xi, \xi^2, \cdots, \xi^{p-1}$. Em particular, os conjugados de ξ são distintos e formam um conjunto linearmente independente.*

Demonstração. De modo análogo à Seção 5.2, sejam σ um gerador do grupo de Galois $Gal(L|\mathbb{Q})$ da extensão $L|\mathbb{Q}$ e $\alpha \in \mathbb{Z}$ um inteiro positivo tal que $\sigma(\xi) = \xi^\alpha$. Assim, os conjugados de ξ são as potências de ξ com expoente inversível módulo p, que são $\xi, \xi^2, \cdots, \xi^{p-1}$. Portanto, os conjugados de ξ são linearmente independentes. □

Lema 5.4. *Sejam p um número primo ímpar e $L = \mathbb{Q}(\xi_p)$ o p-ésimo corpo ciclotômico. Se $K \subseteq L$ é um subcorpo de L e $\theta = Tr_{L|K}(\xi)$ é o traço de ξ na extensão $L|K$, então os conjugados de θ são linearmente independentes e portanto distintos.*

Demonstração. Como $\theta = Tr_{L|K}(\xi)$, segue que θ é uma soma de conjugados de ξ, assim como cada conjugado de θ é uma soma de conjugados de ξ. Note que cada conjugado de θ é soma de diferentes conjugados de θ. Logo, se existir uma combinação linear nula de conjugados de θ, então existirá uma combinação linear nula de conjugados de ξ. Como os conjugados de ξ são linearmente independentes, segue que os coeficientes dos conjugados de ξ são nulos, e assim são os coeficientes dos conjugados de θ. Portanto, os conjugados de θ são linearmente independentes e consequentemente distintos. □

Lema 5.5. *O subcorpo K do p-ésimo corpo ciclotômico $L = Q(\xi_p)$ é dado por $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi)$.*

Demonstração. Pelo Lema 5.4, os conjugados de θ são linearmente independentes e distintos. Pela Proposição 5.6, obtém-se que $\mathbb{Q}(\theta)$ tem o mesmo grau que K. Como L possui apenas um subcorpo de um dado grau, segue que $K = \mathbb{Q}(\theta)$. □

Lema 5.6. [*10, pag.*71], [*36, pag.*57] *Se $K = \mathbb{Q}(\theta)$ é um subcorpo do p-ésimo corpo ciclotômico $L = \mathbb{Q}(\xi_p)$, onde $\theta = Tr_{L|K}(\xi)$, então os conjugados de θ formam uma base para o anel de inteiros $\mathcal{O}_K$ de K.*

Demonstração. Sejam $[K : \mathbb{Q}] = s$, $Gal(K|\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_s\}$, o grupo de Galois da extensão $K|\mathbb{Q}$, e $\theta_k = \sigma_k(\theta)$, para $k = 1, 2 \ldots, s$, os conjugados de θ em K. Claramente, todos $\theta_k \in \mathcal{O}_K$ $(k = 1, 2, \ldots, s)$ e $\{\theta_1, \theta_2, \ldots, \theta_s\}$ é uma base de K sobre $\mathbb{Q}$. Seja A o $\mathbb{Z}$-módulo livre gerado por $\{\theta_1, \theta_2, \ldots, \theta_s\}$. Tem-se que $A \subseteq \mathcal{O}_K$. Dado $x \in \mathcal{O}_K \subseteq K$, segue que $x = a_1\theta_1 + a_2\theta_2 + \cdots + a_s\theta_s$, com $a_k \in \mathbb{Q}$. Por outro lado, $x \in \mathcal{O}_L = \mathbb{Z}[\xi]$, desse modo $x = b_1\xi + b_2\xi^2 + \cdots + b_{p-1}\xi^{p-1}$, com $b_k \in \mathbb{Z}$, de onde tem-se que $a_k \in \mathbb{Z}$, e assim $x \in A$. Portanto $A = \mathcal{O}_K$, ou seja, os conjugados de θ formam uma base integral para $\mathcal{O}_K$, o que prova o lema. □

Teorema 5.3. *O subcorpo K do p-ésimo corpo ciclotômico $L = \mathbb{Q}(\xi_p)$ é dado por $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi)$. Além disso, os conjugados de θ em K formam uma base integral para o anel de inteiros $\mathcal{O}_K$ de K, e o discriminante absoluto de K é dado por $|d_K| = p^u$, onde $u = [K : \mathbb{Q}] - 1$.*

Demonstração. A igualdade $K = \mathbb{Q}(\theta)$ segue do Lema 5.5. Pelo Lema 5.6, segue que os conjugados de θ formam uma base integral para $\mathcal{O}_K$. O valor do discriminante absoluto é dado pelo Corolário 3.1. □

A figura 5.2 fornece um diagrama da estrutura dos subcorpos de $\mathbb{Q}(\xi_p)$, onde os números ao lado das linhas indicam o grau das extensões.

5.4 Subcorpos de $\mathbb{Q}(\xi_{3^r})$

O objetivo desta seção é a classificar os subcorpos de $L = \mathbb{Q}(\xi_{3^r})$. Embora esse caso já esteja feito através do caso genérico, no Teorema 5.2, optamos em fazer tal classificação

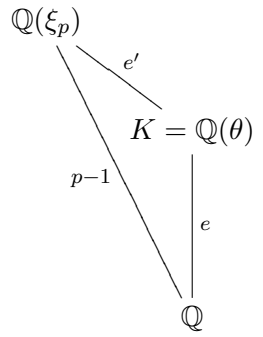

Figura 5.2: Subcorpo de $\mathbb{Q}(\xi_p)$ e grau e.

para tornar mais explícita a expressão de tais subcorpos, e também do seus respectivos discriminantes e anéis de inteiros. Deste modo, provaremos, na Proposição 5.13, que um corpo de condutor potência de 3 é um corpo ciclotômico da forma $\mathbb{Q}(\xi_{3^r})$, para algum inteiro positivo $r > 1$, ou o subcorpo maximal real $\mathbb{Q}(\xi_{3^j} + \xi_{3^j}^{-1})$ de $\mathbb{Q}(\xi_{3^j})$, para algum inteiro positivo $j > 1$. O anel de inteiros e discriminante desses corpos é explicitado no Corolário 5.3.

Seja $G = Gal(L|\mathbb{Q})$ o grupo de Galois da $L|K$, Pela Proposição 5.1, tem-se que G é isomorfo à $(\mathbb{Z}/3^r\mathbb{Z})^*$. Pelo Teorema 5.1, tem-se que $(\mathbb{Z}/3^r\mathbb{Z})^*$ é cíclico. Assim, G é um grupo cíclico com $n = 2.3^{r-1}$ elementos. Como, pela Proposição 5.4, um grupo cíclico finito tem um único subgrupo de uma dada ordem, segue que para cada $m \in \mathbb{N}$ com $m|o(G) = 2.3^{r-1}$, existe um único subgrupo de ordem m, onde $o(G)$ denota a ordem de G. Pelo Teorema Fundamental da Teoria de Galois (Teorema 1.4), segue que existe um único subcorpo K de L tal que $[L : K] = m$.

Proposição 5.11. *O número de subgrupos de G é $2r$, onde G é o grupo de Galois de $L = \mathbb{Q}(\xi_{3^r})$ sobre $\mathbb{Q}$.*

Demonstração. O grupo G possui $n = 2.3^{r-1}$ elementos. Os divisores de n são 3^k, para $k = 0, 1, \ldots, r-1$, e 2.3^k, para $k = 0, 1, \ldots, r-1$. Assim, n tem $2r$ divisores. Pelo Corolário 5.2, segue o resultado. □

Proposição 5.12. *O número de subcorpos de $L = \mathbb{Q}(\xi_{3^r})$ é $2r$.*

Demonstração. Segue diretamente do fato que $L \subseteq \mathbb{Q}$ é uma extensão cíclica (Teorema 5.1), do Teorema Fundamental da Teoria de Galois (Teorema 1.4) e do fato que G tem $2r$ subgrupos. □

Proposição 5.13. *Os subcorpos de $L = \mathbb{Q}(\xi_{3^r})$ são $\mathbb{Q}(\xi_{3^j})$ e $\mathbb{Q}(\xi_{3^j} + \xi_{3^j}^{-1})$, para $j = 1, 2, \ldots, r$.*

Demonstração. Como $\mathbb{Q}(\xi_3 + \xi_3^{-1}) = \mathbb{Q}$, segue que $\mathbb{Q}(\xi_{3^j})$ e $\mathbb{Q}(\xi_{3^j} + \xi_{3^j}^{-1})$, para $j = 1, 2, \ldots, r$ são $2r$ subcorpos de L. Como L tem apenas $2r$ subcorpos, segue que esses são todos os subcorpos de L. □

Corolário 5.3. *Se K é um subcorpo de L, com $[K:\mathbb{Q}] \neq 1$, então existe um inteiro positivo s, com $s \leqslant r$, tal que $K = \mathbb{Q}(\xi_{3^s})$ ou $K = \mathbb{Q}(\xi_{3^s} + \xi_{3^s}^{-1})$. Se $K = \mathbb{Q}(\xi_{3^s})$ então o anel de inteiros de K é $\mathcal{O}_K = \mathbb{Z}[\xi_{3^s}]$, e o discriminante absoluto de K é $3^{2[(r+1)3^{r-1}-(3^r-1)/2]-1}$. Se $K = \mathbb{Q}(\xi_{3^s} + \xi_{3^s}^{-1})$, o anel de inteiros de K é $\mathcal{O}_K = \mathbb{Z}[\xi_{3^s} + \xi_{3^s}^{-1}]$, e o discriminante absoluto é dado por 3^a, onde $a = [(r+1)3^{r-1} - (3^r-1)/2] - 1$.*

Demonstração. Pela Proposição 5.13, segue que $K = \mathbb{Q}(\xi_{3^s})$ ou $K = \mathbb{Q}(\xi_{3^s} + \xi_{3^s}^{-1})$, para algum inteiro positivo $s \in \mathbb{Z}$ com $s \leqslant r$. Pelo Teorema 1.7 e pela Proposição 1.3, segue que o anel de inteiros é $\mathbb{Z}[\xi_{3^s}]$ ou $Z[\xi_{3^s} + \xi_{3^s}^{-1}]$, respectivamente. Pelo Teorema 3.9, obtém-se o valor do discriminante absoluto. □

Na Figura 5.3 descrevemos todos os subcorpos de $\mathbb{Q}(\xi_{3^r})$, onde os números ao lado das linhas representa os graus das extensões.

