

Universidade Estadual Paulista “Júlio de Mesquita Filho”
Instituto de Biociências, Letras e Ciências Exatas

Robson Ricardo de Araujo

Anéis de inteiros de corpos de números e aplicações

São José do Rio Preto
Fevereiro - 2015

Robson Ricardo de Araujo

Anéis de inteiros de corpos de números e aplicações

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

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Universidade Estadual Paulista "Júlio de Mesquita Filho"

São José do Rio Preto

Fevereiro - 2015

Araujo, Robson Ricardo de.

Anéis de inteiros de corpos de números e aplicações / Robson
Ricardo de Araujo. -- São José do Rio Preto, 2015
215 p. : il.

Orientador: Antonio Aparecido de Andrade
Dissertação (mestrado) – Universidade Estadual Paulista “Júlio
de Mesquita Filho”, Instituto de Biociências, Letras e Ciências Exatas

1. Matemática. 2. Álgebra. 3. Teoria dos números algébricos.
4. Anéis (Álgebra) 5. Extensões de corpos (Matemática) 6. Teoria dos
reticulados. I. Andrade, Antonio Aparecido de. II. Universidade Estadual
Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e
Ciências Exatas. III. Título.

CDU – 512

Ficha catalográfica elaborada pela Biblioteca do IBILCE
UNESP - Câmpus de São José do Rio Preto

Folha de Aprovação.

São José do Rio Preto, 27 de fevereiro de 2015.

**Prof. Dr. Antonio Aparecido de
Andrade**
Orientador

**Prof. Dr. Trajano Pires da Nóbrega
Neto**
UNESP - São José do Rio Preto

Prof. Dr. Edson Donizete de Carvalho
UNESP - Ilha Solteira

São José do Rio Preto
Fevereiro - 2015

Aos meus pais,
dedico

Agradecimentos

Ao concluir este trabalho, agradeço:

Primeiramente a Deus, pois Ele me deu força, luz e sabedoria para desenvolver este trabalho.

Aos meus pais, Aparecida e Nelson, que me educaram, me amaram, me ensinaram o valor do trabalho bem feito e responsável, me transmitiram a fé e me deram sustentação em todos esses anos de estudo.

Às minhas avós Alice (in memorian) e Irani, a meu avô Osvaldo, que foram para mim exemplo de sabedoria, de perseverança e de carinho, e também a meus outros avós (in memorian), que certamente intercederam por mim dos céus.

À minha tia Idalina, a meu tio Eurípedes e a todos os demais membros de minha família, pelo apoio e pelos ensinamentos que me deram na vida.

À minha namorada Beatriz, que sempre esteve ao meu lado em todos os momentos e que, com seu carinho e amor, me animou para que eu tivesse força e alegria para perseverar.

Ao meu orientador, Prof. Dr. Antonio Aparecido de Andrade, pelos oito anos que me orientou, pela confiança, pelos conselhos, pela amizade, pelo incentivo e pelas portas que me abriu na vida.

Aos professores que me orientaram durante a iniciação científica júnior da OBMEP, Prof. Dr. João Carlos F. Costa, Profa. Dra. Maria do Socorro N. Rangel e Profa. Ma. Marta L. S. Pignatari, que me incentivaram desde o início.

Aos professores do Departamento de Matemática do Ibilce/Unesp, em especial à Profa. Dra. Maria Gorete C. Andrade, pelo aprendizado que adquiri deles e pela amizade.

Aos professores titulares da banca examinadora, Prof. Dr. Trajano P. N. Neto (Ibilce/Unesp) e Prof. Dr. Edson Donizete de Carvalho (FEIS/Unesp), e aos professores suplentes da banca examinadora Prof. Dr. Eduardo Rogério Fávaro (UFMT) e Prof. Dr. Clotilzio Moreira dos Santos (Ibilce/UNESP).

Aos meus amigos Alex, Flavio, Rodrigo e Tiago, pela harmoniosa e feliz convivência que sempre tivemos juntos e pelas inesquecíveis experiências compartilhadas.

Ao meu amigo e orientador espiritual Pe. Marcio Tadeu, pelo carinho e pelas oportunidades que me apresentou.

À Capes, pelo auxílio financeiro.

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

“Feliz o homem que se dedica à sabedoria, que reflete com inteligência, que medita no coração sobre os caminhos da sabedoria e com a mente penetra os segredos dela.”
(Eclesiástico 14, 20)

Resumo

Esta dissertação apresenta o anel de inteiros de corpos quadráticos, de corpos ciclotômicos, de alguns subcorpos ciclotômicos e de corpos de números abelianos com o objetivo de utilizá-los na produção de reticulados algébricos, os quais são aplicados à teoria da Informação e à teoria dos Códigos Corretores de Erros. O texto desenvolve conceitos básicos sobre Álgebra e Teoria Algébrica dos Números, estuda bases integrais de corpos de números sob dois diferentes aspectos, caracteriza o anel de inteiros dos corpos de números referidos anteriormente e apresenta algumas aplicações dessa teoria aos reticulados algébricos. Os teoremas centrais demonstrados nesta dissertação são o Teorema de Hilbert-Speiser e o Teorema de Leopoldt-Letl. Este fornece o anel de inteiros de qualquer corpo de números abeliano, generalizando aquele. Esta dissertação possui um capítulo dedicado à demonstração do Teorema de Leopoldt-Letl de maneira detalhada. Além disso, este trabalho faz uma análise sobre a monogênese de alguns anéis de inteiros e apresenta um contraexemplo de anel de inteiros não monogênico. O último capítulo é dedicado aos reticulados e mostra exemplos de reticulados algébricos construídos nos espaços de dimensões 2, 4, 6 e 8 via o homomorfismo de Minkowski em ideais de anéis de inteiros de corpos de números. O trabalho que originou esta dissertação consistiu principalmente na pesquisa e no detalhamento das demonstrações do Teorema de Leopoldt-Letl e de três teoremas relacionados ao tema da monogênese de anéis de inteiros. Este empenho deu origem a um desenvolvimento mais claro e menos compacto das demonstrações relacionadas a esses assuntos, o qual é apresentado no texto. Enfim, este trabalho reúne e oferece um grande aparato teórico que tem sido útil ao desenvolvimento da teoria dos reticulados algébricos e que cria a expectativa de sua utilização em futuras aplicações nessa área.

Palavras-chave: Anéis de inteiros. Corpos de números abelianos. Teorema de Leopoldt-Letl. Reticulados algébricos.

Abstract

This master thesis presents the rings of integers of quadratic fields, cyclotomic fields, some cyclotomic subfields and abelian number fields aiming use them to produce algebraic lattices, which are applied in the Information Theory and in the Error Correcting Codes Theory. The text develops basic concepts about Algebra and Algebraic Number Theory, studies integral basis of number fields from two different perspectives, characterizes the ring of integers of the aforementioned number fields and presents some applications of this theory to algebraic lattices. The main proven theorems in this thesis are Hilbert-Speiser Theorem and Leopoldt-Letl Theorem. The second provides the ring of integers of any abelian number field, generalizing the first. This thesis has a chapter dedicated to make the proof of the Leopoldt-Letl Theorem in detail. Furthermore, this work analyses the monogenesis of some ring of integers and presents a counterexample of a ring of integers non-monogenic. The last chapter is aimed at lattices and shows examples of algebraic lattices in spaces of dimensions 2, 4, 6 and 8 constructed by ideals of ring of integers of number fields through Minkowski homomorphism. The work that created this thesis consisted mainly in research and detailing of the proofs of Leopoldt-Letl Theorem and of three theorems linked to the issue of monogenesis of the ring of integers. This effort created a development lighter and less compact of the proofs related to these subjects, which is presented in the text. Finally, this thesis gathers and provides a great theoretical apparatus that has been useful to development of the theory of algebraic lattices and that creates the expectation of its use in future applications in this area.

Keywords: Ring of integers. Abelian Number Fields. Leopoldt-Letl Theorem. Algebraic lattices.

Lista de Símbolos

$\mathbb{N}$	conjunto dos números naturais
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{Q}$	conjunto dos números racionais
$\mathbb{R}$	conjunto dos números reais
$\mathbb{C}$	conjunto dos números complexos
$\partial(f)$	grau do polinômio $f(x)$
$p(x) \equiv q(x)$	$p(x)$ e $q(x)$ são polinômios idênticos
$a \equiv b \pmod{m}$	a e b são congruentes módulo m
$\varphi(m)$	função de Euler aplicada a m
$\mu(m)$	função de Möbius aplicada a m
$\triangleq$	por definição
$(G, *)$	grupo composto do conjunto G e da operação $*$
$o(G)$	ordem do grupo G
$M_{n \times m}(X)$	conjunto das matrizes $n \times m$ com entradas em X
$H < G$	H é um subgrupo do grupo G
$\langle a \rangle$	subgrupo gerado por a
$o(a)$	ordem de um elemento a
$m \mid n$	m divide n em $\mathbb{Z}$
$m \nmid n$	m não divide n em $\mathbb{Z}$
$A \simeq B$	A e B são grupos, anéis ou corpos isomorfos
$\ker(f)$	núcleo do homomorfismo f
f^{-1}	função inversa da função f
aH	classe lateral à esquerda de H

A/B	conjunto quociente de A (grupo, anel, corpo) por B (subgrupo, ideal, subcorpo)
$[A : B]$	índice de A sobre o subgrupo B (para grupos) ou grau do corpo A sobre o corpo B
$(G : H)$	índice de um subgrupo H em um grupo multiplicativo G
$N \triangleleft G$	N é um subgrupo normal de G
$G \times H$	produto direto externo de G e H
GH	produto direto interno de G e H
$(A, +, \cdot)$	anel composto do conjunto A e das operações $+$ e $\cdot$
$A[x]$	anel de polinômios sobre A com variável x
$\mathbb{K}^*$	$= \mathbb{K} - \{0\}$ quando $\mathbb{K}$ é um corpo
$\mathbb{KL}$	corpo composto dos corpos $\mathbb{K}$ e $\mathbb{L}$
$\text{car}(A)$	cardinalidade do anel A
$\mathbb{Z}_m$	conjunto das classes residuais módulo m
$\mathbb{Z}/\mathbb{Z}_m$	idem
$\mathbb{Z}_m^*$	subconjunto de $\mathbb{Z}_m$ cujos elementos são relativamente primos com m
ζ_n	raiz n -ésima da unidade
$A[S]$	menor anel que contém o anel A e seu subconjunto S
$A(S)$	menor corpo que contém o anel A e seu subconjunto S
$f'(x)$	derivada do polinômio $f(x)$
$Df(x)$	idem
$\text{Aut}(\mathbb{L})$	automorfismos de $\mathbb{L}$
$\text{Gal}(\mathbb{L} : \mathbb{K})$	grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$
id	aplicação identidade
$\mathbb{L}_H$	corpo fixo de H em $\mathbb{L}$
$\prod_{i \in I} M_i$	produto cartesiano de M_i (módulos) num conjunto I
$\bigoplus'_{i \in I} M_i$	soma direta externa de módulos
$\bigoplus_{i \in I} M_i$	soma direta interna de módulos
$A^{(I)}$	conjunto de todas as famílias quase nulas em $\prod_{i \in I} A$
$\text{rank}(M)$	posto ou rank do A -módulo M
$\text{rk}_A(M)$	idem
$T(G)$	subgrupo de torção do grupo G
$A[G]$	anel de grupo de G sobre A
$\text{sup}(\alpha)$	suporte de α em $A[G]$

$\det(u)$	determinante do endomorfismo ou da matriz u
$P_u(x)$	polinômio característico do endomorfismo u
m_x	aplicação multiplicação por x
$Tr_{B:A}(x)$	traço de $x \in B$ sobre A
$N_{B:A}(x)$	norma de $x \in B$ sobre A
$P_x(t)$	polinômio característico de x
$D_{B:A}(x_1, \dots, x_n)$	discriminante de $(x_1, \dots, x_n) \in B^n$ sobre A
$\mathfrak{D}_{B:A}$	ideal discriminante de B sobre A
$D_{\mathbb{L}:\mathbb{K}}(u)$	discriminante de $u \in \mathbb{L}$ sobre $\mathbb{K}$
δ_{ij}	delta de Kronecker
IJ	produto de ideais integrais ou de ideais fracionários
IE	produto de um A -módulo E por um ideal I de A
$\mathcal{O}_{\mathbb{K}}$	anel de inteiros de $\mathbb{K}$
$D(\mathbb{K} : \mathbb{Q})$	discriminante do corpo de números $\mathbb{K}$
$D(\mathbb{K})$	idem
$N(I)$	norma do ideal I
$\delta_{\mathbb{L}:\mathbb{K}}$	discriminante relativo de $\mathbb{L}$ sobre $\mathbb{K}$
$Tr_{B:A}(J)$	traço relativo do ideal J de B sobre A
$N_{B:A}(J)$	norma relativa do ideal J de B sobre A
$\mathfrak{d}_{B:A}$	diferente de B sobre A
$\Phi_N(x)$	n -ésimo polinômio ciclotômico
$\mathbb{Q}(\zeta_n)^+$	n -ésimo subcorpo ciclotômico maximal real
$\mathbb{Q}^{(n)}$	n -ésimo corpo ciclotômico
$A[G]\alpha$	veja 4.1
χ	caractere
χ_0	caractere trivial
$\bar{\chi}$	caractere conjugado
$\widehat{G}$	conjunto dos caracteres de G
$\mathbb{C}^\times$	$= \mathbb{C} - \{0\}$
$\iota_a(\chi)$	veja 5.35
$\langle f, g \rangle$	produto interno de f por g
S_a	operador de mudança

S_f	veja 5.53
M_χ	conjunto dos definidores modulares de χ
f_χ	condutor de χ
$X^{(n)}$	conjunto dos caracteres de Dirichlet módulo n
$v_q(m)$	maior potência de q que divide m
$\tau_i(\chi)$	i -ésima soma de Gauss
$\tau(\chi)$	soma de Gauss (primitiva)
$\Omega^{(n)}$	grupo de caracteres de Dirichlet de primeiro tipo módulo n
$\Psi^{(n)}$	grupo de caracteres de Dirichlet de segundo tipo módulo n
$\mathcal{D}(n)$	veja 6.1.1
$q(n)$	função parte potente de n
Φ_d	classe de ramo d em X
ϵ_χ	idempotente ortogonal em $\mathbb{C}[G]$ associado a χ
$y_{\mathbb{K}}(\chi a)$	caractere coordenado de Leopoldt nos parâmetros $\mathbb{K}$, χ e a
$\mathbb{Q}(\chi)$	menor corpo que contém $\mathbb{Q}$ e as imagens de χ
$\mathbb{K}_d$	veja 6.64
η_d	veja 6.64
$[x]$	parte inteira de $x \in \mathbb{R}$
$vol(\Lambda)$	volume do reticulado Λ
$det(\Lambda)$	determinante do reticulado Λ
$\Delta(\Lambda)$	densidade de empacotamento do reticulado Λ
$\delta(\Lambda)$	densidade de centro do reticulado Λ
r_1	número de monomorfismos reais de um corpo de números $\mathbb{K}$
r_2	metade do número de monomorfismos complexos de um corpo de números $\mathbb{K}$
$re(z)$	parte real do complexo z
$im(z)$	parte imaginária do complexo z

Sumário

Introdução	21	
1	CONCEITOS PRELIMINARES DE ÁLGEBRA	25
1.1	Pré-requisitos e notações básicas	25
1.2	Classes residuais e grupos abelianos finitos	30
1.3	Álgebras, ordens e anéis de grupo	37
2	TEORIA ALGÉBRICA DOS NÚMEROS	43
2.1	Elementos integrais e algébricos	43
2.2	Norma e traço	48
2.3	Discriminante	52
2.4	Anéis Noetherianos e Domínios de Dedekind	57
2.5	Corpos de números e anéis de inteiros	65
2.6	Ramificação de ideais primos	71
2.7	Traço relativo, norma relativa e o diferente	76
3	CORPOS QUADRÁTICOS E CICLOTÔMICOS	83
3.1	Corpos quadráticos	83
3.2	Corpos ciclotômicos	86
3.3	Subcorpos ciclotômicos	96
4	BASES INTEGRAIS NORMAIS E POTENTES	109
4.1	Bases normais e bases potentes	109
4.2	Bases integrais normais	112
4.3	Bases integrais potentes	118
5	CARACTERES	123
5.1	Caracteres de grupos abelianos finitos	123

5.2	Caracteres de $\mathbb{Z}_n^*$	131
5.3	Relações de ortogonalidade entre caracteres	132
5.4	Caracteres de Dirichlet	136
5.5	Condutores dos caracteres de Dirichlet	143
5.6	Soma de Gauss	146
6	ANÉIS DE INTEIROS DE CORPOS DE NÚMEROS ABELIANOS	151
6.1	Classes de ramos	151
6.2	Caracteres coordenados de Leopoldt	159
6.3	Teorema de Leopoldt-Lettl	167
7	RETICULADOS ALGÉBRICOS	181
7.1	Reticulados	181
7.2	Empacotamento no $\mathbb{R}^n$	187
7.3	Reticulados algébricos	192
7.4	Construção de reticulados algébricos	199
	Conclusão	205
	Referências	209
	Índice	213

Introdução

Uma das áreas mais clássicas, belas e fascinantes da Matemática é a Teoria dos Números. Desde os tempos babilônicos há referências de estudos nessa área envolvendo equações e números naturais. A escola pitagórica grega, Diofanto de Alexandria, matemáticos hindus, o árabe Al-Khowarizmi, o italiano Cardano, entre outros, foram estudiosos que alimentaram a Teoria dos Números durante os séculos. Porém, esta teoria ganhou mais destaque no século XVII com Pierre de Fermat, quando este afirmou que o polinômio $p(x, y, z) = x^n + y^n - z^n$ não tem solução com coordenadas *inteiras* não trivial para naturais $n \geq 3$. Fermat afirmou que isso era fato, mas não provou, justificando que a margem do papel onde ele escreveu era pequena demais para conter a demonstração. Ao longo do tempo, matemáticos gastaram suas forças tentando provar este resultado, que é conhecido como Último Teorema de Fermat.

Com o passar dos anos, novos problemas em Teoria dos Números foram surgindo, novas teorias foram desenvolvidas e muitas falsas provas do Último Teorema de Fermat foram sendo relatadas. Com o desenvolvimento da Teoria Algébrica dos Números a partir dos conceitos de números algébricos e de inteiros algébricos, os estudos de Gauss, Lamé, Liouville, Kummer e Dedekind abriram novas portas à pesquisa em Matemática e permitiram avanços à Teoria dos Números e também a outras áreas, como Teoria de Grupos, Geometria Algébrica, Topologia e Análise. Finalmente, em 1995, o matemático britânico Andrew Wiles concluiu uma demonstração do Último Teorema de Fermat utilizando funções elípticas, formas modulares e representações de Galois.

A Teoria Algébrica dos Números nasceu do estudo dos inteiros algébricos, que são os números complexos que solucionam alguma equação

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

em que $a_i \in \mathbb{Z}$, $0 \leq i \leq n - 1$, para algum n inteiro positivo. Conforme estudaremos, os inteiros algébricos de um corpo $\mathbb{K}$ de extensão finita sobre $\mathbb{Q}$ (corpo de números) formam um anel chamado

anel de inteiros do corpo $\mathbb{K}$.

É interessante o fato de que a Teoria dos Números se desenvolveu ao longo dos anos pelo simples fato de ser bela e desafiadora. Antes, assim como a própria Álgebra, essa área não possuía aplicações diretas à engenharia, à indústria ou a outros ramos da Matemática Aplicada. Porém, essa história mudou desde a publicação do artigo *A Mathematical Theory of Communication* em 1948 pelo norte-americano Claude Shannon. O referido artigo deu origem à Teoria da Informação, uma área de intersecção entre a Matemática e a Engenharia Elétrica na qual se objetiva garantir uma transmissão segura e eficiente de informações por meio dos canais de comunicação. Nasceu disso também a teoria dos Códigos Corretores de Erros, a qual analisa e propõe estruturas matemáticas e algoritmos capazes de detectar e corrigir erros numa transmissão de dados. Atualmente, a Álgebra, a Teoria dos Números clássica e a Teoria Algébrica dos Números são aplicadas à Teoria da Informação.

Um problema da Matemática Aplicada enfrentado por vários pesquisadores hoje em dia é o do empacotamento esférico. Tal problema consiste em buscar uma maneira de preencher o espaço $\mathbb{R}^n$ com esferas maciças idênticas, de mesmo raio, de modo que duas esferas ou não se interceptem ou se tangenciem em apenas um ponto e de modo que o preenchimento por esferas de $\mathbb{R}^n$ ocupe o maior espaço possível. Soluções desse problema são úteis à Teoria dos Códigos Corretores de Erros. De fato, suponha que os centros das esferas que cobrem o espaço n -dimensional sejam palavras de um código. Dessa forma, erros na transmissão de uma mensagem podem fazer com que tais palavras se modifiquem e sejam enviadas a outros vetores do espaço. Se o vetor modificado estiver em uma das esferas que cobrem o espaço, podemos bem aproximá-lo pelo centro dessa esfera. Caso contrário, é menos provável conseguir uma “correção correta” desse vetor.

O problema do empacotamento esférico é bem solucionado em algumas dimensões quando supomos que os centros das esferas que cobrem o espaço devem formar uma estrutura algébrica chamada de *reticulado*. Reticulados são grupos discretos em $\mathbb{R}^n$ (definiremos esses conceitos no texto). Assim, pode-se cobrir o espaço com esferas centradas nos discretos pontos de um reticulado cujos raios não ultrapassem a metade da menor distância entre dois pontos quaisquer desse reticulado.

Nesse ponto, quando a Teoria Algébrica dos Números e o problema do empacotamento esférico reticulado conversam, surge uma nova linha de pesquisa. O conhecido homomorfismo de Minkowski faz essa ligação. Tal função leva um $\mathbb{Z}$ -módulo do anel de inteiros de um corpo de números de dimensão n sobre $\mathbb{Q}$ em um reticulado no espaço $\mathbb{R}^n$. Concebido dessa forma, um reticulado Λ é chamado de *reticulado algébrico*. Se Λ é um reticulado algébrico produzido por um ideal I no anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de um corpo de números $\mathbb{K}$ totalmente real ou totalmente imaginário, a densidade

de centro do empacotamento esférico desse reticulado (conceito relacionado ao de densidade do preenchimento do espaço por esferas) em relação ao espaço $\mathbb{R}^n$ é dado pela fórmula

$$\delta = \frac{t_I^{n/2}}{2^n \sqrt{|D(\mathbb{K})|} N(I)}$$

em que t_I é uma forma quadrática (que definiremos quando for conveniente), $N(I)$ é a norma do ideal e $D(\mathbb{K})$ é o discriminante do corpo de números.

Como pode ser notado, o conhecimento do anel de inteiros do corpo de números $\mathbb{K}$ é importante para construir um reticulado via o homomorfismo de Minkowski e para calcular sua densidade de centro. Nesse sentido, o presente trabalho tem por objetivo estudar os anéis de inteiros de alguns tipos de corpos de números, sem perder de vista as aplicações desses estudos à teoria de reticulados e à Teoria da Informação. Para cumprir esse objetivo, organizamos este trabalho em sete capítulos. Os dois primeiros apresentam alguns pré-requisitos para a compreensão do trabalho. Os capítulos 3, 4 e 6 estudam propriamente os anéis de inteiros de alguns corpos de números. O capítulo 5 é necessário para a compreensão do capítulo 6. O último capítulo aplica os conceitos estudados nos capítulos anteriores aos reticulados. Detalharemos cada um dos capítulos a seguir.

Inicialmente, o primeiro capítulo trata de alguns pré-requisitos para a compreensão do texto e de conceitos relacionados ao estudo de Álgebra. Por sua vez, o segundo capítulo apresenta a Teoria Algébrica dos Números e seus conceitos básicos. Leitores que já tiveram um primeiro curso de Teoria Algébrica dos Números notarão que podem evitar a leitura de algumas seções do segundo capítulo.

No terceiro capítulo, estudamos os corpos quadráticos, os corpos ciclotômicos e seus respectivos anéis de inteiros. Anéis de inteiros desses corpos são mais conhecidos, pois são estudados em primeiros cursos de Teoria Algébrica dos Números. Na terceira seção deste capítulo demonstramos qual é o anel de inteiros do subcorpo maximal real de um corpo ciclotômico e apresentamos o anel de inteiros do subcorpo ciclotômico gerado pelo período de Gauss em dois casos.

O interessante a notar no terceiro capítulo é que todos os anéis de inteiros apresentados são monogênicos, isto é, têm base de potências gerada por um elemento α . Ver que isso nem sempre ocorre é um dos objetivos do quarto capítulo, o qual estuda bases potentes e normais de corpos de números e $\mathbb{Z}$ -bases potentes e normais dos respectivos anéis de inteiros. Provaremos que todo corpo de números possui base potente, mas que nem todo anel de inteiros possui $\mathbb{Z}$ -base potente. Além disso, veremos que toda extensão finita galoisiana admite base normal e conheceremos o Teorema de Hilbert-Speiser, o qual nos dará uma condição necessária e suficiente para que um anel de inteiros possua uma $\mathbb{Z}$ -base normal.

O quinto capítulo trata de caracteres de um grupo abeliano finito. Os tópicos estudados nesse capítulo são de extrema importância para a compreensão do sexto capítulo e são úteis a outras linhas de pesquisa em Teoria Algébrica dos Números. Conheceremos o que são caracteres de Dirichlet, definiremos e estudaremos seus condutores, apresentaremos a soma de Gauss e veremos que há relações de ortogonalidade envolvendo caracteres de um mesmo grupo.

O sexto capítulo é o principal desta dissertação. Nele, generalizamos o Teorema de Hilbert-Speiser ao dar uma expressão para o anel de inteiros de qualquer corpo de números *abeliano*, segundo a teoria desenvolvida por Günter Lettl em 1990, a qual complementa um teorema provado por Leopoldt em 1959. A expressão do anel de inteiros de qualquer corpo de números abeliano como soma direta de $\mathbb{Z}$ -módulos é dada no resultado central desta dissertação, o Teorema de Leopoldt-Lettl. O objetivo do sexto capítulo é demonstrar esse teorema. Para isso, definimos e utilizamos vários conceitos, como o de classes de ramos e o de caracteres coordenados de Dirichlet, tratados nas duas primeiras seções.

De posse de várias classes de anéis de inteiros de corpos de números, o sétimo capítulo visa aplicar a teoria desenvolvida nos seis primeiros capítulos desta dissertação à teoria de reticulados. Nesse capítulo, tratamos sobre reticulados, empacotamento esférico, reticulados algébricos e terminamos dando exemplos de reticulados algébricos com densidade de centro ótima produzidos por anéis de inteiros de corpos de números via o homomorfismo de Minkowski nas dimensões 2, 4, 6 e 8.

Esta dissertação resultou principalmente do estudo detalhado dos artigos [32] e [20]. Nisso, o objetivo foi detalhar de maneira minuciosa cada uma das linhas que compunha tais artigos, de modo a compreendê-los ao máximo. O estudo do artigo [32] foi relatado nas seções 3.3 e 4.3. Por sua vez, o capítulo 6 resultou do detalhamento do artigo [20].

Enfim, esta dissertação envolve conceitos de todas as grandes áreas da Matemática. Podem ser notados tópicos relacionados à Álgebra (majoritária no texto), à Topologia, à Análise Matemática e à Matemática Aplicada. Com isso, esperamos propiciar ao leitor uma compreensão de que há interessantes conexões entre elas e que tópicos tradicionalmente teóricos podem ser aplicados às engenharias e a outros ramos que dependem da Matemática.

Desejamos a todos uma boa leitura!

Capítulo 1

Conceitos preliminares de Álgebra

Neste capítulo apresentaremos definições e resultados sobre Álgebra que serão úteis no decorrer desta dissertação. Inicialmente, na primeira seção mencionaremos pré-requisitos que suporemos conhecidos pelo leitor desta dissertação e estabeleceremos algumas notações envolvendo conjuntos, aplicações, polinômios, matrizes, Teoria dos Números básica, grupos, anéis, corpos, Teoria de Galois e módulos. Nas outras seções, estudaremos alguns conceitos e resultados envolvendo classes residuais módulo m , grupos abelianos finitos, álgebra, ordens e anéis de grupo.

1.1 Pré-requisitos e notações básicas

Em todo este trabalho, iremos supor conhecidas pelo leitor as noções e notações básicas de teoria dos conjuntos e de lógica matemática. Por exemplo, adotaremos de maneira usual as notações $\in$, $\subset$, $\cup$, $\cap$, $\forall$, $\exists$, entre outras. Ressaltamos que o símbolo ∞ representa o “infinito”, ou uma quantidade infinita de elementos. A notação utilizada para denotar a cardinalidade de um conjunto A será $\#(A)$. O conjunto vazio será representado por $\emptyset$ ou por $\{\}$. A diferença entre dois conjuntos A e B será denotada usualmente por $A - B$. Os conjuntos dos números inteiros, racionais, reais e complexos serão denotados usualmente por $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, respectivamente. Vale ressaltar que os naturais serão considerados como sendo o conjunto $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, a menos de menção contrária extraindo o zero. Para todos esses conjuntos $\mathbb{A}$ especificamente mencionados, a notação $\mathbb{A}^*$ representará $\mathbb{A} - \{0\}$. Será frequente a utilização do Princípio da Boa Ordem, ou Princípio do Menor Inteiro, o qual nos garante que todo subconjunto de $\mathbb{N}$ não vazio possui um menor elemento.

Admitiremos que o leitor conheça noções gerais de relações e aplicações. Se A e B são dois conjuntos, $f : A \longrightarrow B$ denota uma aplicação entre eles, enquanto a notação $a \longmapsto b$ denota a

aplicação de um elemento de A em um elemento de B pela aplicação mencionada. A notação $Im(f)$ denota a imagem de uma função f . As noções de injetividade, sobrejetividade, bijetividade, função composta e função inversa devem ser conhecidas.

Será admitido também o conhecimento de noções básicas sobre ordem entre elementos, conjuntos parcialmente ordenados e conjuntos ordenados. Dessa temática, utilizaremos o seguinte resultado, conhecido como Lema de Zorn:

Lema 1.1.1 ([18], capítulo zero. Lema de Zorn). *Seja X um conjunto não vazio e parcialmente ordenado. Se todo subconjunto $S \subset X$ totalmente ordenado possui uma cota superior então X tem um elemento maximal.*

Para uma leitura inicial sobre conjuntos, relações e aplicações, recomendamos os primeiros capítulos de [6]. Para um conhecimento mais geral sobre a Teoria de Conjuntos e das noções de ordem acima mencionadas, sugerimos a leitura do capítulo zero de [18].

Neste texto, iremos supor que o leitor conheça a teoria básica de polinômios: definição de polinômio, identidade de polinômios, grau de polinômio, operações (soma, subtração, multiplicação e divisão) de polinômios, algoritmo da divisão euclidiana para polinômios, raízes de polinômios, irreducibilidade de polinômios, Critério de Eisenstein e outros critérios de irreducibilidade, entre outros. Em termos de nomenclatura, será comum usarmos a notação $f(x)$ para um polinômio $f : A \longrightarrow B$ ao invés de apenas f . Nesse caso, fique claro que $f(x) \in A[x]$, sendo x a indeterminada sobre A . Denotaremos grau de um polinômio $f(x)$ por $\partial(f)$. Sobre a teoria básica de polinômios, recomendamos a leitura do capítulo VI de [6].

A teoria de matrizes, determinantes e sistemas lineares também deve ser conhecida para um bom entendimento deste texto. O conjunto das matrizes $m \times n$ (m linhas por n colunas) com entradas em um conjunto X (munido com operações de soma e multiplicação) será denotado por $M_{m \times n}(X)$. Se $m = n$, podemos simplesmente denotar tal conjunto por $M_n(X)$. O determinante de uma matriz A será denotado por $\det(A)$. A matriz transposta e a matriz inversa (caso exista) de A serão denotadas, respectivamente, por A^T e por A^{-1} .

É recomendável ainda que o leitor conheça aspectos básicos da Teoria dos Números. Sugerimos que o leitor esteja familiarizado com as noções de máximo divisor comum (mdc), mínimo múltiplo comum (mmc), divisão euclidiana, números primos, números relativamente primos, divisibilidade entre inteiros, congruência modular entre inteiros módulo m , função de Euler, entre outras. Uma definição que utilizaremos é a da função de Möbius: se $n = \prod_{j=1}^r p_j^{a_j}$ é a fatoração de n em primos,

então a função μ de Möbius é dada por

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1 \\ (-1)^r, & \text{se } a_j = 1 \text{ para todo } j \\ 0, & \text{se } a_j > 1 \text{ para algum } j \end{cases} \quad (1.1)$$

Será frequente mencionarmos no texto o Algoritmo da Divisão Euclidiana entre inteiros, que é um resultado que nos permite afirmar que, para quaisquer $a, b \in \mathbb{Z}$, existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$, em que $0 \leq r < b$. Se $r = 0$, dizemos que b divide a e denotamos esse fato por $b \mid a$. Dizemos que dois números a e x são congruentes módulo m , e denotamos por $a \equiv x \pmod{m}$, se $m \mid a - x$. Chamaremos de Identidade de Bezout ao resultado que afirma que $\text{mdc}(a, b) = 1$ (ou seja, dois inteiros a e b são relativamente primos) se, e somente se, existem inteiros x e y tais que $ax + by = 1$. Outro teorema que o leitor deve ter conhecimento é o Teorema Fundamental da Aritmética, o qual afirma que todo número natural maior do que 1 é escrito de maneira única como produto de números primos, a menos da ordem dos fatores. Recomendamos ainda o conhecimento do Teorema de Euler, que afirma que $a^{\varphi(m)} \equiv 1 \pmod{m}$, em que $\text{mdc}(a, m) = 1$ e φ denota a função de Euler. Ademais, será algumas vezes citado o conhecido Teorema Chinês do Resto. Para uma introdução à Teoria dos Números, sugerimos a leitura de [31].

Admitiremos conhecidas algumas noções de espaço métrico, análise real, análise no $\mathbb{R}^n$ e Teoria da Medida, tais como a desigualdade de Cauchy-Schwarz, a medida de Lebesgue, o Teorema da Mudança de Variáveis para integrais, entre outros. Porém, o conhecimento de tais requisitos será poucas vezes necessário no decorrer deste texto.

Em relação à Álgebra, assumiremos que o leitor conheça a teoria básica de grupos, anéis, corpos e módulos.

Sobre a Teoria de Grupos, o leitor deve ter familiaridade com as noções de grupo, subgrupo, ordem de grupo (que denotaremos por $o(G)$), potência, grupo cíclico, grupo abeliano, conjunto gerador, classe lateral, conjunto quociente, subgrupo normal, grupo quociente, índice de um subgrupo H em um grupo G (denotado por $[G : H]$), Teorema de Lagrange, produto direto interno, produto direto externo, entre outros. Em alguns trechos deste texto, iremos supor ainda conhecidas as noções de p -grupo, p -subgrupo e p -subgrupo de Sylow. Para saber mais sobre grupos, recomendamos a leitura do capítulo IV de [6] (básico), dos capítulos I e II de [15] ou de [29] (avanzado).