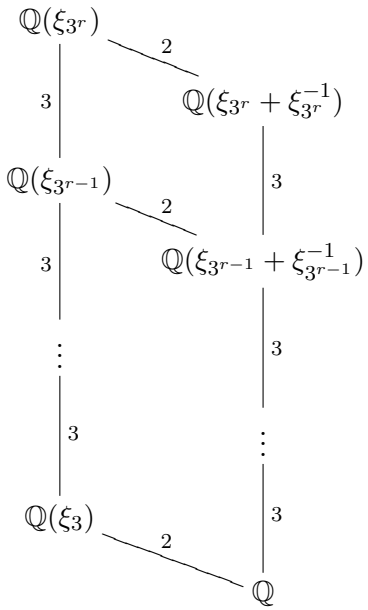

Figura 5.3: Subcorpos de $\mathbb{Q}(\xi_{3^r})$.

5.5 Demais casos

Na Seção 5.4 provamos que existe somente duas famílias de corpos de números abelianos que possuem como condutor uma potência de três, consistindo uma destas famílias de corpos ciclotômicos do tipo $\mathbb{Q}(\xi_{3^r})$ e a outra família de corpos maximais reais $\mathbb{Q}(\xi_{3^r}+\xi_{3^r}^{-1})$ de corpos ciclotômicos. Entretanto, esse raciocínio não pode ser estendido para outros primos ímpares, conforme os exemplos abaixo.

Exemplo 5.1. *Motivados pelo trabalho [14, pags.41-42], a figura 5.4 apresenta todos os subcorpos do corpo ciclotômico $L = \mathbb{Q}(\xi_{125})$, onde $K_3 = \mathbb{Q}(\theta_3)$ é o subcorpo de L com grau 25, onde $\theta_3 = Tr_{\mathbb{Q}(\xi_{125})|K_3}(\xi_{125})$ e $K_2 = \mathbb{Q}(\theta_2)$ é o subcorpo de L com grau 5, onde $\theta_2 = Tr_{\mathbb{Q}(\xi_{25})|K_2}(\xi_{25})$, conforme pode ser observado na Figura 5.4.*

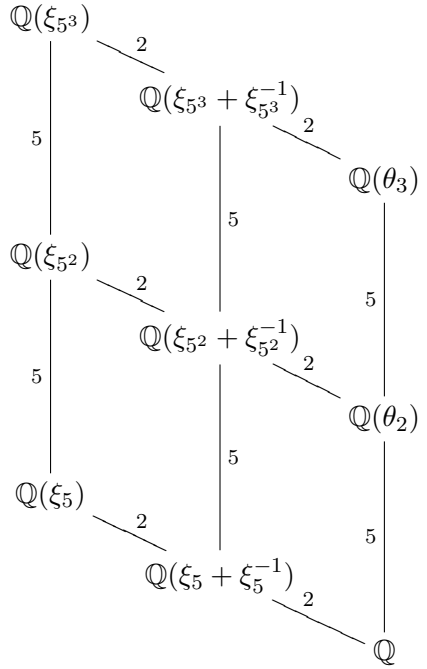

Figura 5.4: Subcorpos de $\mathbb{Q}(\xi_{125})$.

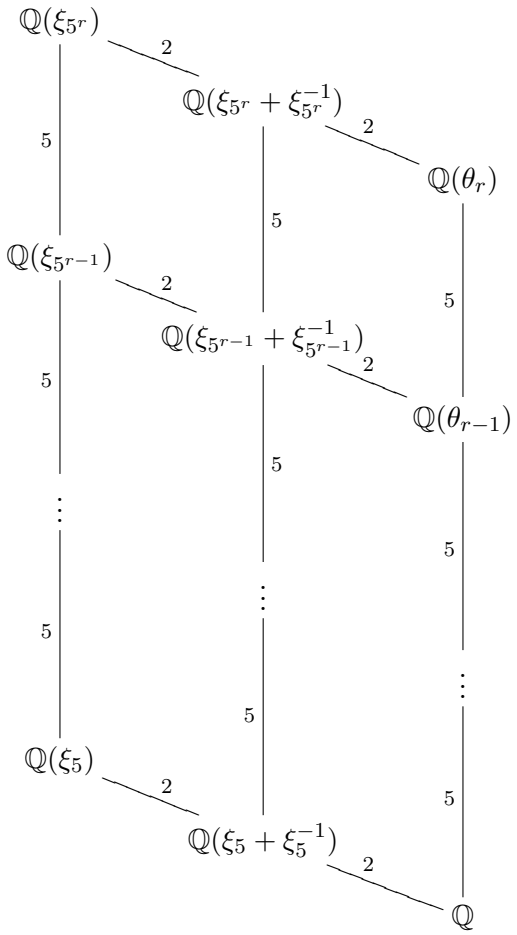

Figura 5.5: Subcorpos de $\mathbb{Q}(\xi_{5^r})$.

Exemplo 5.2. *Temos três famílias de corpos de números abelianos cujo condutor é uma potência do primo cinco. Para cada $r \in \mathbb{Z}$, com $r > 0$, seja $K_r \subseteq \mathbb{Q}(\xi_{5^r})$ o subcorpo de grau 5^{r-1} e condutor 5^r. O corpo K_r é único pois a extensão $\mathbb{Q}(\xi_{5^r})|\mathbb{Q}$ é cíclica. Pelo Teorema 5.2, tem-se que $K_r = \mathbb{Q}(\theta_r)$, onde $\theta_r = Tr_{\mathbb{Q}(\xi_{5^r})|K_r}(\xi_{5^r})$. Os corpos $K_r = \mathbb{Q}(\theta_r)$ formam uma família de corpos de condutor potência de cinco. As demais família são a dos corpos ciclotômicos $\mathbb{Q}(\xi_{5^r})$ e a dos subcorpos maximais reais $\mathbb{Q}(\xi_{5^r} + \xi_{5^r})$ de $\mathbb{Q}(\xi_{5^r})$. Um diagrama pode ser observado na Figura 5.5.*

Exemplo 5.3. *De modo análogo ao Exemplo 5.2, existem três famílias de corpos de números abelianos cujo condutor é uma potência do primo sete. Os corpos ciclotômicos $\mathbb{Q}(\xi_{7^r})$ formam uma família de corpos de condutor potência de sete, assim como os subcorpos maximais reais $\mathbb{Q}(\xi_{7^r}+\xi_{7^r})$ de $\mathbb{Q}(\xi_{5^r})$ formam outra família com a mesma propriedade. Para cada $r\in\mathbb{Z}$, com $r>0$, seja $K_r\subseteq\mathbb{Q}(\xi_{7^r})$ o subcorpo de grau 7^{r-1} e condutor 7^r. O corpo K_r é único pois a extensão $\mathbb{Q}(\xi_{7^r})|\mathbb{Q}$ é cíclica. Pelo Teorema 5.2, tem-se que $K_r=\mathbb{Q}(\theta_r)$, onde $\theta_r=Tr_{\mathbb{Q}(\xi_{5^r})|K_r}(\xi_{5^r})$, conforme pode ser observado na Figura 5.6.*

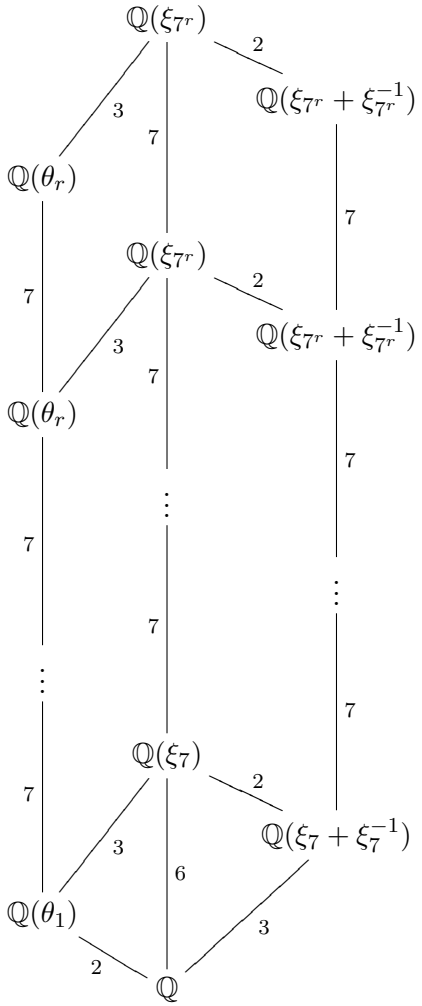

Figura 5.6: Subcorpos de $\mathbb{Q}(\xi_{7^r})$.

5.6 Conclusões

Este capítulo foi dedicado a obter novas contribuições na descrição explícita para corpos de condutor potência de primo ímpar, que são corpos contidos em extensões ciclotômicas cíclicas. Desse modo, provamos que para um corpo K de condutor p^r, tomando $L = \mathbb{Q}(\xi_{p^r})$, tem-se que $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi_{p^r})$. O caso particular $p = 3$ foi tratado na Seção 5.4. Na Seção 5.3 apresentamos uma demonstração alternativa para a descrição dos corpos de condutor p, onde p é um primo ímpar, o que resulta também numa base integral para os anéis de inteiros desses corpos.

Estando os subcorpos das extensões ciclotômicas cíclicas $\mathbb{Q}(\xi_{p^r})$, onde p é um primo ímpar, encontrados, uma primeira generalização que pode ser feita para tal construção é encontrar a descrição para corpos cíclicos contidos em algum $\mathbb{Q}(\xi_n)$, onde n é, inicialmente, da forma pq, com p e q primos ímpares, com a expectativa de poder ser estendido para qualquer natural $n \in \mathbb{N}$. Feito isso, a próxima meta é encontrar a descrição para corpos abelianos, contidos em $\mathbb{Q}(\xi_n)$, cujo grupo de Galois é gerado por dois elementos, e assim sucessivamente, até encontrar uma descrição para todos corpos de números abelianos.

A obtenção desses resultados possibilitará obter reticulados no $\mathbb{R}^n$, via o homomorfismo de Minkowski ou via a perturbação do homomorfismo canônico, com boas densidades de centro e distância produto mínima.

Capítulo

6

Subcorpos de $\mathbb{Q}(\xi_{2^r})$ e os respectivos anéis de inteiros

Neste capítulo apresentamos novas contribuições na descrição para os corpos cujo condutor é uma potência de dois e, também, caracterizamos os anéis de inteiros desses corpos. Pelo Teorema de Kronecker-Weber (Teorema 1.5) esses corpos são subcorpos dos corpos ciclotômicos $\mathbb{Q}(\xi)$, onde $\xi = \xi_{2^r}$ é uma raiz p^r-ésima primitiva da unidade e $r > 1$ um inteiro. Pela Proposição 5.2, tem-se que a extensão $\mathbb{Q}(\xi)|\mathbb{Q}$ não é uma extensão cíclica, entretanto o grupo de Galois é gerado por dois elementos, um de ordem 2 e outro de ordem 2^{r-2}. Provamos, neste capítulo, que os subcorpos de $\mathbb{Q}(\xi)$ pode ser expressos por $\mathbb{Q}(\theta)$, para algum $\theta \in \mathbb{Q}(\xi)$ conveniente, e o anel de inteiros desses subcorpos pode ser expresso por $\mathbb{Z}[\theta]$.

Em 1997, Giraud et al. [12], conjecturou que o homomorfismo canônico do anel de inteiros de $\mathbb{Q}[\theta]$, onde $\theta = \sqrt{2+\sqrt{2+\ldots\sqrt{2}}}$, pode ser utilizado para construir um reticulado $\mathbb{Z}^n$-rotacionado. Posteriormente em [1], 2006, e em [29], 2007, de modo independente, os autores apresentam uma construção de reticulados $\mathbb{Z}^n$-rotacionados utilizando o subcorpo maximal do 2^r-ésimo corpo ciclotômico $\mathbb{Q}(\xi_{2^r})$, onde a Proposição 6.7 apresenta uma dessas construções. A expressão para o discriminante de um corpo de números $K \subseteq \mathbb{Q}(\xi_{2^r})$, onde $r > 1$ é um inteiro positivo, é apresentada em [18]. Entretanto, não existe um método na literatura que descreva a estrutura quando K é um subcorpo de $\mathbb{Q}(\xi_{2^r})$, exceto quando K é um subcorpo maximal. Obtendo a descrição para os subcorpos de $\mathbb{Q}(\xi_{2^r})$, onde $r > 1$ é um inteiro positivo, tem-se que a conjectura apresentada em [12] foi respondida em [1] e [29].

Ao longo deste capítulo, consideramos $r > 2$ um inteiro positivo e $L = \mathbb{Q}(\xi)$ o 2^r-ésimo corpo ciclotômico, onde $\xi = \xi_{2^r}$ é um raiz 2^r-ésima primitiva da unidade, uma vez que, para $r = 1$ e $r = 2$, tem-se que os subcorpos de L são os triviais.

6.1 Número de subcorpos de $\mathbb{Q}(\xi_{2^r})$

O objetivo, desta seção, é apresentar os resultados básicos sobre grupos que serão necessários para obtermos os subcorpos do 2^r-ésimo corpo ciclotômico $L = \mathbb{Q}(\xi_{2^r})$, onde $r > 2$ é um inteiro. Fazendo uso desses resultados, na Seção 6.2, apresentamos uma nova contribuição na interpretação da estrutura dos subcorpos de L.

Considere $r \geqslant 3$ um inteiro positivo, $G = Gal(L|\mathbb{Q})$ o grupo de Galois da extensão $L|\mathbb{Q}$. Tem-se que a extensão não é cíclica, entretanto é possível classificar todos os subcorpos de L. Pela Proposição 5.1, tem-se que G é isomorfo ao grupo multiplicativo $(\mathbb{Z}/2^r\mathbb{Z})^*$. Pela Proposição 5.2, segue que o grupo G é gerado por dois elementos, ou seja, $G = \langle \alpha, \beta \rangle$, onde α é a imagem de -1 em $\mathbb{Z}/2^r\mathbb{Z}$ pelo projeção canônica, que possui ordem multiplicativa 2, e β é a imagem de 5 em $\mathbb{Z}/2^r\mathbb{Z}$ pela projeção canônica, que possui ordem 2^{r-2} no grupo multiplicativo $(\mathbb{Z}/2^r\mathbb{Z})^*$.

Proposição 6.1. *Se G é um grupo cíclico de ordem 2^{r-2}, onde $r \geqslant 3$, então G possui $r-1$ subgrupos.*

Demonstração. Os divisores de 2^{r-2} são $1 = 2^0, 2, 2^2, \cdots, 2^{r-2}$, isto é, 2^{r-2} possui $r-1$ divisores. Assim, pelo Corolário 5.2, segue o resultado. □

Lema 6.1. *Seja $\beta \in (\mathbb{Z}/2^r\mathbb{Z})^*$ um elemento de ordem 2^{r-2}. Se $\beta_k = \beta^{2^{r-2-k}}$, para $k = 0, 1, \cdots, r-2$, então β_k possui ordem 2^k.*

Demonstração. Como o elemento β possui ordem 2^{r-2} e $\beta_k = \beta^{2^{r-2-k}}$ segue que $\beta_k^s = (\beta^{2^{r-2-k}})s = \beta^{2^{r-2-k}s}$. Portanto, $\beta_k^s = 1$ se, e somente se, $2^{r-2} | 2^{r-2-k}s$, o que ocorre se, e somente se, existe $c \in \mathbb{Z}$ tal que $2^{r-2-k}s = c2^{r-2}$. Multiplicando essa última igualdade por 2^k segue que $2^{r-2}s = 2^{r-2}c2^k$, de onde obtém-se que $s = c2^k$, isto é, $2^k | s$. Assim, $\beta_k^s = 1$ se, e somente se, 2^k divide s. Portanto, β_k possui ordem 2^k. □

Observe que o Lema 6.1 pode ser visto com uma aplicação da Proposição 5.3. De fato, como $\beta_k = \beta^{2-r-k}$ tem ordem 2^{r-2}, segue que β^k possui ordem $2^{r-2}/\text{mdc}(2^{r-2}, 2^{r-2-k}) = 2^{r-2}/2^{r-2-k} = 2^k$.

Lema 6.2. *Sejam G o grupo multiplicativo de $\mathbb{Z}/2^r\mathbb{Z}$, $\alpha, \beta \in G$ elementos com ordem 2 e 2^{r-2}, respectivamente, tais que $G = \langle \alpha, \beta \rangle$ e $\beta_k = \beta^{2^{r-2-k}}$ é um elemento de ordem 2^k, para $k = 0, 1, \cdots, r-2$. Os subgrupos de G que possuem ordem 2^k são $\langle \beta_k \rangle$, $\langle \alpha\beta_k \rangle$ e $\langle \alpha, \beta_{k-1} \rangle$, onde $k = 0, 1, \cdots, r-2$.*

Demonstração. Seja $x = \alpha^s\beta^t$ um elemento de G com ordem 2^k. Assim $(\alpha^s\beta^t)^{2^k} = \alpha^{s2^k}\beta^{t2^k} = 1$ e, consequentemente, $\alpha^{s2^k} = 1$ e $\beta^{t2^k} = 1$. Portanto, $2^{r-2}|t2^k$, o que é o mesmo que $2^{r-2-k}|t$, ou que $t = c2^{r-2-k}$, com $c \in \mathbb{Z}$. Desse modo, $\beta^t = (\beta^{2^{r-2-k}})^c = \beta_k^c$ possui ordem 2^r para algum inteiro positivo $r \in \mathbb{Z}$ com $0 \leqslant r \leqslant k$. Pela Proposição 5.3, segue que β_k^c possui ordem 2^k se, e somente se, $\text{mdc}(c, 2^k) = 1$, o que ocorre se, e somente se, c é ímpar. Deste modo, qualquer elemento $x \in G$ de ordem 2^k pode ser expresso como $x = \alpha^s\beta_k^c$, onde $c \in \mathbb{Z}$ é um inteiro positivo ímpar. Pela Proposição 5.4, como $\langle\beta_k\rangle$ é um grupo cíclico de ordem 2^k e, pela unicidade dos subgrupos de G, segue que $\langle\beta_k^c\rangle = \langle\beta_k\rangle$ para cada inteiro positivo ímpar $c \in \mathbb{Z}$. Deste modo, os elementos β_k^c, com c um inteiro positivo ímpar, geram o mesmo subgrupo. Como o elemento α possui ordem 2, segue que, para cada inteiro positivo ímpar $c \in \mathbb{Z}$, o elemento $\alpha\beta_k^c$ possui ordem 2^k, e cada um desses elementos geram o mesmo subgrupo. Como consequência, G possui apenas dois subgrupos cíclicos de ordem 2^k, onde esses subgrupos são $\langle\beta_k\rangle$ e $\langle\alpha\beta_k\rangle$. A outra possibilidade para obter outro subgrupo de ordem 2^k em G, que é gerado por dois elementos, consiste em um grupo gerado por dois elementos. Como α, que possui ordem dois, é um dos geradores de G, segue que o subgrupo desejado tem necessariamente que conter α. O outro gerador tem necessariamente ordem 2^{k-1}. Como os elementos de ordem 2^{k-1} são β_{k-1} e $\alpha\beta_{k-1}$, segue que $\langle\alpha, \beta_{k-1}\rangle$ e $\langle\alpha, \alpha\beta_{k-1}\rangle$ possuem a mesma ordem e $\alpha\beta_{k-1} \in \langle\alpha, \beta_{k-1}\rangle$. Assim, $\langle\alpha, \beta_{k-1}\rangle = \langle\alpha, \alpha\beta_{k-1}\rangle$. Portanto, conclui-se que existe apenas um subgrupo de G gerado por dois elementos com ordem 2^k. □

Corolário 6.1. *Se $k \in \mathbb{Z}$ é um inteiro positivo, com $0 < k < r$, então o número de subcorpos de $L = \mathbb{Q}(\xi_{2^r})$ com grau 2^k é 3.*

Demonstração. Segue diretamente do Lema 6.2 e pelo Teorema Fundamental da Teoria de Galois (Teorema 1.4). □

Corolário 6.2. *O número de subcorpos de $L = \mathbb{Q}(\xi_{2^r})$ é $2 + 3(r-2)$.*

Demonstração. Seja K um subcorpo de L. Se $[K : \mathbb{Q}] = 1$, então L possui apenas um subcorpo, ou seja, o subcorpo K pode ser apenas o subcorpo trivial $\mathbb{Q}$. Se $[K : \mathbb{Q}] = 2, 4, \cdots, 2^{r-1}$, então, pelo Corolário 6.1, segue que L possui 3 subcorpos de grau $[L : \mathbb{Q}]$. Finalmente, se $[K : \mathbb{Q}] = 2^{r-1}$, então L possui apenas um subcorpo de grau desejado, ou seja, o próprio L. Desse modo, L possui $2 + 3(r-2)$ subcorpos. □

6.2 Estrutura dos subcorpos de $\mathbb{Q}(\xi_{2^r})$

Na Seção 6.1 obtivemos a quantidade de subcorpos que o 2^r-ésimo corpo ciclotômico $L = \mathbb{Q}(\xi_{2^r})$ possui, que é dado por $2+3(r-2)$. Nesta seção, utilizando radicais e um pouco de trigonometria, descrevemos explicitamente esses subcorpos, assim como os respectivos anéis de inteiros. Para isso, iniciamos com a relação da formula cosseno da metade do arco, afim de obtermos as relações $\xi_{2^k} + \xi_{2^k}^{-1} = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$ e $\xi_{2^k} - \xi_{2^k}^{-1} = i\sqrt{2 - \sqrt{2 + \cdots + \sqrt{2}}}$.