Sobre a Teoria de Anéis, admitiremos conhecidos os conceitos e resultados básicos envolvendo anel, subanel, anel de polinômios e característica de um anel. Ressaltamos que um anel A é chamado anel de integridade se é comutativo com unidade e se, para todo $a, b \in A$, $a.b = 0$ implica $a = 0$ ou

$b = 0$. Várias vezes chamaremos um anel de integridade de domínio de integridade, ou simplesmente de domínio. Além disso, o leitor deve saber sobre ideal, ideal gerado, ideal principal, domínio principal, ideal primo, ideal maximal, anel quociente, elemento associado, elemento irredutível, elemento primo, domínio de fatoração única (DFU), domínio euclidiano (DE), máximo divisor comum, mínimo múltiplo comum, lema de Euclides, entre outros. Lembramos que todo DE é domínio principal e que todo domínio principal é DFU. Para saber mais da teoria básica de anéis, recomendamos a leitura dos capítulos V, VI e VII de [6].

Sobre a Teoria de Corpos e sobre extensões de corpos, suporemos conhecidas as noções e resultados básicos envolvendo corpo, subcorpo, corpo de frações, extensão, extensão finita (o grau de uma extensão finita $\mathbb{K} \subset \mathbb{L}$ será denotado por $[\mathbb{L} : \mathbb{K}]$), elemento algébrico, polinômio minimal, extensão algébrica, corpo de raízes (ou corpo de decomposição), corpo algebricamente fechado, fecho algébrico, elementos conjugados, polinômio separável, extensão separável, extensão normal, corpo composto, entre outros. Destacamos o enunciado do Teorema do Elemento Primitivo, que será importante no decorrer do trabalho:

Proposição 1.1.1 ([15], capítulo V, proposição 6.15.). *Seja $\mathbb{L}$ uma extensão finita e separável de $\mathbb{K}$. Então existe $u \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(u)$. Um elemento u que satisfaz $\mathbb{L} = \mathbb{K}(u)$ é chamado elemento primitivo.*

Para cada uma das estruturas algébricas comentadas anteriormente (grupos, anéis e corpos), é possível definir o conceito de homomorfismo, o qual também suporemos conhecido, bem como o Teorema do Homomorfismo de cada uma delas. Porém, a seguir, vamos formalizar alguns termos. Seja f um homomorfismo. Se f é uma aplicação injetora, então f é chamado homomorfismo injetor ou monomorfismo. Se f é uma aplicação sobrejetora, dizemos que f é um homomorfismo sobrejetor ou epimorfismo. No caso de f ser bijetora, dizemos que f é um isomorfismo. Se existir um isomorfismo $f : G \longrightarrow J$ dizemos que G e J são grupos isomorfos e denotamos essa relação por $G \simeq J$. Se um homomorfismo tem como domínio e contradomínio o mesmo grupo, então ele é chamado de endomorfismo. Se f for um isomorfismo e um endomorfismo dizemos que f é um automorfismo. O núcleo, ou kernel, do homomorfismo f será denotado por $\ker(f)$.

Sejam $\mathbb{K} \subset \mathbb{L}$ e $\mathbb{K} \subset \mathbb{M}$ extensões de corpos. Um homomorfismo (monomorfismo, isomorfismo) $\sigma : \mathbb{L} \longrightarrow \mathbb{M}$ será chamado $\mathbb{K}$ -homomorfismo ($\mathbb{K}$ -monomorfismo, $\mathbb{K}$ -isomorfismo, respectivamente) se $\sigma(a) = a$, para todo $a \in \mathbb{K}$. Por sua vez, um automorfismo $\sigma : \mathbb{L} \longrightarrow \mathbb{L}$ é chamado $\mathbb{K}$ -automorfismo de $\mathbb{L}$ se $\sigma(a) = a$, para todo $a \in \mathbb{K}$.

Ainda sobre corpos, esperamos que o leitor já tenha tido um primeiro contato com a Teoria de Galois e com extensões galoisianas. Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão de corpos, denotaremos por $\text{Aut}(\mathbb{L})$ ao conjunto dos automorfismos de $\mathbb{L}$ e por $\text{Gal}(\mathbb{L} : \mathbb{K})$ ao grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$, que é o conjunto dos $\mathbb{K}$ -automorfismos de $\mathbb{L}$. Quando necessário, o corpo fixo de um grupo H em um corpo $\mathbb{L}$ será denotado por $\mathbb{L}_H$. Dessa teoria, o principal resultado é o Teorema Fundamental de Galois, enunciado a seguir:

Teorema 1.1.1 ([15], capítulo 5, teorema 2.5. Teorema Fundamental de Galois). *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana. Então existe uma correspondência biunívoca entre o conjunto de todos os corpos intermediários desta extensão e o conjunto de todos os subgrupos de $\text{Gal}(\mathbb{L} : \mathbb{K})$ dada pela bijeção $\mathbb{M} \mapsto \mathbb{M}' = \text{Aut}(\mathbb{L} : \mathbb{M})$. Além disso:*

$$(a) \ o(\text{Gal}(\mathbb{L} : \mathbb{K})) = [\mathbb{L} : \mathbb{K}].$$

(b) $\mathbb{L}$ é Galois sobre todo corpo intermediário $\mathbb{M}$, mas $\mathbb{M}$ é Galois sobre $\mathbb{K}$ se, e somente se, o correspondente subgrupo $\mathbb{M}' = \text{Aut}(\mathbb{L} : \mathbb{M})$ é normal em $G = \text{Gal}(\mathbb{L} : \mathbb{K})$. Neste caso,

$$\frac{\text{Gal}(\mathbb{L} : \mathbb{K})}{\text{Gal}(\mathbb{L} : \mathbb{M})} \simeq \text{Gal}(\mathbb{M} : \mathbb{K}). \quad (1.2)$$

Para saber mais sobre corpos e extensões de corpos, recomendamos a leitura de [8] ou dos capítulos V e VII de [15].

Suporemos que os conceitos de Álgebra Linear são bem conhecidos pelo leitor. Assim, por exemplo, admitiremos conhecidas as noções de espaço vetorial, conjunto gerador, conjunto linearmente independente (LI), conjunto linearmente dependente (LD), transformação linear, produto interno, produto externo, entre outras, além dos resultados conhecidos em um primeiro curso de Álgebra Linear. Sobre esse assunto, recomendamos [14].

Sobre a Teoria de Módulos, também admitiremos que o leitor conheça noções e resultados básicos envolvendo módulo, submódulo, homomorfismo¹, produto direto, sequência quase nula, soma direta interna, soma direta externa, base, módulo livre, módulo finitamente gerado, posto, módulo sobre domínios principais, entre outros. O posto, ou rank, de um A -módulo M será denotado por $\text{rk}_A(M)$, por $\text{rank}_A(M)$ ou por $\text{rank}(M)$.

Os próximos resultados dão propriedades interessantes dos módulos sobre domínios principais:

Proposição 1.1.2 ([30], seção 1.5, teorema 1). *Sejam A um domínio principal, M um A -módulo livre de posto n e M' um submódulo de M . Então:*

¹ O comentário e as nomenclaturas feitos para homomorfismo de grupos, anéis e corpos também valem para homomorfismo de módulos.

- (a) M' é livre de rank $q \leq n$;
- (b) Se $M' \neq \{0\}$ então existe uma base $\{e_1, e_2, \dots, e_n\}$ de M e existem $a_1, a_2, \dots, a_q \in A$ tais que $\{a_1 e_1, a_2 e_2, \dots, a_q e_q\}$ é uma base de M' , com $a_i \mid a_{i+1}$ para todo $1 \leq i \leq q - 1$.

Corolário 1.1.1 ([30], seção 1.5, corolários 1 e 2). *Seja A um domínio principal.*

- (a) *Se M é um A -módulo finitamente gerado e $\{I_j\}_{1 \leq j \leq n}$ é um conjunto de ideais de A tais que $I_j \subset I_{j-1}$ ($2 \leq j \leq n$) então $M = (A/I_1) \times (A/I_2) \times \dots (A/I_n)$.*
- (b) *Todo submódulo de um A -módulo finitamente gerado é finitamente gerado.*

Se G é um grupo abeliano, podemos encarar G como $\mathbb{Z}$ -módulo. Nesses moldes, o teorema a seguir, conhecido como Teorema Fundamental dos Grupos Abelianos Finitamente Gerados, nos diz que todo grupo abeliano finitamente gerado pode ser decomposto (como soma direta) em uma parte finita (de torção) e uma parte livre.

Teorema 1.1.2 (Teorema Fundamental dos Grupos Abelianos Finitamente Gerados). *Seja $G \neq \{e\}$ um grupo abeliano finitamente gerado, em que e é o elemento neutro do grupo. Então:*

- (a) $G = M_1 \oplus \dots \oplus M_k \oplus K$, em que cada M_i é um subgrupo cíclico de G de ordem igual a uma potência de primo e K é um subgrupo livre de G .
- (b) $T(G) = M_1 \oplus \dots \oplus M_k$.

O teorema anterior não foi demonstrado, mas uma prova dele pode ser encontrada generalizada para módulos finitamente gerados sobre domínios principais nos teoremas 7.3, 7.5 e 7.7 de [22] ou no teorema 6.12 de [15]. Para saber mais sobre módulos, recomendamos [22], [15] ou [24].

1.2 Classes residuais e grupos abelianos finitos

Nesta seção, estudaremos as classes residuais módulo um inteiro m , o grupo aditivo formado por essas classes, o grupo multiplicativo formado pelas classes invertíveis e terminaremos citando (mas não demonstrando) a proposição que permite decompor grupos abelianos finitos em produto de grupos cíclicos, entre outros resultados.

Definição 1.2.1. *Seja m um inteiro positivo. Dois inteiros a e b são ditos **congruentes módulo m** se as divisões euclidianas de a e de b por m tiverem o mesmo resto. Neste caso, denotamos $a \equiv b \pmod{m}$.*

Equivalentemente, a e b são congruentes módulo m quando $m \mid a - b$. Como a relação de congruência módulo m é de equivalência, podemos considerar a classe residual de um inteiro a módulo m dada pelo conjunto $\bar{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\} = \{a + km : k \in \mathbb{Z}\}$. Como em toda divisão euclidiana com divisor m os únicos restos possíveis são os valores inteiros entre 0 e $m - 1$, então o conjunto das classes residuais módulo m tem m elementos. Denotaremos esse conjunto por $\mathbb{Z}_m$ ou por $\mathbb{Z}/\mathbb{Z}m$. Assim, $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$. Definimos duas operações sobre $\mathbb{Z}_m$: a soma de dois elementos $\bar{a}$ e $\bar{b}$ em $\mathbb{Z}$ é dada por $\bar{a} + \bar{b} = \overline{a + b}$, enquanto a multiplicação entre eles é dada por $\bar{a}\bar{b} = \overline{ab}$. Facilmente verifica-se que $(\mathbb{Z}_m, +)$ é um grupo cujo elemento neutro é $\bar{0}$. Nesse grupo, o elemento oposto de $\bar{a}$ é $\overline{m - a}$. Por sua vez, $\mathbb{Z}_m$ sobre a operação multiplicativa não é um grupo, pois nem todo elemento é invertível. Daí, vem a necessidade da proposição seguinte:

Proposição 1.2.1. *Um elemento $\bar{a} \in \mathbb{Z}_m$ é invertível (sobre a multiplicação) se, e somente se, $\text{mdc}(a, m) = 1$.*

Demonstração. Por um lado, seja $\bar{a} \in \mathbb{Z}_m$ um elemento invertível. Então, existe $\bar{b} \in \mathbb{Z}_m$ tal que $\bar{a}\bar{b} = \overline{ab} = \bar{1}$. Logo, $ab \equiv 1 \pmod{m}$, donde segue que $m \mid ab - 1$. Se existisse um primo p que dividisse m e a ao mesmo tempo, então p dividiria 1, o que é um absurdo. Logo, $\text{mdc}(m, a) = 1$. Por outro lado, se $\text{mdc}(a, m) = 1$, então a Identidade de Bezout nos garante que existem b e q tais que $ab + qm = 1$. Logo, $m \mid ab - 1$. Daí, $\bar{a}\bar{b} = \overline{ab} = \bar{1}$, ou seja, $\bar{a}$ é invertível. $\square$

O conjunto dos elementos invertíveis (sobre a multiplicação) de $\mathbb{Z}_m$ será denotado por $\mathbb{Z}_m^*$ ou por $(\mathbb{Z}/\mathbb{Z}m)^*$. Assim, a proposição anterior nos mostra que $\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m : \text{mdc}(a, m) = 1\}$. Dessa forma, verifica-se facilmente que $(\mathbb{Z}_m^*, \cdot)$ é um grupo. Em termos da teoria de anéis, claramente $\mathbb{Z}_m$ é um anel. Porém, esse conjunto nem sempre é um corpo. Por exemplo, $\mathbb{Z}_4$ não é um corpo, já que $\bar{2}$ não tem inverso multiplicativo. Para finalizar essa discussão, vem o resultado a seguir:

Proposição 1.2.2. *$\mathbb{Z}_p$ é um corpo se, e somente se, p é primo.*

Demonstração. Por um lado, se $\mathbb{Z}_p$ é um corpo, então $\mathbb{Z}_p - \{0\}$ é um grupo multiplicativo. Logo, $\text{mdc}(a, p) = 1$ para todo $1 \leq a < p$. Logo, não existe $a < p$ diferente de 1 que divida p . Portanto, p é primo. Por outro lado, se p é primo, então $\text{mdc}(a, p) = 1$ para todo $1 \leq a < p$. Daí, o conjunto dos elementos invertíveis de $\mathbb{Z}_p$ é $\{\bar{a} \in \mathbb{Z}_p : \text{mdc}(a, p) = 1\} = \mathbb{Z}_p - \{0\}$, ou seja, $\mathbb{Z}_p$ é um corpo. $\square$

Se p é primo então o corpo $\mathbb{Z}_p$ é um corpo finito (com p elementos) de característica p e pode ser denotado por $GF(p)$ ou por $\mathbb{F}_p$.

Definição 1.2.2. A aplicação $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ que associa cada número natural m ao número de elementos naturais menores que m que são primos com m é chamada **função de Euler**. Assim, $\varphi(m) = \#\{a \in \mathbb{N}^* : a < m \text{ e } \text{mdc}(a, m) = 1\}$.

Observação 1.2.1. O grupo multiplicativo $\mathbb{Z}_m^*$ tem $\varphi(m)$ elementos.

Proposição 1.2.3. Todo grupo cíclico com m elementos é isomorfo a $\mathbb{Z}_m$.

Demonstração. Seja G um grupo cíclico escrito aditivamente com m elementos cujo gerador é g . Considere $\theta : \mathbb{Z} \longrightarrow G$ definida por $\theta(n) = ng$, para todo $n \in \mathbb{Z}$. Essa aplicação é um homomorfismo sobrejetor de grupos. Além disso, $\theta(n) = 0$ se, e só se, $ng = 0$, se, e só se, $m \mid n$ (pois g tem ordem m). Logo, $\ker(\theta) = m\mathbb{Z}$. Portanto, o Teorema do Homomorfismo de Grupos garante que $G \simeq \mathbb{Z}/m\mathbb{Z}$. Por sua vez, a aplicação $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ dada por $\phi(n) = \bar{n}$, para todo $n \in \mathbb{Z}$, também é um homomorfismo sobrejetor de grupos aditivos. Como $\phi(n) = \bar{0}$ se, e só se, $\bar{n} = \bar{0}$ se, e só se, $m \mid n$, então $\ker(\phi) = m\mathbb{Z}$. Logo, o Teorema do Homomorfismo de Grupos garante que $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$. Por fim, como a relação $\simeq$ é transitiva, $\mathbb{Z}_m \simeq G$. $\square$

Proposição 1.2.4. Se a é um inteiro positivo, então $\bar{a}$ é gerador de $\mathbb{Z}_m^*$ se, e só se, $\text{mdc}(a, m) = 1$.

Demonstração. Por um lado, se $\bar{a}$ é um gerador de $\mathbb{Z}_m^*$ e $d = \text{mdc}(a, m)$ então $(m/d)a \equiv m(a/d) \equiv 0 \pmod{m}$. Como a tem ordem m então $m \mid m/d$. Logo, $d = 1$. Por outro lado, se $\text{mdc}(a, m) = 1$ e h é a ordem de $\bar{a}$ então $m \mid ha$, pois $ha \equiv 0 \pmod{m}$. Daí, $m \mid h$. Além disso, $m\bar{a} = \bar{0}$ implica que $h \mid m$. Portanto, $m = h$. $\square$

Proposição 1.2.5. Seja $m = \prod_{i=1}^r p_i^{e_i} > 1$, em que cada p_i é primo e $e_i > 0$, $1 \leq i \leq r$. Então existe um isomorfismo de anéis

$$\phi : \mathbb{Z}_m \longrightarrow \prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}. \quad (1.3)$$

Demonstração. Considere $\theta : \mathbb{Z} \longrightarrow \prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}$ definida por $\theta(n) = (v_1, v_2, \dots, v_r)$ para todo $n \in \mathbb{Z}$, em que v_i é a classe residual de n módulo $p_i^{e_i}$. Assim, θ é um homomorfismo de anéis com $\ker(\theta) = m\mathbb{Z}$, pois n é múltiplo de m se, e somente se, n é um múltiplo de todo $p_i^{e_i}$ ($1 \leq i \leq r$). Logo, a aplicação induzida $\phi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}$ é injetora. Como o número de elementos de $\prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}$ é $\prod_{i=1}^r p_i^{e_i} = m$, segue que ϕ é bijetora. Como $\mathbb{Z}_m \simeq \mathbb{Z}/m\mathbb{Z}$, então o resultado segue. $\square$

O seguinte corolário é conhecido como **Teorema Chinês do Resto**:

Corolário 1.2.1. Se $p_1, p_2, \dots, p_r$ são primos distintos, $e_1, e_2, \dots, e_r$ são inteiros positivos e $a_1, a_2, \dots, a_r$ são inteiros quaisquer, então existe $n \in \mathbb{Z}$ tal que $n \equiv a_i \pmod{p_i^{e_i}}$, para todo $1 \leq i \leq r$. Além disso, n é único módulo $\prod_{i=1}^r p_i^{e_i}$.

Demonstração. Seja v_i a classe residual de a_i módulo $p_i^{e_i}$. Devido ao isomorfismo estabelecido na proposição 1.2.5, existe único $v \in \mathbb{Z}$ tal que $\phi(v) = (v_1, v_2, \dots, v_r)$. Assim, n satisfaz as congruências $n \equiv a_i \pmod{p_i^{e_i}}$, para todo $1 \leq i \leq r$, se, e somente se, $n \equiv v \pmod{m}$, donde segue o resultado. $\square$

Como consequência da proposição 1.2.5, temos outros resultados envolvendo a função de Euler:

Proposição 1.2.6. Se $\text{mdc}(a, m) = 1$ então $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Demonstração. Como $\text{mdc}(a, m) = 1$ então $\bar{a} \in \mathbb{Z}_m^*$. Além disso, como $o(\mathbb{Z}_m^*) = \varphi(m)$, o Teorema de Lagrange nos permite afirmar que $\bar{a}^{\varphi(m)} = \bar{1}$, donde segue a congruência desejada. $\square$

Proposição 1.2.7. Se $m = \prod_{i=1}^r p_i^{e_i}$ é uma decomposição de m em produto de primos então

$$\mathbb{Z}_m^* \simeq \prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}^* \quad e \quad \varphi(m) = m \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right). \quad (1.4)$$

Demonstração. Considere o isomorfismo $\phi : \mathbb{Z}_m \longrightarrow \prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}$ da proposição 1.2.5. Sabe-se que um elemento de $\mathbb{Z}_m$ é invertível se, e somente se, seu correspondente em $\prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}$ for invertível, o que ocorre se, e somente se, cada componente desse correspondente em $\mathbb{Z}_{p_i^{e_i}}$ for invertível. Logo, $\mathbb{Z}_m^* \simeq \prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}^*$. Assim, $\varphi(m) = \prod_{i=1}^r \varphi(p_i^{e_i})$. Portanto, basta analisar o valor de $\varphi(p^e)$, em que p é primo e $e \geq 1$ é um inteiro. Para $1 \leq a \leq p^e$, temos que $\text{mdc}(a, p^e) = 1$ se, e somente se, a não é múltiplo de p . Então, por contagem, $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - 1/p)$, pois a cada p elementos no intervalo $1 \leq a \leq p^e$ existe um múltiplo de p (e existem p^{e-1} destes intervalos). Disso e da igualdade $\varphi(m) = \prod_{i=1}^r \varphi(p_i^{e_i})$, segue imediatamente o resultado. $\square$

Vamos agora estudar a estrutura de $\mathbb{Z}_m^*$. Devido à proposição 1.2.7, vimos que basta estudar $\mathbb{Z}_{p^e}^*$ (p primo, $e \geq 1$) para obter informações sobre $\mathbb{Z}_m^*$.

Lema 1.2.1. Sejam G um grupo multiplicativo e $x, y \in G$ tais que $xy = yx$, $o(x) = h$, $o(y) = k$ e $\text{mdc}(h, k) = 1$. Então $o(xy) = hk$.

Demonstração. Das propriedades de potência, $(xy)^{hk} = (x^h)^k (y^k)^h = e$ (identidade de G). Portanto, a ordem l de xy divide hk . Como $x^l y^l = (xy)^l = e$ então $a = x^l = y^{-l}$. A ordem de a deve dividir h , pois $a \in \langle x \rangle$, e deve dividir k , pois $a \in \langle y \rangle$. Devido ao fato de que $\text{mdc}(h, k) = 1$ segue que $o(a) = 1$. Portanto, $x^l = y^{-l} = e$, donde segue que $h \mid l$ e que $k \mid l$. Logo, $hk \mid l$. Assim, $l = hk$. $\square$

Primeiramente, trataremos de $\mathbb{Z}_p^*$, em que p é primo.

Proposição 1.2.8. *Se p é primo então o grupo multiplicativo $\mathbb{Z}_p^*$ é cíclico.*

Demonstração. Pela observação 1.2.1, $o(\mathbb{Z}_p^*) = \varphi(p) = p - 1$. Seja $\bar{a} \in \mathbb{Z}_p^*$ o elemento de maior ordem entre todos os elementos de $\mathbb{Z}_p^*$. Denotemos $o(\bar{a}) = h$. Pelo Teorema de Lagrange, $h \mid p - 1$, ou seja, $h \leq p - 1$. Seja agora $\bar{x} \in \mathbb{Z}_p^*$ um elemento qualquer, cuja ordem é r .

Então $r \mid h$. De fato, suponha que exista $\bar{y} \in \mathbb{Z}_p^*$ tal que $k = o(\bar{y})$ não divida h . Então existem um primo p e inteiros $n > m \geq 0$, h' e k' tais que $h = p^m h'$ ($\text{mdc}(p, h') = 1$) e $k = p^n k'$, pois algum primo de h não divide k em sua maior potência. Sejam $\bar{a}' = \bar{a}^{p^m}$ e $\bar{y}' = \bar{y}^{k'}$. Assim, $\bar{a}'$ tem ordem h' e $\bar{y}'$ tem ordem p^n . Pelo lema 1.2.1, $\bar{x}'\bar{y}' \in \mathbb{Z}_p^*$ tem ordem $p^n h' > p^m h' = h$, o que é um absurdo, pois a ordem máxima em $\mathbb{Z}_p^*$ é h .

Logo, como todo elemento de $\mathbb{Z}_p^*$ tem ordem dividindo h então $\bar{x}^h = \bar{1}$ para todo $\bar{x} \in \mathbb{Z}_p^*$. Portanto, todo elemento de $\mathbb{Z}_p^*$ é raiz do polinômio $x^h - 1 \in \mathbb{Z}_p^*[x]$, o qual tem no máximo h raízes. Logo, $p - 1 \leq h$. Portanto, $h = p - 1$. Logo, existe um elemento de $\mathbb{Z}_p^*$ cuja ordem é igual à do grupo, comprovando que o grupo é cíclico. $\square$

Agora, estudemos $\mathbb{Z}_{p^e}$, em que p é primo e $e \geq 1$, em dois casos: $p \neq 2$ e $p = 2$.

Proposição 1.2.9. *Se $p \neq 2$ e $e \geq 1$, então $\mathbb{Z}_{p^e}^*$ é um grupo cíclico e*

$$\mathbb{Z}_{p^e}^* \simeq \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}}. \quad (1.5)$$

Demonstração. Se $e = 1$, devido às proposições 1.2.3 e 1.2.8 tem-se que $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$, comprovando a tese. Por isso, podemos supor $e \geq 2$. Denotemos por $\bar{a}$ a classe residual de um inteiro a módulo p^e e por $\bar{\bar{a}}$ a classe residual de a módulo p . Considere $f : \mathbb{Z}_{p^e}^* \longrightarrow \mathbb{Z}_p^*$ a aplicação definida por $f(\bar{a}) = \bar{\bar{a}}$, a qual é um homomorfismo sobrejetor de grupos cujo núcleo é

$$C = \{\bar{a} \in \mathbb{Z}_{p^e}^* : a \equiv 1 \pmod{p}\}. \quad (1.6)$$

Devido ao Teorema do Homomorfismo de Grupos temos $\mathbb{Z}_{p^e}^*/C \simeq \mathbb{Z}_p^*$. Logo, C é um subgrupo de $\mathbb{Z}_{p^e}^*$ cuja ordem é $\varphi(p^e)/\varphi(p) = p^{e-1}$. Mostremos que C é um grupo cíclico com gerador $\overline{1+p}$. De fato, note primeiramente que $p+1 \in C$ e $o(p+1) \mid o(C) = p^{e-1}$. É suficiente mostrar que $(1+p)^{p^{e-2}} \not\equiv 1 \pmod{p^e}$. Para $e = 2$ isso é claramente verdade. Portanto, assumamos que essa equivalência é válida para $e-1$, ou seja, que $(1+p)^{p^{e-3}} \not\equiv 1 \pmod{p^{e-1}}$ e que $(1+p)^{p^{e-3}} \equiv 1 \pmod{p^{e-2}}$. Portanto, $(1+p)^{p^{e-3}} = 1 + rp^{e-2}$, em que p não divide r . Assim,

$$(1+p)^{p^{e-2}} = ((1+p)^{p^{e-3}})^p = (1 + rp^{e-2})^p = 1 + \binom{p}{1}rp^{e-2} + \dots + r^p p^{p(e-2)} = 1 + rp^{e-1} + sp^e. \quad (1.7)$$

Logo, $(1+p)^{p^{e-2}} \not\equiv 1 \pmod{p^e}$ e $(1+p)^{p^{e-2}} \equiv 1 \pmod{p^{e-1}}$.

Agora, seja $B = \{\bar{a} \in \mathbb{Z}_{p^e}^* : \bar{a}^{p-1} = \bar{1}\}$. Facilmente verifica-se que B é um subgrupo de $\mathbb{Z}_{p^e}^*$ e que $B \cap C = \{1\}$, pois, exceto o 1, B não tem elemento cuja ordem seja uma potência de p . Então $B \times C \simeq BC \subset \mathbb{Z}_{p^e}^*$. Logo, B tem ordem no máximo $\varphi(p^e)/p^{e-1} = p-1$.

Tem-se que $\bar{a}^{p^{e-1}} \in B$ para todo $\bar{a} \in \mathbb{Z}_{p^e}^*$. Como $f(\bar{a}^{p^{e-1}}) = \bar{a}^{p^{e-1}} = \bar{a}$ então pertencem a B todos os elementos (distintos) $\bar{1}^{p^{e-1}}, \bar{2}^{p^{e-1}}, \dots, \overline{p-1}^{p^{e-1}}$, já que todos são imagens distintas de f . Assim, B tem exatos $p-1$ elementos e podemos concluir que $\mathbb{Z}_{p^e}^* = BC \simeq B \times C$.

Verifiquemos que B é um grupo cíclico. De fato, seja b um número tal que o menor $n > 1$ satisfazendo $b^n \equiv 1 \pmod{p}$ seja $n = \varphi(p) = p-1$ (isto é, b é uma raiz primitiva módulo p). Então $b^{p^{e-1}}$ tem ordem d tal que $d \mid p-1$, pois o subgrupo $\langle b \rangle$ tem ordem $p-1$. Como $b^{p^{e-1}} \equiv b \pmod{p}$ então $b^d \equiv (b^d)^{p^{e-1}} \equiv 1 \pmod{p}$ e, daí, $p-1 \mid d$. Portanto, $d = p-1$. Assim, como $B \cap C = \{1\}$, B tem um elemento $\bar{b}$ de ordem $p-1$ e C tem um elemento $\overline{1+p}$, o lema 1.2.1 garante que $\overline{b(1+p)} \in \mathbb{Z}_{p^e}^*$ tem ordem $(p-1)p^{e-1} = \varphi(p^e)$, comprovando que $\mathbb{Z}_{p^e}^*$ é cíclico. Pela proposição 1.2.3, segue que $B \simeq \mathbb{Z}_{p-1}$ e que $C \simeq \mathbb{Z}_{p^{e-1}}$, comprovando que $\mathbb{Z}_{p^e}^* \simeq \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}}$. $\square$

Lema 1.2.2. Se $e \in \mathbb{Z}$, $e \geq 3$, e a é um número ímpar, então $a^{\varphi(2^e)/2} \equiv 1 \pmod{2^e}$.

Demonstração. Suponha $e = 3$ e $a = 2n+1$, pois a é ímpar. Assim, $a^2 = (2n+1)^2 = 4n(n+1) + 1$. Como $n(n+1)$ é par, $8 \mid 4n(n+1)$, donde segue que $a^2 \equiv 1 \pmod{8}$, que é a expressão desejada. Suponha, por indução, que valha $a^{\varphi(2^e)/2} = a^{2^{e-2}} \equiv 1 \pmod{2^e}$. Portanto, existe $m \in \mathbb{Z}$ tal que $a^{2^{e-2}} = 1 + m2^e$. Assim, $(a^{2^{e-2}})^2 = (1 + m2^e)^2 = 1 + m2^{e+1} + m^2 2^{2e}$. Portanto, $a^{2^{e-1}} = 1 + 2^{e+1}(m + m^2 2^{e-1})$, o que implica que $a^{2^{e-1}} \equiv 1 \pmod{2^{e+1}}$, como queríamos. $\square$

Proposição 1.2.10. O grupo multiplicativo $\mathbb{Z}_4^*$ é cíclico gerado por $\bar{3} = \overline{-1}$. Se $e \geq 3$, então $\mathbb{Z}_{2^e}^* \simeq \langle -1 \rangle \times \langle 5 \rangle$, sendo $5^{2^{e-1}} \equiv 1 \pmod{2^e}$. Consequentemente, $\mathbb{Z}_{2^e}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$ e $\mathbb{Z}_{2^e}^*$ não é um grupo cíclico.

Demonstração. Inicialmente, como $\mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}$ e $3^2 \equiv 1 \pmod{4}$ segue que esse grupo é gerado por $\bar{3}$. Suponha agora $e \geq 3$. Denotemos por $\bar{a}$ a classe residual de a módulo 2^e e por $\bar{\bar{a}}$ a classe residual de a módulo 4. Considere a aplicação $f : \mathbb{Z}_{2^e}^* \rightarrow \mathbb{Z}_4^*$ definida por $f(\bar{a}) = \bar{\bar{a}}$. A aplicação f está bem definida, é sobrejetora e é um homomorfismo multiplicativo de grupos. Seja $C \triangleq \ker(f) = \{\bar{a} \in \mathbb{Z}_{2^e}^* : a \equiv 1 \pmod{4}\}$. Sabemos que C é um subgrupo (normal) de $\mathbb{Z}_{2^e}^*$. Pelo Teorema do Homomorfismo de Grupos segue que $\mathbb{Z}_{2^e}^*/C \simeq \mathbb{Z}_4^*$. Logo, o número de elementos de C é $\phi(2^e)/\phi(4) = 2^{e-2}$.

Mostremos que C é um grupo cíclico gerado por $\bar{5}$. Para isso, note primeiramente que $5^{\phi(2^e)/2} \equiv 5^{2^{e-2}} \equiv 1 \pmod{2^e}$ (lema 1.2.2). Assim, para garantir que a ordem de 5 módulo 2^e é 2^{e-2} basta

mostrar que $5^{2^{e-3}} \not\equiv 1 \pmod{2^e}$. Isso ocorre, pois

$$5^{2^{e-3}} \equiv (1 + 2^2)^{2^{e-3}} \equiv 1 + 2^2 \cdot 2^{e-3} \equiv 1 + 2^{e-1} \pmod{2^e}. \quad (1.8)$$

Como 2^e não divide 2^{e-1} então $5^{2^{e-3}} \equiv 1 + 2^{e-1}$ não pode ser equivalente a 1 módulo 2^e .

Por fim, mostremos que $\mathbb{Z}_{2^e}^* \simeq \{1, -1\} \times C$. Com efeito, seja $\theta : \mathbb{Z}_{2^e}^* \longrightarrow \{1, -1\} \times C$ dada por $\theta(\bar{a}) = ((-1)^r, \bar{a}^*)$, em que

$$\bar{a}^* = \begin{cases} \bar{a} & \text{se } a \equiv 1 \pmod{4} \\ -\bar{a} & \text{se } a \equiv -1 \pmod{4} \end{cases} \quad (1.9)$$

e

$$r = \begin{cases} 0 & \text{se } a \equiv 1 \pmod{4} \\ 1 & \text{se } a \equiv -1 \pmod{4} \end{cases} \quad (1.10)$$

(note que não há outros possíveis valores para essa congruência módulo 4, já que os elementos a tais que $\bar{a} \in \mathbb{Z}_{2^e}^*$ são ímpares). Então $\bar{a} = (-1)^r \bar{a}^*$. Assim, vê-se que a aplicação ϕ está bem definida, é injetora e é um homomorfismo de grupos. Como $\mathbb{Z}_{2^e}^*$ e $\{1, -1\} \times C$ têm o mesmo número de elementos, θ é sobrejetora. Isso comprova que $\mathbb{Z}_{2^e}^*$ e $\{1, -1\} \times C$ são isomorfos. Como vimos que C é gerado por $\bar{5}$, então $\mathbb{Z}_{2^e}^* \simeq \langle -1 \rangle \times \langle \bar{5} \rangle$ e, pela proposição 1.2.3, $\mathbb{Z}_{2^e}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$. Para comprovar que $\mathbb{Z}_{2^e}^*$ não é cíclico, basta notar que a ordem de cada um de seus elementos divide 2^{e-2} . $\square$

Em suma, os valores inteiros m tais que $\mathbb{Z}_m^*$ é cíclico são sintetizados na proposição a seguir:

Proposição 1.2.11. $\mathbb{Z}_m^*$ é um grupo cíclico se, e somente se, $m = 2, 4, p^e, 2p^e$.

Demonstração. Por um lado, devido às proposições 1.2.8, 1.2.9 e 1.2.10, temos que $\mathbb{Z}_2^*$, $\mathbb{Z}_4^*$ e $\mathbb{Z}_{p^e}^*$ são cíclicos. Como $\mathbb{Z}_{2p^e}^* \simeq \mathbb{Z}_2^* \times \mathbb{Z}_{p^e}^* = \mathbb{Z}_{p^e}^*$, então $\mathbb{Z}_{2p^e}^*$ também é cíclico.