Lema 6.3. [2, p.102] *Se $\gamma \in \mathbb{R}$, então* $\cos(\gamma) = \pm\sqrt{\dfrac{1+cos(2\gamma)}{2}}$.

Lema 6.4. *Para cada $k \in \mathbb{N}$ tem-se que* $cos(\dfrac{\pi}{2^{k+1}}) = \dfrac{1}{2}\sqrt{2+2cos(\dfrac{\pi}{2^k})}$.

Demonstração. Pelo Lema 6.3, segue que

$$\cos(\frac{\pi}{2^{k+1}}) = \sqrt{\frac{1+\cos(\frac{\pi}{2^k})}{2}} = \sqrt{\frac{2+2\cos(\frac{\pi}{2^k})}{4}} = \frac{1}{2}\sqrt{2+2\cos(\frac{\pi}{2^k})},$$

o que prova o resultado. □

Lema 6.5. *Se $k \in \mathbb{N}$, então* $\operatorname{sen}(\dfrac{\pi}{2^{k+1}}) = \dfrac{1}{2}\sqrt{2-2cos(\dfrac{\pi}{2^k})}$.

Demonstração. Pelo Lema 6.4, tem-se que $\cos^2(\frac{\pi}{2^{k+1}}) = \frac{2+2\cos(\frac{\pi}{2^k})}{4}$. Assim, $\operatorname{sen}^2(\frac{\pi}{2^{k+1}}) = 1-\cos^2(\frac{\pi}{2^{k+1}}) = \frac{2-2\cos(\frac{\pi}{2^k})}{4}$, e portanto $\operatorname{sen}(\frac{\pi}{2^{k+1}}) = \frac{\sqrt{2-2\cos(\frac{\pi}{2^k})}}{2}$, o que prova o lema. □

Proposição 6.2. *Se $\xi_{2^k} = e^{\frac{2\pi i}{2^k}}$ é uma raiz 2^k-ésima primitiva da unidade, então*

$$\xi_{2^k} + \xi_{2^k}^{-1} = 2\cos(\frac{2\pi}{2^k}) = 2\cos(\frac{\pi}{2^{k-1}}) = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}},$$

onde o algarismo 2 aparece $k-2$ vezes.

Demonstração. A primeira e a segunda igualdade são imediatas. A terceira igualdade é demonstrada por indução sobre k. Se $k=3$ então $2\cos(\frac{\pi}{2^{k-1}}) = 2cos(\frac{\pi}{4}) = \sqrt{2}$. Se $k=4$ então $2cos(\frac{\pi}{2^{k-1}}) = 2cos(\frac{\pi}{8}) = \sqrt{2+2cos(\frac{\pi}{4})} = \sqrt{2+\sqrt{2}}$. Agora, suponha que o resultado é valido para n. Assim, para $n+1$, segue que $\xi_{2^{n+1}} + \xi_{2^{n+1}}^{-1} = 2cos(\frac{\pi}{2^n}) = \sqrt{2+2cos(\frac{\pi}{2^{n-1}})} = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$, onde o algarismo 2 aparece $n-1$ vezes, pois pela hipótese de indução, o número 2 aparece $n-2$ vezes em $2cos(\frac{\pi}{2^{n-1}})$. □

Proposição 6.3. *Se $\xi_{2^k} = e^{\frac{2\pi i}{2^k}}$ é um raiz 2^k-ésima primitiva da unidade, com $k>2$, então*

$$\xi_{2^k} - \xi_{2^k}^{-1} = 2isen(\frac{2\pi}{2^k}) = i\sqrt{2-\sqrt{2+\cdots+\sqrt{2}}},$$

onde o número 2 aparece $k-2$ vezes.

Demonstração. Segue diretamente pelo Lema 6.5 e pela Proposição 6.2. □

Seja $\theta_k = \xi_{2^k} + \xi_{2^k}^{-1} = 2cos(\frac{\pi}{2^{k-1}}) = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$, onde o algarismo 2 aparece $k-2$ vezes, e $\theta_k' = -i(\xi_{2^k} - \xi_{2^k}^{-1}) = 2\operatorname{sen}(\frac{\pi}{2^{k-1}}) = \sqrt{2-\sqrt{2+\cdots+\sqrt{2}}}$, onde o algarismo 2 aparece $k-2$ vezes. Utilizando essa notação, obtém-se facilmente o lema a seguir.

Lema 6.6. *Uma raiz 2^k-ésima da unidade ξ_{2^k} pode ser expressa como* $\xi_{2^k} = \dfrac{1}{2}(\theta_k + i\theta_k')$, *sendo θ_k e θ_k' como acima.*

Demonstração. Como $\theta_k = \xi_{2^k} + \xi_{2^k}^{-1}$ e $\theta_k^{'} = -i(\xi_{2^k} - \xi_{2^k}^{-1})$, tem-se que $\theta_k + i\theta_k^{'} = \xi_{2^k} + \xi_{2^k}^{-1} + \xi_{2^k} - \xi_{2^k}^{-1} = 2\xi_{2^k}$, de onde segue o resultado. □

Lema 6.7. *Se $k \in \mathbb{Z}$ é um inteiro positivo então os corpos $\mathbb{Q}(\xi_{2^{k+1}})$, $\mathbb{Q}(\theta_{k+2})$ e $\mathbb{Q}(i\theta_{k+2}^{'})$ possuem grau 2^k, sendo θ_k e $\theta_k^{'}$ como acima. Se $k \leqslant r-2$ então $L = \mathbb{Q}(\xi_{p^r})$ possui apenas esses subcorpos com grau 2^k.*

Demonstração. Fazendo uso das igualdades $\theta_{k+2} = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$ e $\theta_{k+2}^{'} = \sqrt{2-\sqrt{2+\cdots+\sqrt{2}}}$, onde o algarismo 2 aparece k vezes, tem-se que o grau dos corpos $\mathbb{Q}(\theta_{k+2})$ e $\mathbb{Q}(i\theta_{k+2}^{'})$ é 2^k. Por outro lado, é imediato que o grau do corpo $\mathbb{Q}(\xi_{2^{k+1}})$ é 2^k. Pelo Corolário 6.1, tem-se que o número de subcorpos de L com grau 2^k é três, de onde segue o resultado. □

Com base nos resultados anteriores, através do próximo teorema, classificamos os subcorpos de $\mathbb{Q}(\xi_{2^r})$.

Teorema 6.1. *Os subcorpos de $L = \mathbb{Q}(\xi_{2^r})$ são $\mathbb{Q}$, $\mathbb{Q}(\xi_{2^j})$, para $j = 2, 3, \cdots, r$, e $\mathbb{Q}(\theta_k)$, $\mathbb{Q}(i\theta_k^{'})$, para $k = 3, 4, \cdots, r$, sendo $\theta_k = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$ e $\theta_k^{'} = \sqrt{2-\sqrt{2+\cdots+\sqrt{2}}}$, onde o algarismo 2 aparece $k-2$ vezes.*

Demonstração. Pelo Corolário 6.2, segue que L possui $2 + 3(r-2)$ subcorpos. Se contarmos os subcorpos $\mathbb{Q}(\xi_{2^j})$, para $j = 2, 3, \cdots, r$, e os subcorpos $\mathbb{Q}(\theta_k)$ e $\mathbb{Q}(i\theta_k^{'})$, para $j = 3, 4, \cdots, r$, obtém-se o mesmo número. Portanto, são todos os subcorpos de L. □

O próximo lema fornece uma nova expressão para os subcorpos gerados por $i\theta_k^{'}$ sobre $\mathbb{Q}$.

Lema 6.8. *Se $k \in \mathbb{Z}$ é um inteiro positivo, então $\mathbb{Q}(i\theta_k^{'}) = \mathbb{Q}(i\theta_k)$, sendo θ_k e $\theta_k^{'}$ como no Teorema 6.1.*

Demonstração. Como os elementos $i\theta_k$ e $i\theta_k^{'}$ são conjugados em L, segue que esses elementos possuem o mesmo grau sobre $\mathbb{Q}$. Como $i\theta_k \in \mathbb{Q}(i\theta_k^{'})$, segue o resultado. □

Teorema 6.2. *Os subcorpos de $L = \mathbb{Q}(\xi_{2^r})$, onde $r \geqslant 3$ é um inteiro positivo, são $\mathbb{Q}$, $\mathbb{Q}(\xi_{2^j})$, para $j = 2, 3, \ldots, r$, $\mathbb{Q}(\theta_k)$ e $\mathbb{Q}(i\theta_k)$, para $k = 3, 4, \ldots, r$, com $\theta_k = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$, onde o algarismo 2 aparece $k-2$ vezes.*

Demonstração. Segue diretamente do Teorema 6.1 e pelo Lema 6.8. □

Proposição 6.4. *Para todo $k > 2$ um inteiro positivo, o anel de inteiros de $\mathbb{Q}(i\theta_k)$ é $\mathbb{Z}[i\theta_k]$, sendo $\theta_k = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$, onde o algarismo 2 aparece $k-2$ vezes.*

Demonstração. Sejam $K_1 = \mathbb{Q}(\theta_{k+1})$ e $K_2 = \mathbb{Q}(i\theta_{k+1})$. Pelo Teorema 3.8, tem-se que o discriminante absoluto dos dois corpos são iguais, isto é $|d_{K_1}| = |d_{K_2}|$. Pela Proposição 1.3, segue que o anel de inteiros de K_1 é $\mathcal{O}_{K_1} = \mathbb{Z}[\theta_k]$. Pela Proposição 3.2, tem-se que

$$d(1, \theta_k, \ldots, \theta_k^{n-1}) = \prod_{i<j} (\sigma_i(\theta_k) - \sigma_j(\theta_k))^2,$$

e deste modo $|d_{K_1}| = \prod_{j<l} |(\sigma_j(\theta_k) - \sigma_l(\theta_k))|^2$. Os conjugados de θ_k são $\pm\sqrt{2 \pm \sqrt{2 \pm \cdots \pm \sqrt{2 \pm \sqrt{2}}}}$, e os conjugados de $i\theta_k$ são $\pm i\sqrt{2 \pm \sqrt{2 \pm \cdots \pm \sqrt{2 \pm \sqrt{2}}}}$. Assim, $\prod_{j<l} |(\sigma_j(\theta_k) - \sigma_l(\theta_k))|^2 = \prod_{j<l} |(\sigma_j(i\theta_k) - \sigma_l(i\theta_k))|^2$. Logo, como $|d_{K_1}| = |d_{K_2}|$, segue que $|d_{K_2}| = |d(1, i\theta_k, \ldots, (i\theta_k)^{n-1})|$. Portanto, pela Proposição 3.4, segue que o anel de inteiros de $K_2 = \mathbb{Q}(i\theta_{k+1})$ é dado por $\mathcal{O}_{K_2} = \mathbb{Z}[i\theta_k]$. □

Corolário 6.3. *Para o subcorpo $\mathbb{Q}(\xi_{2^j})$ de $L = \mathbb{Q}(\xi_{2^r})$, como no Teorema 6.2, o discriminante absoluto é dado por 2^β, onde $\beta = (j-1)2^{j-1}$, e o anel de inteiros é $\mathbb{Z}[\xi_{2^r}]$. Se o subcorpo é $\mathbb{Q}(\theta_{k+1})$ ou $\mathbb{Q}(i\theta_{k+1})$ então o discriminante absoluto é dado por 2^β, onde $\beta = k2^{k-1} - 1$, e o anel de inteiros é dado por $\mathbb{Z}[\theta_{k+1}]$ ou $\mathbb{Z}[i\theta_{k+1}]$, respectivamente.*

Demonstração. Para o discriminante absoluto, pelo Teorema 3.8, é suficiente observar que $\mathbb{Q}(\theta_{k+1})$ e $\mathbb{Q}(i\theta_{k+1})$ não são corpos ciclotômicos. Os anéis de inteiros são dados pelo Teorema 1.7, e pelas Proposições 1.3 e 6.4. □

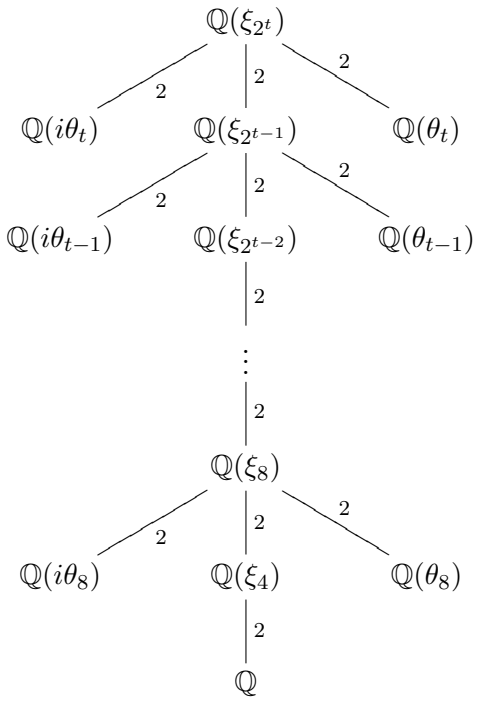

Figura 6.1: Subcorpos de $\mathbb{Q}(\xi_{2^r})$.

A Figura 6.1 apresenta um diagrama explicitando os subcorpos obtidos nesta seção, onde os números ao lado das linhas significa o grau da extensão. Para deixar o diagrama mais claro, algumas inclusões foram omitidas.

6.3 Reticulados $\mathbb{Z}^n$-rotacionados sobre $\mathbb{Q}(\theta)$, onde $\theta = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$

Apresentamos, conforme [1], nesta seção, uma construção de reticulados $\mathbb{Z}^n$-rotacionados sobre o subcorpo maximal real $\mathbb{Q}(\theta)$ do 2^r-ésimo corpo ciclotômico $\mathbb{Q}(\xi_{2^r})$, onde, pela Seção 6.2, segue que $\theta = \xi_{2^r} + \xi_{2^r}^{-1} = 2cos(\frac{\pi}{2^{r-1}}) = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$, onde o algarismo 2 aparece $r-2$ vezes. Uma construção similar pode ser encontrada em [12].

Sejam $r > 2$ um inteiro positivo, $\xi = \xi_{2^r}$ uma raiz 2^r-ésima primitiva da unidade, $L = \mathbb{Q}(\xi_{2^r})$ o 2^r-ésimo corpo ciclotômico, $\theta = \xi_{2^r} + \xi_{2^r}^{-1} = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$, e $K = \mathbb{Q}(\theta)$ o subcorpo maximal real de L.

Proposição 6.5. [*11, pag.*44] *Para todo p primo ímpar e r um inteiro positivo, tem-se que*

$$Tr_{\mathbb{Q}(\xi_{p^r})|\mathbb{Q}}(\xi_{p^r}^k) = \begin{cases} 0, & se\ \text{mdc}(k,p^r) < p^{r-1}; \\ -p^{r-1}, & se\ \text{mdc}(k,p^r) = p^{r-1}; \\ (p-1)p^{r-1}, & se\text{mdc}(k,p^r) > p^{r-1}. \end{cases} \tag{6.1}$$

Corolário 6.4. [*1, pag.*5] *Se $K = \mathbb{Q}(\xi + \xi^{-1})$ então*

$$Tr_{K|\mathbb{Q}}(\xi^k + \xi^{-k}) = \begin{cases} 0, & se\ \text{mdc}(k,2^r) < 2^{r-1}; \\ -2^{r-1}, & se\ \text{mdc}(k,2^r) = 2^{r-1}; \\ 2^{r-1}, & se\ \text{mdc}(k,2^r) > 2^{r-1}. \end{cases} \tag{6.2}$$

Proposição 6.6. [*1, pag.*5] *Considere $e_0 = 1$ e $e_j = \xi^j + \xi^{-j}$, para $j = 1, 2, \ldots, 2^{r-2} - 1$.*

i) Se $j = 1, 2, \ldots, 2^{r-2} - 1$ então $Tr_{K|\mathbb{Q}}(e_j e_j) = \begin{cases} -2^{r-1}, & se\ j = 0; \\ 0, & caso\ contrário. \end{cases}$

ii) Se $j \neq 0$ então $Tr_{K|\mathbb{Q}}(e_j e_0) = \begin{cases} -2^{r-1}, & se\ j = 1; \\ 0, & se\ j \neq 1. \end{cases}$

iii) Se $j \neq 0$, $k \neq 0$ e $j \neq k$, então $Tr_{K|\mathbb{Q}}(e_j e_k) = \begin{cases} -2^{r-1}, & se\ |j-k| = 1; \\ 0, & se\ |j-k| \neq 1. \end{cases}$

Proposição 6.7. [*1, pag.*6] *Sejam $K = \mathbb{Q}(\xi + \xi^{-1})$ o subcorpo maximal real do 2^r-ésimo corpo ciclotômico $\mathbb{Q}(\xi_{2^r})$ e $\alpha = (1-\xi)(1+\xi) = 2 - (\xi + \xi^{-1})$. Considere $f_j = \sum_{k=0}^{2^{r-2}-1} e_k$. O conjunto $\{f_0, f_1, \ldots, f_{2^{r-1}-1}\}$ é uma base integral para o anel de inteiros $\mathcal{O}_K$ de K e vale*

$$\frac{1}{2^{r-1}} Tr_{K|\mathbb{Q}}(\alpha f_j f_k) = \delta_{jk},$$

onde δ_{jk} é o delta de Kronecker, isto é, $\delta_{jk} = 0$, se $j \neq k$, e $\delta_{jj} = 1$. Assim, o reticulado ideal integral $(\mathcal{O}_K, q_\alpha)$ é um reticulado $\mathbb{Z}^n$-rotacionado, onde $q_\alpha : \mathcal{O}_K \times \mathcal{O}_K \longrightarrow \mathbb{Z}$ é a forma bilinear simétrica dada por $q_\alpha(x,y) = \frac{1}{2^{r-1}} Tr_{K|\mathbb{Q}}(\alpha xy)$, para todo $x, y \in \mathcal{O}_K$, e $n = 2^{r-2}$.

6.4 Conclusões

No decorrer deste capítulo encontramos a estrutura dos subcorpos de $\mathbb{Q}(\xi_{2^r})$, onde $r > 2$ é um inteiro, e também caracterizamos os anéis de inteiros de tais subcorpos. Além disso, motivados pela conjectura, presente em [12], de que é possível encontrar um reticulado algébrico congruente ao reticulado $\mathbb{Z}^n$ utilizando o corpo $\mathbb{Q}(\theta)$, onde $\theta = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$ e n é uma potência de 2, provamos que $\mathbb{Q}(\theta)$ é um subcorpo de um corpo ciclotômico $\mathbb{Q}(\xi_{2^r})$. Finalmente, observamos que tais estruturas fornecem a possibilidade do estudo de reticulados rotacionados, seja no espaço euclidiano ou hiperbólico.