Por outro lado, note que $\mathbb{Z}_{p^e}^*$ tem ordem par, desde que $p \neq 2$ e $e \neq 1$. Assim, quando $m = \prod_{i=1}^r p_i^{e_i}$ é um produto de pelo menos dois primos p_i distintos, então a proposição 1.2.7 nos diz que $\mathbb{Z}_m^* \simeq \prod_{i=1}^r \mathbb{Z}_{p_i^{e_i}}^*$, e cada componente desse produto cartesiano tem ordem par se $p_i \neq 2$ e $e_i \neq 1$. Logo, para concluirmos que no caso em que m é um produto de pelo menos dois primos distintos tem-se $\mathbb{Z}_m^*$ não cíclico, basta mostrarmos que $G \times H$ não é cíclico quando G e H têm ordem par. De fato, suponha que $o(G) = 2r$ e $o(H) = 2s$. Logo, para todo $(x, y) \in G \times H$ tem-se $(x, y)^{2rs} = ((x^{2r})^s, (y^{2s})^r) = (1, 1)$, ou seja, não há elementos de $G \times H$ cuja ordem seja $o(G \times H) = (2r)(2s) = 4rs$. $\square$

Para finalizarmos a seção, apenas citamos o importante teorema sobre a decomposição de grupos abelianos finitos em produto cartesiano de grupos cíclicos:

Proposição 1.2.12 ([28], capítulo 3, teorema 3). *Todo grupo abeliano finito é isomorfo a um produto cartesiano de grupos cíclicos cujas ordens são potências de primos. Além disso, se $G \simeq G_1 \times \dots \times G_r \simeq H_1 \times \dots \times H_s$, em que cada G_i e H_i é um grupo cíclico cuja ordem é potência de um número primo, então $r = s$ e $G_i = H_i$, para todo $1 \leq i \leq r$, a menos da ordem dos G_i e dos H_i .*

1.3 Álgebras, ordens e anéis de grupo

Começaremos esta seção definindo o que é uma álgebra. Posteriormente, estudaremos os conceitos e alguns resultados básicos sobre ordens e anéis de grupo, os quais serão muito úteis no capítulo 6.

Definição 1.3.1. *Seja A um anel comutativo. Um A -módulo M é uma A -álgebra se:*

- (a) *existe uma operação de multiplicação definida em M de modo que M seja um anel com esta operação e com a sua operação aditiva;*
- (b) *$a(xy) = (ax)y = a(xy)$, para quaisquer $a \in A$ e $x, y \in M$.*

Exemplo 1.3.1. *Se A é um anel comutativo então o anel de polinômios $A[x]$ é uma A -álgebra com a soma e a multiplicação de polinômios definida de modo usual. Da mesma forma, o conjunto das matrizes quadradas definidas sobre A , $M_n(A)$, também é uma A -álgebra com as operações de soma e de multiplicação definidas usualmente para matrizes quadradas.*

Definição 1.3.2. *Se A é um anel comutativo e M é uma A -álgebra, dizemos que N é uma **subálgebra** de M se N for um submódulo de M e um subanel de M .*

Se M_1 e M_2 são A -álgebras, dizemos que uma aplicação $f : M_1 \longrightarrow M_2$ é um homomorfismo de A -álgebras se f for concomitantemente um homomorfismo de anéis e um homomorfismo de A -módulos.

Adiante, vamos definir de maneira geral o que é uma R -ordem em uma álgebra. Para o que segue, é necessário saber o conceito de domínio Noetheriano. Apesar de utilizado aqui, esse conceito será estudado na seção 2.4.

Definição 1.3.3. *Sejam R um domínio Noetheriano, $\mathbb{K}$ seu corpo de frações e V um espaço vetorial de dimensão finita sobre $\mathbb{K}$. Dizemos que um R -submódulo finitamente gerado M de V é um **R -reticulado completo** se $\mathbb{K}.M = V$, em que*

$$\mathbb{K}.M = \left\{ \sum_{FINITA} k_i m_i : k_i \in \mathbb{K}, m_i \in M \right\} \quad (1.11)$$

A expressão $\mathbb{K}.M = V$ é equivalente a dizer que M contém uma $\mathbb{K}$ -base de V . Um R -reticulado completo M é chamado **R -reticulado completo livre** se M é livre como R -módulo.

Lema 1.3.1. *Se M e N são R -reticulados completos em V então existe $r \in R$, $r \neq 0$, tal que $r.M \subset N$.*

Demonstração. Como N contém uma $\mathbb{K}$ -base para V , então para cada $x \in M$ existe $r_x \in R$, $r_x \neq 0$, tal que $r_x.x \in N$. Com efeito, como $x \in V = \mathbb{K}.N$, então $x = \sum_{i=1}^m (a_i/b_i)y_i$ ($a_i, b_i \in R$ e $y_i \in N$) e, devido a N ser um R -módulo, tomando $r_x = \prod_{i=1}^m b_i$, temos $r_x.x \in N$. Agora, pelo fato de M ser finitamente gerado como um R -módulo, existe uma base $\{x_1, \dots, x_n\}$ para M sobre R . Considerando $r = r_{x_1} \dots r_{x_n}$ tem-se que $rM \subset N$. $\square$

Definição 1.3.4. *Sejam R um domínio Noetheriano, $\mathbb{K}$ seu corpo de frações e A uma $\mathbb{K}$ -álgebra de dimensão finita. Dizemos que um subanel Λ de A é uma **R -ordem** em A se a unidade de A está em Λ e se Λ é um R -reticulado completo em A .*

Exemplo 1.3.2. *Se $A = M_n(\mathbb{K})$ é a álgebra das matrizes $n \times n$ sobre $\mathbb{K}$ e R é um domínio Noetheriano então $\Lambda = M_n(R)$ é uma R -ordem em A .*

Exemplo 1.3.3. *Se a é raiz de um polinômio mônico não nulo com coeficientes em um domínio Noetheriano R então o anel $R[a]$ é uma R -ordem da $\mathbb{K}$ -álgebra $\mathbb{K}[a]$.*

Exemplo 1.3.4. *Seja M um R -reticulado completo em A . Então o conjunto $\mathcal{A}_e(A, M) = \{x \in A : x.M \subset M\}$ é uma R -ordem de A . De fato, note que $\mathcal{A} = \mathcal{A}_e(A, M)$ é um subanel de A e é um R -módulo. Basta checar que $\mathcal{A}$ é um R -reticulado completo em A . Para cada $y \in A$, yM é um R -reticulado completo no $\mathbb{K}$ -subespaço vetorial yA de A . Como $M \cap yA$ é um R -reticulado em yA , o lema 1.3.1 nos diz que há um elemento não nulo $r \in R$ tal que $r.yM \subset M \cap yA \subset M$. Então $ry \in \mathcal{A}$, donde segue que $\mathbb{K}\mathcal{A} = A$. Além disso, existe um elemento $s \in R$ não nulo tal que $s.1_A \in M$. Portanto, $\mathcal{A}.(s.1_A) \subset M$, donde $\mathcal{A} \subset s^{-1}M$. Como R é Noetheriano e $s^{-1}M$ é um R -reticulado completo então $\mathcal{A}$ é finitamente gerado como um R -módulo. Portanto, $\mathcal{A}$ é uma R -ordem em A . A R -ordem $\mathcal{A}_e(A, M)$ é chamada de **ordem à esquerda de M em A** .*

Particularmente, vamos considerar o anel Noetheriano $R = \mathbb{Z}$, cujo corpo de frações é $\mathbb{K} = \mathbb{Q}$. Assim, podemos reescrever a definição de $\mathbb{Z}$ -ordem (ou, simplesmente, ordem) da seguinte maneira:

Definição 1.3.5. *Seja A uma $\mathbb{Q}$ -álgebra de dimensão finita. Um subanel R de A que contém a unidade de A é uma **$\mathbb{Z}$ -ordem** (ou, simplesmente, **ordem**) em A se R é finitamente gerado como um $\mathbb{Z}$ -módulo e se $\mathbb{Q}R = A$.*

Um exemplo importante de uma ordem é o anel de inteiros de um corpo de números, que será estudado no capítulo 2.

Proposição 1.3.1. *Seja A uma $\mathbb{Q}$ -álgebra.*

- (a) *Se R_1 e R_2 são ordens em A então $R_1 \cap R_2$ também é uma ordem em A .*
- (b) *Se um subanel R contendo a unidade de A é finitamente gerado como um $\mathbb{Z}$ -módulo e $R_1 \subset R$ é uma ordem em A então R também é uma ordem.*

Demonstração. (a) Primeiramente, como a unidade de A pertence a R_1 e R_2 então ela também pertence a $R_1 \cap R_2$. Como $R_1 \cap R_2$ é um $\mathbb{Z}$ -submódulo de R_1 e R_1 é finitamente gerado, segue do corolário 1.1.1 que $R_1 \cap R_2$ é finitamente gerado. Por fim, a igualdade $\mathbb{Q}(R_1 \cap R_2) = A$ conclui a demonstração. (b) Basta mostrar que $\mathbb{Q}R = A$. Por um lado, a relação $\mathbb{Q}R \subset A$ segue porque $R \subset A$ e A é um $\mathbb{Q}$ -módulo. Por outro lado, como R_1 é ordem, então $A = \mathbb{Q}R_1$. Como $R_1 \subset R$ então $\mathbb{Q}R_1 \subset \mathbb{Q}R$, donde segue que $A \subset \mathbb{Q}R$. $\square$

Lema 1.3.2. *Sejam $R_1 \subset R_2$ ordens em uma $\mathbb{Q}$ -álgebra A . Então existe um inteiro positivo d tal que $dR_2 \subset R_1$ e tal que o índice de grupos aditivos $[R_1 : dR_2]$ é finito.*

Demonstração. Por definição, R_2 admite um conjunto $\{x_1, \dots, x_t\}$ de geradores. Como $A = \mathbb{Q}R_1$ então existe um número natural d tal que $dx_i \in R_1$ para $1 \leq i \leq t$. De fato, escreva cada um dos x_i como uma combinação de elementos de R_1 com coeficientes em $\mathbb{Q}$ e tome d como sendo o valor absoluto do produto dos denominadores de todos os coeficientes de todas essas combinações. Logo, $dR_2 \subset R_1$. Como R_2 é um grupo abeliano aditivo finitamente gerado (pois é finitamente gerado como um $\mathbb{Z}$ -módulo) então segue do Teorema Fundamental dos grupos abelianos (teorema 1.1.2) que o índice aditivo $[R_2 : dR_2]$ é finito. Portanto, $[R_1 : dR_2] \leq [R_2 : dR_2]$ é finito também. $\square$

Na proposição a seguir, denote por $U(R)$ o conjunto dos elementos invertíveis de um anel R .

Proposição 1.3.2. *Sejam $R_1 \subset R_2$ ordens em uma $\mathbb{Q}$ -álgebra A . Então:*

- (a) *O índice dos grupos multiplicativos dos elementos invertíveis $(U(R_2) : U(R_1))$ é finito.*
- (b) *Se $u \in R_1$ é invertível em R_2 então $u^{-1} \in R_1$.*

Demonstração. Devido ao lema anterior, existe um inteiro positivo d tal que $dR_2 \subset R_1$ e o índice (como grupo aditivo) $[R_1 : dR_2]$ é finito. Para provar que o índice multiplicativo $(U(R_2) : U(R_1))$ é finito nós mostraremos que esse número é limitado por $[R_1 : dR_2]$. De fato, sejam $x, y \in U(R_2)$ tais que $x + dR_2 = y + dR_2$. Então, multiplicando essa igualdade por y^{-1} , temos $y^{-1}x - 1 \in dR_2 \subset R_1$,

ou seja, $y^{-1}x \in R_1$. Analogamente, $x^{-1}y \in R_1$. Então $y^{-1}x \in U(R_1)$, donde segue que $xU(R_1) = yU(R_1)$ e que $x \in yU(R_1)$. Isso mostra que se dois elementos pertencem à mesma classe aditiva módulo dR_2 então eles também pertencem à mesma classe multiplicativa módulo $U(R_1)$. Portanto, as classes multiplicativas de $U(R_1)$ são uniões disjuntas das classes aditivas de dR_2 , provando que $(U(R_2) : U(R_1)) \leq [R_1 : dR_2]$. Logo, o item (a) é válido. Finalmente, para mostrar o item (b), veja inicialmente que se $u \in R_1$ é invertível em R_2 então $R_2 = uR_2$. Agora, considerando seus grupos aditivos, temos claramente que $[R_2 : uR_1] = [uR_2 : uR_1]$. Além disso, se $r_1 \in R_1$ e $r_2 \in R_2$ então $r_2 - r_1 \in R_1$ se, e somente se, $ur_2 - ur_1 \in uR_1$. Disso, segue que $[uR_2 : uR_1] = [R_2 : R_1]$. Portanto, $[R_2 : uR_1] = [R_2 : R_1]$ e, conseqüentemente, $uR_1 = R_1$. Logo, $u \in R_1$ é invertível e seu inverso pertence a R_1 . $\square$

Finalmente, estudemos a estrutura dos anéis de grupo. Sejam G um grupo (não necessariamente finito) e A um anel com unidade. O que faremos é construir um A -módulo que tenha os elementos de G como base e utilizar as operações de A e de G para definir uma estrutura de anel neste A -módulo.

Considere o conjunto de todas as combinações lineares de elementos em G sobre A dado por

$$A[G] = \left\{ \sum_{g \in G} a_g g \text{ (soma finita)} : a_g \in A \right\}. \quad (1.12)$$

Na definição do conjunto $A[G]$, note que $a_g = 0$ exceto possivelmente para uma quantidade finita de termos. Por isso, todas as somas consideradas aqui possuem finitas parcelas, mesmo que o somatório seja indexado em um conjunto infinito. Se for conveniente, podemos escrever os elementos de $A[G]$ como $\alpha = \sum_{g \in G} a(g)g$, com $a(g) \in A$.

Dado um elemento $\alpha = \sum_{g \in G} a_g g \in A[G]$, definimos o **suporte de** α como sendo o conjunto dos elementos em G que aparecem efetivamente na expressão de α , isto é, $\text{sup}(\alpha) = \{g \in G : a_g \neq 0\}$. Note, da definição de $A[G]$, que

$$\sum_{g \in G} a_g g = \sum_{g \in G} b_g g \in A[G] \iff a_g = b_g, \forall g \in G. \quad (1.13)$$

Vamos definir, de maneira “óbvia”, algumas operações em $A[G]$. Sejam $\alpha = \sum_{g \in G} a_g g$, $\beta = \sum_{g \in G} b_g g$ e $\lambda \in A$. Definimos a soma $\alpha + \beta$ entre dois elementos de $A[G]$ por

$$\alpha + \beta = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g)g \quad (1.14)$$

e definimos a multiplicação $\alpha.\beta$ (ou simplesmente $\alpha\beta$) entre dois elementos de $A[G]$ por

$$\alpha.\beta = \left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{g \in G} b_g g \right) = \sum_{g, h \in G} (a_g b_h)g.h \quad (1.15)$$

Note que é equivalente a essa definição dizer que $\alpha\beta = \sum_{u \in G} c_u u$, em que $c_u = \sum_{gh=u} a_g b_h$.

Definimos também a multiplicação por escalar de $\alpha \in A[G]$ por $\lambda \in A$ da seguinte maneira:

$$\lambda\alpha = \lambda \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} (\lambda a_g) g \quad (1.16)$$

Assim, verifica-se que $A[G]$ é um anel com as operações de soma e produto definidas anteriormente. Mais ainda, $A[G]$ é um anel com unidade. De fato, se 1_A é a unidade de A e e é o elemento neutro do grupo G , então o elemento unidade de $A[G]$ é $1 = \sum_{g \in G} a_g g$, em que $a_e = 1_A$ e $a_g = 0$ para $g \neq e$, ou seja, $1 = 1_A e$.

Definição 1.3.6. *O anel $A[G]$ definido sob as operações de soma e produto acima é chamado de **anel de grupo** de G sobre A .*

Além disso, com a multiplicação por escalar definida anteriormente tem-se que $A[G]$ é um A -módulo. Se A for ainda um anel comutativo então $A[G]$ é uma A -álgebra.

Definição 1.3.7. *Se A é um anel comutativo com unidade e G é um grupo então $A[G]$ é chamado de **álgebra de grupo** de G sobre A .*

Se A é um anel com unidade e G é um grupo, podemos definir a aplicação injetiva $i : G \longrightarrow A[G]$ dada por $i(x) = \sum_{g \in G} a_g g$, em que $a_x = 1_A$ e $a_g = 0$ se $g \neq x$, para todo $x \in G$. Dessa forma, vemos que $G \subset A[G]$. Mais ainda, utilizando essa aplicação podemos dizer que G é uma base do A -módulo $A[G]$. Sabe-se que se A é um domínio de integridade então um A -módulo livre finitamente gerado tem a noção de posto bem definida. Logo, se A é um domínio de integridade (um corpo, por exemplo) e se G é um grupo finito então $A[G]$ é um A -módulo livre finitamente gerado por G cujo posto é $o(G)$.

Da mesma forma, sendo e o elemento neutro do grupo G , podemos considerar a aplicação $\nu : A \longrightarrow A[G]$ dada por $\nu(a) = \sum_{g \in G} a_g g$, em que $a_e = a$ e $a_g = 0$ se $g \neq e$, para todo $a \in A$. Facilmente verifica-se que ν é um homomorfismo injetor de anéis. Assim, podemos considerar A como sendo um subanel de $A[G]$.

Para ver mais sobre R -reticulados completos e ordens, consulte [27]. Para saber mais sobre anéis de grupo, recomendamos [25].

Conclusão

Enfim, este capítulo apresentou teorias e conceitos básicos de Álgebra. Aproveitamos ainda para estabelecer notações que serão úteis em outros capítulos desta dissertação. De forma especial, mereceram destaque os resultados envolvendo classes residuais e grupos abelianos finitos, e também a última seção, que tratou de álgebras e anéis de grupo, pois são temas pouco ou nada explorados em cursos introdutórios de Álgebra.

Capítulo 2

Teoria Algébrica dos Números

Teoria Algébrica dos Números é uma área clássica da Matemática. Um de seus problemas mais famosos é o Último Teorema de Fermat, o qual consumiu as forças de vários matemáticos durante muito anos e que só recentemente foi demonstrado. No passado essa teoria era estudada sem um fim prático específico. Atualmente, porém, a Teoria dos Números, assim como a Álgebra, tem sido aplicada, por exemplo, na área de telecomunicações.

Neste capítulo, nosso intuito é desenvolver desde aspectos introdutórios da Teoria Algébrica dos Números até conceitos um pouco mais avançados, cujo conhecimento será útil no decorrer desta dissertação. Estudaremos conceitos envolvendo elementos integrais, traço, norma, discriminante, domínio de Dedekind, anéis de inteiros, ramificação de ideais primos, traço relativo, ideal relativo, o diferente, entre outros. Àqueles que já tem um conhecimento preliminar de Teoria Algébrica dos Números, recomendamos pelo menos a leitura da última seção (sobre traço relativo, norma relativa e diferente), pois este é um assunto pouco comum em cursos introdutórios e serão referenciados algumas vezes na sequência deste trabalho. Para uma leitura complementar sobre os tópicos tratados neste capítulo, recomendamos [33], [30], [28] e [7].

2.1 Elementos integrais e algébricos

Nesta seção, considere R um anel comutativo com unidade.

Definição 2.1.1. *Seja A um subanel do anel R . Dizemos que um elemento $x \in R$ é **integral sobre A** se existem $a_0, a_1, \dots, a_{n-1} \in A$ tais que*

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \tag{2.1}$$

ou seja, se x é raiz de um polinômio mônico com coeficientes em A . A equação 2.1 é chamada **equação de dependência integral** de x sobre A .

Exemplo 2.1.1. Se $R = \mathbb{R}$ e $A = \mathbb{Z}$, então todo elemento a de $\mathbb{Z}$ é integral sobre A , pois é raiz do polinômio mônico $p(x) = x - a \in \mathbb{Z}[x]$. O elemento $x = \sqrt{2}$ também é integral sobre $A = \mathbb{Z}$, pois satisfaz $x^2 - 2 = 0$, que é sua equação de dependência integral.

Naturalmente, note que se R é um corpo e A é um subcorpo de R então $x \in R$ é integral sobre A se, e somente se, x é um elemento algébrico de R sobre A .

A seguir faremos alguns resultados básicos sobre elementos integrais.

Proposição 2.1.1. Sejam A um subanel do anel R e $x \in R$. São equivalentes:

- (a) x é um elemento integral sobre A .
- (b) O anel $A[x]$ é um A -módulo finitamente gerado.
- (c) Existe um subanel B de R que contém A e x (isto é, $A[x] \subset B$) e que é um A -módulo finitamente gerado.

Demonstração. Mostremos que (a) implica (b): como x é um elemento algébrico, então existem $a_0, a_1, \dots, a_{n-1}$ em A tais que

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0. \quad (2.2)$$

Sendo M o A -submódulo de R gerado por $1, x, x^2, \dots, x^{n-1}$, claramente $x^n \in M$. Multiplicando a equação 2.2 por x^j tem-se que $x^{n+j} = -a_{n-1}x^{n+j-1} - \dots - a_0x^j$ para qualquer j inteiro. Para $j = 1$, como $x^n \in M$, vê-se que $x^{n+1} \in M$. Por indução, mostra-se que $x^{n+j} \in M$ para qualquer j inteiro. Logo, $A[x] \subset M$. Como claramente $M \subset A[x]$, então $M = A[x]$. Isso mostra que $A[x]$ é um A -módulo finitamente gerado. Para ver que (b) implica (c) basta tomar $B = A[x]$. Por fim, vejamos que (c) implica (a): seja $\{y_1, y_2, \dots, y_n\}$ um conjunto de geradores de B sobre A . Como $x \in B$ e B é um anel, então $xy_i \in B$ para todo $1 \leq i \leq n$. Assim, para cada i nesse intervalo existem $1 \leq j \leq n$ e $a_{ij} \in A$ tais que $xy_i = \sum_{j=1}^n a_{ij}y_j$. Se I é a matriz identidade, $\overline{0}$ é a matriz nula, $A = [a_{ij}]_{i,j=1}^n$ é a matriz quadrada $n \times n$ formada pelos elementos a_{ij} e $Y = [y_1, y_2, \dots, y_n]$ é a matriz dada pelos geradores de B , então $(Ix + A)Y = \overline{0}$ é um sistema linear $n \times n$ homogêneo com solução Y . Sendo $d = \det(Ix + A)$, a regra de Cramer nos afirma que $dy_i = 0$ para todo $1 \leq i \leq n$. Como $1 \in B$, então existem $c_i \in A$ tais que $1 = \sum_{i=1}^n c_i y_i$. Logo, $d = d.1 = \sum_{i=1}^n c_i dy_i = 0$. Porém, o cálculo de d por meio do chamado método de Laplace nos leva a concluir que d é um polinômio mônico da forma

$x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$, com cada $b_i \in A$. O fato de d ser igual 0 acarreta que qualquer $x \in R$ é solução de um polinômio mônico com coeficientes em A , ou seja, x é integral sobre A . $\square$

Proposição 2.1.2. *Sejam A um subanel do anel R e $\{x_1, x_2, \dots, x_n\}$ um conjunto finito de elementos de R . Se x_1 é integral sobre A e se, para todo $2 \leq i \leq n$, x_i é integral sobre $A[x_1, x_2, \dots, x_{i-1}]$ então $A[x_1, x_2, \dots, x_n]$ é um A -módulo finitamente gerado.*

Demonstração. Demonstremos por indução sobre n . Se $n = 1$, a implicação (a) $\implies$ (b) da proposição 2.1.1 garante a validade da tese. Suponhamos, por indução, que $B = A[x_1, x_2, \dots, x_{n-1}]$ é um A -módulo finitamente gerado. Assim, existem $b_j \in B$ tais que $B = \sum_{j=1}^p Ab_j$. Por hipótese, como x_n é integral sobre B então $A[x_1, x_2, \dots, x_n] = B[x_n]$ é um B -módulo finitamente gerado. Logo, $B[x_n] = \sum_{i=1}^q Bc_i$ em que cada $c_i \in B[x_n]$. Então

$$A[x_1, x_2, \dots, x_n] = \sum_{i=1}^q Bc_i = \sum_{i=1}^q \sum_{j=1}^p Ab_jc_i. \quad (2.3)$$

Assim, o conjunto dos elementos b_jc_i , com $1 \leq j \leq p$ e $1 \leq i \leq q$, é um conjunto finito de geradores de $A[x_1, x_2, \dots, x_n]$ como um A -módulo. $\square$

Em particular, observe que se cada x_i do enunciado acima, $1 \leq i \leq n$, for integral sobre A , então $A[x_1, x_2, \dots, x_n]$ é um A -módulo finitamente gerado.

Corolário 2.1.1. *Sejam A um subanel do anel R e x e y elementos de R integrais sobre A . Então $x + y$, $x - y$ e xy são integrais sobre A .*

Demonstração. Pela proposição 2.1.2, o anel $B = A[x, y]$ é finitamente gerado sobre A , pois y é integral sobre $A[x]$ (já que é integral sobre A). Como $x + y$, $x - y$ e xy pertencem a B , segue da implicação (c) $\implies$ (a) da proposição 2.1.1 que esses elementos são integrais sobre A . $\square$

Corolário 2.1.2. *Seja A um subanel do anel R . O conjunto A' dos elementos de R que são integrais sobre A é um subanel de R contendo A ($A \subset A' \subset R$).*

Demonstração. Primeiramente, note que $A \subset A'$, pois todo elemento a de A é raiz do polinômio mônico $p(x) = x - a \in A[x]$. Por fim, o corolário 2.1.1 implica que A' é um subanel de R . $\square$

O corolário anterior sugere a seguinte definição:

Definição 2.1.2. *Considere A um subanel do anel R .*

(a) *O subanel A' formado pelos elementos de R que são integrais sobre A é chamado de **fecho***

integral de A em R .

(b) Se A é um domínio de integridade e $\mathbb{K}$ é o corpo de frações de A , então o fecho integral de A em $\mathbb{K}$ é simplesmente chamado de **fecho integral de A** .

Outra definição importante é a seguinte:

Definição 2.1.3. *Seja A um subanel do anel R . Dizemos que R é **integral sobre A** se R é o fecho integral de A em R , ou seja, se todo elemento de R é integral sobre A .*

Proposição 2.1.3 (Transitividade). *Sejam $A \subset B$ subanéis de R . Se B é integral sobre A e R é integral sobre B , então R é integral sobre A .*

Demonstração. Considere $x \in R$. Como R é integral sobre B , então x é integral sobre B . Logo, existem $b_0, b_1, \dots, b_{n-1} \in B$ tais que $x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0$. Seja $B' = A[b_0, b_1, \dots, b_{n-1}]$. Assim, x é integral sobre B' . Como B é integral sobre A então cada b_i é integral sobre A . Logo, pela proposição 2.1.2, B' é um A -módulo finitamente gerado. Pela implicação (a) $\implies$ (b) da proposição 2.1.1, segue que $C = B'[x] = A[b_0, b_1, \dots, b_{n-1}, x]$ é um A -módulo finitamente gerado que contém A e x . Pela implicação (c) $\implies$ (a) da proposição 2.1.1 concluímos que x é integral sobre A . $\square$

Proposição 2.1.4. *Seja A um subanel do domínio de integridade R e suponha que R é integral sobre A . Então R é um corpo se, e somente se, A é um corpo.*

Demonstração. Por um lado, suponha que A seja um corpo e considere $x \in R$ um elemento não nulo. Como x é integral sobre A , então a implicação (a) $\implies$ (b) da proposição 2.1.1 acarreta que $A[x]$ é um espaço vetorial de dimensão finita sobre A . Considere $T : A[x] \rightarrow A[x]$ a transformação linear dada por $T(y) = xy$, para todo $y \in A[x]$. Essa transformação é injetora, pois, para quaisquer $y, z \in A[x]$,

$$T(y) = T(z) \implies xy = xz \implies x(y - z) = 0 \implies y - z = 0 \implies y = z \quad (2.4)$$

já que R é um domínio de integridade e $x \neq 0$. Portanto, T é bijetora. Logo, existe $y \in A[x]$ tal que $xy = 1$, ou seja, x é invertível. Portanto, R é corpo. Por outro lado, suponha que R é um corpo e considere a um elemento não nulo de A . Logo, a tem inverso multiplicativo $a^{-1} \in R$. Como R é integral sobre A , existem $b_0, b_1, \dots, b_{n-1} \in A$ tais que $a^{-n} + b_{n-1}a^{-n+1} + \dots + b_1a^{-1} + b_0 = 0$. Multiplicando a equação anterior por a^{n-1} , temos $a^{-1} = -(b_{n-1} + \dots + b_1a^{n-2} + b_0a^{n-1}) \in A$. Portanto, existe $a^{-1} \in A$ tal que $aa^{-1} = 1$ para todo $a \neq 0$ em A . Logo, A é corpo. $\square$

Definição 2.1.4. *Seja A um domínio de integridade. Dizemos que A é **integralmente fechado** se o fecho integral de A for o próprio A .*

Exemplo 2.1.2. Se A é um domínio de integridade então seu fecho integral A' (dentro do corpo de frações de A) é integralmente fechado. De fato, seja B o fecho integral de A' sobre A' . Como B é integral sobre A' e A' é integral sobre A , segue da proposição 2.1.3 (transitividade) que B é integral sobre A . Porém, A' é o maior anel dentro do corpo de frações de A cujos elementos são integrais sobre A . Logo, $B = A'$. Portanto, o fecho integral de A' é o próprio A' .

Exemplo 2.1.3. Todo domínio de fatoração única (DFU) é integralmente fechado. De fato, seja A um DFU. Considere $x = b/c$ um elemento do fecho integral de A (no corpo de frações de A), em que $b, c \in A$ são relativamente primos (como o anel é DFU, existe o máximo divisor comum entre dois números quaisquer nesse anel). Então existem $a_0, a_1, \dots, a_{n-1} \in A$ tais que $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$. Substituindo $x = b/c$ nesta equação e multiplicando-a por c^n , tem-se

$$c(a_{n-1}b^{n-1} + \dots + a_1bc^{n-2} + a_0c^{n-1}) = -b^n \quad (2.5)$$

Como A é DFU, vale o Lema de Euclides. Logo c divide b em A . Portanto, $x = b/c \in A$, donde conclui-se que $A' \subset A$. Então $A = A'$, o que significa que A é integralmente fechado.

Exemplo 2.1.4. Todo domínio principal é domínio de fatoração única. Logo, todo domínio principal também é integralmente fechado. Em particular, $\mathbb{Z}$ é integralmente fechado.

Proposição 2.1.5. Se R é um domínio de integridade e A é um subanel de R tal que R é integral sobre A , então para todo ideal não-zero J de R vale $J \cap A \neq \{0\}$.

Demonstração. Seja $x \neq 0$ um elemento de J . Como R é integral, existem $a_0, a_1, \dots, a_{n-1} \in A$ tais que $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$, em que n é o menor natural possível (ou seja, não existe outro polinômio mônico do anel de polinômios $A[t]$ que tenha raiz x e que tenha grau menor que n). Então $a_0 \neq 0$, pois, caso contrário, como R é anel de integridade e $x \neq 0$, teríamos $x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1 = 0$, o que é um absurdo pela minimalidade de n . Assim, $a_0 \in J \cap A$ e $a_0 \neq 0$, comprovando que $J \cap A \neq \{0\}$. $\square$

Proposição 2.1.6. Seja A um subanel do domínio de integridade R tal que R é integral sobre A . Considere P um ideal primo de R . Então P é um ideal maximal de R se, e somente se, $P \cap A$ é um ideal maximal de A .

Demonstração. Por um lado, se P é maximal em R , então R/P é um corpo. Seja $\theta : R \rightarrow R/P$ o homomorfismo canônico. Como R é integral sobre A , então R/P é integral sobre $\theta(A) = A/(A \cap P)$. Pela proposição 2.1.4, $A/(A \cap P)$ é um corpo. Logo, $A \cap P$ é um ideal maximal de A . Por outro

lado, se $P \cap A$ é um ideal maximal de A , então o fato de R/P ser integral sobre o corpo $A/(P \cap A)$ acarreta da proposição 2.1.4 que R/P é corpo, já que R/P é um domínio de integridade (pois P é ideal primo). Logo, P é um ideal maximal de R . $\square$

2.2 Norma e traço

Nesta seção, utilizaremos algumas noções de Álgebra Linear para módulo sobre anéis comutativos, as quais são generalizadas das noções de Álgebra Linear sobre espaços vetoriais. Caso queira saber mais sobre o assunto, consulte o capítulo XIII de [22].

Sejam A um anel e E um A -módulo livre finitamente gerado. Considere $u : E \rightarrow E$ um endomorfismo, $\mathcal{B} = \{e_1, \dots, e_n\}$ uma base de E sobre A e $U = [a_{ij}]$ a matriz de u com relação à base $\mathcal{B}$, assim como definido na Álgebra Linear, isto é, cada a_{ij} é coeficiente de e_i na expressão $u(e_j) = \sum_{i=1}^n a_{ij}e_i$ (veja a seção 3.4 de [14]). Definimos o **traço** de u e o **determinante** de u como sendo, respectivamente,

$$\text{Tr}(u) = \text{Tr}(U) = \sum_{i=1}^n a_{ii} \quad e \quad \det(u) = \det(U). \quad (2.6)$$

Além disso, definimos também o polinômio característico de u como sendo $P_u(x) = \det(xI - U)$, em que I é a matriz identidade $n \times n$.

Proposição 2.2.1. *Com as notações acima, sendo v outro endomorfismo de E e $a \in A$, então:*

- (a) $\text{Tr}(uv) = \text{Tr}(vu)$;
- (b) as definições de traço, de norma e de polinômio característico independem da base escolhida;
- (c) $\text{Tr}(au + v) = a\text{Tr}(u) + \text{Tr}(v)$;
- (d) $\det(uv) = \det(u)\det(v)$;
- (e) $P_u(x) = x^n - \text{Tr}(u)x^{n-1} + \dots + (-1)^n \det(u)$.

Demonstração. (a) Considere $V = [b_{ij}]$ a matriz de v . Assim, $\text{Tr}(uv) = \sum_{i=1}^n \sum_{j=1}^n a_{ij}b_{ji}$ e $\text{Tr}(vu) = \sum_{j=1}^n \sum_{i=1}^n b_{ji}a_{ij}$, donde segue diretamente que $\text{Tr}(uv) = \text{Tr}(vu)$. (b) Sejam $\mathcal{C} = \{f_1, \dots, f_n\}$ outra base de M sobre A e $U' = [b'_{ij}]$ a matriz de u com relação a essa base. Então b'_{ij} corresponde ao coeficiente de f_i em $u(f_j) = \sum_{i=1}^n b'_{ij}f_i$. Escrevendo os elementos da base $\mathcal{B}$ em função dos elementos da base $\mathcal{C}$, temos $e_j = \sum_{i=1}^n c_{ij}f_i$. Também escrevemos os elementos da base $\mathcal{C}$ em função dos elementos da base $\mathcal{B}$ como $f_j = \sum_{i=1}^n d_{ji}e_i$. Assim, sendo C a matriz $[c_{jk}]$ e D a matriz $[d_{ji}]$, vemos que C e D são invertíveis e que C é a inversa de D , ou seja, $CD = I$. Além disso, $U = DU'C$. Utilizando a definição de traço, temos $\text{Tr}(u) = \text{Tr}(U) = \text{Tr}(DU'C) = \text{Tr}(DCU') = \text{Tr}(U')$. Portanto, o

traço independe da base escolhida. Para o determinante, temos $\det(u) = \det(U) = \det(DU'C) = \det(D)\det(U')\det(C) = \det(D)\det(C)\det(U') = \det(DC)\det(U') = \det(I)\det(U') = \det(U')$. Por fim, $P_u(x) = \det(xI - U) = \det(xDC - DU'C) = \det(DxC - DU'C) = \det(D(xI - U')C) = \det(D)\det(xI - U')\det(C) = \det(xI - U')$, donde segue que o polinômio característico independe da escolha da base.

(e) Pelo chamado método de Laplace para resolução de determinantes, temos:

$$P_u(x) = \det(xI - U) = \begin{vmatrix} x - a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & x - a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & x - a_{nn} \end{vmatrix} = \prod_{i=1}^n (x - a_{ii}) + r(x), \quad (2.7)$$

em que $r(x)$ é um polinômio mônico de grau menor do que $n - 1$, já que, ao descartar linha 1 e a coluna $j \neq 1$ descarta-se automaticamente $x - a_{11}$ e $x - a_{jj}$ da matriz quadrada de ordem $n - 1$ cujo determinante será calculado e que será uma das parcelas do determinante final. Logo, $P_u(x) = x^n + q_{n-1}x^{n-1} + \dots + q_1x + q_0$ e o coeficiente de x^{n-1} no desenvolvimento de $P_u(x)$ coincide com o coeficiente de x^{n-1} do desenvolvimento de $\prod_{i=1}^n (x - a_{ii})$, que é $-(a_{11} + \dots + a_{nn}) = -\text{Tr}(u)$. Portanto, $q_{n-1} = -\text{Tr}(u)$. Além disso, calculando $x = 0$ tem-se $q_0 = P_u(0) = \det(0I - U) = \det(-U) = (-1)^n \det(U)$, concluindo o item (e). O item (c) segue facilmente da definição de soma de matrizes e o item (d) segue da propriedade de determinantes que diz que o determinante do produto de duas matrizes é o produto do determinante de cada uma. $\square$

Agora, considere B um anel e A um subanel de B tal que B seja um A -módulo livre finitamente gerado de posto n (por exemplo, A pode ser um corpo e B uma extensão finita de grau n sobre A). Considere também, para cada $x \in B$, a aplicação $m_x : B \rightarrow B$, chamada *multiplicação por x* , a qual é dada por $m_x(y) = yx$, para todo $y \in Y$. Facilmente verifica-se que cada m_x é um endomorfismo do A -módulo B . Dessa forma, podemos fazer a seguinte definição:

Definição 2.2.1. Com as notações anteriores e sendo $x \in B$ qualquer, chama-se **traço de x** ao traço de m_x , o qual é denotado por $\text{Tr}_{B:A}(x)$. O determinante de m_x é chamado **norma de x** e é denotado por $N_{B:A}(x)$. Analogamente, chama-se **polinômio característico de x** ao polinômio característico de m_x .

Quando não houver confusão sobre os anéis A e B em questão, podemos simplificar a notação denotando o traço e a norma de $x \in B$ simplesmente por $\text{Tr}(x)$ e $N(x)$, respectivamente. Evidentemente, por definição, o polinômio característico de $x \in B$ tem coeficientes em A . Devido ao item

(e) da proposição 2.2.1, podemos então inferir que $Tr(x)$ e $N(x)$ são elementos de A , mesmo sendo calculados sobre elementos de B .

Proposição 2.2.2. *Seja A e B como acima, $x, y \in B$ e $a \in A$, então $Tr(x + y) = Tr(x) + Tr(y)$, $T(ax) = aT(x)$, $Tr(a) = na$, $N(xy) = N(x)N(y)$, $N(a) = a^n$ e $N(ax) = a^n N(x)$.*

Demonstração. Como $m_x + m_y = m_{x+y}$, $m_x \circ m_y = m_{x+y}$, $m_{ax} = am_x$ e m_a correspondente à matriz diagonal aI , então a proposição 2.2.1 comprova a tese. $\square$

Proposição 2.2.3. *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão finita de corpos com grau $[\mathbb{L} : \mathbb{K}] = n$, $x \in \mathbb{L}$ e $d = [\mathbb{K}(x) : \mathbb{K}]$. Se $x_1, \dots, x_d$ são as raízes do polinômio minimal de x , $f(t)$, no seu corpo de raízes e se $P_x(t)$ é o polinômio característico de x então*

$$Tr(x) = \frac{n}{d} \sum_{i=1}^d x_i, \quad N(x) = \left(\prod_{i=1}^d x_i \right)^{n/d} \quad e \quad P_x(t) = (f(t))^{n/d}. \quad (2.8)$$

Demonstração. Mostremos inicialmente que $P_x(t) = (f(t))^{n/d}$. Seja $r = n/d$, $\mathcal{B} = \{y_1, \dots, y_d\}$ uma $\mathbb{K}$ -base para $\mathbb{K}(x)$ e $\mathcal{C} = \{z_1, \dots, z_r\}$ uma $\mathbb{K}(x)$ -base para $\mathbb{L}$. Logo, $\mathcal{D} = \{y_i z_j : 1 \leq i \leq d, 1 \leq j \leq r\}$ é uma $\mathbb{K}$ -base para $\mathbb{L}$. Seja $M = [a_{ij}]_{d \times d}$ a matriz da multiplicação m_x em relação à base $\mathcal{B}$. Assim, $xy_i = \sum_{h=1}^d a_{ih} y_h$ e, daí, $x(y_i z_j) = (\sum_{h=1}^d a_{ih} y_h) z_j = \sum_{h=1}^d a_{ih} (y_h z_j)$. Considerando a base $\mathcal{D}$ ordenada na ordem lexicográfica, isto é, $\mathcal{D} = \{y_1 z_1, y_1 z_2, \dots, y_1 z_r, y_2 z_1, \dots, y_d z_r\}$, vê-se que a matriz M_1 da multiplicação por x em $\mathbb{L}$ com relação a essa base é da forma

$$M_1 = \begin{bmatrix} M & 0 & \dots & 0 \\ 0 & M & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M \end{bmatrix}, \quad (2.9)$$

formada por r blocos M na sua diagonal. Assim, a matriz $tI_n - M_1$ possui r blocos diagonais $tI_d - M$. Consequentemente, $P_x(t) = \det(tI_n - M_1) = (\det(tI_d - M))^r$ (I). Mostremos agora que $\det(tI_d - M)$ coincide com o polinômio minimal de x . Como $f(t)$ é o polinômio minimal de x , então $\mathcal{E} = \{1, x, \dots, x^{d-1}\}$ é uma $\mathbb{K}$ -base para $\mathbb{K}(x)$. Suponhamos que $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$. Então a matriz do endomorfismo m_x com respeito à base $\mathcal{E}$ é

$$M_2 = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{d-1} \end{bmatrix}. \quad (2.10)$$

A partir dessa expressão, calcula-se $tI_d - M$ e, pelo método de Laplace, mostra-se que $\det(tI_d - M) = f(t)$. Portanto, de (I), tem-se que $P_x(t) = (f(t))^{n/d}$. Agora, suponha que $f(t) = x^d + b_{d-1}x^{d-1} + \dots + b_0$ (II). Como $x_1, \dots, x_d$ são raízes de $f(t)$ então $f(t) = \prod_{i=1}^d (t - x_i)$. Abrindo esta última expressão e igualando com (II), tem-se que $b_{n-1} = -\sum_{i=1}^d x_i$ e $b_0 = \prod_{i=1}^d x_i$. Por fim, da igualdade $P_x(t) = (f(t))^{n/d}$ e do item (e) da proposição 2.2.1, concluímos que $Tr(x) = -(n/d)b_{n-1} = (n/d)\sum_{i=1}^d x_i$ e que $N(x) = (b_0)^{n/d} = (\prod_{i=1}^d x_i)^{n/d}$. $\square$

Sejam $\mathbb{K}$ um corpo e $\mathbb{L}$ uma extensão separável de $\mathbb{K}$ de grau n . Existem n distintos $\mathbb{K}$ -monomorfismos $\sigma_1 = id, \sigma_2, \dots, \sigma_n$ de $\mathbb{L}$ em um fecho algébrico Ω de $\mathbb{K}$ contendo $\mathbb{K}$.

Corolário 2.2.1. *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão separável e finita de grau n e $\sigma_1 = id, \sigma_2, \dots, \sigma_n$ os n distintos $\mathbb{K}$ -monomorfismos de $\mathbb{L}$ em um fecho algébrico Ω de $\mathbb{K}$ contendo $\mathbb{L}$. Então, para qualquer $x \in \mathbb{L}$,*

$$N_{\mathbb{L}:\mathbb{K}}(x) = \prod_{i=1}^n \sigma_i(x), \quad Tr_{\mathbb{L}:\mathbb{K}}(x) = \sum_{i=1}^n \sigma_i(x), \quad e \quad P_x(t) = \prod_{i=1}^n (t - \sigma_i(x)). \quad (2.11)$$

Demonstração. Seja $d = [\mathbb{L} : \mathbb{K}(x)]$. Cada um dos d distintos $\mathbb{K}$ -monomorfismos τ_i de $\mathbb{K}(x)$ em Ω leva x em um único conjugado x_i e se estende para exatamente n/d $\mathbb{K}$ -monomorfismos de $\mathbb{L}$ em Ω , todos levando x em x_i . Então os elementos $\sigma_1(x), \dots, \sigma_n(x)$ são os elementos $\tau_i(x)$, $1 \leq i \leq d$, cada um deles contado n/d vezes. Assim, o resultado é consequência da proposição 2.2.3. $\square$

O resultado a seguir é conhecido como propriedade transitiva do traço e da norma.

Proposição 2.2.4. *Seja $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ uma extensão de corpos, com $\mathbb{K} \subset \mathbb{M}$ finita e separável. Então, para qualquer $x \in \mathbb{M}$,*

$$Tr_{\mathbb{M}:\mathbb{K}}(x) = Tr_{\mathbb{L}:\mathbb{K}}(Tr_{\mathbb{M}:\mathbb{L}}(x)) \quad e \quad N_{\mathbb{M}:\mathbb{K}}(x) = N_{\mathbb{L}:\mathbb{K}}(N_{\mathbb{M}:\mathbb{L}}(x)). \quad (2.12)$$

Demonstração. Sejam $\{\sigma_i(x)\}_{i=1}^n$ o conjunto dos $\mathbb{K}$ -monomorfismos de $\mathbb{L}$ em Ω e $\{\tau_j\}_{j=1}^m$ o conjunto dos $\mathbb{L}$ -monomorfismos de $\mathbb{M}$ em Ω , em que Ω é um fecho normal de $\mathbb{M}$ contendo $\mathbb{K}$ e $\mathbb{L}$. Assim, $\mathbb{K} \subset \Omega$ é uma extensão galoisiana e cada monomorfismo σ_i e τ_j pode ser considerado um automorfismo de Ω . Portanto, podemos compor tais automorfismos. Assim, por um lado, $Tr_{\mathbb{L}:\mathbb{K}}(Tr_{\mathbb{M}:\mathbb{L}}(x)) = \sum_{i=1}^n \sum_{j=1}^m \sigma_i(\tau_j(x))$. Por outro lado, cada $\sigma_i \circ \tau_j$ é um $\mathbb{K}$ -monomorfismo de $\mathbb{M}$ em Ω . Além disso, existem $mn = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}] = [\mathbb{M} : \mathbb{K}]$ $\mathbb{K}$ -monomorfismos de $\mathbb{M}$ em Ω . Afirmamos que os automorfismos $\sigma_i \circ \tau_j$, $1 \leq i \leq n$, $1 \leq j \leq m$, são distintos em $\mathbb{M}$. De fato, se $\sigma_i \circ \tau_j = \sigma_k \circ \tau_l$ em $\mathbb{M}$ então $\sigma_i = \sigma_k$ em $\mathbb{K}$, pois τ_j e τ_l coincide com a identidade de $\mathbb{K}$. Então $i = k$ e $\tau_j = \tau_l$ em $\mathbb{M}$, donde segue que $j = l$. Logo, do corolário 2.2.1 concluímos que $Tr_{\mathbb{M}:\mathbb{K}}(x) = \sum_{i=1}^n \sigma_i \circ \tau_j(x)$, donde segue a igualdade $Tr_{\mathbb{M}:\mathbb{K}}(x) = Tr_{\mathbb{L}:\mathbb{K}}(Tr_{\mathbb{M}:\mathbb{L}}(x))$. Analogamente mostra-se que $N_{\mathbb{M}:\mathbb{K}}(x) = N_{\mathbb{L}:\mathbb{K}}(N_{\mathbb{M}:\mathbb{L}}(x))$. $\square$

Outro fato interessante é que se $\mathbb{K} \subset \mathbb{L}$ é uma extensão separável então existe $x \in \mathbb{L}$ tal que $Tr_{\mathbb{L}:\mathbb{K}}(x) = 0$. Mais ainda, se $[\mathbb{L}:\mathbb{K}] = n < \infty$ e a característica de $\mathbb{K}$ não divide n então existe um elemento primitivo θ de $\mathbb{L}$ sobre $\mathbb{K}$ tal que $Tr_{\mathbb{L}:\mathbb{K}}(\theta) = 0$.¹

A seguir, apresentamos dois resultados sobre traços e normas de elementos integrais:

Proposição 2.2.5. *Sejam A um domínio de integridade, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e x um elemento integral de $\mathbb{L}$ sobre $\mathbb{K}$. Se $\mathbb{K}$ tem característica zero então os coeficientes do polinômio característico de x relativo a $\mathbb{L}$ e $\mathbb{K}$ são integrais sobre A . Em particular, $Tr_{\mathbb{L}:\mathbb{K}}(x)$ e $N_{\mathbb{L}:\mathbb{K}}(x)$ são integrais sobre A .*

Demonstração. Seja $P_x(t) = (t - x_1) \dots (t - x_n)$ o polinômio característico de x . Os coeficientes de $P_x(t)$ são, devido às famosas relações de Girard (para polinômios), dependentes de somas e produtos das raízes x_i . Por isso, para comprovar a tese desta proposição, basta mostrar que cada x_i é integral sobre A . Cada x_i é conjugado de x sobre $\mathbb{K}$, pois são raízes do mesmo polinômio minimal, e existe um $\mathbb{K}$ -isomorfismo $\sigma_i: \mathbb{K}(x) \rightarrow \mathbb{K}(x_i)$ tal que $\sigma_i(x) = x_i$. Como x é integral sobre A , então existem $a_0, a_1, \dots, a_{n-1} \in A$ tais que $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$. Aplicando σ_i a essa equação, obtemos $\sigma_i(x)^n + a_{n-1}\sigma_i(x)^{n-1} + \dots + a_1\sigma_i(x) + a_0 = 0$ e, daí, $x_i^n + a_{n-1}x_i^{n-1} + \dots + a_1x_i + a_0 = 0$. Portanto, cada x_i é integral sobre A , como queríamos demonstrar. $\square$

Corolário 2.2.2. *Seja A um domínio de integridade que é integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e x um elemento integral de $\mathbb{L}$ sobre $\mathbb{K}$. Então os coeficientes do polinômio característico de $x \in \mathbb{L}$ são elementos de A . Em particular, $Tr_{\mathbb{L}:\mathbb{K}}(x)$ e $N_{\mathbb{L}:\mathbb{K}}(x)$ pertencem a A .*

Demonstração. Devido à proposição 2.2.5, os coeficientes do polinômio característico de x são integrais sobre A . Como A é integralmente fechado então eles pertencem a A . $\square$

2.3 Discriminante

Definição 2.3.1. *Sejam B um anel e A um subanel de B tal que B é um A -módulo livre finitamente gerado de posto n . Se $(x_1, \dots, x_n) \in B^n$, chama-se **discriminante** de $(x_1, \dots, x_n)$ ao elemento*

$$D_{B:A}(x_1, \dots, x_n) = \det(Tr_{B:A}(x_i x_j)) \in A. \quad (2.13)$$

¹ Esse comentário foi extraído de [28], página 20.

Quando não houver risco de confusão, denotaremos o discriminante $D_{B:A}(x_1, \dots, x_n)$ simplesmente por $D(x_1, \dots, x_n)$.

Proposição 2.3.1. *Mantendo as notações da definição anterior, se $(y_1, \dots, y_n) \in B^n$ é outro conjunto de elementos de B tal que $y_i = \sum_{j=1}^n a_{ij}x_j$, $a_{ij} \in A$, então*

$$D(y_1, \dots, y_n) = (\det(a_{ij}))^2 D(x_1, \dots, x_n). \quad (2.14)$$

Demonstração. De fato, utilizando as propriedades do traço, temos:

$$\text{Tr}(y_p y_q) = \text{Tr} \left(\sum_{i=1}^n \sum_{j=1}^n a_{pi} a_{qj} x_i x_j \right) = \sum_{i=1}^n \sum_{j=1}^n a_{pi} a_{qj} \text{Tr}(x_i x_j). \quad (2.15)$$

Dessa equação segue que $[\text{Tr}(y_p y_q)] = [a_{pi}][\text{Tr}(x_i x_j)][a_{qj}]^T$. Finalmente, tomando o determinante de cada matriz, tem-se a tese, já que $\det(a_{pi}) = \det(a_{qj}) = \det([a_{qj}]^T)$. $\square$

Devido à proposição anterior, note que um conjunto $\{x_1, \dots, x_n\}$ forma uma base do A -módulo B se, e somente se, $\det(a_{ij})$ é invertível em A . Nesse sentido, é possível estabelecer a seguinte definição:

Definição 2.3.2. *Sejam B um anel e A um subanel de B tal que B é um A -módulo livre finitamente gerado de posto n . O ideal principal de A gerado pelo discriminante de qualquer base de B sobre A é chamado de **ideal discriminante de B sobre A** , o qual será denotado por $\mathfrak{D}_{B:A}$.*

Para a próxima proposição, saiba que um elemento a em um anel A é dito ser um **divisor de zero** se for não nulo e se $ab = 0$ para algum $b \neq 0$ no mesmo anel.

Proposição 2.3.2. *Suponha que $\mathfrak{D}_{B:A}$ possua um elemento que não é divisor de zero. Então, $\{x_1, \dots, x_n\} \subset B$ é uma base para B sobre A se, e somente se, o ideal discriminante $\mathfrak{D}_{B:A}$ é gerado por $D(x_1, \dots, x_n)$.*

Demonstração. Por um lado, se $\{x_1, \dots, x_n\} \subset B$ é uma base para B sobre A então $d = D(x_1, \dots, x_n)$ é um gerador para $\mathfrak{D}_{B:A}$, pois, segundo a proposição 2.3.1, d é associado ao gerador de $\mathfrak{D}_{B:A}$ e, então, $\mathfrak{D}_{B:A} = (d) = dA$. Por outro lado, suponha que $\mathfrak{D}_{B:A} = (D(x_1, \dots, x_n))$, tome $d = D(x_1, \dots, x_n)$ e considere $\mathcal{B} = \{e_1, \dots, e_n\}$ uma base do A -módulo B . Denote $d' = D(e_1, \dots, e_n)$. Como $\mathcal{B}$ é base, temos $x_i = \sum_{j=1}^n a_{ij}e_j$, com $1 \leq i \leq n$ e $a_{ij} \in A$. Da proposição 2.3.1, sabemos que $d = (\det(a_{ij}))^2 d'$. Por hipótese, $(d) = \mathfrak{D}_{B:A} = (d')$ e, portanto, existe $b \in A$ tal que $d' = bd$. Assim, $d(1 - b(\det(a_{ij}))^2) = 0$. Sabe-se que d não é um divisor de zero, pois, caso contrário, todo elemento de $(d) = \mathfrak{D}_{B:A}$ também seria (absurdo por hipótese). Logo, $b(\det(a_{ij}))^2 = 1$, donde segue que $\det(a_{ij})$ é invertível. Logo, $[a_{ij}]$ é invertível e $\{x_1, \dots, x_n\}$ é base para o A -módulo B . $\square$

Proposição 2.3.3. *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos separável e finita de grau n e $\sigma_1, \dots, \sigma_n$ os n distintos $\mathbb{K}$ -isomorfismos de $\mathbb{L}$ em um fecho algébrico Ω de $\mathbb{L}$. Assim, $D(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$.*

Demonstração. De fato,

$$\begin{aligned} D(x_1, \dots, x_n) &= \det(\text{Tr}(x_i x_j)) = \det\left(\sum_{k=1}^n \sigma_k(x_i x_j)\right) = \det\left(\sum_{k=1}^n \sigma_k(x_i) \sigma_k(x_j)\right) = \\ &= \det(\sigma_k(x_i)) \det(\sigma_k(x_j)) = \det(\sigma_k(x_i))^2. \end{aligned} \quad (2.16)$$

□

A proposição a seguir é um exemplo de cálculo de discriminante de uma importante base de extensões finitas e separáveis.

Proposição 2.3.4. *Sejam $\mathbb{K} \subset \mathbb{L} = \mathbb{K}(u)$ uma extensão de corpos finita e separável de grau n e $f(x)$ o polinômio minimal de u sobre $\mathbb{K}$. Então*

$$D(1, u, \dots, u^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{L}:\mathbb{K}}(f'(u)) \neq 0 \quad (2.17)$$

em que $f'(x)$ denota a derivada do polinômio $f(x)$.

Demonstração. Sejam $x_1, \dots, x_n$ as raízes do polinômio minimal de u , $f(x)$, em uma extensão de $\mathbb{K}$. Considere $\sigma_1, \dots, \sigma_n$ os n distintos $\mathbb{K}$ -isomorfismos de $\mathbb{L}$ em um fecho algébrico Ω de $\mathbb{L}$. Assim, podemos tomar $\sigma_i(u) = x_i$, $1 \leq i \leq n$. Devido à proposição 2.3.3 e ao desenvolvimento do determinante de uma matriz de Vandermonde, temos:

$$D(1, x, \dots, x^{n-1}) = \det(\sigma_i(x^j))^2 = \det(x_i^j)^2 = \left(\prod_{i < j} (x_i - x_j)\right)^2 = c \prod_{i \neq j} (x_i - x_j) \quad (2.18)$$

em que $c = (-1)^{\frac{n(n-1)}{2}}$. Devido ao fato de $\mathbb{L}$ ser uma extensão separável sobre $\mathbb{K}$ então $x_i \neq x_j$, para $i \neq j$. Logo, já podemos afirmar que $D(1, x, \dots, x^{n-1}) \neq 0$. Voltando à equação 2.18, temos finalmente que

$$D(1, x, \dots, x^{n-1}) = c \prod_{i=1}^n \left(\prod_{j \neq i} (x_i - x_j)\right) = c \prod_{i=1}^n f'(x_i) = c N_{\mathbb{L}:\mathbb{K}}(f'(u)). \quad (2.19)$$

□

Definição 2.3.3. *Se u é um elemento primitivo da extensão finita $\mathbb{K} \subset \mathbb{L}$, com $[\mathbb{L} : \mathbb{K}] = n$, então o valor $D(1, u, \dots, u^{n-1})$ é chamado de **discriminante de u sobre $\mathbb{K}$** e é denotado por $D_{\mathbb{L}:\mathbb{K}}(u)$.*

Devido à proposição 2.3.4, o discriminante de qualquer conjugado de u também é igual a $D_{\mathbb{L}:\mathbb{K}}(u)$.

A proposição seguinte nos mostra que é possível caracterizar a base de uma extensão finita e separável de corpos por meio do seu discriminante.

Proposição 2.3.5. *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos separável e finita de grau n . Assim, $S = \{x_1, \dots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ se, e somente se, $D(x_1, \dots, x_n) \neq 0$.*

Demonstração. Seja u um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$, cuja existência é garantida pelo teorema do elemento primitivo (proposição 1.1.1). Assim, considere $\sigma_1, \dots, \sigma_n$ os n distintos $\mathbb{K}$ -isomorfismos de $\mathbb{L}$ em um fecho algébrico Ω de $\mathbb{L}$. Logo, variando $1 \leq i \leq n$, $\sigma_i(u)$ são todos distintos (pois $\mathbb{K} \subset \mathbb{L}$ é separável) e $D(1, u, \dots, u^{n-1}) \neq 0$ (proposição 2.3.4). Como $\{1, u, \dots, u^{n-1}\}$ é uma $\mathbb{K}$ -base para $\mathbb{L}$ então existem $b_{ij} \in \mathbb{K}$ tais que $x_i = \sum_{j=1}^n b_{ij} u^{j-1}$, $1 \leq i \leq n$. Assim, S é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ se, e somente se, $\det(b_{ij}) \neq 0$, o que ocorre se, e somente se, $D(x_1, \dots, x_n) \neq 0$, já que $D(x_1, \dots, x_n) = (\det(b_{ij}))^2 D(1, u, \dots, u^{n-1})$ (proposição 2.3.1). $\square$

Usando a proposição 2.3.5, mostraremos que toda base de $\mathbb{L}$ sobre $\mathbb{K}$ possui uma base dual. Antes de demonstrar esse fato, porém, precisamos do seguinte lema:

Lema 2.3.1. *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos separável finita de grau n e $\mathcal{B} = \{x_1, \dots, x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Para quaisquer $c_1, \dots, c_n \in \mathbb{K}$ existe um, e um só, $a \in \mathbb{L}$ tal que $Tr_{\mathbb{L}:\mathbb{K}}(x_i a) = c_i$.*

Demonstração. Considere o sistema de equações em X : $\sum_{j=1}^n Tr_{\mathbb{L}:\mathbb{K}}(x_i x_j) X_j = c_i$, $1 \leq i \leq n$. Tal sistema possui uma, e uma só, solução $a_1, \dots, a_n \in \mathbb{K}$, pois $\det(Tr_{\mathbb{L}:\mathbb{K}}(x_i x_j)) = D(x_1, \dots, x_n) \neq 0$ (proposição 2.3.5). Assim, $a = \sum_{k=1}^n a_k x_k$ é o único elemento de $\mathbb{L}$ que satisfaz $Tr_{\mathbb{L}:\mathbb{K}}(x_i a) = c_i$. $\square$

Proposição 2.3.6. *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos separável finita de grau n . Para cada base $\{x_1, \dots, x_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$ existe uma única base $\{y_1, \dots, y_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$ tal que, para quaisquer $1 \leq i \leq n$ e $1 \leq j \leq n$,*

$$Tr_{\mathbb{L}:\mathbb{K}}(x_i y_j) = \delta_{ij} = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases} \quad (\text{delta de Kronecker}). \quad (2.20)$$

Além disso, para todo $a \in \mathbb{L}$, vale que $a = \sum_{j=1}^n Tr_{\mathbb{L}:\mathbb{K}}(x_j a) y_j$.

Demonstração. Devido ao lema 2.3.1, para cada $1 \leq j \leq n$, existe um único $y_j \in \mathbb{L}$ tal que $Tr_{\mathbb{L}:\mathbb{K}}(x_i y_j) = 1$ se $i = j$ e $Tr_{\mathbb{L}:\mathbb{K}}(x_i y_j) = 0$ se $i \neq j$ ($1 \leq i \leq n$). Assim, o conjunto $\{y_1, \dots, y_n\} \subset \mathbb{L}$ satisfaz $Tr_{\mathbb{L}:\mathbb{K}}(x_i y_j) = \delta_{ij}$. Agora, para quaisquer $a_1, \dots, a_n \in \mathbb{K}$ tem-se que, para todo $1 \leq i \leq n$,

$$Tr_{\mathbb{L}:\mathbb{K}} \left(x_i \cdot \left(\sum_{j=1}^n a_j y_j \right) \right) = \sum_{j=1}^n a_j Tr_{\mathbb{L}:\mathbb{K}}(x_i y_j) = a_i. \quad (2.21)$$

Portanto, se $a = \sum_{j=1}^n a_j y_j$ então $a_j = \text{Tr}_{\mathbb{L}:\mathbb{K}}(x_j a)$, $1 \leq j \leq n$ (I). Então, se $a = 0$, segue que $a_j = 0$ para todo $1 \leq j \leq n$, donde segue que $\{y_1, \dots, y_n\}$ é linearmente independente sobre $\mathbb{K}$. Como $\mathbb{L}$ é um $\mathbb{K}$ -espaço vetorial, segue das propriedades da Álgebra Linear que $\{y_1, \dots, y_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Por fim, como todo $a \in \mathbb{L}$ pode ser escrito como $a = \sum_{j=1}^n a_j y_j$, com cada $a_j \in \mathbb{K}$ (já que $\{y_1, \dots, y_n\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$), então, de (II), segue que $a_j = \text{Tr}_{\mathbb{L}:\mathbb{K}}(x_j a)$, comprovando a igualdade $a = \sum_{j=1}^n \text{Tr}_{\mathbb{L}:\mathbb{K}}(x_j a) y_j$. $\square$

Nas condições da proposição 2.3.6, a base $\{y_1, \dots, y_n\}$ é chamada de **base dual** da base $\{x_1, \dots, x_n\}$.

Proposição 2.3.7. *Sejam A um anel (domínio) integralmente fechado, $\mathbb{K}$ seu corpo de frações, o qual tem característica zero, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e A' o fecho integral de A em $\mathbb{L}$. Então A' é um submódulo de um A -módulo livre finitamente gerado de posto n .*

Demonstração. Seja $\{x_1, \dots, x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Como cada x_i é algébrico sobre $\mathbb{K}$ (pois $\mathbb{K} \subset \mathbb{L}$ é uma extensão algébrica, já que é finita), então, para cada $i \in \{1, \dots, n\}$, existem $a_j \in A$, $0 \leq j \leq n$, $a_n \neq 0$, tais que $\sum_{j=0}^n a_j x_i^j = 0$ (I). Multiplicando (I) por a_n^{n-1} , vemos que $a_n x_i$ é integral sobre A , pois é raiz do polinômio mônico $p(t) = t^n + a_n^{n-1} \sum_{j=1}^n a_j x_i^j \in A[x]$. Seja $x'_i = a_n x_i$. Claramente, $\{x'_1, \dots, x'_n\} \subset A'$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. De acordo com a proposição 2.3.6, existe uma base dual $\{y_1, \dots, y_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$ tal que $\text{Tr}_{\mathbb{L}:\mathbb{K}}(x'_i y_j) = \delta_{ij}$. Considere $z \in A'$. Como $\{y_1, \dots, y_n\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$ então existem $b_1, \dots, b_n \in \mathbb{K}$ tais que $z = \sum_{j=1}^n b_j y_j$. Para todo $1 \leq i \leq n$, como $x'_i z \in A'$ então o corolário 2.2.2 garante que $\text{Tr}_{\mathbb{L}:\mathbb{K}}(x'_i z) \in A$ (já que A é integralmente fechado). Assim, $\text{Tr}_{\mathbb{L}:\mathbb{K}}(x'_i z) = \text{Tr}_{\mathbb{L}:\mathbb{K}}(\sum_{j=1}^n b_j x'_i y_j) = \sum_{j=1}^n b_j \text{Tr}_{\mathbb{L}:\mathbb{K}}(x'_i y_j) = \sum_{j=1}^n b_j \delta_{ij} = b_i \in A$, para todo $1 \leq i \leq n$. Portanto, $z \in A'$ implica que $z \in M = \sum_{j=1}^n A y_j$, ou seja, $A' \subset M$ é um submódulo do A -módulo livre e finitamente gerado M , de posto n . $\square$

Corolário 2.3.1. *Sejam A um anel integralmente fechado e um domínio principal, $\mathbb{K}$ seu corpo de frações, o qual tem característica zero, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e A' o fecho integral de A em $\mathbb{L}$. Então A' é um A -módulo livre finitamente gerado de posto n .*

Demonstração. Da proposição 2.3.7 já sabemos que A' é submódulo de um A -módulo livre e finitamente gerado M de posto n . Como A é principal, a proposição 1.1.2 nos garante que A' tem posto q menor ou igual a n . Além disso, como vimos na demonstração da proposição 2.3.7, A' contém uma base de $\mathbb{L}$ sobre $\mathbb{K}$ (com n elementos). Portanto, $q = n$. $\square$

2.4 Anéis Noetherianos e Domínios de Dedekind

Nesta seção, estudaremos os domínios de Dedekind. Esse conceito é importante, pois está relacionado com a fatoração de elementos e ideais no anel de inteiros de corpos de números (seção 2.5). Para iniciar esta seção, faremos um estudo sobre anéis noetherianos, os quais serão necessários na definição de domínio de Dedekind.

Se T é uma coleção de conjuntos, dizemos que um conjunto $E \in T$ é maximal em T se para todo $X \in T$ tal que $E \subset X$ tem-se $E = X$.

Definição 2.4.1. *Seja A um anel comutativo com unidade. Um A -módulo M é chamado **Noetheriano** se toda coleção não vazia de submódulos de M contém um elemento maximal.*

Proposição 2.4.1. *Sejam A um anel comutativo com unidade e M um A -módulo. São equivalentes:*

- (a) M é Noetheriano;
- (b) Se $(M_i)_{i \geq 0}$ é uma sequência crescente de submódulos de M , então existe $k \in \mathbb{Z}$ positivo tal que $M_k = M_i$ para todo $i \geq k$. Isto é, toda sequência crescente de submódulos de M é estacionária.
- (c) Todo submódulo de M é finitamente gerado.

Demonstração. (a) $\implies$ (c) : Seja N um A -submódulo de M e seja Λ o conjunto de todos os submódulos finitamente gerados de N , a qual é não vazia, pois $\{0\} \in \Lambda$. Por hipótese, Λ possui um elemento maximal F , o qual obviamente satisfaz $F \subset N$. Para qualquer $x \in N$, $F + (x)$ é um submódulo finitamente gerado por x e pelos elementos de uma base de F . Assim, $F + (x) \in \Lambda$. Como $F \subset F + (x)$ e F é maximal então $F = F + (x)$, donde segue que $x \in F$. Portanto, $N \subset F$. Logo, $N = F$ e, então, N é finitamente gerado. (c) $\implies$ (b) : Seja $(M_n)_{n \geq 0}$ uma sequência crescente de submódulos de M . Por isso, $E = \bigcup_{n \geq 0} M_n$ é um A -submódulo de M . Por hipótese, E é gerado por um conjunto $\{x_1, \dots, x_n\}$. Logo, para cada $1 \leq i \leq n$, existe um índice $n(i)$ tal que $x_i \in M_{n(i)}$. Seja n_0 o maior dentre esses n valores $n(i)$. Logo, $E \subset M_{n_0}$. Como $M_{n_0} \subset E$ então $M_{n_0} = E$. Daí, para todo $n \geq n_0$, tem-se $M_{n_0} \subset M_n \subset E$, donde vem que $M_n = M_{n_0}$ (pois $E = M_{n_0}$). Portanto, $(M_n)_{n \geq 0}$ é estacionária. (b) $\implies$ (a) : Considere T o conjunto dos A -submódulos de M . Suponha que existe $S \subset T$ que não contenha um elemento maximal. Logo, para todo elemento N de S , o conjunto de elementos de S que contém estritamente N é não vazio. Como S é não vazio, tome $N_0 \in S$. Pelo que foi observado, existe $N_1 \in S$ tal que $N_0 \subsetneq N_1$. Indutivamente, para todo N_i , $i \geq 1$, existe $N_{i+1} \in S$ tal que $N_i \subsetneq N_{i+1}$. Logo, tem-se a sequência $N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \dots \subsetneq N_i \subsetneq N_{i+1} \subsetneq \dots$, a qual é uma sequência de submódulos estritamente crescente de submódulos de M (ou seja, não estacionária), contrariando o item (b). Logo, todo $S \subset T$ possui um elemento maximal. $\square$

Definição 2.4.2. Um anel com unidade A é dito **anel Noetheriano** se, como um A -módulo, ele for Noetheriano. Neste caso, note que os A -submódulos de A são seus ideais.