Capítulo

7

Corpos de grau p e condutor p^2, onde p é um primo ímpar

Nesta capítulo apresentamos resultados sobre a forma traço de corpo de grau primo ímpar p e condutor p^2. Com a descrição da forma traço, apresentamos novas construções de reticulados e as respectivas matrizes de Gram. Sejam, a menos de menção contrária, $L = \mathbb{Q}(\xi)$ o p^2-ésimo corpo ciclotômico, onde p é um número primo ímpar, $\xi = \xi_{p^2}$ uma raiz p^2-ésima da unidade e K um subcorpo de L de grau ep, onde $e, e' \in \mathbb{Z}$ são inteiros positivos com $ee' = p - 1$. Pelo Teorema 5.2, tem-se $K = \mathbb{Q}(Tr_{L|K}(\xi))$, e $[L : K] = e'$. Entretanto, para gerar um reticulado ou um reticulado ideal precisamos de mais informações sobre esse corpo. Utilizando as técnicas de [3] e [22], assim como o discriminante, apresentamos, neste capítulo, as ferramentas necessárias para a obtenção de um reticulado ideal de dimensão p e de uma base integral para o subcorpo K de grau p de L. Na Seção 7.2 apresentamos um limitante para o mínimo euclidiano de K, valendo a conjectura de Minkowski para K.

7.1 Forma traço

Apresentamos, nesta seção, uma descrição sobre a forma traço do subcorpo K de grau p em $L = \mathbb{Q}(\xi_{p^2})$. A partir da forma traço para corpos ciclotômicos $\mathbb{Q}(\xi_{p^r})$, dada pela Proposição 7.2, obtemos a forma traço sobre K para um subconjunto de $\mathcal{O}_K$, onde $K \subseteq \mathbb{Q}(\xi_{p^2})$. Utilizando as ferramentas e notações de [22], tem-se que a matriz da forma traço para esse subconjunto de $\mathcal{O}_K$ é dado pelo Lema 7.2. Deste modo, o Lema 7.2 fornece

um conjunto de elementos de $\mathcal{O}_K$ que possui discriminante $p^{2(p-1)}$, que, pela Proposição 7.1, esse é o mesmo valor que o discriminante absoluto de K. Utilizando a Proposição 3.4, obtemos, no Teorema 7.2, que tal conjunto é uma base integral para K. Com isso, a forma traço apresentada é a forma traço sobre K.

Nesta seção, salvo menção contrário, p é um primo ímpar, $L = \mathbb{Q}(\xi_{p^2})$ é o p^2-ésimo corpo ciclotômico e K é um subcorpo de grau p de L. Denotando $\theta_j = Tr_{L|K}(\xi^j)$, tem-se que $\theta_j = \sigma_j(\theta)$ é um conjugado de θ. Pela Proposição 5.9, segue que $\sigma^p(\theta_j) = \theta_j$ e, pela Proposição 5.10, tem-se que θ tem p conjugados distintos.

Como caso particular do Teorema 5.2, tem-se seguinte proposição.

Proposição 7.1. *Se $L = \mathbb{Q}(\xi_{p^2})$ e K é o subcorpo de L, com grau p, então $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi_{p_2})$, e o discriminante absoluto de K é dado por $|d_K| = p^{2(p-1)}$.*

A Figura 7.1 apresenta um diagrama contendo o subcorpo de p em $\mathbb{Q}(\xi_{p^2})$, onde os números ao lado das linhas expressa os graus das extensões.

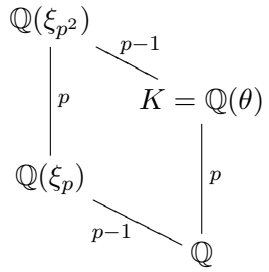

Figura 7.1: Subcorpo de $\mathbb{Q}(\xi_{p^2})$ e grau p.

Proposição 7.2. [22] *Seja $\xi = \xi_{p^2}$ uma raiz p^2-ésima da unidade. Se $L = \mathbb{Q}(\xi)$, então*

$$Tr_{L|\mathbb{Q}}(\xi^j) = \begin{cases} 0, & \text{se } j \not\equiv 0 \ mod\ p, \\ -p, & \text{se } j \equiv 0 \ mod\ p,\ j \neq 0, \\ p(p-1), & \text{se } j = 0. \end{cases} \tag{7.1}$$

Pela Proposição 7.2, tem-se que

$$Tr_{K|\mathbb{Q}}(\theta_j) = Tr_{K|\mathbb{Q}}(Tr_{L|K}(\xi^j)) = Tr_{L|\mathbb{Q}}(\xi^j) \quad = \quad \begin{cases} 0, & \text{se } j \not\equiv 0 \ mod\ p, \\ -p, & \text{se } j \equiv 0 \ mod\ p,\ j \neq 0, \\ p(p-1), & \text{se } j = 0. \end{cases}$$

Além disso, como $\theta_j = Tr_{L|K}(\xi) = \sum_{l=1}^{p-1} \xi^{j\alpha^{lp}}$, segue que

$$\theta_i\theta_j = \sum_{l=1}^{p-1} \xi^{i\alpha^{kp}} \sum_{k=1}^{p-1} \xi^{j\alpha^{lp}} = \sum_{k,l=1}^{p-1} \xi^{i\alpha^{kp}+j\alpha^{lp}}.$$

Proposição 7.3. *Sejam $L = \mathbb{Q}(\xi_{p^2})$ o p^2-ésimo corpo ciclotômico e K é o subcorpo de L, com grau p^2. Se $\theta_j = Tr_{L|K}(\xi_{p^2})$ então*

$$\begin{aligned}
Tr_{L|\mathbb{Q}}(\theta_p\theta_p) &= p(p-1); \\
Tr_{L|\mathbb{Q}}(\theta_p\theta_j) &= 0, \qquad\quad se\ \mathrm{mdc}(p,j)=1; \\
Tr_{L|\mathbb{Q}}(\theta_i\theta_j) &= p(p-1), \quad se\ \mathrm{mdc}(p,i)=\mathrm{mdc}(p,j)=1, i \not\equiv j \pmod{p^2}; \\
Tr_{L|\mathbb{Q}}(\theta_j\theta_j) &= p(p-1)^2, \quad se\ \mathrm{mdc}(p,j)=1.
\end{aligned}$$

Demonstração. Calculando o traço de cada $\xi^{i\alpha^{kp}+j\alpha^{lp}}$, pela Proposição 7.2, segue o resultado. □

Corolário 7.1. *Sejam $L = \mathbb{Q}(\xi_{p^2})$ o p^2-ésimo corpo ciclotômico e K é o subcorpo de L, com grau p. Se $\theta_j = Tr_{L|K}(\xi_{p^2})$ então*

$$\begin{aligned}
Tr_{K|\mathbb{Q}}(\theta_p\theta_p) &= p; \\
Tr_{K|\mathbb{Q}}(\theta_p\theta_j) &= 0, \qquad\quad se\ \mathrm{mdc}(p,j)=1; \\
Tr_{K|\mathbb{Q}}(\theta_i\theta_j) &= -p, \qquad\quad se\ \mathrm{mdc}(p,i)=\mathrm{mdc}(p,j)=1, i \not\equiv j \pmod{p^2}; \\
Tr_{K|\mathbb{Q}}(\theta_j\theta_j) &= p(p-1), \quad se\ \mathrm{mdc}(p,j)=1.
\end{aligned}$$

Demonstração. Como $Tr_{K|\mathbb{Q}}(\alpha) = \dfrac{1}{p-1} Tr_{L|\mathbb{Q}}(\alpha)$, para todo $\alpha \in K$, o resultado segue diretamente da Proposição 7.2. □

Teorema 7.1. *[22] Sejam $n \in \mathbb{N}$ e $b \in \mathbb{R}$ com $b > n$. Se $L_{b,n}$ é um reticulado no $\mathbb{R}^n$ com matriz de Gram*

$$A = bI_n - J_n = \begin{pmatrix} b-1 & -1 & \cdots & -1 \\ -1 & b-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & & b-1 \end{pmatrix}, \tag{7.2}$$

onde I_n é a matriz identidade de ordem n e $J_n \in \{1\}^{n\times n}$ é uma matriz $n \times n$ com todas entradas 1, então $L_{b,n}$ é um reticulado definido positivo com determinante $(b-n)b^{n-1}$.

Corolário 7.2. *O reticulado $L_{p,p-1}$ de dimensão $p-1$ possui como matriz de Gram a matriz de ordem $(p-1)\times(p-1)$ dada por*

$$A = \begin{pmatrix} p-1 & -1 & \cdots & -1 \\ -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & & p-1 \end{pmatrix} \tag{7.3}$$

e possui determinante p^{p-2}.

Demonstração. Segue do Teorema 7.1, tomando $b = p$ e $n = p-1$. □

Antes de enunciar o Teorema 7.2, apresentamos os Lemas 7.1 e 7.2, que serão utilizados para calcular a forma traço do corpo K e o seu anel de inteiros.

Lema 7.1. *A matriz*

$$A = p\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & p-1 & -1 & \cdots & -1 \\ 0 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & -1 & & p-1 \end{pmatrix}$$

possui determinante $p^{2(p-1)}$.

Demonstração. Pelo Corolário 7.2, segue que $L_{p,p-1}$ possui determinante p^{p-2}. Assim, $\det(A) = p^{2(p-1)}$, o que demonstra o resultado. □

Agora, como θ possui p conjugados, tome $p-1$ desses conjugados, e denote-os por $\theta_{j_1}, \theta_{j_2}, \ldots, \theta_{j_{p-1}}$. Seja ainda $\theta_{j_0} = \theta_p$. Desse modo, tem-se o conjunto $\{\theta_{j_0}, \theta_{j_1}, \ldots, \theta_{j_{p-1}}\}$.

Lema 7.2. *O conjunto* $\{\theta_{j_0}, \theta_{j_1}, \ldots, \theta_{j_{p-1}}\}$ *possui matriz de Gram dada por*

$$p\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & p-1 & -1 & \cdots & -1 \\ 0 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & -1 & & p-1 \end{pmatrix}$$

e discriminante $p^{2(p-1)}$.