Corolário 2.4.1. Todo domínio principal A é Noetheriano. Consequentemente, toda família não vazia de ideais possui um elemento maximal.

Demonstração. Seja A um A -módulo. Neste caso, os submódulos de A são exatamente os ideais de A . Pelo fato de A ser um domínio principal, segue que todo ideal de A é principal, ou seja, é finitamente gerado. Logo, todo submódulo de M é finitamente gerado. Como (c) implica (a) na proposição 2.4.1, então A é Noetheriano, donde segue (da definição) que toda família não vazia de ideais de A possui um elemento maximal. $\square$

A proposição a seguir enumera alguns resultados sobre A -módulos Noetherianos:

Proposição 2.4.2. ([30], seção 3.1) Seja A um anel comutativo com unidade.

- (a) Se M é um A -módulo e M' é um submódulo de M , então M é Noetheriano se, e somente se, M' e M/M' são Noetherianos.
- (b) Se $M_1, \dots, M_n$ são A -módulos Noetherianos então o A -módulo $\prod_{i=1}^n M_i$ é Noetheriano.
- (c) Se A é um anel Noetheriano e M é um A -módulo finitamente gerado então M é Noetheriano.

Enfim, introduzamos o conceito de domínio de Dedekind:

Definição 2.4.3. Um domínio A é chamado **domínio de Dedekind** (ou anel de Dedekind) se:

- (a) A for anel Noetheriano;
- (b) A for integralmente fechado;
- (c) todo ideal primo não zero de A é maximal.

Sabe-se que todo ideal maximal é primo em um anel comutativo. Nesta definição, exigimos que valha também a recíproca desta proposição para os domínios de Dedekind.

Exemplo 2.4.1. Todo domínio principal é domínio de Dedekind. De fato, seja A um domínio principal. Pelo corolário 2.4.1, A é Noetheriano. Pelo exemplo 2.1.4, A é integralmente fechado. Por fim, verifiquemos que vale o item (c) da definição de domínio de Dedekind: seja (p) um ideal primo de A . Então p é irredutível em A . Com efeito, se $p = ab$ então $ab \in (p)$ e, daí, $a \in (p)$ ou $b \in (p)$ (já que o ideal é primo). Sem perda de generalidade, suponhamos que $a \in (p)$. Então $a = qp$, $q \in A$. Logo, $p = qbp$ e, daí, $qb = 1$, ou seja, b é invertível em A . Suponha que existe um ideal $N = (n)$ contendo (p) . Assim, $p = rn$, com $r \in A$. Como p é irredutível então r é invertível em

A ou n é invertível em A . No primeiro caso, tem-se que $(n) = (p)$ e, no segundo caso, tem-se que $(n) = A$. Logo, (p) é maximal.

Exemplo 2.4.2. Como $\mathbb{Z}$ é domínio principal então, do exemplo anterior, segue que $\mathbb{Z}$ é domínio de Dedekind.

Lema 2.4.1. Sejam A um anel Noetheriano integralmente fechado, $\mathbb{K}$ seu corpo de frações, de característica zero, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e A' o fecho integral de A em $\mathbb{L}$. Então A' é um A -módulo finitamente gerado e A' é um anel Noetheriano.

Demonstração. Devido à proposição 2.3.7, A' é submódulo de um A -módulo finitamente gerado de posto $n = [\mathbb{L} : \mathbb{K}]$. Pela proposição 2.4.2, A' é um A -módulo finitamente gerado e é um A -módulo Noetheriano. Agora, seja I um ideal de A' . Mostremos que I é um A -submódulo de A' . Considere $a \in A$ e $x, y \in I$. Como $A \subset A'$, segue que $a \in A'$. Pelo fato de I ser um ideal de A' , temos $ax + y \in I$. Portanto, I é um A -submódulo de A' . Seja S uma coleção não vazia de ideais de A' . Pelo que foi mostrado acima, S é uma coleção de A -submódulos de A' e, então, S contém um elemento maximal (já que o A -módulo A' é Noetheriano). Logo, toda coleção de ideais de A' possui um elemento maximal, o que implica que A' é um anel Noetheriano. $\square$

Lema 2.4.2. Se A é um anel, P é um ideal primo de A e B é um subanel de A então $P \cap B$ é um ideal primo de B .

Demonstração. Considere os homomorfismos $\phi : B \rightarrow A$ dada por $\phi(x) = x$, para todo $x \in B$, e $\psi : A \rightarrow A/P$ tal que $\psi(x) = x + P$, para todo $x \in A$. Então, $\eta = \psi \circ \phi : B \rightarrow A/P$ também é um homomorfismo cujo núcleo é $P \cap B$. Pelo Teorema do Homomorfismo de Anéis, $B/(P \cap B)$ é isomorfo a um subanel de A/P . Como A/P é um domínio então $B/(P \cap B)$ é um domínio. Logo, tem-se que $P \cap B$ é um ideal primo de B . $\square$

Proposição 2.4.3. Sejam A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, de característica zero, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e A' o fecho integral de A em $\mathbb{L}$. Então A' é um anel de Dedekind e é um A -módulo finitamente gerado.

Demonstração. Devido ao lema 2.4.1, A' é um A -módulo finitamente gerado e é um anel Noetheriano. Seja B o fecho integral de A' sobre A' , ou seja, o anel formado pelos elementos do corpo de frações de A' (contido em $\mathbb{L}$) que são integrais sobre A' . Como B é integral sobre A' e A' é integral sobre A , segue da proposição 2.1.3 que B é integral sobre A . Como A' é o maior anel de $\mathbb{L}$ que contém todos os

elementos integrais sobre A , então $B = A'$. Logo, A' é integralmente fechado. Por fim, vamos mostrar que todo ideal primo não zero P' de A' é maximal. Para isso, seja $x \in P'$, $x \neq 0$. Como $x \in A'$ então x é integral sobre A . Portanto, considere $f(t) = t^n + a_{n-1}t^{n-1} + \dots + a_1t + a_0 \in A[t]$ um polinômio de grau mínimo tal que $f(x) = 0$. Devido a essa minimalidade do grau de $f(t)$, podemos garantir que $a_0 \neq 0$ (senão, poderíamos tomar um polinômio de grau $n - 1 < n$ sobre $A[x]$ tendo x como raiz). Como $a_0 = -\sum_{i=1}^n a_i x^i$ então $a_0 \in xA' \cap A \subset P' \cap A$, donde concluímos que $P' \cap A \neq \{0\}$. Devido ao lema 2.4.2, $P' \cap A$ é um ideal primo de A , donde segue que $P' \cap A$ é maximal (já que A é domínio de Dedekind). Assim, $A/(P' \cap A)$ é um corpo. Considere o homomorfismo $\phi : A \rightarrow A'/P'$ dado por $\phi(x) = x + P'$, para todo $x \in A$. Assim, $\ker(\phi) = P' \cap A$. Pelo Teorema do Homomorfismo de Anéis, $A/(P' \cap A) \simeq \phi(A)$. Como $\phi(A)$ é um subanel de A'/P' então $A/(P' \cap A)$ pode ser considerado um subanel de A'/P' . Afirmamos que todo ideal maximal de A'/P' é integral sobre $\phi(A) \simeq A/(P' \cap A)$. De fato, como A' é integral sobre A então, para todo $\alpha + P'$, $\alpha \in A'$, existe $p(t) \in A[t]$ mônico tal que $p(\alpha) = 0$. Considere $P(t)$ o polinômio sobre $\phi(A)$ construído a partir de $p(t)$, trocando cada um dos coeficientes deste último pela imagem de sua classe módulo $P' \cap A$. Assim, $P(\alpha + P') = 0$. Logo, todo elemento de A'/P' é integral sobre $A/(P' \cap A)$. Finalmente, devido à proposição 2.1.4, segue que A'/P' é corpo. Portanto, P' é um ideal maximal. $\square$

Antes de prosseguirmos, precisamos de alguns conceitos envolvendo ideais e da definição de ideal fracionário. Inicialmente, se I e J são ideais de um anel A , definimos o **produto dos ideais I e J** como sendo o conjunto $IJ = \{\sum_{FINITA} a_i b_i : a_i \in I, b_i \in J\}$, ou seja, o conjunto de todas as somas com finitos termos de produtos de elementos de I por elementos de J . O conjunto IJ também é um ideal de A . Além disso, $IJ \subset I \cap J$ ($I \cap J$ também é um ideal de A). Se o anel A é principal, IJ é gerado pelo produto dos geradores de I e de J , enquanto $I \cap J$ é o mínimo múltiplo comum desses geradores.

Seja S o conjunto dos ideais de um anel comutativo com unidade A . Assim, uma operação $r : S \times S \rightarrow S$ dada por $r(I, J) = IJ$, para quaisquer $I, J \in S$ é associativa (isto é, $(IJ)K = I(JK)$, para quaisquer $I, J, K \in S$) e comutativa (isto é, $IJ = JI$). Como $AI = I = IA$, para qualquer $I \in S$, então A é um elemento neutro da operação r . Devido a essas propriedades, podemos dizer que S com a operação r (multiplicação de ideais) é um monoide comutativo (veja seção 1, capítulo I, [22]).

Se E é um A -módulo, F é um submódulo de E e I é um ideal de A então definimos, analogamente, o produto $IE = \{\sum_{FINITA} a_i e_i : a_i \in I, e_i \in E\}$, o qual é um submódulo de E .

Lema 2.4.3. *Sejam A um anel comutativo com unidade e P um ideal primo de A . Se P contém um produto de ideais $I_1 \dots I_n$ de A então existe $k \in \{1, \dots, n\}$ tal que $I_k \subset P$.*

Demonstração. Suponha que $I_k \not\subset P$ para qualquer $k \in \{1, \dots, n\}$. Logo, existe $a_k \in I_k - P$, para qualquer k . Como P é primo então $\prod_{i=1}^n a_i \notin P$ (senão, obrigatoriamente algum a_k deveria pertencer a P). Porém, $\prod_{i=1}^n a_i \in I_1 \dots I_n \subset P$, o que é um absurdo. $\square$

Lema 2.4.4. *Em um anel Noetheriano A , todo ideal contém um produto de ideais primos. Se A for ainda um domínio então todo ideal não zero de A contém um produto de ideais primos não zeros.*

Demonstração. Seja Φ o conjunto dos ideais de A não zeros que não contêm produto de ideais primos não zeros. Para mostrar a segunda parte da afirmação deste lema, precisamos mostrar que $\Phi = \emptyset$. Suponhamos que $\Phi \neq \emptyset$. Como A é Noetheriano, Φ possui um elemento maximal B . Da definição do conjunto Φ , segue que B não é primo. Logo, existem $x, y \in A - B$ tais que $xy \in B$. Note que $B \subsetneq B + xA$ e $B \subsetneq B + yA$ (pois $x, y \notin B$ e $1 \in A$). Devido à maximalidade de B , então $B + xA$ e $B + yA$ não pertencem a Φ . Logo, esses conjuntos possuem um produto de ideais primos não zeros, digamos: $P_1 \dots P_n \subset B + xA$ e $Q_1 \dots Q_m \subset B + yA$ (P_i, Q_i ideais primos de A). Como $xy \in B$ então para qualquer $\alpha \in (B + xA)(B + yA)$ conclui-se que $\alpha \in B$. Daí, $P_1 \dots P_n Q_1 \dots Q_m \subset (B + xA)(B + yA) \subset B$, o que é um absurdo (pois $B \in \Phi$). Logo, $\Phi = \emptyset$. A primeira parte da afirmação segue de maneira análoga. $\square$

Definição 2.4.4. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Um **ideal fracionário** de A é um A -submódulo I de $\mathbb{K}$ tal que $dI \subset A$ para algum $d \in A$, $d \neq 0$.*

A definição acima significa que todos os elementos de um ideal fracionário de A possuem um “denominador comum” $d \in A$. Observe que todo ideal (usual) de A é um ideal fracionário. De fato, tome $d = 1 \in A$ na definição de ideal fracionário. Não confunda ideal com ideal fracionário. O ideal usual será simplesmente chamado de ideal, como fizemos até o momento neste texto. Caso seja necessário esclarecer a distinção, podemos chamar os ideais usuais de *ideais integrais*.

Proposição 2.4.4. *Mantidas as notações anteriores, vale o seguinte:*

- (a) *Todo A -submódulo I finitamente gerado de $\mathbb{K}$ é um ideal fracionário.*
- (b) *Todo ideal fracionário I é um A -módulo finitamente gerado se A for um anel Noetheriano.*

Demonstração. Para o item (a), seja $\{x_1, \dots, x_n\}$ um conjunto de geradores de I sobre A . Como cada $x_i \in \mathbb{K}$ então $x_i = a_i/b_i$ ($a_i, b_i \in A$, $b_i \neq 0$). Tome $d = \prod_{i=1}^n b_i$. Então $dI \subset A$. O item (b) segue da proposição 2.4.1. $\square$

Sejam I e J dois ideais fracionários de um anel A comutativo com unidade. O produto IJ é definido como sendo o conjunto de todas as somas com finitas parcelas de produtos $a_i b_i$, com $a_i \in I$ e $b_i \in J$ (análogo ao que foi feito para produto de ideais). Assim, IJ , $I \cap J$ e $I + J$ são ideais fracionários de A . Da mesma forma como foi visto para ideais, também o conjunto dos ideais fracionários é um monoide comutativo sobre a operação de multiplicação de ideais fracionários. O elemento neutro deste monoide é o próprio anel A .

Voltemos agora aos nossos estudos sobre domínios de Dedekind.

Proposição 2.4.5. *Seja A um domínio de Dedekind que não é um corpo. Então todo ideal maximal de A é invertível no monoide dos ideais fracionários de A .*

Demonstração. Seja M um ideal maximal de A . Como A não é um corpo, então M é não zero (senão $A/M = A$ seria um corpo). Considere $M' = \{x \in \mathbb{K} : xM \subset A\}$, o qual é um A -submódulo de $\mathbb{K}$, o corpo de frações de A . Pela definição de M' , note que para qualquer $y \in M$, $y \neq 0$, tem-se $yM' \subset A$, ou seja, $MM' \subset A$. Logo, M' é um ideal fracionário de A . Para comprovar a tese, basta mostrar que M e M' são inversos um do outro, ou seja, que $MM' = A$. Veja que $A \subset M'$, pois, para todo $a \in A$, tem-se que $aM \subset A$ (já que M é um ideal de A). Então $M = AM \subset M'M$. Como M é maximal e $M \subset M'M \subset A$ então: $M = M'M$ (I) ou $M'M = A$ (II). Suponha que valha (I). Neste caso, se $x \in M'$ então $xM \subset M$, $x^2M \subset xM \subset M$ e, sucessivamente, $x^n M \subset M$ para qualquer n natural. Logo, para qualquer $d \in M$ existe $m_n \in M$ tal que $x^n d = m_n \in M$. Assim, $dA[x] \subset A$ e $A[x]$ é um ideal fracionário de A . Claramente, como A é Noetheriano então $A[x]$ é um A -módulo finitamente gerado. A proposição 2.1.1 acarreta que x é integral sobre A . Devido ao fato de A ser algebricamente fechado (pois A é domínio de Dedekind) então $x \in A$. Portanto, $M' \subset A$ e, assim, $M' = A$. Agora, seja $a \in M$ não nulo. Devido ao lema 2.4.4, o ideal aA contém um produto de ideais primos $P_1 \dots P_n$ não zeros. Assumamos que n seja mínimo. Então $P_1 \dots P_n \subset aA \subset M$ implica que $P_k \subset M$ para algum k (lema 2.4.3). Como P_k é primo e A é domínio de Dedekind então P_k é maximal. Logo, $M = P_k$. Seja $B = P_1 \dots P_{i-1} P_{i+1} \dots P_n$. Então $MB \subset aA$ e $B \not\subset aA$, já que n é o menor possível. Por isso, existe $b \in B$ tal que $b \notin aA$. Como $MB \subset aA$ e $bM \subset aA$ então $ba^{-1}M \subset A$. De acordo com a definição de M' , $ba^{-1} \in M'$. Porém, $b \notin aA$ e $ba^{-1} \notin A$, o que contraria o fato de M' ser igual a A . Portanto, o item (I) é falso e, daí, vale (II), comprovando a tese. $\square$

Seja M um ideal maximal (primo) de um domínio de Dedekind A que possui um inverso M' no monoide dos ideais fracionários deste domínio. Denotaremos M' por M^{-1} . Assim, $MM^{-1} = A$. Se $n \in \mathbb{Z}$ for negativo, então definimos $M^n = (M^{-1})^{-n}$.

Lema 2.4.5. *Todo ideal próprio de um anel está contido em algum ideal maximal.*

Demonstração. Sejam A um anel e Λ a coleção dos ideais $I \subsetneq A$. Considere Λ' um subconjunto totalmente ordenado qualquer de Λ . Tome $J = \bigcup_{I \in \Lambda'} I$. Mostremos que J é um ideal de A . Se $x, y \in J$ e $a \in A$ então $x \in I_x \in \Lambda'$ e $y \in I_y \in \Lambda'$. Como Λ' é totalmente ordenado, podemos supor $I_2 \subset I_1$, donde segue que $ax + y \in I_1 \subset J$. Além disso, $J \neq A$, pois $1 \notin J$ e $I \subset J$ para todo $I \in \Lambda'$. Logo, Λ' tem uma cota superior. Pelo lema de Zorn (lema 1.1.1), Λ tem um elemento maximal. $\square$

Teorema 2.4.1. *Seja A um domínio de Dedekind. Então:*

(a) *Todo ideal fracionário não zero de A pode ser expresso de maneira única como produto de ideais primos não zeros de A . Assim, para todo ideal fracionário I não zero de A , existem ideais primos não zeros $P_1, \dots, P_m$ de A tais que*

$$I = \prod_{i=1}^m P_i^{n_i}, \quad n_i \in \mathbb{Z}, \quad \forall i \quad (2.22)$$

de maneira única.

(b) *Os ideais fracionários não zeros de A formam um grupo multiplicativo.*

Demonstração. (a) Dividiremos essa demonstração em três partes. *Parte I:* Mostremos que todo ideal (integral) de A é produto de primos. De fato, seja Φ a coleção de ideais não zeros de A que não são produtos de ideais primos e suponha $\Phi \neq \emptyset$. Como A é Noetheriano então Φ possui um elemento maximal J . Então $J \subsetneq A$, já que, por convenção, A é o produto da coleção vazia de ideais primos e, portanto, não pertence a Φ . Pelo lema 2.4.5, todo ideal próprio de A está contido em algum ideal maximal e, então, $J \subset P$, em que P é um ideal maximal (e primo) de A . Se S é a coleção dos ideais próprios de A que contêm J então P é um elemento maximal de S . Seja P' o ideal fracionário inverso de P (garantido pela proposição 2.4.5), ou seja, tal que $P'P = A$. Assim, $J \subset P$ implica que $JP' \subset PP' = A$ e, como $A \subset P'$, então $J \subsetneq JP'$ (de fato, se $J = JP'$ e $x \in P'$ teríamos $x^n J \subset J$ para todo $n > 0$, ou seja, x integral sobre A e x integral em A - análogo à demonstração da proposição 2.4.5). Devido à maximalidade de J em Φ , temos $JP' \notin \Phi$. Logo, $JP' = P_1 \dots P_n$ é um produto de ideais primos e, multiplicando essa expressão por P , $J = PP_1 \dots P_n$, o que contraria o fato de J pertencer a Φ . Logo, $\Phi = \emptyset$. *Parte II:* Todo ideal fracionário é produto de ideais primos. De fato, seja B um ideal fracionário de A . Por definição, existe $d \in A - \{0\}$ tal que $dB \subset A$. Assim, dB é um ideal (integral) de A . Se $\mathbb{K}$ é o corpo de frações de A , como $d \neq 0$ então $1/d \in \mathbb{K}$. Sejam I o ideal gerado por d em A e o ideal fracionário $J = \{x \in \mathbb{K} : xI \subset A\}$ (como na demonstração da proposição 2.4.5). Então $IJ \subset A$. Logo, como $1/d \in J$, então, para todo $a \in A$, $a = ad(1/d) \in IJ$.

Logo, $A = IJ$ e, portanto, J é o inverso de I . Por fim, como $1/d \in J$, verifica-se que $B = (dB)J$. Como dB e I são ideais, a igualdade $B = (dB)J = (dB)I^{-1}$ mostra que B é produto de primos (com expoentes não necessariamente todos positivos). *Parte III: Unicidade.* Suponha que um ideal seja fatorado em produtos de ideais primos distintos P_i de duas maneiras como $\prod_{i=1}^r P_i^{n_i} = \prod_{i=1}^r P_i^{m_i}$, permitindo que existam n_i e m_j iguais a zero. Logo, $A = \prod_{i=1}^r P_i^{n_i - m_i}$ e, separando os expoentes positivos dos negativos e reindexando primos e potências, obtemos $Q_1^{e_1} \dots Q_s^{e_s} = Q_{s+1}^{e_{s+1}} \dots Q_t^{e_{t+1}}$, em que cada Q_i é um dos primos P_j e $e_i > 0$. Então $Q_{s+1}^{e_{s+1}} \dots Q_t^{e_{t+1}} \subset Q_1$. Pelo lema 2.4.3, sem perda de generalidade, podemos supor $Q_{s+1} \subset Q_1$. Como Q_{s+1} é ideal maximal então $Q_{s+1} = Q_1$, o que é um absurdo de termos suposto que os primos são distintos. Isso finaliza a demonstração do item (a).
 (b) Já sabemos que o conjunto Λ dos ideais fracionários não zeros de A é um monoide comutativo (ou seja, associativo, tem elemento neutro e é comutativo). Como todo ideal fracionário de A é da forma $I = \prod_{i=1}^r P_i^{n_i}$ então $J = \prod_{i=1}^r P_i^{-n_i}$ é seu inverso, comprovando que Λ é um grupo multiplicativo. $\square$

Note, do teorema anterior, que o grupo dos ideais fracionários não zeros de A é um grupo abeliano livre gerado pelos ideais primos de A .

Sejam A um domínio de Dedekind e I e J dois ideais fracionários não zeros de A . Pelo teorema anterior, I e J podem ser escritos, de maneira única, como produto de ideais primos. Suponha que $I = \prod_{i=1}^r P_i^{n_P(i)}$ e $J = \prod_{i=1}^s Q_i^{n_Q(i)}$, em que P_i e Q_j são primos, com $n_P(i), n_Q(i) \in \mathbb{Z}$ não nulos. Então, suponha que P seja um primo da fatoração de I e de J nas seguintes fórmulas 2.23 e 2.25. Assim, verifica-se que valem as seguintes fórmulas (veja [30], seção 3.4):

$$n_P(IJ) = n_P(I) + n_P(J). \quad (2.23)$$

$$I \subset A \iff n_P(I) \geq 0, \text{ para todo primo } P \text{ na fatoração de } I. \quad (2.24)$$

$$I \subset J \iff n_P(I) \geq n_P(J). \quad (2.25)$$

Por fim, estabeleçamos mais alguns resultados sobre divisibilidade entre ideais:

Definição 2.4.5. *Sejam I e J ideais fracionários de um domínio A . Dizemos que I divide J quando existe um ideal integral Q de A tal que $J = IQ$. Notação: $I \mid J$.*

Note que se $I \mid J$ então $J \subset I$. De fato, se $I \mid J$ então existe um ideal integral Q de A tal que $J = IQ$. Daí, $J = IQ \subset IA = I$.

Definição 2.4.6. Se A é um domínio e I é um ideal integral de A , dizemos que I é **irredutível** se qualquer produto $I = JJ'$, J e J' ideais de A , acarretar $I = J$ ou $I = J'$.

Proposição 2.4.6. Se A é um domínio de Dedekind, um ideal não zero de A é irredutível se, e somente se, é primo.

Demonstração. Por um lado, seja P um ideal primo e suponha que ele não é irredutível. Então $P = JJ'$, em que J e J' ideais de A são ideais diferentes de P . Como $J \mid P$ e $J' \mid P$ então $P \subsetneq J$ e $P \subsetneq J'$. Portanto, existem $a \in J$ e $a' \in J'$ que não estão em P . Porém, $aa' \in JJ' = P$, o que contraria o fato de P ser primo. Isso prova que todo ideal primo é irredutível. Por outro lado, seja J um ideal irredutível de A . Assim, J pode ser escrito como produto de ideais primos. Por ser irredutível, $J = P$, em que P é o único ideal primo de sua fatoração. Logo, todo ideal não zero irredutível é primo. $\square$

Proposição 2.4.7. Se P é um ideal primo em um anel de Dedekind A e se I e J são ideais de A tais que $P \mid IJ$ então $P \mid I$ ou $P \mid J$.

Demonstração. Por hipótese, existe um ideal Q de A tal que $IJ = PQ$. Pela unicidade da decomposição de ideais primos, segue que $P \mid I$ ou $P \mid J$. $\square$

Proposição 2.4.8. Sejam I e J ideais fracionários não zeros em um domínio de Dedekind A . Então, $I \mid J$ se, e somente se, $J \subset I$.

Demonstração. Já vimos que $I \mid J$ implica $J \subset I$. Então, suponha $J \subset I$. Como o conjunto dos ideais fracionários forma um grupo multiplicativo, existe um ideal fracionário I^{-1} de A . Assim, $J I^{-1} \subset I I^{-1} = A$, donde vem que $J I^{-1}$ é um ideal integral de A que satisfaz $(J I^{-1}) I = J$, mostrando que $I \mid J$. $\square$

Proposição 2.4.9. Se I é um ideal não zero de um domínio de Dedekind A então existe uma quantidade finita de ideais de A dividindo I .

Demonstração. Fatore I em produto de ideais primos de A : $I = \prod_{i=1}^m P_i^{e_i}$. Logo, os únicos ideais que dividem I são os da forma $\prod_{i=1}^m P_i^{f_i}$, em que $0 \leq f_i \leq e_i$, para todo $i \in \{1, \dots, m\}$. $\square$

2.5 Corpos de números e anéis de inteiros

Nesta seção, nos dedicaremos a estudar os elementos integrais sobre $\mathbb{Z}$ de extensões finitas de $\mathbb{Q}$.

Definição 2.5.1. Se $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$ então $\mathbb{K}$ é chamado de **corpo de números algébricos**, ou simplesmente de **corpo de números**.

Na definição acima, o termo “números algébricos” é justificado pelo fato de que toda extensão de corpos finita é algébrica. Note que todo corpo de números tem característica zero, pois é uma extensão do corpo dos números racionais.

Se $\mathbb{K}$ é um corpo de números, chamamos de **grau de $\mathbb{K}$** ao grau da extensão $[\mathbb{K} : \mathbb{Q}]$. Em particular, um corpo de números de grau 2 é chamado de **corpo quadrático** e um corpo de números de grau 3 é chamado de **corpo cúbico** (ou, simplesmente, de **cúbica**).

Por definição, todo corpo de números $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$. Além disso, $\mathbb{Q} \subset \mathbb{K}$ também é uma extensão separável, pois $\mathbb{Q}$ tem característica zero. Então, como consequência à proposição 1.1.1, vale o **Teorema do Elemento Primitivo** para corpos de números:

Proposição 2.5.1. Se $\mathbb{K}$ é um corpo de números então existe $u \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(u)$. □

Definição 2.5.2. Os elementos de um corpo de números $\mathbb{K}$ que são integrais sobre $\mathbb{Z}$ são chamados de **inteiros algébricos** de $\mathbb{K}$, ou simplesmente, **inteiros** de $\mathbb{K}$.

No texto, para evitar confundir os inteiros algébricos com os elementos de $\mathbb{Z}$, é comum chamarmos os elementos de $\mathbb{Z}$ de inteiros racionais quando há risco de confusão. Como já vimos no exemplo 2.1.4, se $x \in \mathbb{Q}$ é um inteiro algébrico então $x \in \mathbb{Z}$.

Pelo corolário 2.1.2, o conjunto dos elementos integrais de $\mathbb{K}$ sobre $\mathbb{Z}$ forma um anel A contendo $\mathbb{Z}$. Isso nos permite dar a seguinte definição:

Definição 2.5.3. Se $\mathbb{K}$ é um corpo de números, chamamos de **anel de inteiros algébricos de $\mathbb{K}$** , ou simplesmente de **anel de inteiros de $\mathbb{K}$** , ao conjunto dos elementos inteiros de $\mathbb{K}$, o qual denotamos por $\mathcal{O}_{\mathbb{K}}$.

Note que, se $\mathbb{K}$ é um corpo de números, então $\mathbb{Z} \subset \mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$. O resultado a seguir é importante, pois nos garante que todo anel de inteiros é um $\mathbb{Z}$ -módulo livre com posto igual ao grau do corpo de números.

Proposição 2.5.2. Se $\mathbb{K}$ é um corpo de números de grau n então o seu anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo livre de posto n .

Demonstração. Como $\mathbb{Z}$ é integralmente fechado (exemplo 2.1.4), é um domínio principal e como $A' = \mathcal{O}_{\mathbb{K}}$ é o fecho integral de $\mathbb{Z}$ em $\mathbb{K}$ então o corolário 2.3.1 nos garante que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo livre finitamente gerado de posto igual ao grau da extensão $[\mathbb{K} : \mathbb{Q}]$. □

Devido à proposição anterior, podemos fazer a seguinte definição:

Definição 2.5.4. Se $\mathbb{K}$ é um corpo de números então qualquer base do $\mathbb{Z}$ -módulo livre $\mathcal{O}_{\mathbb{K}}$ é chamada de **base integral** de $\mathbb{K}$.

Note que se $\mathcal{B} = \{x_1, \dots, x_n\}$ é uma base integral de $\mathbb{K}$ então $\mathcal{B}$ também é uma base para o espaço vetorial $\mathbb{K}$ sobre $\mathbb{Q}$. De fato, sendo $a_i/b_i \in \mathbb{Q}$ ($a_i \in \mathbb{Z}, 0 \neq b_i \in \mathbb{Z}$),

$$\sum_{i=1}^n \frac{a_i}{b_i} x_i = 0 \implies \sum_{i=1}^n \left(\prod_{j=1}^n b_j \right) a_i x_i = 0 \implies \left(\prod_{j=1}^n b_j \right) a_i = 0, \quad 1 \leq i \leq n \implies a_i = 0, \quad 1 \leq i \leq n. \quad (2.26)$$

Disso, segue que $\mathcal{B} \subset \mathbb{K}$ é linearmente independente sobre $\mathbb{Q}$. Como esse conjunto possui $[\mathbb{K} : \mathbb{Q}]$ elementos, então $\mathcal{B}$ é uma $\mathbb{Q}$ -base para $\mathbb{K}$.

Corolário 2.5.1. Seja $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros do corpo de números $\mathbb{K}$ de grau n . Todo ideal não zero I de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo livre finitamente gerado de posto n .

Demonstração. O ideal I é um $\mathbb{Z}$ -submódulo de $\mathcal{O}_{\mathbb{K}}$. Como $\mathbb{Z}$ é principal, segue da proposição 1.1.2 que I é livre finitamente gerado de posto $q \leq n$. Se $\{x_1, \dots, x_n\}$ é uma base integral de $\mathbb{K}$ e $0 \neq a \in I$ então $\{ax_1, \dots, ax_n\}$ é um conjunto linearmente independente de I . Portanto, $q = n$. $\square$

A seguir, caracterizamos os elementos invertíveis de um anel de inteiros por meio da norma:

Proposição 2.5.3. Seja $\mathbb{K}$ um corpo de números. Um inteiro algébrico $x \in \mathcal{O}_{\mathbb{K}}$ é invertível neste anel se, e somente se, $|N_{\mathbb{K}:\mathbb{Q}}(x)| = 1$.

Demonstração. Por um lado, se $x \in \mathcal{O}_{\mathbb{K}}$ é invertível então existe $x' \in \mathcal{O}_{\mathbb{K}}$ tal que $xx' = 1$. Tomando a norma destes elementos e utilizando uma das propriedades da proposição 2.2.2, temos $N(x)N(x') = N(xx') = N(1) = 1^{[\mathbb{K}:\mathbb{Q}]} = 1$. Devido ao corolário 2.2.2, $N(x) \in \mathbb{Z}$. Portanto, $|N(x)| = 1$.

Por outro lado, suponha que $|N(x)| = 1$ e considere x' o produto de todos os conjugados de x , distintos de x . Então, da proposição 2.2.3, $N(x) = xx' = 1$. Como vimos na demonstração da proposição 2.2.5, todo conjugado de um inteiro algébrico x é um inteiro algébrico. Portanto, x' é inteiro algébrico. Logo, x' é o inverso de x no anel de inteiros. $\square$

A proposição seguinte garante que o anel de inteiros de um corpo de números é um domínio de Dedekind. Uma das vantagens desse fato é que o teorema 2.4.1 vale para anéis de inteiros.

Proposição 2.5.4. O anel de inteiros de um corpo de números é um domínio de Dedekind. Em particular, esse anel é Noetheriano.

Demonstração. Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Como $\mathbb{Z}$ é um domínio de Dedekind (exemplo 2.4.2) e $\mathcal{O}_{\mathbb{K}}$ é o fecho integral de $\mathbb{Z}$ em $\mathbb{K}$ então segue da proposição 2.4.3 que $\mathcal{O}_{\mathbb{K}}$ é um domínio de Dedekind. Por definição de domínio de Dedekind, segue também que esse anel é Noetheriano. $\square$

Nesse momento, poderíamos estar nos perguntando se $\mathcal{O}_{\mathbb{K}}$ tem a mesma estrutura de $\mathbb{Z}$ e todos os benefícios deste último. Até agora, parece que sim. A última proposição é um exemplo disso. Porém, uma desvantagem de $\mathcal{O}_{\mathbb{K}}$ em relação a $\mathbb{Z}$ é que, ao contrário do anel dos inteiros racionais, nem sempre o anel de inteiros do corpo de números $\mathbb{K}$ é principal, como exemplificaremos a seguir:

Exemplo 2.5.1. *Mostraremos na proposição 3.1.2 da seção 3.1 que o anel de inteiros do corpo de números $\mathbb{Q}(\sqrt{-5})$ é $A = \mathbb{Z}[\sqrt{-5}]$. No anel A , observe que $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$. A norma de cada um dos fatores da igualdade acima é dada da seguinte forma: $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, $N(2) = 4$ e $N(3) = 9$ (de fato, verifique que $N(a + b\sqrt{-5}) = a^2 + 5b^2$, para qualquer $a, b \in \mathbb{Z}$). Utilizando a norma, verifica-se que $1 + \sqrt{-5}$ não tem divisor não trivial em A , pois não existe solução inteira para as equações diofantinas $a^2 + 5b^2 = 2$ e $a^2 + 5b^2 = 3$. Logo, se A fosse principal, o elemento irredutível $1 + \sqrt{-5}$ de A seria primo e deveria dividir 2 ou 3. Suponha, sem perda de generalidade, que existe $x \in A$ tal que $2 = x(1 + \sqrt{-5})$. Tomando a norma na igualdade anterior, vemos que $N(2) = 4 = N(x) \cdot 6$, com $N(x) \in \mathbb{Z}$. Isso é um absurdo, pois 6 não divide 4. Logo, A não é principal.*

Outro fato interessante é que se $\mathbb{K}$ é um corpo de números, então todo elemento não nulo de $\mathcal{O}_{\mathbb{K}}$, que não é uma unidade, é produto de elementos irredutíveis (consulte [28], capítulo 5, (O)). Porém, essa escrita pode não ser de maneira única, o que mostra outra diferença entre $\mathcal{O}_{\mathbb{K}}$ e $\mathbb{Z}$.

A seguir, faremos algumas considerações sobre os discriminantes em anéis de inteiros.

Proposição 2.5.5. *Se $\mathbb{K}$ é um corpo de números e $\{x_1, \dots, x_n\}$ é uma base integral de $\mathbb{K}$ então $\{y_1, \dots, y_n\}$ também é uma base integral se, e somente se,*

$$D_{\mathbb{K}:\mathbb{Q}}(x_1, \dots, x_n) = D_{\mathbb{K}:\mathbb{Q}}(y_1, \dots, y_n). \quad (2.27)$$

Demonstração. Se n é o grau de $\mathbb{K}$ e $\{y_1, \dots, y_n\}$ é um subconjunto de $\mathbb{K}$ então, para cada $1 \leq i \leq n$, tem-se que $y_i = \sum_{j=1}^n a_{ij}x_j$, com $a_{ij} \in \mathbb{Z}$. Devido à proposição 2.3.1, $D_{\mathbb{K}:\mathbb{Q}}(y_1, \dots, y_n) = (\det(a_{ij}))^2 D_{\mathbb{K}:\mathbb{Q}}(x_1, \dots, x_n)$. Assim, vale a igualdade 2.27 se, e somente se, $|\det(a_{ij})| = 1$ se, e somente se, $[a_{ij}]$ é invertível, o que ocorre se, e somente se, $\{y_1, \dots, y_n\}$ é uma base integral de $\mathbb{K}$. $\square$

Devido à proposição acima, a seguinte definição fica bem posta:

Definição 2.5.5. Se $\mathbb{K}$ é um corpo de números, chama-se de **discriminante de $\mathbb{K}$** ao valor do discriminante de qualquer base integral de $\mathbb{K}$, ao qual denotamos por $D(\mathbb{K} : \mathbb{Q})$ ou, simplesmente, por $D(\mathbb{K})$.

Sendo $\mathbb{K}$ um corpo de números, a proposição 2.3.5 garante que $D(\mathbb{K}) \neq 0$. Além disso, $D(\mathbb{K}) \in \mathbb{Z}$. De fato, se $\{x_1, \dots, x_n\}$ é uma base integral de $\mathbb{K}$ então $x_i x_j \in \mathcal{O}_{\mathbb{K}}$, para quaisquer $i, j \in \{1, \dots, n\}$. Logo, $\text{Tr}_{\mathbb{K}:\mathbb{Q}}(x_i x_j) \in \mathbb{Z}$ (corolário 2.2.2). Portanto, $D(\mathbb{K}) = \det(\text{Tr}_{\mathbb{K}:\mathbb{Q}}(x_i x_j)) \in \mathbb{Z}$.

Observe também que o ideal discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ (definição 2.3.2), $\mathfrak{D}_{\mathbb{K}:\mathbb{Q}}$, é gerado pelo discriminante de $\mathbb{K}$.

Proposição 2.5.6. Se $\mathbb{K} = \mathbb{Q}(u)$ é um corpo de números de grau n (proposição 2.5.1) e se u é um inteiro algébrico então $D(\mathbb{K}) \mid D_{\mathbb{K}:\mathbb{Q}}(u)$ e o quociente da divisão é o quadrado de um inteiro positivo.

Demonstração. Seja $\{x_1, \dots, x_n\}$ uma base integral de $\mathbb{K}$. Assim, para $1 \leq j \leq n$, temos $u^{j-1} = \sum_{i=1}^n a_{ij} x_i$, com cada $a_{ij} \in \mathbb{Z}$. Considere a matriz $M = [a_{ij}]$. Enfim, a proposição 2.3.1 garante que $D_{\mathbb{K}:\mathbb{Q}}(u) = D_{\mathbb{K}:\mathbb{Q}}(1, u, \dots, u^{n-1}) = (\det(a_{ij}))^2 D(\mathbb{K})$, donde segue o resultado. $\square$

A proposição seguinte pode ser útil para determinar o anel de inteiros de um corpo de números.

Proposição 2.5.7. Sejam $\mathbb{L}$ um corpo de números de grau n sobre $\mathbb{Q}$ e $\{x_1, \dots, x_n\}$ uma $\mathbb{Q}$ -base para $\mathbb{L}$ contida em $\mathcal{O}_{\mathbb{L}}$. Se o discriminante $D(x_1, \dots, x_n)$ é livre de quadrados então $\{x_1, \dots, x_n\}$ é uma base integral de $\mathbb{L}$.

Demonstração. Seja $\{e_1, \dots, e_n\}$ uma base integral de $\mathbb{L}$. Então $x_i = \sum_{j=1}^n a_{ij} e_j$ ($a_{ij} \in \mathbb{Z}$). Daí, $D(x_1, \dots, x_n) = \det(a_{ij})^2 D(e_1, \dots, e_n)$ (proposição 2.3.1). Como $D(x_1, \dots, x_n)$ é livre de quadrados então $\det(a_{ij}) = \pm 1$, donde segue que $\{x_1, \dots, x_n\}$ é uma base integral de $\mathbb{L}$. $\square$

Proposição 2.5.8. Sejam $\{x_1, \dots, x_n\}$ uma base de um corpo de números $\mathbb{K}$ de grau n sobre $\mathbb{Q}$ contida em $\mathcal{O}_{\mathbb{K}}$ e $d = D(x_1, \dots, x_n)$. Então todo $x \in \mathcal{O}_{\mathbb{K}}$ pode ser escrito como

$$x = \frac{m_1 x_1 + \dots + m_n x_n}{d} \quad (2.28)$$

em que $m_i \in \mathbb{Z}$ e $d \mid m_i^2$, para todo $1 \leq i \leq n$.²

Demonstração. Seja $x = a_1 x_1 + \dots + a_n x_n$, com $a_i \in \mathbb{Q}$. Sejam $\sigma_1, \dots, \sigma_n$ os $\mathbb{Q}$ -monomorfismos de $\mathbb{K}$ em um fecho algébrico de $\mathbb{K}$ (pode ser considerado $\mathbb{C}$). Aplicando cada monomorfismo na expressão

² Note que devido à proposição 2.3.5, o fato de $\{x_1, \dots, x_n\}$ ser uma base de $\mathbb{K}$ implica que $d \neq 0$. Além disso, como cada x_i é algébrico, então $\text{Tr}_{\mathbb{K}:\mathbb{Q}}(x_i x_j) \in \mathbb{Z}$ (corolário 2.2.2). Por isso e pela definição de discriminante de um conjunto de elementos tem-se que $d \in \mathbb{Z}$.

de x , obtém-se $\sigma_i(x) = \sum_{j=1}^n a_j \sigma_i(x_j)$, $1 \leq i \leq n$. Isso nos dá um sistema $n \times n$ de equações nas variáveis a_j . Pela regra de Cramer, $a_j = y_j/\delta$, em que $\delta = \det(\sigma_i(x_j))$ e y_j é o determinante da matriz obtida ao trocar a j -ésima coluna de $[\sigma_i(x_j)]$ pela coluna dos $\sigma_i(x)$. É claro que y_j e δ são inteiros algébricos e que $d = \delta^2$ (proposição 2.3.3). Então $da_j = \delta y_j$, o que mostra que todo número racional da_j é um inteiro algébrico. Então $m_j \triangleq da_j \in \mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$. Falta mostrar que $m_j^2/d \in \mathbb{Z}$. De fato, $m_j^2/d = da_j^2 = dy_j^2/\delta^2 = y_j^2$ implica que $m_j^2/d \in \mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$. $\square$

Por fim, vamos estabelecer o conceito de norma de um ideal em um anel de inteiros.

Proposição 2.5.9. *Sejam $\mathbb{K}$ um corpo de números e x um elemento não nulo de $\mathcal{O}_{\mathbb{K}}$. Então $|N(x)| = \#(\mathcal{O}_{\mathbb{K}}/(x))$, em que $(x) = x\mathcal{O}_{\mathbb{K}}$ e $N(x) = N_{\mathbb{K}:\mathbb{Q}}(x)$.³*

Demonstração. Seja n o grau de $\mathbb{K}$. Devido à proposição 2.5.2 e ao corolário 2.5.1, $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo livre finitamente gerado de posto n e o ideal (x) é um $\mathbb{Z}$ -submódulo de $\mathcal{O}_{\mathbb{K}}$ livre finitamente gerado também de posto n . Por isso, a proposição 1.1.2 garante que existem uma base $\{e_1, \dots, e_n\}$ do $\mathbb{Z}$ -módulo $\mathcal{O}_{\mathbb{K}}$ e elementos $c_1, \dots, c_n \in \mathbb{N}$ tais que $\{c_1 e_1, \dots, c_n e_n\}$ é base de (x) . Ademais, são isomorfos os grupos abelianos $\mathcal{O}_{\mathbb{K}}/(x)$ e $\prod_{i=1}^n \mathbb{Z}/(c_i \mathbb{Z})$, cuja ordem é $c_1 c_2 \dots c_n$. Considere o homomorfismo de $\mathbb{Z}$ -módulos $u : \mathcal{O}_{\mathbb{K}} \rightarrow (x)$ dado por $u(e_i) = c_i e_i$, para cada $1 \leq i \leq n$. Então $\det(u) = c_1 \dots c_n$. Por sua vez, $\{x e_1, \dots, x e_n\}$ também é base para (x) . Logo, existe um automorfismo v do $\mathbb{Z}$ -módulo (x) definido por $v(c_i e_i) = x e_i$, $1 \leq i \leq n$. Portanto, $\det(v)$ é invertível em $\mathbb{Z}$ e, portanto, $|\det(v)| = 1$. Agora, note que a multiplicação por x é dada por $m_x = v \circ u$ e que $N(x) = \det(m_x)$ (por definição). Assim, $N(x) = \det(m_x) = \det(v \circ u) = \det(v)\det(u) = \pm \det(u) = \pm c_1 \dots c_n = \pm \#(\mathcal{O}_{\mathbb{K}}/(x))$, donde segue o resultado. $\square$

Definição 2.5.6. *Se $\mathbb{K}$ é um corpo de números e I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, chama-se **norma do ideal** I o número de elementos do anel quociente $\mathcal{O}_{\mathbb{K}}/I$, a qual é denotada por $N(I)$.*

Observe que $\#(\mathcal{O}_{\mathbb{K}}/I)$ é um número finito. De fato, seja $x \in I$ não nulo. Assim, $(x) \subset I$ e $\mathcal{O}_{\mathbb{K}}/I \simeq (\mathcal{O}_{\mathbb{K}}/(x))/(\mathcal{O}_{\mathbb{K}}/I)$. Então $\#(\mathcal{O}_{\mathbb{K}}/I) \leq \#(\mathcal{O}_{\mathbb{K}}/(x))$, enquanto $\#(\mathcal{O}_{\mathbb{K}}/(x))$ é finito devido à proposição 2.5.9.

Note que se $I = (x)$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$ então $N(I) = N((x)) = \#(\mathcal{O}_{\mathbb{K}}/(x)) = |N_{\mathbb{K}:\mathbb{Q}}(x)|$.

Proposição 2.5.10. *Se I e J são ideais não zeros do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ então $N(IJ) = N(I)N(J)$.*

³ A igualdade da tese desta proposição está bem definida, pois, como $x \in \mathcal{O}_{\mathbb{K}}$, então $N(x) \in \mathbb{Z}$ (corolário 2.2.2).

Demonstração. Pelo teorema 2.4.1, o ideal J pode ser fatorado em um produto de ideais primos (maximais). Portanto, basta mostrar que $N(IM) = N(I)N(M)$, para qualquer ideal maximal M . Como $IM \subset I$ então

$$\#(\mathcal{O}_{\mathbb{K}}/IM) = \#(\mathcal{O}_{\mathbb{K}}/I)\#(I/IM). \quad (2.29)$$

De fato, para mostrar esta última igualdade, aplique o Teorema do Homomorfismo de anéis ao epimorfismo $\phi : \mathcal{O}_{\mathbb{K}}/(IM) \rightarrow \mathcal{O}_{\mathbb{K}}/I$ dado por $\phi(x+IM) = x+I$, para qualquer $x \in \mathcal{O}_{\mathbb{K}}$, o qual tem núcleo I/IM . Utilizando o Teorema de Lagrange (aplicado nos grupos aditivos em questão), comprova-se a igualdade 2.29. Logo, para demonstrar a tese, basta mostrar que $\#(I/IM) = \#(\mathcal{O}_{\mathbb{K}}/M)$. Para isso, note que o teorema 2.4.1 garante que $I \neq IM$, ou seja, $IM \subsetneq I$. Agora, note que não existe um ideal B estritamente entre I e IM , pois, caso contrário,

$$IM \subset B \subset I \implies I^{-1}IM \subset I^{-1}B \subset I^{-1}I \implies M \subset I^{-1}B \subset \mathcal{O}_{\mathbb{K}} \quad (2.30)$$

Como $I^{-1}B \subset \mathcal{O}_{\mathbb{K}}$, o qual é de fato um ideal, e como M é maximal então $I^{-1}B = \mathcal{O}_{\mathbb{K}}$ ou $I^{-1}B = M$, donde segue que $B = I$ ou $B = IM$. Portanto, não há um ideal estritamente entre I e IM . Isto significa que, para qualquer elemento $a \in I - IM$, temos $IM + (a) = I$. Fixe um elemento $a \in I - IM$ e defina $\theta : \mathcal{O}_{\mathbb{K}} \rightarrow I/IM$ por $\theta(x) = IM + ax$, para qualquer $x \in \mathcal{O}_{\mathbb{K}}$. A aplicação θ é um epimorfismo de $\mathcal{O}_{\mathbb{K}}$ -módulos cujo núcleo é um ideal que satisfaz $M \subset \ker(\theta)$. Como $I \neq IM$, então $\ker(\theta) \neq \mathcal{O}_{\mathbb{K}}$. Como M é maximal, $\ker(\theta) = M$. Portanto, $\mathcal{O}_{\mathbb{K}}/M \simeq I/IM$, comprovando que $\#(I/IM) = \#(\mathcal{O}_{\mathbb{K}}/M)$, donde segue o resultado. $\square$

Para ver mais sobre normas de ideais e para ver uma aplicação desse conceito, consulte o capítulo 5 de [33].

2.6 Ramificação de ideais primos

Sabemos que o número 5 é um número primo em $\mathbb{Z}$. Apesar disso, caso estejamos em $\mathbb{Z}[i] \supset \mathbb{Z}$, 5 não é primo, pois $5 = (2+i)(2-i)$. Além disso, mesmo 2 e 3 sendo ideais primos em $\mathbb{Z}$ e sendo elementos irredutíveis de $\mathbb{Z}[\sqrt{-5}]$, os ideais (2) e (3) gerados nesse anel não são ideais primos, pois $(2) = (2, 1+\sqrt{-5})^2$ e $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Esse fenômeno se chama *ramificação de ideais* e é objeto de nosso estudo nesta seção. Em síntese e sem rigor, o que estamos interessados é em saber como um ideal primo em um domínio de Dedekind se fatora em um produto de ideais primos em um anel maior.

Esta seção tem o intuito apenas de ser informativa e de explicitar definições e resultados necessários para o prosseguimento do texto. Portanto, não desenvolveremos essa teoria de maneira minuciosa, pois isso mereceria um trabalho à parte. Por conta disso, grande parte dos resultados aqui apresentados não serão demonstrados. Porém, nesses casos, deixaremos indicada uma referência para o leitor interessado em ver a demonstração. Caso queira ter acesso a essa teoria de maneira mais completa, recomendamos algumas referências: [30] (capítulos V e VI), [7] (capítulos III e IV), [28] (capítulos 11, 12 e 14) ou [23] (capítulos 3 e 4). Esta última referência trata especificamente de ramificação em anéis de inteiros.

Em toda esta seção, considere A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações (de característica zero), $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e B o fecho integral de A em $\mathbb{L}$. Nessas condições, a proposição 2.4.3 garante que B também é um domínio de Dedekind.

Se P é um ideal primo de A , nem sempre o ideal BP de B é primo. Devido ao teorema 2.4.1 e à fórmula 2.24 (seguinte à demonstração do teorema), garantimos que

$$BP = \prod_{i=1}^q \mathfrak{P}_i^{e_i} \quad (2.31)$$

em que os $\mathfrak{P}_i$ são primos distintos de B e os e_i são inteiros positivos.

Lema 2.6.1. *Sejam P um ideal primo de A e $\mathfrak{P}$ um ideal primo de B . São equivalentes:*

- (i) $\mathfrak{P} \cap A = P$.
- (ii) $P \subset \mathfrak{P}$.
- (iii) $BP \subset \mathfrak{P}$.

Demonstração. (i) $\implies$ (ii) : se $p \in P$ então o item (i) garante que $p \in \mathfrak{P} \cap A$, donde segue que $p \in \mathfrak{P}$. Portanto, vale (ii). (ii) $\implies$ (iii) : Seja $\sum_i b_i p_i \in BP$ ($b_i \in B, p_i \in P$). Como $P \subset \mathfrak{P}$ então cada $p_i \in \mathfrak{P}$. Enfim, pelo fato de $\mathfrak{P}$ ser um ideal de B segue que $\sum_i b_i p_i \in \mathfrak{P}$, donde segue que $BP \subset \mathfrak{P}$. (iii) $\implies$ (i) : Como $\mathfrak{P}$ é um ideal primo de B então $\mathfrak{P} \cap A$ é um ideal primo de A (claro). Assim, pelo item (iii), $BP \subset \mathfrak{P}$, donde segue que $P \subset (BP) \cap A \subset \mathfrak{P} \cap A$, ou seja, $P \subset \mathfrak{P} \cap A$. Como P é maximal e $\mathfrak{P} \cap A \neq A$ (pois $\mathfrak{P} \cap A$ é ideal primo) então $P = \mathfrak{P} \cap A$. $\square$

Definição 2.6.1. *Se um ideal $\mathfrak{P}$ de B e um ideal P de A satisfazem uma das condições equivalentes do lema 2.6.1, dizemos que o ideal $\mathfrak{P}$ **está acima de** P ou que o ideal P **está abaixo de** $\mathfrak{P}$.*

Proposição 2.6.1. *Um ideal primo $\mathfrak{P}$ de B é um dos $\mathfrak{P}_i$ da equação 2.31 se, e somente se, $\mathfrak{P} \cap A = P$. Em outras palavras, os ideais primos da fatoração de BP são aqueles que estão acima de P .*

Demonstração. Inicialmente, note que $BP = \prod_{i=1}^q \mathfrak{P}_i^{e_i}$ se, e somente se, $BP \subset \mathfrak{P}_i$, para todo $1 \leq i \leq q$. Então $\mathfrak{P}_i$ aparece na fatoração de BP se, e somente se, $BP \subset \mathfrak{P}_i$, o que ocorre (devido ao lema 2.6.1) se, e somente se, $\mathfrak{P} \cap A = P$. $\square$

Seja P um ideal de A tal que BP é fatorado como na fórmula 2.31. Como P é ideal maximal do domínio de Dedekind A e cada $\mathfrak{P}_i$ é ideal maximal do domínio de Dedekind B então A/P e $B/\mathfrak{P}_i$ são corpos.

Proposição 2.6.2. *Nas notações acima, se $\mathfrak{I}$ é um ideal de B tal que $\mathfrak{I} \cap A = P$ então o espaço vetorial $B/\mathfrak{I}$ sobre A/P tem dimensão finita.*

Demonstração. Devido à proposição 2.4.3, B é um A -módulo finitamente gerado. Seja $\{x_1, \dots, x_n\}$ um conjunto de geradores de B sobre A . Então o conjunto $\{x_1 + \mathfrak{I}, \dots, x_n + \mathfrak{I}\}$ é um conjunto gerador do espaço vetorial $B/\mathfrak{I}$ sobre A/P . Logo, tal espaço vetorial tem dimensão finita. $\square$

Para cada i , seja $\phi_i : A \longrightarrow B/\mathfrak{P}_i$ a aplicação dada por $\phi(a) = a + \mathfrak{P}_i$, para todo $a \in A$. Essa aplicação é um homomorfismo de anéis. Além disso,

$$\phi_i(a) = \bar{0} \iff a + \mathfrak{P}_i = \mathfrak{P}_i \iff a \in \mathfrak{P}_i \cap A. \quad (2.32)$$

ou seja, $\ker(\phi_i) = \mathfrak{P}_i \cap A = P$. Assim, pelo Teorema do Homomorfismo de Anéis, $\bar{\phi} : A/P \longrightarrow B/\mathfrak{P}_i$ é um homomorfismo injetor de corpos. Logo, A/P pode ser considerado um subcorpo de $B/\mathfrak{P}_i$. Pela proposição 2.6.2, $B/\mathfrak{P}_i$ é um espaço vetorial de dimensão finita sobre A/P .

Definição 2.6.2. *Nas notações acima, chama-se de **grau residual de $\mathfrak{P}_i$ sobre A** ou **grau de inércia de $\mathfrak{P}_i$ sobre A** e denota-se por f_i à dimensão do espaço vetorial $B/\mathfrak{P}_i$ sobre A/P . O expoente e_i de $\mathfrak{P}_i$ na fatoração de BP em 2.31 é chamado **índice de ramificação de $\mathfrak{P}_i$ sobre A** .*

Agora, veja que $BP \cap A = P$. De fato, por um lado, se $p \in P \subset A$ então $p = 1.p \in BP \cap A$, donde segue que $P \subset BP \cap A$. Por outro lado, se $a \in BP \cap A$ então $a \in \prod_{i=1}^q \mathfrak{P}_i^{e_i} \cap A$ e, daí, para todo i , $a \in \mathfrak{P}_i \cap A = P$. Logo, $BP \cap A \subset P$. Portanto, $BP \cap A = P$. Novamente devido à proposição 2.6.2, tem-se que B/BP é um espaço vetorial sobre o corpo A/P , também de dimensão finita. Daí, vem o seguinte (e importante) resultado, chamado de **Igualdade Fundamental**:

Teorema 2.6.1 ([30], seção 5.2, teorema 1). *Com as notações acima,*

$$\sum_{i=1}^q e_i f_i = [B/BP : A/P] = n. \quad (2.33)$$

Além disso, vê-se também que o anel B/BP é isomorfo ao anel $\prod_{i=1}^q B\mathfrak{P}_i^{e_i}$.

Definição 2.6.3. *Considere as notações anteriores.*

(a) Diz-se que um ideal primo P de A **se ramifica** (ou que ele é **ramificado**) em B se existe $i \in \{1, \dots, q\}$ tal que $e_i > 1$ na fatoração de BP (equação 2.31). Caso contrário, diz-se que P **não se ramifica** (ou que ele é **não ramificado**) em B .

(b) Diz-se que um ideal primo $\mathfrak{P}$ de B tal que $\mathfrak{P} \cap A = P$ **se ramifica** (ou que é **ramificado**) na extensão $\mathbb{K} \subset \mathbb{L}$ quando o índice de ramificação de $\mathfrak{P}$ na fatoração de BP é maior do que 1.

Ainda devido à Igualdade Fundamental (proposição 2.5.7), outras classificações são feitas a um ideal primo P de A em alguns casos especiais de acordo com sua fatoração em B , como veremos na definição seguinte:

Definição 2.6.4. *Considere as notações anteriores, P um ideal primo de A e a fatoração de BP dada pela equação 2.31.*

(a) P é dito **totalmente decomposto** em B quando $e_i = f_i = 1$, para todo $i \in \{1, \dots, q\}$.

(b) P é dito **totalmente inerte** em B quando $e_1 = 1$ e $f_i = n$, para algum $i \in \{1, \dots, q\}$.

(c) P é dito **totalmente ramificado** em B quando $e_i = n$ e $f_i = 1$, para algum $i \in \{1, \dots, q\}$.

Note que, se $n = 2$, os únicos casos possíveis são os listados na definição anterior (devido à Igualdade Fundamental).

A seguir, veremos que quando $\mathbb{K} \subset \mathbb{L}$ é uma extensão galoisiana, os índices de ramificação e os graus residuais de um ideal primo P de A são todos iguais. Adiante, considere $\mathbb{L} = \mathbb{K}'$ uma extensão galoisiana de $\mathbb{K}$ de grau n , $G = \text{Gal}(\mathbb{K}' : \mathbb{K})$ e $A' = B$ o fecho integral de A em $\mathbb{K}'$.

Se $x \in A'$ (ou seja, x é integral sobre A) então $\sigma(x) \in A'$ para todo $\sigma \in G$. De fato, basta aplicar σ à equação de dependência integral de x sobre A . Como também $\sigma^{-1}(A') \subset A'$, então $\sigma(A') = A'$, para todo $\sigma \in G$.

Agora, se P é um ideal primo de A e P' é um ideal primo de A' que está acima de P , isto é, tal que $P' \cap A = P$ então $\sigma(P') \cap A = P$. Isso nos faz concluir que $\sigma(P')$ também está acima de P . Além disso, $\sigma(P')$ tem mesmo índice de ramificação de P' . Neste caso, nós dizemos que P' e $\sigma(P')$ são **ideais primos conjugados de A'** . O que a proposição a seguir mostra é que todos os ideais primos acima de P em A' são conjugados:

Proposição 2.6.3 ([30], seção 6.2, proposição 1). *Se P é um ideal primo de A então os índices de ramificação e os graus residuais de todos os ideais de A' que estão acima de P são iguais. Denotando*

por e o índice de ramificação e por f o grau residual desses primos, tem-se que $A'P = (\prod_{i=1}^q \mathfrak{P}_i)^e$ e que $n = efg$.

Por fim, vejamos que é possível caracterizar ideais de A que se ramificam em B por meio do discriminante relativo de B sobre A (uma noção mais geral do que a de ideal discriminante descrita na definição 2.3.2).

Definição 2.6.5. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos de números tais que $\mathbb{K} \subset \mathbb{L}$. O **discriminante relativo de $\mathbb{L}$ sobre $\mathbb{K}$** (ou de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathcal{O}_{\mathbb{K}}$) é o ideal de $\mathcal{O}_{\mathbb{K}}$ gerado pelos discriminantes das bases de $\mathbb{L}$ sobre $\mathbb{K}$ que estão contidas em $\mathcal{O}_{\mathbb{L}}$. Notação: $\delta_{\mathbb{L}:\mathbb{K}}$ ou $\delta_{\mathcal{O}_{\mathbb{L}}:\mathcal{O}_{\mathbb{K}}}$.*

Observação 2.6.1. *Se $\{x_1, \dots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathcal{O}_{\mathbb{L}}$ então $\text{Tr}_{\mathbb{L}:\mathbb{K}}(x_i x_j) \in \mathcal{O}_{\mathbb{K}}$, devido ao corolário 2.2.2. Logo, $D(x_1, \dots, x_n) \in \mathcal{O}_{\mathbb{K}}$ e, portanto, $\delta_{\mathbb{L}:\mathbb{K}}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$. Mais ainda, $\delta_{\mathbb{L}:\mathbb{K}}$ é não zero devido à proposição 2.3.5.*

Se $\mathcal{O}_{\mathbb{L}}$ é um $\mathcal{O}_{\mathbb{K}}$ -módulo livre (por exemplo, se $\mathcal{O}_{\mathbb{K}}$ é principal), já definimos a noção de ideal discriminante, $\mathfrak{D}_{\mathcal{O}_{\mathbb{L}}:\mathcal{O}_{\mathbb{K}}}$, na definição 2.3.2 como sendo o ideal gerado por $D(e_1, \dots, e_n)$, em que $\{e_1, \dots, e_n\}$ é qualquer base para o $\mathcal{O}_{\mathbb{K}}$ -módulo $\mathcal{O}_{\mathbb{L}}$. A proposição a seguir garante que, nesse caso, o ideal discriminante coincide com o ideal relativo definido anteriormente:

Proposição 2.6.4 ([28], seção 13.2, (G)). *Seja $\{x_1, \dots, x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathcal{O}_{\mathbb{L}}$. Então $\delta_{\mathbb{L}:\mathbb{K}} = \mathfrak{D}_{\mathcal{O}_{\mathbb{L}}:\mathcal{O}_{\mathbb{K}}} = D_{\mathbb{L}:\mathbb{K}}(x_1, \dots, x_n)\mathbb{Z}$ se, e somente se, $\mathcal{O}_{\mathbb{L}}$ é um $\mathcal{O}_{\mathbb{K}}$ -módulo livre e $\{x_1, \dots, x_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathcal{O}_{\mathbb{K}}$.*

O teorema a seguir conecta ramificação e discriminante e é conhecido como Teorema de Dedekind:

Teorema 2.6.2 ([28], seção 13.2, teorema 1). *Mantidas as notações anteriores, um ideal primo P de $\mathcal{O}_{\mathbb{K}}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\delta_{\mathbb{L}:\mathbb{K}} \subset P$.*

Corolário 2.6.1. *Há uma quantidade finita de ideais primos de $\mathcal{O}_{\mathbb{K}}$ que se ramificam em $\mathcal{O}_{\mathbb{L}}$.*

Demonstração. De fato, isto segue do teorema anterior e do fato de que $\delta_{\mathbb{L}:\mathbb{K}}$ é um ideal não zero de $\mathcal{O}_{\mathbb{K}}$. □

Agora, seja $\mathfrak{P}$ um ideal maximal de B tal que $\mathfrak{P} \cap A = P$. Os automorfismos $\sigma \in G$ tais que $\sigma(\mathfrak{P}) = \mathfrak{P}$ formam um subgrupo D de G , chamado **grupo de decomposição de $\mathfrak{P}$** . Se g denota o número de conjugados de $\mathfrak{P}$, então $g = \#(G)(\#(D))^{-1}$, ou, $\#(D) = n/g = ef$. Para qualquer $\sigma \in D$, as relações $\sigma(B) = B$ e $\sigma(\mathfrak{P}) = \mathfrak{P}$ implicam que σ induz um automorfismo $\bar{\sigma}$ de $B/\mathfrak{P}$

$(x \equiv y \pmod{\mathfrak{P}})$ acarreta $\sigma(x) \equiv \sigma(y) \pmod{\mathfrak{P}}$). É claro que $\bar{\sigma}$ é um (A/P) -automorfismo. A aplicação $\sigma \mapsto \bar{\sigma}$ é um homomorfismo de grupos, cujo núcleo é o subgrupo $I \subset D$ que consiste dos automorfismos σ de D tais que $\sigma(x) - x \in \mathfrak{P}$, para todo $x \in B$. Dessa forma, I é um subgrupo normal de D , o qual é chamado de **subgrupo inercial de $\mathfrak{P}$** .

Proposição 2.6.5 ([30], seção 6.2, proposição 2). *Com as notações acima, suponha que A/P é finito ou tem característica zero. Então $B/\mathfrak{P}$ é uma extensão galoisiana de grau f sobre A/P e a aplicação $\sigma \mapsto \bar{\sigma}$ é um homomorfismo sobrejetor de D no grupo de Galois de $B/\mathfrak{P}$ sobre A/P . Além disso, $\#(I) = e$.*

Corolário 2.6.2. *Com as notações anteriores, P não se ramifica em B se, e somente se, o grupo inercial I de $\mathfrak{P}$ é o trivial para qualquer $\mathfrak{P}$ acima de P .*

2.7 Traço relativo, norma relativa e o diferente

Na seção anterior, conhecemos o Teorema de Dedekind, que dá condições necessárias e suficientes para que, sendo $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos de números, um ideal primo P de $\mathcal{O}_{\mathbb{K}}$ se ramifique em $\mathcal{O}_{\mathbb{L}}$. Um problema mais preciso é determinar os ideais $\mathfrak{P}$ de $\mathcal{O}_{\mathbb{L}}$ que são ramificados em $\mathbb{K} \subset \mathbb{L}$, conforme a definição 2.6.3. Claro que se $\mathfrak{P}$ se ramifica e $\mathfrak{P} \cap \mathcal{O}_{\mathbb{K}} = P$ (P ideal primo de $\mathcal{O}_{\mathbb{K}}$) então P é ramificado. Reciprocamente, se P se ramifica, se $\mathbb{K} \subset \mathbb{L}$ é uma extensão galoisiana e se $\mathfrak{P} \cap \mathcal{O}_{\mathbb{K}} = P$ então $\mathfrak{P}$ se ramifica (2.6.3). No entanto, se $\mathbb{K} \subset \mathbb{L}$ não é uma extensão galoisiana, nem sempre $\mathfrak{P}$ é ramificado, mesmo que P seja. Para determinar quais primos de $\mathcal{O}_{\mathbb{L}}$ se ramificam em $\mathbb{K} \subset \mathbb{L}$ introduziremos a noção de diferente nesta seção. Para tanto, precisaremos conhecer sobre traço relativo e norma relativa de um ideal em uma extensão.

Nosso intuito é apenas de apresentar os conceitos de traço relativo, norma relativa e de diferente, além dos principais resultados que os envolvem, a fim de que isso possa ser usado adiante nesta dissertação. O desenvolvimento da teoria de maneira mais completa necessitaria de um capítulo à parte e fugiria dos propósitos deste texto. Portanto, não demonstraremos a maioria dos resultados aqui citados. Para ter acesso a essa teoria de maneira mais completa, recomendamos a leitura do capítulo 13 de [28].

Adiante, considere A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita e separável de $\mathbb{K}$ e B o fecho integral de A em $\mathbb{L}$. Pela proposição 2.4.3, B também é um domínio de Dedekind.

Seja J um ideal fracionário de $\mathbb{L}$ (relativo a B). Assim, o conjunto $\{Tr_{\mathbb{L}:\mathbb{K}}(x) : x \in J\}$ é um A -módulo. Pelo fato de J ser finitamente gerado como um B -módulo (2.4.4) por um conjunto $\{x_1/a_1, \dots, x_m/a_m\}$ (cada $a_i \in A, x_i \in B$) tem-se que $a = \prod_{i=1}^m a_i \in A$, $aJ \subset B$ e $a\{Tr_{\mathbb{L}:\mathbb{K}}(x) : x \in J\} \subset \{Tr_{\mathbb{L}:\mathbb{K}}(ax) : x \in J\} \subset A$, donde segue que $\{Tr_{\mathbb{L}:\mathbb{K}}(x) : x \in J\}$ é um ideal fracionário de $\mathbb{K}$ (relativo a A).