Demonstração. A matriz de Gram segue diretamente pelo Corolário 7.1, pois $\theta_{j_0} = \theta_p$ e cada θ_{j_s} é um θ_t com $\mathrm{mdc}(p,t) = 1$, onde $s = 1, 2, \ldots, p-1$. Pelo Lema 7.1, segue o valor do discriminante. □

Com base nesses resultados, apresentamos a seguir o teorema mais importante desta seção, que apresenta uma base integral para o corpo K e a forma traço para esse corpo.

Teorema 7.2. *Sejam* K *um subcorpo de* $L = \mathbb{Q}(\xi_{p^2})$ *de dado grau* p, $\theta = Tr_{L|K}(\xi_{p^2})$ *e* $\theta_{j_0} = Tr_{L|K}(\xi_{p^2}^p) = Tr_{L|K}(\xi_p)$. *O discriminante absoluto de* K *é* $p^{2(p-1)}$. *Se* $\theta_{j_1}, \theta_{j_2}, \ldots, \theta_{j_{p-1}}$ *são* $p-1$ *conjugados distintos de* θ *em* K, *então o conjunto* $B = \{\theta_{j_0}, \theta_{j_1}, \ldots, \theta_{j_{p-1}}\}$ *é uma base integral para o anel de inteiros* $\mathcal{O}_K$ *de* K *e a matriz de Gram do reticulado algébrico gerado, a partir do anel de inteiros* $\mathcal{O}_K$ *de* K, *pelo homomorfismo canônico* $\sigma : K \longrightarrow \mathbb{R}^p$, *é a matriz* A *de ordem* $p \times p$ *dada por*

$$A = p\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & p-1 & -1 & \cdots & -1 \\ 0 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & -1 & & p-1 \end{pmatrix}.$$

Demonstração. Pelo Lema 7.2, tem-se que A é a matriz de Gram do conjunto B, que possui discriminante $p^{2(p-1)}$. Pela Proposição 7.1, segue que o discriminante absoluto de K é $d_K = p^{2(p-1)}$. Como $B \subseteq \mathcal{O}_K$, segue que B é uma base integral para $\mathcal{O}_K$. □

Com base no Teorema 7.2, obtemos como consequência imediata o seguinte corolário.

Corolário 7.3. *Sejam K um subcorpo de $L = \mathbb{Q}(\xi_{p^2})$ de dado grau p, $\theta = Tr_{L|K}(\xi_{p^2})$, $\theta_{j_0} = Tr_{L|K}(\xi_{p^2}^p) = Tr_{L|K}(\xi_p)$ e $B = \{\theta_{j_0}, \theta_{j_1}, \ldots, \theta_{j_{p-1}}\}$ a base integral para K dada pelo Teorema 7.2. A forma traço sobre K*

$$\begin{aligned} Tr : K \times K &\longrightarrow \mathbb{Q} \\ (x, y) &\longmapsto Tr_{K|\mathbb{Q}}(xy), \end{aligned}$$

é caracterizada pela matriz

$$A = p \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & p-1 & -1 & \cdots & -1 \\ 0 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & -1 & & p-1 \end{pmatrix}.$$

Além disso, $(\mathcal{O}_K, Tr)$ é um reticulado ideal integral.

7.2 Mínimo euclidiano para corpos de grau p e condutor p^2

Nesta seção, seja K um subcorpo de grau p em $L = \mathbb{Q}(\xi_{p^2})$, onde $\xi = \xi_{p^2}$ é uma raiz p^2-ésima da unidade com p um primo ímpar. O objetivo principal dessa seção é demonstrar a desigualdade $M(K) \leqslant \frac{1}{2^p}\sqrt{|d_K|}$.

Sendo $L \subseteq \mathbb{R}^n$ um reticulado n-dimensional, da definição de máximo de um reticulado, apresentado na Seção 4.5, Definição 4.13, relembramos que o máximo de L é definido por

$$\max(L) = \sup\{\min\{\langle x - l, x - l\rangle; l \in L\}; x \in \mathbb{R}\},$$

que é a máxima distância de um ponto do $\mathbb{R}^n$ até L.

Desse modo, tem-se que $\max\ \mathbb{Z} = \frac{1}{4}$. Por [22], $\max\ L_{p,p-1} = \frac{p^2-1}{12}$. Do Corolário 7.3, $(\mathcal{O}_K, Tr(1)) = p(\mathbb{Z} \perp L_{p,p-1})$. Consequentemente,

$$\max \mathcal{O}_K = p\left[\frac{1}{4} + \frac{p^2-1}{12}\right] = p\frac{p^2+2}{12}.$$

Teorema 7.3. *Sejam $p \geqslant 5$ um primo e K o único corpo de grau p e condutor p^2. O mínimo euclidiano do corpo K é dado por $M(K) \leqslant \frac{1}{2^p}\sqrt{|d_K|}$.*

Demonstração. É suficiente provar que $\dfrac{M(K)}{\sqrt{|d_K|}} \leqslant c^p$, com $c \leqslant \dfrac{1}{2}$. Tem-se que

$$\begin{aligned}
\frac{M(K)}{\sqrt{|d_K|}} &= \frac{\left(\dfrac{\max \mathcal{O}_K}{p}\right)^{p/2}}{\sqrt{|d_K|}} \\
&= \frac{\left(\dfrac{p^2+2}{12}\right)^{p/2}}{p^{p-1}} \\
&= p\left(\frac{p^2+2}{12}\right)^{p/2}\frac{1}{p^p} \\
&= p\left(\frac{p^2+2}{12p^2}\right)^{p/2} \\
&= \left[p^{1/p}\left(\frac{p^2+2}{12p^2}\right)^{1/2}\right]^p \\
&= c^p,
\end{aligned}$$

onde $c = p^{1/p}\left(\dfrac{p^2+2}{12p^2}\right)^{1/2}$, para todo $p \geqslant 5$ primo. Agora, $c \leqslant \dfrac{1}{2}$, uma vez que $p^2+2 \leqslant \dfrac{11p^2}{10}$. Assim, $\dfrac{p^2+2}{12p^2} \leqslant 11/120 < \dfrac{1}{9}$. Por [17], tem-se que $p^{1/p} \leqslant \dfrac{3}{2}$. Disto resulta que $c \leqslant \dfrac{1}{2}$, o que prova o teorema. □

Corolário 7.4. *Seja p um primo. Qualquer corpo de condutor p^2 e grau p satisfaz a conjectura de Minkowski.*

Demonstração. É uma consequência imediata do Teorema 7.3. □

7.3 Conclusões

Motivados pela construção de reticulados e reticulados ideais, neste capítulo, prosseguimos na descrição de corpos cujo condutor é uma potência de um primo ímpar p. Descrevemos neste capítulo o anel de inteiros e a forma traço para corpos de grau p cujo condutor é p^2. Com isto, obtemos um reticulado ideal gerado pelo anel de inteiros através do homomorfismo de Minkowski do corpo de grau p cujo condutor é p^2. Com isso, dois parâmetros importantes podem serem encontrados para esse reticulado, que é a distância produto mínima e a densidade de centro. Finalmente, concluímos o capítulo apresentando um limitante para o mínimo euclidiano para tais corpos. Esses resultados fornecem perspectivas para futuros estudos no sentido de calcular o mínimo euclidiano para todos os corpos cujo condutor é potência de um primo ímpar.

Capítulo

8

Conclusões e perspectivas futuras

Descrevemos, brevemente, os resultados apresentados neste trabalho, juntamente com as possíveis extensões ou generalizações dos resultados aqui apresentados.

No Capítulo 1, apresentamos os fundamentos da Teoria Algébrica dos Números, que é um dos pilares para o desenvolvimento deste trabalho. Os principais resultados do capítulo são o Teorema Fundamental da Teoria de Galois, apresentado no Teorema 1.4, e o Teorema de Kronecker-Weber, apresentado no Teorema 1.5, a partir do qual faz sentido falar em condutor de um corpo abeliano.

No Capítulo 2 foram introduzidos os corpos p-ádicos, sendo que o conceito de fracamente ramificado foi essencial para apresentarmos uma nova demonstração para a fórmula do discriminante de corpos de números cujo condutor é uma potência de um primo ímpar.

O Capítulo 3 foi dedicado ao cálculo do discriminante de corpos de números abelianos. Na Seção 3.2 foram apresentados os principais resultados conhecidos na literatura sobre discriminante de corpos de números abelianos. Nota-se que esses resultados, embora se mostrando muito úteis, como ferramenta de análise durante a geração de reticulados via corpos de números, ainda não são tão amplamente utilizados na pesquisa. Na Seção 3.4 apresentamos uma nova demonstração para a fórmula do discriminante para corpos de números abelianos cujo condutor é uma potência de primo ímpar.

No Capítulo 4 apresentamos os conceitos de reticulados e a conjectura de Minkowski. Embora tenhamos apresentados os principais parâmetros de um reticulado, não fizemos menção aos parâmetros referente à geração de códigos para o canal gaussiano, que são o raio de empacotamento e a densidade de centro do reticulado. Com esses resultados, torna-se possível o

estudo de tais parâmetros, com o intuito de obter bons reticulados, seja em relação à densidade de centro ou em relação à distância produto mínima. Na Seção 4.5 introduzimos o mínimo euclidiano, que é necessário para entender a conjectura de Minkowski. O mínimo euclidiano também foi utilizado no Capítulo 7, onde provamos que todo corpo de números de grau p e condutor p^2, onde p é um primo ímpar, satisfaz a conjectura de Minkowski. Apresentamos na Seção 4.6 a conjectura de Minkowski, que é devida aos trabalhos de Minkowski.

Em especial, destacamos os trabalhos [38] e [39], que trabalham com a conjectura de Woods, que por sua vez implica na conjectura de Minkowski. Acreditamos que o raciocínio apresentado por esses trabalhos possa ser estendido para dimensões superiores. Entretanto, fazer tal extensão exige uma quantidade cada vez maior de cálculos. Para $n = 7$ foi necessário analisar 64 casos e para $n = 8$ será necessário analisar 128 casos, o que impossibilita extender este raciocínio para dimensões n muito maiores, a menos que seja possível utilizar modelos computacionais para isto.

Na Seção 4.7 foram apresentados algumas cotas conhecidas para o mínimo euclidiano de alguns corpos de números abelianos. Nossa contribuição para explicitar a forma traço e encontrar o mínimo euclidiano, no Capítulo 7, foi inspirado nos artigos que fornecem tais cotas, a saber, [3] e [22].