Definição 2.7.1. *O traço relativo em $\mathbb{K} \subset \mathbb{L}$ do ideal fracionário J de $\mathbb{L}$ (relativo a B) é*

$$Tr_{\mathbb{L}:\mathbb{K}}(J) = \{Tr_{\mathbb{L}:\mathbb{K}}(x) : x \in J\}. \quad (2.34)$$

Observe que, se J é um ideal integral de B , então $Tr_{\mathbb{L}:\mathbb{K}}(J)$ também é. Além disso, vale a propriedade transitiva do traço: se $\mathbb{M}$ é uma extensão separável e finita de $\mathbb{L}$, se C é o fecho integral de B em $\mathbb{M}$ e se I é um ideal fracionário de $\mathbb{M}$ (relativo a C) então

$$Tr_{\mathbb{M}:\mathbb{K}}(I) = Tr_{\mathbb{L}:\mathbb{K}}(Tr_{\mathbb{M}:\mathbb{L}}(I)). \quad (2.35)$$

Agora, sejam $\mathfrak{P}$ um ideal primo não zero de B e $P = \mathfrak{P} \cap A$. Denote $f = [B/\mathfrak{P} : A/P]$. Se $\{x_1, \dots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em B e se $\overline{x_i}$ denota a imagem canônica de cada x_i em $B/\mathfrak{P}$ então $\{\overline{x_1}, \dots, \overline{x_n}\}$ é um conjunto de geradores do espaço vetorial $B/\mathfrak{P}$ sobre A/P . Assim, $f \leq n$.

Definição 2.7.2. *Com as notações anteriores, define-se a **norma relativa** de $\mathfrak{P}$ como sendo*

$$N_{B:A}(\mathfrak{P}) = P^f. \quad (2.36)$$

A definição anterior pode ser estendida para qualquer ideal fracionário J de B , como segue:

Definição 2.7.3. *Se $J = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ é a fatoração do ideal fracionário J de B em produto de primos distintos $\mathfrak{P}_i$ então a **norma relativa** de J é*

$$N_{B:A}(J) = \prod_{i=1}^r N_{B:A}(\mathfrak{P}_i)^{e_i}. \quad (2.37)$$

Se J é um ideal integral de B então $N_{B:A}(J)$ é um ideal integral de A . Além disso, vale a propriedade multiplicativa da norma relativa: se I e J são ideais fracionários de B então

$$N_{B:A}(IJ) = N_{B:A}(I)N_{B:A}(J). \quad (2.38)$$

Apesar da definição geral de norma relativa, há algumas vantagens em considerar $\mathbb{K}$ e $\mathbb{L}$ corpos de números. Então, adiante, sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão corpos de números de grau n , $A = \mathcal{O}_{\mathbb{K}}$ e

$B = \mathcal{O}_{\mathbb{L}}$. Neste caso, é mais comum usar a notação $N_{\mathbb{L}:\mathbb{K}}(J)$ para a norma relativa do ideal fracionário J de $\mathbb{L}$ (relativo a $\mathcal{O}_{\mathbb{L}}$), ao invés de $N_{\mathcal{O}_{\mathbb{L}}:\mathcal{O}_{\mathbb{K}}}(J)$.

Neste caso, podemos comparar a norma de um ideal (já definida na definição 2.5.6) com a sua norma relativa. Se $\mathbb{K}$ é um corpo de números e J um ideal de $\mathcal{O}_{\mathbb{K}}$ então

$$N_{\mathbb{K}:\mathbb{Q}}(J) = N(J)\mathbb{Z}, \quad (2.39)$$

ou seja, $N_{\mathbb{K}:\mathbb{Q}}(J)$ é um ideal de $\mathbb{Z}$ gerado por $N(J)$ (consulte [28], capítulo 13, (B)).

Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão de corpos de números de grau n e I é um ideal não zero de $\mathcal{O}_{\mathbb{K}}$ então

$$N_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}}I) = I^n. \quad (2.40)$$

(consulte [28], capítulo 13, (C)).

Para corpos de números, vale a transitividade da norma relativa: se $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ é uma cadeia de corpos de números e J é um ideal fracionário de $\mathbb{M}$ então

$$N_{\mathbb{M}:\mathbb{K}}(J) = N_{\mathbb{L}:\mathbb{K}}(N_{\mathbb{M}:\mathbb{L}}(J)). \quad (2.41)$$

(consulte [28], capítulo 13, (D)).

Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão galoisiana de corpos de números de grau n e $G = \text{Gal}(\mathbb{L} : \mathbb{K}) = \{\sigma_i\}_{i=1}^n$ então, para qualquer ideal fracionário não zero J de $\mathcal{O}_{\mathbb{L}}$, vale também a seguinte igualdade:

$$\prod_{i=1}^n \sigma_i(J) = \mathcal{O}_{\mathbb{L}} N_{\mathbb{L}:\mathbb{K}}(J). \quad (2.42)$$

(consulte [28], capítulo 13, (E)).

Além disso, se $x \in \mathbb{L}$ é um elemento não nulo então

$$N_{\mathbb{L}:\mathbb{K}}(x\mathcal{O}_{\mathbb{L}}) = N_{\mathbb{L}:\mathbb{K}}(x)A. \quad (2.43)$$

(consulte [28], capítulo 13, (F)).

A seguir, vamos estudar o conceito de diferente. Daqui em diante, considere A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita e separável de grau n sobre $\mathbb{K}$ e B o fecho integral de A em $\mathbb{L}$. Então, B também é um domínio de Dedekind, $\mathbb{L}$ é seu corpo de frações e $B \cap \mathbb{K} = A$.

Definição 2.7.4. *Seja M qualquer subconjunto do corpo $\mathbb{L}$. Então o **conjunto complementar de M em relação a A** é o conjunto*

$$M^* = \{x \in \mathbb{L} : \text{Tr}_{\mathbb{L}:\mathbb{K}}(xy) \in A, \forall y \in M\}. \quad (2.44)$$

A proposição seguinte resume algumas propriedades do conjunto complementar.

Proposição 2.7.1 ([28], capítulo 13, (H)). *Seja $M \subset \mathbb{L}$ e M^* seu conjunto complementar em relação a A . Então:*

- (a) M^* é um A -módulo;
- (b) Se $BM \subset M$ então M^* é um B -módulo;
- (c) Se $M_1 \subset M_2 \subset \mathbb{L}$ então $M_2^* \subset M_1^* \subset \mathbb{L}$;
- (d) $B \subset B^*$ e $\text{Tr}_{\mathbb{L}:\mathbb{K}}(B^*) \subset A$;
- (e) Se M é um A -módulo livre com base $\mathcal{B}$ então M^* é um A -módulo livre que tem como base a base dual de $\mathcal{B}$ (proposição 2.3.6);
- (f) $M^{**} = M$.

Proposição 2.7.2. B^* é um ideal fracionário de $\mathbb{L}$ (em relação a B).

Demonstração. Mostremos que B^* é um B -módulo finitamente gerado. Como o anel $A[b]$ é um A -módulo livre finitamente gerado, para qualquer $b \in B$ (pois B é fecho integral de A em $\mathbb{L}$) então, da proposição 2.7.1, $A[b]^*$ é um A -módulo finitamente gerado. Além disso, de $A[b] \subset B$ segue que $B^* \subset A[b]^*$. Como A é um domínio de Dedekind então é um anel Noetheriano (por definição). Da proposição 2.4.2, item (c), segue que $A[b]^*$ é um A -módulo Noetheriano. Pelo item (a) da mesma proposição, segue que B^* é um A -módulo finitamente gerado. Daí, de fato, B^* é finitamente gerado como B -módulo. Agora, seja b o produto dos denominadores (não nulos) de todos os finitos geradores de B^* sobre B . Então, $bB^* \subset B$, o que comprova que B^* é um ideal fracionário de $\mathbb{L}$. $\square$

Definição 2.7.5. O ideal de B que é o inverso do ideal fracionário B^* é chamado de **diferente** de B sobre A e é denotado por $\mathfrak{d}_{B:A}$.

Como $B \subset B^*$ então $\mathfrak{d}_{B:A}$ é um ideal integral não zero de B . Pelo fato de B ser um domínio de Dedekind, então o ideal $\mathfrak{d}_{B:A}$ pode ser escrito de modo único como $\mathfrak{d}_{B:A} = \prod \mathfrak{P}_i^{s_i}$, em que cada $\mathfrak{P}_i$ é um ideal primo não zero de B e $s_i \geq 0$ é um número inteiro. Além disso, $s_i > 0$ somente para uma quantidade finita de ideais primos $\mathfrak{P}_i$. O número s_i é chamado expoente em $\mathfrak{P}_i$ do diferente $\mathfrak{d}_{B:A}$.

Lema 2.7.1 ([28], capítulo 13, (J)). *Se $\mathbb{L} = \mathbb{K}(t)$, em que t é um elemento integral sobre A com polinômio minimal $g(x) = x^n + \sum_{i=1}^n c_i x^{n-i} \in A[x]$ sobre $\mathbb{K}$, e $g'(x)$ é a derivada de $g(x)$ então:*

- (a) $\text{Tr}_{\mathbb{L}:\mathbb{K}}\left(\frac{t^i}{g'(t)}\right) = 0$, se $i \in \{0, 1, \dots, n-2\}$, e $\text{Tr}_{\mathbb{L}:\mathbb{K}}\left(\frac{t^{n-1}}{g'(t)}\right) = 1$;
- (b) $A[t]^* = \frac{1}{g'(t)}A[t]$.

Abaixo está um exemplo de quando o diferente pode ser explicitamente determinado:

Proposição 2.7.3. *Sejam $\mathbb{L} = \mathbb{K}(t)$, em que $t \in B$, e $g(x) \in A[x]$ o polinômio minimal de t sobre $\mathbb{K}$. Então $\mathfrak{d}_{B:A} = g'(t)B$ se, e somente se, $B = A[t]$.*

Demonstração. Por um lado, se $B = A[t]$, o lema 2.7.1 garante que $B^* = (1/g'(t))B$, donde, por definição, tem-se que $\mathfrak{d}_{B:A} = g'(t)B$. Por outro lado, como $A[t] \subset B$ então a proposição 2.7.1 implica que $B^* \subset A[t]^*$ e, do lema 2.7.1, $B = g'(t)B^* \subset g'(t)A[t]^* = A[t]$. $\square$

Proposição 2.7.4. *Seja J um ideal fracionário de B . Então $\text{Tr}_{\mathbb{L}:\mathbb{K}}(J) \subset A$ se, e somente se, $J \subset B^* = \mathfrak{d}_{B:A}^{-1}$.*

Demonstração. Por um lado, se $J \subset B^*$ então $\text{Tr}_{\mathbb{L}:\mathbb{K}}(J) \subset \text{Tr}_{\mathbb{L}:\mathbb{K}}(B^*) \subset A$. Por outro lado, como $J = BJ$ então $\text{Tr}_{\mathbb{L}:\mathbb{K}}(J) \subset A$ então $J \subset B^*$. $\square$

A proposição a seguir é conhecida como propriedade transitiva do diferente.

Proposição 2.7.5 ([28], capítulo 13, (M)). *Mantidas as notações anteriores, se $\mathbb{M} \subset \mathbb{L}$ é uma extensão separável de grau finito e se C é um domínio de Dedekind que tem $\mathbb{M}$ como corpo de frações e é igual ao fecho integral de B em $\mathbb{M}$ então:*

$$\mathfrak{d}_{B:A} = C\mathfrak{d}_{B:A}\mathfrak{d}_{C:B}. \quad (2.45)$$

A seguir, vamos destacar os resultados envolvendo o diferente em extensões de corpos de números.

Definição 2.7.6. *Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão de corpos de números de grau n então o diferente $\mathfrak{d}_{\mathcal{O}_{\mathbb{L}}:\mathcal{O}_{\mathbb{K}}}$ pode ser denotado por $\mathfrak{d}_{\mathbb{L}:\mathbb{K}}$ e chamado de **diferente de $\mathbb{L}$ sobre $\mathbb{K}$** .*

O resultado a seguir responde à motivação feita no início desta seção:

Teorema 2.7.1 ([28], capítulo 13, teorema 2). *Um ideal $\mathfrak{P}$ de $\mathcal{O}_{\mathbb{L}}$ é ramificado em $\mathbb{K} \subset \mathbb{L}$ se, e somente se, $\mathfrak{P} \mid \mathfrak{d}_{\mathbb{L}:\mathbb{K}}$.*

A proposição seguinte relaciona o diferente de uma extensão de corpos de números ao discriminante relativo da mesma.

Proposição 2.7.6 ([28], capítulo 13, (P)). *Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão de corpos de números,*

$$N_{\mathbb{L}:\mathbb{K}}(\mathfrak{d}_{\mathbb{L}:\mathbb{K}}) = \delta_{\mathbb{L}:\mathbb{K}}. \quad (2.46)$$

Usando esta proposição e a propriedade da transitividade do diferente, mostra-se a transitividade do discriminante relativo:

Proposição 2.7.7 ([28], capítulo 13, (Q)). *Se $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ é uma cadeia de corpos de números então*

$$\delta_{\mathbb{M}:\mathbb{K}} = \delta_{\mathbb{L}:\mathbb{K}}^{[\mathbb{M}:\mathbb{L}]} N_{\mathbb{L}:\mathbb{K}}(\delta_{\mathbb{M}:\mathbb{L}}). \quad (2.47)$$

Se $x \in \mathbb{L}$ e $\{\sigma_1 = id, \sigma_2, \dots, \sigma_n\}$ é o conjunto dos $\mathbb{K}$ -isomorfismos de $\mathbb{L}$ em $\mathbb{C}$, considere $g(t) = P_x(t) = \prod_{i=1}^n (t - \sigma_i(x))$ o polinômio característico de x (corolário 2.2.1). Por ser o polinômio característico de x , note que $g(x) = 0$ e que $g(t) \in \mathbb{K}[t]$. Pela proposição 2.2.3, o polinômio minimal de x divide $g(t)$. Então, $g'(t) = \prod_{i=2}^n (t - \sigma_i(x))$ e $g'(t) \neq 0$ se, e somente se, $\mathbb{L} = \mathbb{K}(x)$, isto é, se t é um elemento primitivo da extensão $\mathbb{K} \subset \mathbb{L}$. Em outras palavras, t é diferente dos seus conjugados sobre $\mathbb{K}$ e, por isso, costuma-se chamar $g'(t)$ de **o diferente** de t em $\mathbb{K} \subset \mathbb{L}$.

Se assumirmos que t é um elemento primitivo de $\mathbb{K} \subset \mathbb{L}$ e que $t \in \mathcal{O}_{\mathbb{L}}$ então $g'(t) \neq 0$ e $g'(t) \in A$ (corolário 2.2.2).

A proposição seguinte dá uma relação entre o ideal diferente e o elemento diferente definido acima:

Proposição 2.7.8 ([28], capítulo 13, (T)). *O diferente $\mathfrak{d}_{\mathbb{L}:\mathbb{K}}$ é o ideal de $\mathcal{O}_{\mathbb{L}}$ gerado pelos diferentes $g'(t)$ de todos os elementos primitivos $t \in \mathcal{O}_{\mathbb{L}}$.*

Note que a proposição acima pode ser comparada com a proposição 2.3.4. Se $D_{\mathbb{L}:\mathbb{K}}(x)$ denota o discriminante de qualquer $x \in \mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{K}$ (definição 2.3.3), então é garantida a existência de um ideal integral I_x de $\mathcal{O}_{\mathbb{K}}$ tal que $D_{\mathbb{L}:\mathbb{K}}(x) = I_x^2 \delta_{\mathbb{L}:\mathbb{K}}$.

Para finalizar esta seção, citamos os resultados a seguir, que relacionam grau, anel de inteiros e discriminantes de corpos $\mathbb{K}_1$ e $\mathbb{K}_2$ ao corpo composto $\mathbb{L} = \mathbb{K}_1 \mathbb{K}_2$. Lembremos que, se $\mathbb{K}_1$ e $\mathbb{K}_2$ são corpos, então o **corpo composto** deles é o menor corpo que contenha ambos e é denotado por $\mathbb{K}_1 \mathbb{K}_2$.

Proposição 2.7.9 ([28], capítulo 13, (U)). *Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ corpos de números que são extensões de um mesmo corpo $\mathbb{K}$. Considere ainda $\mathbb{L} = \mathbb{K}_1 \mathbb{K}_2$ o corpo composto desses corpos e P um ideal primo não zero de $\mathcal{O}_{\mathbb{K}}$. Então:*

- (a) *O diferente $\mathfrak{d}_{\mathbb{L}:\mathbb{K}_2}$ divide $\mathcal{O}_{\mathbb{L}} \mathfrak{d}_{\mathbb{K}_1:\mathbb{K}}$, enquanto o diferente $\mathfrak{d}_{\mathbb{L}:\mathbb{K}_1}$ divide $\mathcal{O}_{\mathbb{L}} \mathfrak{d}_{\mathbb{K}_2:\mathbb{K}}$;*
- (b) *A norma $N_{\mathbb{K}_2:\mathbb{K}}(\delta_{\mathbb{L}:\mathbb{K}_2})$ divide $\delta_{\mathbb{K}_1:\mathbb{K}}^{[\mathbb{L}:\mathbb{K}_1]}$ e a norma $N_{\mathbb{K}_1:\mathbb{K}}(\delta_{\mathbb{L}:\mathbb{K}_1})$ divide $\delta_{\mathbb{K}_2:\mathbb{K}}^{[\mathbb{L}:\mathbb{K}_2]}$;*
- (c) *P é não ramificado em $\mathbb{K} \subset \mathbb{L}$ se, e somente se, P é não ramificado em $\mathbb{K} \subset \mathbb{K}_1$ e em $\mathbb{K} \subset \mathbb{K}_2$.*

Corolário 2.7.1 ([28], capítulo 13, (V)). *Seja $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ uma sequência de corpos de números tal que $\mathbb{M}$ é o menor corpo contendo $\mathbb{L}$ para o qual $\mathbb{K} \subset \mathbb{M}$ é uma extensão galoisiana. Se P é um ideal primo não zero de $\mathcal{O}_{\mathbb{K}}$ então P é não ramificado em $\mathbb{K} \subset \mathbb{L}$ se, e somente se, P é não ramificado em $\mathbb{K} \subset \mathbb{M}$.*

Por fim, para corpos de números cujos discriminantes relativos sejam relativamente primos vale a seguinte proposição:

Proposição 2.7.10 ([28], capítulo 13, (W)). *Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ dois corpos de números de graus n_1 e n_2 , respectivamente, e tais que $\delta_{\mathbb{K}_1:\mathbb{Q}}$ e $\delta_{\mathbb{K}_2:\mathbb{Q}}$ são relativamente primos. Então:*

- (a) $[\mathbb{K}_1\mathbb{K}_2 : \mathbb{Q}] = n_1n_2$;
- (b) $\delta_{\mathbb{K}_1\mathbb{K}_2:\mathbb{Q}} = \delta_{\mathbb{K}_1:\mathbb{Q}}^{n_2} \delta_{\mathbb{K}_2:\mathbb{Q}}^{n_1}$;
- (c) $\mathcal{O}_{\mathbb{K}_1\mathbb{K}_2} = \mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2}$;
- (d) Se $\{x_1, \dots, x_{n_1}\}$ é uma base integral de $\mathbb{K}_1$ e $\{y_1, \dots, y_{n_2}\}$ é uma base integral de $\mathbb{K}_2$ então $\{x_1y_1, \dots, x_{n_1}y_{n_2}\}$ é uma base integral de $\mathbb{K}_1\mathbb{K}_2$.

Conclusão

Demos destaque neste capítulo ao estudo dos elementos integrais sobre um anel ou sobre um corpo. Apresentamos conceitos que são fundamentais na Teoria Algébrica dos Números, como o conceito de traço, o de norma e o de discriminante. Em especial, tratamos do anel de inteiros de um corpo de números e de suas propriedades. Vimos, por exemplo, que o anel de inteiros de um corpo de números admite $\mathbb{Z}$ -base com mesmo número de elementos do grau do corpo e que o anel de inteiros é um domínio de Dedekind. Descrevemos, sem muito aprofundamento, a teoria da ramificação de ideais primos em anéis de inteiros de corpos de números, a qual só foi possível desenvolver devido ao fato de tais anéis serem domínios de Dedekind. Nesse ponto, fomos capazes de notar uma conexão importante entre discriminante e ramificação de primos (teorema 2.6.2). Finalmente, na última seção definimos e explicitamos as principais propriedades envolvendo traço relativo, norma relativa e o diferente. Analogamente ao comentado acima, também pudemos perceber uma conexão entre o diferente e a ramificação de primos (teorema 2.7.1). Em suma, neste capítulo fornecemos ferramentas e resultados importantes ao decorrer desta dissertação, cuja leitura deve ser útil principalmente por aqueles que nunca tiveram contato com a teoria ou com algum tópico aqui desenvolvido.

Capítulo 3

Corpos quadráticos e ciclotômicos

Já estudamos no capítulo anterior o que são anéis de inteiros de corpos de números e suas principais propriedades. Agora, nosso objetivo é conhecer alguns exemplos importantes de corpos de números: os corpos quadráticos, os corpos ciclotômicos e alguns subcorpos dos ciclotômicos. Em cada caso, nosso principal interesse é conhecer o anel de inteiros desses corpos. Em alguns desses casos, apresentaremos ainda o discriminante dos corpos. Na última seção, demonstraremos detalhadamente dois teoremas menos conhecidos que dão o anel de inteiros dos corpos $\mathbb{Q}(\eta)$, em que $\eta = \zeta_m - \zeta_m^{-1}$ é o período de Gauss, para $m = 2^n$ e $m = 4p^n$ ($p > 2$ primo). Tais teoremas foram provados originalmente em [32] e seu detalhamento foi um dos principais objetivos desse trabalho.

3.1 Corpos quadráticos

Nesta seção, estudaremos os corpos quadráticos, seus anéis de inteiros e discriminantes.

Definição 3.1.1. *Um **corpo quadrático** é um corpo de números $\mathbb{K}$ de grau 2 sobre $\mathbb{Q}$.*

Se $\mathbb{K}$ é um corpo quadrático, então pelo Teorema do Elemento Primitivo (proposição 2.5.1) existe $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Como para todo $x \in \mathbb{K}$, existe $c \in \mathbb{Z}$ não nulo tal que $cx \in \mathcal{O}_{\mathbb{K}}$, então podemos supor que θ é um inteiro algébrico. Portanto, existem $a, b \in \mathbb{Z}$ tais que θ tem polinômio minimal $p(x) = x^2 + ax + b$. Logo,

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}. \quad (3.1)$$

Como $a^2 - 4b \in \mathbb{Z}$, podemos fatorá-lo em um produto de primos. Assim, podemos supor

$$a^2 - 4b = r^2 d \quad (3.2)$$

em que d é um número inteiro livre de quadrados e $r \in \mathbb{Z}$. Dessa forma,

$$\theta = \frac{-a \pm r\sqrt{d}}{2} \quad (3.3)$$

o que demonstra a seguinte proposição:

Proposição 3.1.1. *Todo corpo quadrático $\mathbb{K}$ é da forma $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, em que $d \in \mathbb{Z}$ é um número livre de quadrados.* $\square$

A seguir, determinaremos o anel de inteiros $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ de um corpo quadrático $\mathbb{Q}(\sqrt{d})$ qualquer. Antes, porém, precisamos do seguinte lema:

Lema 3.1.1. *Um elemento $r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ pertence a $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ se, e somente se, $2r = u \in \mathbb{Z}$, $2s = v \in \mathbb{Z}$ e $u^2 - dv^2 \equiv 0 \pmod{4}$.*

Demonstração. Por um lado, suponha que $\alpha = r + s\sqrt{d}$ pertença ao anel de inteiros de $\mathbb{Q}(\sqrt{d})$. Então seu conjugado $\beta = r - s\sqrt{d}$ também deve pertencer ao anel de inteiros. Logo, a soma $\alpha + \beta$ e o produto $\alpha\beta$ também pertencem ao anel de inteiros, ou seja, $\alpha + \beta = 2r \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$ e $\alpha\beta = r^2 - ds^2 \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$. Assim, obviamente $u^2 - dv^2 = (2r)^2 - (2s)^2d \equiv 0 \pmod{4}$. Como $(2r)^2 \in \mathbb{Z}$ então $(2s)^2d \in \mathbb{Z}$. Sendo $2s = a/b$, $a, b \in \mathbb{Z}$ e $\text{mdc}(a, b) = 1$, o fato de d ser livre de quadrados nos leva à conclusão de que $b = 1$. Caso contrário, existiria um primo p divisor de b tal que p^2 dividiria d , o que constituiria um absurdo. Logo, $v = 2s \in \mathbb{Z}$. Por outro lado, se $2r = u \in \mathbb{Z}$, $2s = v \in \mathbb{Z}$ e $u^2 - dv^2 \equiv 0 \pmod{4}$ tem-se $r^2 - s^2d \in \mathbb{Z}$. Assim, o polinômio $p(x) = x^2 - ux + (r^2 - s^2d) \in \mathbb{Z}[x]$ possui $r + s\sqrt{d}$ como raiz, do que se conclui que $r + s\sqrt{d}$ é um inteiro algébrico. $\square$

Proposição 3.1.2. *Seja $\mathbb{Q}(\sqrt{d})$ um corpo quadrático, em que d é um número inteiro livre de quadrados. Assim, o seu anel de inteiros $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ é:*

- (a) $\mathbb{Z}[\sqrt{d}]$, se $d \not\equiv 1 \pmod{4}$;
- (b) $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right]$, se $d \equiv 1 \pmod{4}$.

Demonstração. Note inicialmente que $d \equiv 0 \pmod{4}$ não ocorre, pois, caso contrário, 4 dividiria d , e este último é um número livre de quadrados, ao contrário daquele. Sejam $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, em que $r, s \in \mathbb{Q}$, $u = 2r$ e $v = 2s$. Pelo lema 3.1.1, $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ se, e somente se, $u, v \in \mathbb{Z}$ e $u^2 - dv^2 \equiv 0 \pmod{4}$. Assim, analisaremos a paridade de u e v e o valor da congruência $u^2 - dv^2$ em cada possibilidade de congruência de d módulo 4:

- Caso $d \equiv 2 \pmod{4}$:

u	par	par	ímpar	ímpar
v	par	ímpar	par	ímpar
$u^2 - dv^2 \equiv$	0	2	1	3 (mod 4)

Logo, $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ se, e somente se, u e v são pares, isto é, $r = u/2$ e $s = v/2$ são números inteiros. Portanto, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$.

- Caso $d \equiv 3 \pmod{4}$:

u	par	par	ímpar	ímpar
v	par	ímpar	par	ímpar
$u^2 - dv^2 \equiv$	0	1	1	2 (mod 4)

Logo, $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ se, e somente se, u e v são pares, isto é, $r = u/2 \in \mathbb{Z}$ e $s = v/2 \in \mathbb{Z}$. Portanto, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$.

- Caso $d \equiv 1 \pmod{4}$:

u	par	par	ímpar	ímpar
v	par	ímpar	par	ímpar
$u^2 - dv^2 \equiv$	0	3	1	0 (mod 4)

Logo, $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ se, e somente se, $u = 2r$ e $v = 2s$ têm a mesma paridade (ambos pares ou ambos ímpares). Mas isso ocorre se, e somente se, $\alpha = \frac{u+v\sqrt{d}}{2}$ com $u \equiv v \pmod{2}$. Se u e v são ambos pares, então $r, s \in \mathbb{Z}$, donde segue que

$$\alpha = \frac{u + v\sqrt{d}}{2} = r + s\sqrt{d} = (r - s)1 + 2s \left(\frac{1 + \sqrt{d}}{2} \right) \quad (3.4)$$

No outro caso, se u e v são ambos ímpares, então $u - 1$ e $v - 1$ são pares. Logo,

$$\alpha = \frac{u + v\sqrt{d}}{2} = \frac{1 + \sqrt{d}}{2} + \left(\frac{u - 1}{2} + \frac{v - 1}{2}\sqrt{d} \right) \quad (3.5)$$

sendo que a última parcela é uma combinação linear de 1 e de $(1 + \sqrt{d})/2$, analogamente ao que foi feito na equação 3.4. Portanto, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z} \left[\frac{1}{2} + \frac{1}{2}\sqrt{d} \right]$. $\square$

Consequentemente, se $d \equiv 2 \pmod{4}$ ou se $d \equiv 3 \pmod{4}$ tem-se que o corpo de números $\mathbb{Q}(\sqrt{d})$ tem *base integral* $\{1, \sqrt{d}\}$, enquanto que se $d \equiv 1 \pmod{4}$ então a base integral desse corpo é $\{1, (1 + \sqrt{d})/2\}$.

Os monomorfismos $\mathbb{K} \longrightarrow \mathbb{C}$ são dados por $\sigma_1(r + s\sqrt{d}) = r + s\sqrt{d}$ e $\sigma_2(r + s\sqrt{d}) = r - s\sqrt{d}$. Daí, podemos calcular o discriminante dos corpos quadráticos:

Proposição 3.1.3. *Seja d um número inteiro livre de quadrados. Se $d \equiv 1 \pmod{4}$ então o discriminante de $\mathbb{Q}(\sqrt{d})$ é d . Caso contrário, se $d \not\equiv 1 \pmod{4}$, então o seu discriminante é $4d$.*

Demonstração. No caso $d \equiv 1 \pmod{4}$, tem-se pela proposição 3.1.2 que $\{x_1 = 1, x_2 = (1 + \sqrt{d})/2\}$ é uma base integral de $\mathbb{Q}(\sqrt{d})$. Então, pela proposição 2.3.3,

$$D(\mathbb{Q}(\sqrt{d})) = \det(\sigma_i(x_j))^2 = \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d. \quad (3.6)$$

No caso $d \not\equiv 1 \pmod{4}$, a proposição 3.1.2 nos informa que $\{x_1 = 1, x_2 = \sqrt{d}\}$ é uma base integral de $\mathbb{Q}(\sqrt{d})$. Logo,

$$D(\mathbb{Q}(\sqrt{d})) = \det(\sigma_i(x_j))^2 = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d})^2 = d. \quad (3.7)$$

□

Exemplo 3.1.1. *O corpo quadrático $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ é chamado de **corpo gaussiano**. Como $-1 \equiv 3 \pmod{4}$ a proposição 3.1.2 nos mostra que seu anel de inteiros é $\mathbb{Z}[i]$, o qual é chamado de **anel de inteiros gaussiano**. A proposição 3.1.3 nos dá ainda que o discriminante do corpo gaussiano é -4 .*

3.2 Corpos ciclotômicos

Corpos ciclotômicos são exemplos muito importantes de corpos de números. Um n -ésimo corpo ciclotômico é a menor extensão de $\mathbb{Q}$ que contém as raízes do polinômio $x^n - 1$ ($n \in \mathbb{N}$, $n \geq 2$). Nosso objetivo, nesta seção, é explicitar resultados básicos da teoria de corpos ciclotômicos e mostrar qual é o anel de inteiros e o discriminante de cada um desses corpos. Faremos esse estudo em três casos: quando n é primo, quando n é uma potências de primo e, por fim, quando n é qualquer natural maior ou igual a 2.

Definição 3.2.1. *Seja $n \geq 2$ um número natural.*

- (a) *Toda raiz do polinômio $x^n - 1$ é chamada de **raiz n -ésima da unidade**.*
- (b) *Se ζ_n é uma raiz de $x^n - 1$ (ou seja, $\zeta_n^n = 1$) e se ζ_n não é raiz de $x^m - 1$ (ou seja, $\zeta_n^m \neq 1$), para $1 \leq m < n$, então ζ_n é dita **raiz n -ésima primitiva da unidade**.*
- (c) *Se ζ_n é uma raiz n -ésima primitiva da unidade, o corpo $\mathbb{Q}(\zeta_n)$ é chamado **n -ésimo corpo ciclotômico**.*

Se $n = 2$, as únicas raízes de $x^2 - 1$ são ± 1 . Logo, 2-ésimo corpo ciclotômico é $\mathbb{Q}$ e esse caso é considerado trivial. Em geral, o elemento $e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ (i é a unidade imaginária complexa) é uma raiz n -ésima primitiva da unidade.

Sejam $\zeta_1, \dots, \zeta_n$ as n raízes (complexas) do polinômio $x^n - 1$. Note que um desses ζ_i é o número 1, pois $1^n - 1 = 0$. Se denotarmos por U_n o conjunto formado por essas n raízes, prova-se que U_n é um grupo multiplicativo cíclico, gerado por uma raiz n -ésima primitiva da unidade ζ . Além disso, as únicas geradoras de U_n são as raízes ζ^k , em que $\text{mdc}(k, n) = 1$. Denotando por φ a função de Euler, percebe-se que o número possível de geradores de U_n é $\varphi(n)$.

Se $\text{mdc}(m, n) = 1$ então $U_m \times U_n$ é isomorfo a U_{mn} pela função $\phi : U_m \times U_n \rightarrow U_{mn}$, que é definida por $\phi(a, b) = ab$, para quaisquer $a \in U_m$ e $b \in U_n$. Além disso, nessas condições, $\zeta_m^k \zeta_n^l$ ($0 \leq k \leq m, 0 \leq l \leq n$) é uma raiz mn -ésima primitiva da unidade se, e somente se, ζ_m^k é uma raiz m -ésima primitiva da unidade e ζ_n^l é uma raiz n -ésima primitiva da unidade.

Como $\mathbb{Q}(\zeta_n)$ é uma extensão finita de $\mathbb{Q}$, chamada de **extensão ciclotômica**, então $\mathbb{Q}(\zeta_n)$ é um corpo de números. Por isso, podemos falar em anel de inteiros e em discriminante desse corpo. A seguir, provaremos que o anel de inteiros desse corpo é $\mathbb{Z}[\zeta_n]$ e descreveremos o seu discriminante. Inicialmente, consideraremos o caso em que n é um número primo.

Seja $p > 2$ um primo ($p = 2$ é o caso trivial) e denote por ζ uma raiz p -ésima primitiva da unidade (podemos considerar $\zeta = e^{2\pi i/p}$). Como $\zeta \neq 1$ é raiz de $x^p - 1$ e $x^p - 1 = (x - 1)(x^{p-1} + \dots + x + 1)$ então ζ é raiz do polinômio

$$\Phi_p(x) = x^{p-1} + \dots + x + 1 \quad \in \mathbb{Z}[x]. \quad (3.8)$$

Dessa forma, denotando por $A = \mathcal{O}_{\mathbb{Q}(\zeta)}$ o anel de inteiros de $\mathbb{Q}(\zeta)$, tem-se que $\mathbb{Z}[\zeta] \subset A$. Além disso:

Proposição 3.2.1. *O polinômio $\Phi_p(x)$ é o polinômio minimal de ζ sobre $\mathbb{Q}$.*

Demonstração. Como ζ é raiz de $\Phi_p(x)$, basta mostrar que $\Phi_p(x)$ é irredutível sobre $\mathbb{Q}$. Mostraremos que $\Phi_p(x+1)$ é irredutível, pois, assim, $\Phi_p(x)$ também é irredutível. Temos:

$$\Phi_p(x+1) = (x+1)^{p-1} + \dots + (x+1) + 1 = \frac{(x+1)^p - 1}{(x+1) - 1} = \sum_{r=1}^p \binom{p}{r} x^{r-1}. \quad (3.9)$$

Para $1 \leq r \leq p-1$, $\binom{p}{r}$ é divisível por p . Também, $\binom{p}{1} = p$ não é divisível por p^2 . Logo, o Critério de Eisenstein garante a irredutibilidade de $\Phi_p(x+1)$. Portanto, $\Phi_p(x)$ é irredutível. $\square$

Devido à proposição anterior, podemos inferir que o grau de $\mathbb{Q}(\zeta)$ é $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$. Como U_p é cíclico, então ζ^i , $1 \leq i \leq p-1$, são as raízes de $\Phi_p(x)$, isto é, $\Phi_p(x) = \prod_{i=1}^{p-1} (x - \zeta^i)$. Desta igualdade e da igualdade 3.8, tem-se que $p = \prod_{i=1}^{p-1} (1 - \zeta^i)$.