No Capítulo 5, nosso objetivo foi obtenção de uma descrição explícita para corpos cujo condutor é potência de um primo ímpar, que são corpos contidos em extensões ciclotômicas cíclicas. Neste sentido, provamos que para um corpo K de condutor p^r, tomando $L = \mathbb{Q}(\xi_{p^r})$, tem-se que $K = \mathbb{Q}(\theta)$, onde $\theta = Tr_{L|K}(\xi_{p^r})$. O caso particular em que $p = 3$ foi tratado na Seção 5.4. Na Seção 5.3 apresentamos uma demonstração alternativa para a descrição dos corpos de condutor p, onde p é um primo ímpar, o que resulta também numa base integral para os anéis de inteiros desses corpos.

Como os subcorpos das extensões ciclotômicas cíclicas $\mathbb{Q}(\xi_{p^r})$, onde p é um primo ímpar foram encontrados, segue que uma proposta para uma primeira generalização para tal construção é encontrar a descrição para corpos cíclicos contidos em algum $\mathbb{Q}(\xi_n)$, onde n é, inicialmente, da forma pq, com p e q primos ímpares, com a expectativa de extender para qualquer natural $n \in \mathbb{N}$. E um passo seguinte é encontrar a descrição para corpos abelianos, contidos em $\mathbb{Q}(\xi_n)$, cujo grupo de Galois é gerado por dois elementos, e assim sucessivamente, até encontrar uma descrição para todos os corpos de números abelianos.

Inspirados na conjectura apresentada por Girald et al em 1997, [12], que diz que o anel de inteiros de $\mathbb{Z}[\theta]$, onde $\theta = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$ pode ser utilizado para gerar um reticulado ideal $\mathbb{Z}^n$-rotacionado, desenvolvemos o Capítulo 6 . Neste sentido, provamos que $\mathbb{Z}[\theta]$ é o anel de inteiros do subcorpo maximal de $\mathbb{Q}(\xi_{2^r})$, para algum $r \in \mathbb{N}$. Além disso, expressamos todos os subcorpos de $\mathbb{Q}(\xi_{2^r})$, juntamente com o respectivo anel de inteiros. Com isso, tem-se que os trabalhos [1] e [29] respondem a conjectura que motivou este capítulo.

Optamos por dedicar o Capítulo 7 a uma melhor caracterização dos corpos K de grau p e condutor p^2, onde p é um primo ímpar. Utilizando a forma traço para os corpos ciclotômicos

cíclicos $\mathbb{Q}(\xi_{p^r})$, obtemos a forma traço para um conjunto de elementos de K. Como o valor do discriminante de K já é conhecido, obtivemos, deses modo, a forma traço e o anel de inteiros para o corpo K. Desta forma, o anel de inteiros de K, munido da forma traço, é um reticulado ideal integral. Na Seção 7.2 calculamos uma cota superior para o mínimo euclidiano para este corpo, onde provamos que K satisfaz a conjectura de Minkowski. Logo, todo corpo de grau p e condutor p^2 satisfaz a conjectura de Minkowski.

Pelos artigos [3] e [22], sabe-se que a conjectura de Minkowski é satisfeita para os corpos ciclotômicos cíclicos da forma $\mathbb{Q}(\xi_{p^r})$ e seus respectivos subcorpos maximais, onde p é um primo ímpar. Com isso, uma expectativa futura é provar que a conjectura de Minkowski vale para todo subcorpo de um corpo ciclotômico cíclico $\mathbb{Q}(\xi_{p^r})$. Uma alternativa para tratar deste problema seria utilizar a expressão da forma traço para corpos ciclotômicos cíclicos $\mathbb{Q}(\xi_{p^r})$ dado por [11], onde a forma traço é tratada como uma forma quadrática, sabendo-se explicitamente onde ocorre o valor mínimo desta forma quadrática.

Como outras perspectivas futuras para trabalhos, destacamos alguns pontos que podem ser desenvolvidos sobre reticulados e reticulados ideais. Para o reticulado ideal gerado no Capítulo 7, é interessante encontrar a distância produto mínima, pois a distância produto mínima esta ligada ao desempenho que o código gerado por esse reticulado ideal possui em canais ruidosos do tipo Rayleigh. Por outro lado, olhando o mesmo como um reticulado no $\mathbb{R}^n$, isto é, como um reticulado no $\mathbb{R}^n$ gerado pelo anel de inteiros de K através do homomorfismo canônico, deve-se encontrar a distância produto mínima entre dois pontos do reticulado e a densidade de centro deste reticulado. Para tal podemos utilizar os vários resultados e técnicas presentes na literatura para este fim, como por exemplo, [1], [4], [5], [10], [11], [12], [29], [36], entre outros.

Índice Remissivo

Referências Bibliográficas

[1] A. A. Andrade, C. Alves, , T. C. Carlos. T. B., *Rotated Lattices via the Cyclotomic Field* $\mathbb{Q}(\xi_{2^r})$, International Journal of Applied Mathematics, Vol. 19, p. 321-331, 2006.

[2] F. Ayres Jr., R. E. Moyer, *Theory and Problems of trigonometry*, Thirt Editon, McGraw-Hill, New York, 1999.

[3] E. Bayer-Fluckiger, *Upper bounds for Euclidean minima of algebraic number fields*, J. Number Theory, Vol. 121, n. 2, 2006.

[4] E. Bayer-Fluckiger, *Lattices and Number Fields*, Contemp. Math., Vol. 241, p. 69-84, 1999.

[5] E. Bayer-Fluckiger, *Ideal Lattices*, Proc. of the conference in honor of Alan Baker, Number Theory and Diophantine Geometry, Cambridge Univ. Press, p. 168-184, 2002.

[6] H. Cohen. *A Couse in Computational Algebraic Number Theory*. Spring-Verlag, Berlin, 1993.

[7] J. H. Conway, J. N. A. Sloane, *Sphere packing, lattices and groups*, Third Edition, Springer, New York, 1999.

[8] F. J. Dyson. *On the product of four non-homogeneous linear forms*. Annals of Math., Vol. 49, p. 82-109, 1948.

[9] O. Endler, *Teoria do números algébricos*, IMPA, Rio de Janeiro, 2006.

[10] A. J. Ferrari, *Reticulados Algébricos via Corpos Abelianos*, Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto, 2008.

[11] A. L. Flores, *Reticulados em corpos abelianos*. Tese de doutorado, Unicamp, Campinas, 2000.

[12] X. Giraud, E. Boutilon, J. C. Belfiore, *Algebraic Tools to Build Modulation Schemes for Fading Channels*, IEEE Transacions on Information Theory, Vol. 43, n. 3, 1997.

[13] J. C. Interlando, J. O D. Lopes, T. P. da Nobrega Neto, *The discriminant of abelian number fields*, J. Algebra Appl., Vol. 5, p. 35-41, 2006.

[14] C. H. S de Jesus, *Discriminante dos Subcorpos de Corpos Ciclotômicos de Condutores Potência de um Primo Impar*, Dissertação de Mestrado, UFPB, João Pessoa, 2006.

[15] J. F. Koksma. *Diophantische Approximationen*. Springer-Verlag, 1936.

[16] S. Lang, *Algebraic Number Theory*, 2th edition, Springer, 1994.

[17] E. L. Lima, *Analise Real Vol. 1*, 10th edition, SBM, Rio de Janeiro, 2008.

[18] J. O. D. Lopes, *The discriminant of subfields of* $\mathbb{Q}(\xi_{2^r})$, Journal of Algebra and Its Applications, Vol. 2, n. 4, p. 463-469, 2003.

[19] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1987.

[20] H. Minkowski, *Diophantische Approximationen*, Zeipzig, 1907.

[21] L. H. J. Monteiro, *Teoria de Galois*, Colóquio Brasileiro de Matemática, IMPA, Poços de Caldas, 1969.

[22] G. Nebe, E. Bayer-Fluckiger, *On the Euclidean minimum of some real number fields*, J. Théorie de nombres de Bordeaux, Vol. 17, p. 437-454, 2005.

[23] J. Neukirch,, *Algebraic Number Theory*, Translated from the German, Springer, Berlin, 1999.

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

[25] R. Remak. *Verallgemeinerrung eines Minkowskichen Satzes*. Math. Zeitscher, 1928.

[26] P. Ribenboin, P., *Classical Theory of Algebraic Numbers* Universitext, Springer, New York, 2001.

[27] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer, New York, 1996.

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

[29] B. Sethuraman, F. Oggier, *Constructions of Orthonormal Lattices and Quaternion Division Algebras for Totally Real Number Fields*, AAECC 17, p. 138-147, Bangalore, 2007.

[30] M. A. Simachew, *A Survey on Euclidean Number Fieds*, Dissertação de Mestrado, University of Bordeaux I, 2009.

[31] B. F. Skubenko. *A new variant of the proof of the inhomogeneous Minkowski conjecture for* $n = 5$. Trudy Mat. Inst. Steklov. Vol 142, p. 240-253,271, 1976.

[32] B. F. Skubenko. *A proof of Minkowski's conjecture on the product of n linear inhomogeneous forms in n variables for* $n \leqslant 5$. J. Soviet Math., Vol. 6, p. 627-650, 1976.

[33] I. N. Stewart, *Galois Theory*, Third Edition, Champan Hall, Boca Rotan, 2004.

[34] I. N. Stewart, D. O. Tall., *Algebric Number Theory*, Second Edition, Champan Hall, London, 1992.

[35] H.P. F. Swinnerton-Dyer. *A brief guide to algebraic number theory.* Cambridge Unviversity Press, 2001.

[36] J. P. G. Vicente, *Reticulados de posto 3 em corpos de núumeros.* 2000, Dissertação de Mestrado, Unesp, São José do Rio Preto, 2000.

[37] L. C. Washington, *Introduction to Cyclotomic Fields*, Second Edition, Springer, New York, 1996.

[38] R. J. Hans-Gill, M. Raka, R. Sehmi, Sucheta, *A unified simple proof of a conjecture of Woods for* $n \leqslant 6$, Journal of Number Theory, Vol. 129, n. 5, p. 1000-1010, 2009.

[39] R. J. Hans-Gill, M. Raka, R. Sehmi, *On conjectures of Minkowski and Woods for* $n = 7$, Journal of Number Theory, Vol. 129, n. 5, p. 1011-1033, 2009.