Lema 3.2.1. *Se r e s são inteiros tais que $\text{mdc}(p, rs) = 1$ então $(\zeta^r - 1)/(\zeta^s - 1)$ é um elemento invertível de $\mathbb{Z}[\zeta]$.*

Demonstração. Como $\text{mdc}(p, rs) = 1$ então existe um número inteiro t tal que $r \equiv st \pmod{p}$. Então

$$\frac{\zeta^r - 1}{\zeta^s - 1} = \frac{\zeta^{st} - 1}{\zeta^s - 1} = 1 + \zeta^s + \dots + \zeta^{s(t-1)} \in \mathbb{Z}[\zeta]. \quad (3.10)$$

Analogamente mostra-se que $\frac{\zeta^s - 1}{\zeta^r - 1} \in \mathbb{Z}[\zeta]$. Daí, segue que $\frac{\zeta^r - 1}{\zeta^s - 1}$ é invertível em $\mathbb{Z}[\zeta]$. $\square$

Definição 3.2.2. *O elemento invertível do lema 3.2.1 é chamado de **unidade ciclotômica**.*

Proposição 3.2.2. *Mantendo as notações acima, o ideal $(1 - \zeta)A$ é um ideal primo de A e $((1 - \zeta)A)^{p-1} = pA$. Portanto, p é totalmente ramificado em $\mathbb{Q}(\zeta)$.*

Demonstração. Como observamos antes, $p = \prod_{i=1}^{p-1} (1 - \zeta^i)$. Pelo lema 3.2.1, para $1 \leq i \leq p-1$, os ideais $(1 - \zeta)A$ e $(1 - \zeta^i)A$ são iguais. Portanto $pA = ((1 - \zeta)A)^{p-1}$. Pelo fato de pA ter no máximo $p-1 = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ fatores primo em A (teorema 2.6.1) então $(1 - \zeta)A$ é um ideal primo de A , completando a prova. $\square$

Sabendo que os conjugados de ζ são os elementos $\zeta, \zeta^2, \dots, \zeta^{p-1}$, podemos calcular o traço e a norma de ζ . Como $\zeta^{p-1} + \dots + \zeta + 1 = \Phi_p(\zeta) = 0$ então $\text{Tr}_{\mathbb{Q}(\zeta):\mathbb{Q}}(\zeta) = -1$. Analogamente, $\text{Tr}_{\mathbb{Q}(\zeta^i):\mathbb{Q}}(\zeta^i) = -1$, para todo $i \in \{1, \dots, p-1\}$.

Lema 3.2.2. *Com as notações anteriores, $(1 - \zeta)A \cap \mathbb{Z} = p\mathbb{Z}$.*

Demonstração. Pela proposição 3.2.2, $((1 - \zeta)A)^{p-1} = pA$. Daí, $p \in (1 - \zeta)A$. Assim, $p\mathbb{Z} \subset (1 - \zeta)A \cap \mathbb{Z}$. O fato de $p\mathbb{Z}$ ser um ideal maximal de $\mathbb{Z}$ acarreta que $(1 - \zeta)A \cap \mathbb{Z} = p\mathbb{Z}$ ou que $(1 - \zeta)A \cap \mathbb{Z} = \mathbb{Z}$. O segundo caso implicaria que $1 - \zeta$ é um elemento invertível de A , donde seguiria que p também deveria ter um inverso em A e, como p tem inverso em $\mathbb{Q}$, p deveria ter um inverso em $\mathbb{Z} = A \cap \mathbb{Q}$ (absurdo). Logo, $(1 - \zeta)A \cap \mathbb{Z} = p\mathbb{Z}$. $\square$

Proposição 3.2.3. *$\{1, \zeta, \dots, \zeta^{p-2}\}$ é uma base integral de $\mathbb{Q}(\zeta)$ e $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$.*

Demonstração. Continuemos denotando $A = \mathcal{O}_{\mathbb{Q}(\zeta)}$. O conjunto $\{1, \zeta, \dots, \zeta^{p-2}\}$ é linearmente independente sobre $\mathbb{Q}$, pois, caso contrário ζ seria raiz de um polinômio com grau menor do que $p-1$ (absurdo do fato de $\Phi_p(x)$ ser o polinômio minimal de ζ). Logo, $\{1, \zeta, \dots, \zeta^{p-2}\}$ é uma base de $\mathbb{Q}(\zeta)$

sobre $\mathbb{Q}$. Como já observamos anteriormente, $\mathbb{Z}[\zeta] \subset A$. Para mostrar que $A \subset \mathbb{Z}[\zeta]$, considere $x \in A$. Logo, existem únicos $a_0, a_1, \dots, a_{p-2} \in \mathbb{Q}$ tais que

$$x = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}. \quad (3.11)$$

Queremos mostrar que cada a_i pertence a $\mathbb{Z}$. Multiplicando a igualdade 3.11 por ζ , tem-se que $x\zeta = \sum_{i=0}^{p-2} a_i\zeta^{i+1}$ e, subtraindo essa expressão da primeira,

$$x(1 - \zeta) = a_0(1 - \zeta) + a_1(\zeta - \zeta^2) + \dots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1}). \quad (3.12)$$

Como vimos, $Tr(\zeta^i) = -1$. Então, pelas propriedades de traço (proposição 2.2.2),

$$Tr(x(1 - \zeta)) = Tr(a_0(1 - \zeta)) = a_0Tr(1 - \zeta) = a_0(Tr(1) - Tr(\zeta)) = a_0((p-1) + 1) = a_0p. \quad (3.13)$$

Para mostrar que $a_0 \in \mathbb{Z}$, calculemos $Tr(x(1 - \zeta))$ diretamente. Pelo corolário 2.2.1, $Tr(x(1 - \zeta)) = \sum_{i=1}^{p-1} \sigma_i(x(1 - \zeta)) = \sum_{i=1}^{p-1} \sigma_i(x)\sigma_i(1 - \zeta)$, em que cada σ_i é um $\mathbb{Q}$ -isomorfismo de $\mathbb{Q}(\zeta)$ em $\mathbb{C}$. Como $x_i = \sigma_i(x) \in A$, $1 \leq i \leq p-1$, pois cada x_i é raiz do polinômio minimal de x , então

$$Tr(x(1 - \zeta)) = \sum_{i=1}^{p-1} x_i(1 - \zeta^i) = (1 - \zeta)y \in (1 - \zeta)A, \quad (3.14)$$

já que $(1 - \zeta_i)/(1 - \zeta) = 1 + \zeta + \dots + \zeta^{i-1} \in A$. Assim, como $Tr(x(1 - \zeta)) \in \mathbb{Q}$, então $Tr(x(1 - \zeta)) \in (1 - \zeta)A \cap \mathbb{Q} = \mathbb{Z}$. Pelo lema 3.2.2, $Tr(x(1 - \zeta)) \in (1 - \zeta)A \cap \mathbb{Z} = p\mathbb{Z}$, isto é, $Tr(x(1 - \zeta)) = pa_0 = pz$, com $z \in \mathbb{Z}$. Daí, $a_0 = z \in \mathbb{Z}$. Mostremos, por indução, que $a_i \in \mathbb{Z}$ ($1 \leq i \leq p-2$). Suponha que $a_{j-1} \in \mathbb{Z}$. Para provar que $a_j \in \mathbb{Z}$, multipliquemos por ζ^{p-j} a expressão 3.11, donde segue que $x\zeta^{p-j} = \sum_{i=0}^{p-2} a_i\zeta^{p-j+i} = a_0\zeta^{p-j} + a_1\zeta^{p-j+1} + \dots + a_{j-1}\zeta^{p-1} + a_j + a_{j+1}\zeta + \dots + a_{p-2}\zeta^{p-j-2}$. Expressando ζ^{p-1} em potências de ζ com expoente menor do que $p-1$, podemos escrever

$$x\zeta^{p-j} = (a_j - a_{j-1}) + a'_1\zeta + a'_2\zeta^2 + \dots + a'_{p-2}\zeta^{p-2}. \quad (3.15)$$

Como, por hipótese de indução, $a_{j-1} \in \mathbb{Z}$, então fazendo o mesmo processo feito para demonstrar que $a_0 \in \mathbb{Z}$ mostra-se que $a_j - a_{j-1} \in \mathbb{Z}$, donde segue que $a_j \in \mathbb{Z}$, para todo $j \in \{0, 1, \dots, p-2\}$. Portanto, $A = \mathbb{Z}[\zeta]$. $\square$

A seguir, explicitaremos o valor do discriminante de $\mathbb{Q}(\zeta)$. Antes, porém, precisamos calcular a norma de ζ e de $1 - \zeta$. Por definição, $N(\zeta) = \prod_{i=1}^{p-1} \zeta^i$ (produto dos conjugados de ζ). Como $\Phi_p(x) = \prod_{i=1}^{p-1} (x - \zeta^i)$, fazendo $x = 0$ tem-se que $N(\zeta) = (-1)^{p-1}\Phi_p(0) = \Phi_p(0)$ (pois $p-1$ é par). Daí, pondo $x = 0$ na equação 3.8, conclui-se que $N(\zeta) = 1$. Além disso, como já vimos, $p = \prod_{i=1}^{p-1} (1 - \zeta^i)$. Assim, $N(1 - \zeta) = \prod_{i=1}^{p-1} (1 - \zeta^i) = p$.

Proposição 3.2.4. *Se ζ é uma raiz p -ésima primitiva da unidade, $p > 2$ primo, então o discriminante de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ é*

$$D(\mathbb{Q}(\zeta)) = (-1)^{\frac{p-1}{2}} p^{p-2}. \quad (3.16)$$

Demonstração. Pelas proposições 2.3.4, 3.2.3 e 2.5.5,

$$D(\mathbb{Q}(\zeta)) = D(1, \zeta, \dots, \zeta^{n-1}) = (-1)^{\frac{(p-1)(p-2)}{2}} N(\Phi'_p(x)) \quad (3.17)$$

em que $\Phi_p(x)$ é o polinômio minimal de ζ . Como $\Phi_p(x) = \frac{x^p-1}{x-1}$ então $\Phi'_p(x) = \frac{(x-1)px^{p-1} - (x^p-1)}{(x-1)^2}$. Substituindo $x = \zeta$, temos $\Phi'_p(\zeta) = \frac{-p\zeta^{p-1}}{1-\zeta}$. Calculando a norma desse elemento, como $N(-p) = (-p)^{p-1}$, $N(\zeta) = 1$ e $N(1-\zeta) = p$, temos $N(\Phi'_p(\zeta)) = p^{p-2}$. O resultado segue ao observarmos que $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{p-1}{2}}$ (pois $\frac{(p-1)(p-2)}{2} \equiv \frac{p-1}{2} \pmod{2}$). $\square$

Antes de continuarmos a análise do anel de inteiros e do discriminante dos n -ésimos corpos ciclotômicos, em que n é potência de um primo ou qualquer natural maior do que 2, generalizemos alguns resultados sobre raízes primitivas e corpos ciclotômicos que vimos para n primo.

Definição 3.2.3. *Seja ζ_n uma raiz n -ésima primitiva da unidade, $n \geq 2$. O polinômio*

$$\Phi_n(x) = \prod_{\substack{\text{mdc}(i,n)=1 \\ 1 \leq i \leq n}} (x - \zeta_n^i) \quad (3.18)$$

é chamado de n -ésimo polinômio ciclotômico.

Note que $\Phi_p(x)$, com p primo, satisfaz a definição anterior. Observe também que ζ_n é raiz do n -ésimo polinômio ciclotômico. Além disso,

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \quad (3.19)$$

pois ambos os lados são iguais ao produto de todos os fatores lineares $x - \zeta^r$, para todo $r \in 1, 2, \dots, n$.

Daí,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d < n}} \Phi_d(x)} \quad (3.20)$$

nos permite calcular, por recorrência, cada polinômio ciclotômico. Por exemplo,

$$\Phi_1(x) = x - 1 \quad \Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1$$

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 \quad \Phi_4(x) = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1 \quad (3.21)$$

assim por diante.

Lema 3.2.3 (Lema de Gauss). *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio mônico e suponha $f(x) = g(x)h(x)$, em que $g(x)$ e $h(x)$ são polinômios mônicos com coeficientes em $\mathbb{Q}$. Então $g(x), h(x) \in \mathbb{Z}[x]$.*

Demonstração. Sejam m o menor inteiro positivo tal que $mg(x)$ tenha coeficientes em $\mathbb{Z}$ e n o menor inteiro positivo tal que $nh(x)$ tenha coeficientes em $\mathbb{Z}$. Como $g(x)$ é mônico, então os coeficientes de $mg(x)$ não tem fator comum. Caso contrário, m poderia ter sido trocado por um número menor. O mesmo vale para o polinômio $nh(x)$. Mostremos que $n = m = 1$. Se $nm > 1$ então existe um primo p tal que $p \mid nm$. Reduzindo os coeficientes da igualdade $mnf(x) = mg(x)nh(x)$ módulo p obtém-se que $\bar{0} = \overline{mg(x)nh(x)}$, em que a barra indica a redução dos coeficientes do polinômio módulo p . Como $\mathbb{Z}_p$ é um domínio então $\mathbb{Z}_p[x]$ também é. Pelo fato de $\overline{mg(x)}$ e de $\overline{nh(x)}$ serem polinômios em $\mathbb{Z}_p[x]$ então $\overline{mg(x)} = \bar{0}$ ou $\overline{nh(x)} = \bar{0}$. Então p divide todos os coeficientes de $mg(x)$ ou todos os coeficientes de $ng(x)$, o que é um absurdo do que supomos inicialmente. Logo, $mn = 1$ e, então, $m = n = 1$. Portanto, $g(x), h(x) \in \mathbb{Z}[x]$. $\square$

Proposição 3.2.5. *Se ζ é uma raiz n -ésima primitiva da unidade ($n \geq 2$) então cada ζ^k , $1 \leq k \leq n$ e $\text{mdc}(k, n) = 1$, é um conjugado de ζ .*

Demonstração. Seja $\theta = \zeta^k$, com $1 \leq k \leq n$ e $\text{mdc}(k, n) = 1$. Considere $f(x) \in \mathbb{Q}[x]$ o polinômio minimal de θ em $\mathbb{Q}$. Então existe $g(x) \in \mathbb{Q}[x]$ tal que $x^n - 1 = f(x)g(x)$. Pelo lema 3.2.3, $f(x), g(x) \in \mathbb{Z}[x]$. Seja p um número primo que não divide n . Claramente, θ^p é raiz de $x^n - 1$. Logo, θ^p é raiz de $f(x)$ ou de $g(x)$. Queremos mostrar que θ^p é raiz de $f(x)$. Suponhamos, porém, que θ^p seja raiz de $g(x)$. Logo, θ é raiz do polinômio $g(x^p)$. Daí segue que $g(x^p)$ é divisível por $f(x)$ em $\mathbb{Q}[x]$. Aplicando o lema 3.2.3 novamente, segue que $g(x^p)$ é divisível por $f(x)$ em $\mathbb{Z}[x]$. Reduzindo os coeficientes desses polinômios módulo p tem-se que $\overline{f(x)}$ divide $\overline{g(x^p)}$ em $\mathbb{Z}_p[x]$. Como $\overline{g(x^p)} = \overline{g(x)}^p$ e $\mathbb{Z}_p[x]$ é um DFU então $\overline{f(x)}$ e $\overline{g(x)}$ admitem máximo divisor comum $h(x) \in \mathbb{Z}_p[x]$. Então $h(x)^2 \mid \overline{f(x)g(x)} = x^n - 1$. Por regras de derivação, tem-se $h(x)$ divide $\overline{nx^{n-1}}$, a derivada de $x^n - 1$. Como p não divide n então $\bar{p}$ não divide $\bar{n}$. Então, $h(x) = \overline{m_1}x^r$, $r \leq n - 1$. Como $h(x) \mid x^n - 1$, isso é impossível. Logo, θ^p é raiz $f(x)$, para todo primo p que não divide n . Portanto, para cada p que não divide n tem-se que ζ^{kp} é conjugado de ζ^k . Como $\text{mdc}(k, n) = 1$ então existem $\alpha, \beta \in \mathbb{Z}$ tais que $\alpha k + \beta n = 1$. Além disso, $\text{mdc}(\alpha, n) = 1$. Considere p um primo da fatoração de α . Então θ^p é conjugado de θ . Considere agora q (não necessariamente diferente de p) um primo de α/p . Então θ^{pq} é conjugado de θ (por transitividade, já que θ^p é conjugado de θ). Esse processo continua até que se obtenha que $\theta^\alpha = \zeta^{k\alpha} = \zeta^{1-\beta n} = \zeta$ é conjugado de $\theta = \zeta^k$. Portanto, todo ζ^k (k nas condições da hipótese) são conjugados de ζ . $\square$

Corolário 3.2.1. *Se ζ é uma raiz n -ésima primitiva da unidade, o grau $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ é $\varphi(n)$ e o polinômio minimal de ζ é $\Phi_n(x)$.*

Demonstração. Pela proposição 3.2.5, cada expressão $x - \zeta^i$, para $1 \leq i \leq n$ e $\text{mdc}(i, n) = 1$, é um fator do polinômio minimal de ζ , $p(x)$. Como $\partial(p) \mid \partial(\Phi_n)$ então $\partial(p) \leq \partial(\Phi_n) = \varphi(n)$. Porém, cada um dos polinômios $x - \zeta^i$ acima são os únicos fatores de Φ_n , donde segue que $p(x) = \Phi_n(x)$ e que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. $\square$

Se ζ_n é uma raiz n -ésima primitiva da unidade, o grupo $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ é formado pelos $\mathbb{Q}$ -automorfismos que levam ζ_n em seus conjugados. Como vimos na proposição 3.2.5 e no corolário 3.2.1, o polinômio $\Phi_n(x) = \prod_{\substack{\text{mdc}(i,n)=1 \\ 1 \leq i \leq n}} (x - \zeta_n^i)$ é o minimal de ζ_n . Logo, $\{\zeta_n^i : 1 \leq i \leq n, \text{mdc}(i, n) = 1\}$ é o conjunto dos conjugados de ζ_n . Portanto, definindo o $\mathbb{Q}$ -automorfismo $\sigma_k(\zeta_n) = \zeta_n^k$, para cada $1 \leq k \leq n$ com $\text{mdc}(k, n) = 1$, tem-se que $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ é o conjunto desses σ_k .

Corolário 3.2.2. *Se ζ é uma raiz n -ésima primitiva da unidade, $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ é extensão de Galois.*

Demonstração. Pelo comentário acima e pelo corolário 3.2.1, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = \#\text{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$, donde segue que a extensão é galoisiana. $\square$

Corolário 3.2.3. *Se ζ_n é uma raiz n -ésima primitiva da unidade então $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ é isomorfo ao grupo multiplicativo $\mathbb{Z}_n^*$. Consequentemente, $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ é abeliano.*

Demonstração. Considere $\phi : \mathbb{Z}_n^* \rightarrow \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ dado por $\phi(k) = \sigma_k$, em que $\sigma_k \in \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ é tal que $\sigma_k(\zeta_n) = \zeta_n^k$. Pela proposição 3.2.5, ϕ está bem definida e é injetora. Pelo corolário anterior, $\#\text{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) = \varphi(n) = \#\mathbb{Z}_n^*$, donde segue a sobrejetividade de ϕ . Por fim, para quaisquer $k, l \in \mathbb{Z}_n^*$, $\phi(kl) = \sigma_{kl}$. Agora, $\sigma_{kl}(\zeta) = \zeta^{kl} = (\zeta^l)^k = \sigma_k(\sigma_l(\zeta))$, donde segue que $\sigma_{kl} = \sigma_k \circ \sigma_l$ e, portanto, $\phi(kl) = \phi(k) \circ \phi(l)$, mostrando que ϕ é um homomorfismo. Logo, ϕ é um isomorfismo de grupos entre $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ e $\mathbb{Z}_n^*$. $\square$

Agora, vamos encontrar o anel de inteiros e o discriminante dos n -ésimos corpos ciclotômicos. Primeiramente, consideremos o caso $n = p^k > 2$, em que p é primo e $k \geq 1$ é um número inteiro. Daqui em diante, considere $\zeta = \zeta_{p^k}$ a p^k -ésima raiz primitiva da unidade e $A = \mathcal{O}_{\mathbb{Q}(\zeta_{p^k})}$ o anel de inteiros do p^k -ésimo corpo ciclotômico. Como $\varphi(p^k) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ então $\{1, \zeta, \dots, \zeta^{\mu-1}\}$ é uma $\mathbb{Q}$ -base para $\mathbb{Q}(\zeta)$, em que $\mu = \varphi(p^k)$. Como ζ é raiz de $x^n - 1$ obviamente, $\mathbb{Z}[\zeta] \subset A$.

Proposição 3.2.6. *Nas condições anteriores,*

$$D(1, \zeta, \dots, \zeta^{\mu-1}) = (-1)^{\frac{\varphi(p^k)}{2}} p^{p^{k-1}(k(p-1)-1)}. \quad (3.22)$$

Demonstração. Pela proposição 2.3.4, $D(1, \zeta, \dots, \zeta^{\mu-1}) = (-1)^{\frac{\mu(\mu-1)}{2}} N(\Phi'_n(x))$, em que $n = p^k$. Pela equação 3.19, $x^n - 1 = (x^{n/p} - 1)\Phi_n(x)$. Derivando essa expressão, temos

$$nx^{n-1} = \frac{n}{p}x^{(n/p)-1}\Phi_n(x) + (x^{n/p} - 1)\Phi'_n(x) \implies n\zeta^{n-1} = (\zeta^{n/p} - 1)\Phi'_n(\zeta). \quad (3.23)$$

Considerando os conjugados dessa última expressão e fazendo o produto de todos eles, temos:

$$m^\mu \left(\prod_{\substack{1 \leq a \leq n \\ \text{mdc}(a,n)=1}} \zeta^a \right)^{n-1} = \prod_{\substack{1 \leq a \leq n \\ \text{mdc}(a,n)=1}} (\zeta^{ap^{k-1}} - 1) \prod_{\substack{1 \leq a \leq n \\ \text{mdc}(a,n)=1}} \Phi'_n(\zeta^a). \quad (3.24)$$

Por um lado, como o polinômio minimal de ζ é $\Phi_n(x) = \prod_{\substack{1 \leq i \leq n \\ \text{mdc}(i,n)=1}} (x - \zeta^i)$, vê-se que $N_{\mathbb{Q}(\zeta):\mathbb{Q}}(\zeta) = (-1)^\mu \Phi_n(0)$. Por outro lado, $x^n - 1 = (x^{n/p} - 1)\Phi_n(x)$, então $\Phi_n(0) = 1$, donde segue que $N_{\mathbb{Q}(\zeta):\mathbb{Q}}(\zeta) = (-1)^\mu \Phi_n(0) = (-1)^\mu = 1$, pois $\mu = \varphi(p^k) = p^{k-1}(p-1)$ é par. Daí, $\prod_{\substack{1 \leq a \leq n \\ \text{mdc}(a,n)=1}} \zeta^a = N_{\mathbb{Q}(\zeta):\mathbb{Q}}(\zeta) = 1$.

Como $\xi = \zeta^{p^{k-1}}$ é uma raiz p -ésima primitiva da unidade então $\prod_{\substack{1 \leq a \leq p \\ \text{mdc}(a,p)=1}} (1 - \xi^a) = \Phi_p(1) = p$. Além disso, cada índice b tal que $1 \leq b \leq p$ e $\text{mdc}(b, p) = 1$ provém de p^{k-1} elementos $a \in 1, 2, \dots, p^k$ tais que $\text{mdc}(a, p^k) = 1$. Portanto,

$$\prod_{\substack{1 \leq a \leq n \\ \text{mdc}(a,n)=1}} (\zeta^{ap^{k-1}} - 1) = \left(\prod_{\substack{1 \leq a \leq p \\ \text{mdc}(a,p)=1}} (1 - \xi^a) \right)^{p^{k-1}} = p^{p^{k-1}}. \quad (3.25)$$

Então $n^\mu = p^{p^{k-1}} N_{\mathbb{Q}(\zeta):\mathbb{Q}}(\Phi'_n(\zeta))$ e, daí,

$$D(1, \zeta, \dots, \zeta^{\mu-1}) = (-1)^{\frac{\mu(\mu-1)}{2}} N(\Phi'_n(x)) = (-1)^{\frac{\mu(\mu-1)}{2}} p^{p^{k-1}(k(p-1)-1)} = (-1)^{\frac{\varphi(p^k)}{2}} p^{p^{k-1}(k(p-1)-1)}, \quad (3.26)$$

pois $\mu(\mu-1)/2 \equiv \mu/2 \equiv \varphi(p^k)/2 \pmod{2}$. $\square$

Lema 3.2.4. *Nas condições acima, se $n = p^k > 3$ (p primo), $\mu = \varphi(p^k)$ e ζ é uma raiz n -ésima primitiva da unidade então $\mathbb{Z}[1 - \zeta] = \mathbb{Z}[\zeta]$ e $D_{\mathbb{Q}(\zeta):\mathbb{Q}}(\zeta) = D_{\mathbb{Q}(\zeta):\mathbb{Q}}(1 - \zeta)$.*

Demonstração. Como $\zeta = 1 - (1 - \zeta)$ então $\mathbb{Z}[1 - \zeta] = \mathbb{Z}[\zeta]$. Agora, se $\alpha_1, \dots, \alpha_\mu$ denotam os conjugados de ζ então $1 - \alpha_1, \dots, 1 - \alpha_\mu$ são os conjugados de $1 - \zeta$. Pela demonstração da proposição 2.3.4, $D_{\mathbb{Q}(\zeta):\mathbb{Q}}(\zeta) = \prod_{1 \leq r < s \leq \mu} (\alpha^r - \alpha^s)^2 = \prod_{1 \leq r < s \leq \mu} ((1 - \alpha^r) - (1 - \alpha^s))^2 = D_{\mathbb{Q}(\zeta):\mathbb{Q}}(1 - \zeta)$. $\square$

Lema 3.2.5. *Se $n = p^k > 3$ (p primo) e ζ é uma raiz n -ésima primitiva da unidade então*

$$\prod_{\substack{1 \leq i \leq n \\ \text{mdc}(n,i)=1}} (1 - \zeta^i) = p. \quad (3.27)$$

Demonstração. Por um lado, $\Phi_n(x) = \prod_{\substack{1 \leq i \leq n \\ \text{mdc}(i,n)=1}} (x - \zeta^i)$ implica que $\Phi_n(1) = \prod_{\substack{1 \leq i \leq n \\ \text{mdc}(i,n)=1}} (1 - \zeta^i)$. Por outro lado,

$$\Phi_n(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \dots + x^{(p-1)p^{k-1}} \quad (3.28)$$

donde segue que $\Phi_n(1) = p$, concluindo a demonstração. $\square$

Proposição 3.2.7. *Se $n = p^k > 2$ (p primo), ζ é uma raiz n -ésima primitiva da unidade e $\mu = \varphi(p^k)$ então $\{1, \zeta, \dots, \zeta^{\mu-1}\}$ é uma base integral de $\mathbb{Q}(\zeta)$, $A = \mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ e o discriminante de $\mathbb{Q}(\zeta)$ é*

$$D(\mathbb{Q}(\zeta)) = (-1)^{\frac{\varphi(p^k)}{2}} p^{p^{k-1}(k(p-1)-1)}. \quad (3.29)$$

Demonstração. Já sabemos que $\mathbb{Z}[\zeta] \subset A$. Pela proposição 3.2.6,

$$D(1, \zeta, \dots, \zeta^{\mu-1}) = (-1)^{\frac{\varphi(p^k)}{2}} p^{p^{k-1}(k(p-1)-1)}. \quad (3.30)$$

Logo, se mostrarmos que $A \subset \mathbb{Z}[\zeta]$ então $\{1, \zeta, \dots, \zeta^{\mu-1}\}$ é base integral de $\mathbb{Q}(\zeta)$ (pois gera A e é linearmente independente sobre $\mathbb{Q}$ - logo, sobre $\mathbb{Z}$) e podemos concluir que $D(\mathbb{Q}(\zeta)) = D(1, \zeta, \dots, \zeta^{\mu-1})$ (definição 2.5.5). Portanto, falta mostrar que $A \subset \mathbb{Z}[\zeta]$.

Se $x \in A$, a proposição 2.5.8 garante que

$$x = \frac{m_1 + m_2(1 - \zeta) + \dots + m_\mu(1 - \zeta)^{\mu-1}}{d} \quad (3.31)$$

em que cada $m_i \in \mathbb{Z}$ e $d = D_{\mathbb{Q}(\zeta):\mathbb{Q}}(\zeta) = D_{\mathbb{Q}(\zeta):\mathbb{Q}}(1 - \zeta)$ (lema 3.2.4). Mostremos que $d \mid n^{\varphi(n)}$. De fato, se $f(x)$ denota o polinômio minimal de ζ então $x^n - 1 = f(x)g(x)$ para algum $g(x) \in \mathbb{Z}[x]$ (lema 3.2.3). Derivando essa igualdade, temos $nx^{n-1} = f'(x)g(x) + f(x)g'(x)$. Aplicando ζ , temos $n\zeta^{n-1} = f'(\zeta)g(\zeta)$, ou seja, $n = \zeta f'(\zeta)g(\zeta)$. Tomando a norma nessa última expressão, obtém-se que $n^{\varphi(n)} = \pm dN(\zeta g(\zeta))$, em que $N(\zeta g(\zeta)) \in \mathbb{Z}$, pois $\zeta g(\zeta)$ é um inteiro algébrico. Logo, $d \mid n^{\varphi(n)}$.

Como $\mathbb{Z}[1 - \zeta] = \mathbb{Z}[\zeta]$ (lema 3.2.4), mostremos que $A = \mathbb{Z}[1 - \zeta]$. É claro que $\mathbb{Z}[1 - \zeta] \subset A$. Suponhamos que $\mathbb{Z}[1 - \zeta] \subsetneq A$. Portanto, deve existir $x \in A$, dado por 3.31, tal que nem todos os m_i sejam divisíveis por d . Considere i o menor índice tal que m_i não é divisível por p . Por isso, subtraindo a expressão de x da expressão $(m_1/p) + \dots + (m_{i-1}/p)(1 - \zeta)^{i-2} \in \mathbb{Z}[1 - \zeta] \subset A$ tem-se que

$$\beta = \frac{m_i(1 - \zeta)^{i-1} + m_{i+1}(1 - \zeta)^i + \dots + m_\mu(1 - \zeta)^{\mu-1}}{p} \in A. \quad (3.32)$$

Como $1 - \zeta^i = (1 - \zeta)y$, $y \in \mathbb{Z}[\zeta]$, para $1 \leq i \leq n$, então o lema 3.2.5 garante que $p/(1 - \zeta)^\mu \in \mathbb{Z}[\zeta]$. Daí, como $i \leq \mu$, então $p/(1 - \zeta)^i \in \mathbb{Z}[\zeta] \subset A$ e $\beta p/(1 - \zeta)^i \in A$. Mas,

$$\beta \frac{p}{(1 - \zeta)^i} = \frac{m_1}{1 - \zeta} + m_{i+1} + m_{i+2}(1 + \zeta) + \dots + m_\mu(1 - \zeta)^{\mu-i-1}. \quad (3.33)$$

Logo, $m_i/(1-\zeta) = \beta \frac{p}{(1-\zeta)^i} - (m_{i+1} + m_{i+2}(1+\zeta) + \dots + m_\mu(1-\zeta)^{\mu-i-1}) \in A$. Logo, $m_i = (1-\zeta)z$, com $z \in A$. Aplicando a norma $N = N_{\mathbb{Q}(\zeta):\mathbb{Q}}$ a essa igualdade, temos $N(m_i) = N(1-\zeta)N(z)$. Como z é algébrico, $N(z) \in \mathbb{Z}$. Portanto, $N(1-\zeta) \mid N(m_i) = m_i^\mu$. Porém $N(1-\zeta) = p$ (lema 3.2.5). Logo, $p \mid m_i^\mu$, ou seja, $p \mid m_i$, o que é um absurdo pelo que foi suposto inicialmente. Assim, $A = \mathbb{Z}[1-\zeta]$, concluindo a demonstração. $\square$

Por fim, tratemos o caso geral $n > 2$. Seja $\zeta_m = e^{\frac{2\pi i}{m}}$ uma m -ésima raiz primitiva da unidade. Note que se n é ímpar então $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$. De fato, por um lado $\zeta_n = (\zeta_{2n})^2$, donde segue que $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_{2n})$. Por outro lado, $(\zeta_{2n}^n)^2 = 1$ implica que $\zeta_{2n}^n = 1$ ou $\zeta_{2n}^n = -1$. Como o primeiro caso não ocorre, então $(-\zeta_{2n})^n = 1$ e, assim, $-\zeta_{2n} \in \mathbb{Q}(\zeta_n)$, donde segue que $\mathbb{Q}(\zeta_{2n}) \subset \mathbb{Q}(\zeta_n)$.

Teorema 3.2.1. *Sejam $n > 2$ e ζ uma raiz n -ésima primitiva da unidade.*

(a) $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$;

(b) O discriminante de $\mathbb{Q}(\zeta)$ é dado por

$$D(\mathbb{Q}(\zeta)) = (-1)^{s\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{q|n} q^{\varphi(n)/(q-1)}} \quad (3.34)$$

em que s é o número de fatores primos de n e os divisores q são primos.

Demonstração. A prova é feita por indução sobre s . Se $s = 1$, então $n = p^k$ (p primo). Neste caso, a proposição 3.2.7 mostra que os itens (a) e (b) são verdadeiros. Suponhamos por indução que o resultado vale para $s - 1$ e mostremos que o resultado vale para s . Sejam p um primo divisor de n e p^k a maior potência de p que divide n . Então $n = p^k m$, em que m não é divisível por p , ou seja, $\text{mdc}(m, p^k) = 1$. Pela relação de Bezout, existem inteiros a e b tais que $ap^k + bm = 1$. Assim, $\zeta = \zeta^{ap^k} \zeta^{bm}$, com $(\zeta^{ap^k})^m = 1$ e $(\zeta^{bm})^{p^k} = 1$. Seja ξ uma raiz m -ésima primitiva da unidade e η uma raiz p^k -ésima primitiva da unidade. Então ζ^{ap^k} é uma potência de ξ , enquanto ζ^{bm} é uma potência de η . Portanto, $\mathbb{Q}(\zeta) = \mathbb{Q}(\xi)\mathbb{Q}(\eta)$ (corpo composto).

Pela proposição 3.2.7, $\mathcal{O}_{\mathbb{Q}(\xi)} = \mathbb{Z}[\xi]$ e, por hipótese de indução, $\mathcal{O}_{\mathbb{Q}(\eta)} = \mathbb{Z}[\eta]$. Pelas mesmas causas,

$$D(\mathbb{Q}(\xi)) = (-1)^{\frac{\varphi(p^k)}{2}} \frac{(p^k)^{\varphi(p^k)}}{p^{p^k-1}} \quad e \quad D(\mathbb{Q}(\eta)) = (-1)^{(s-1)\varphi(m)/2} \frac{m^{\varphi(m)}}{\prod_{q|m} q^{\varphi(m)/(q-1)}}. \quad (3.35)$$

Devido à proposição 2.7.10, como os discriminantes acima são relativamente primos, segue que o discriminante de $\mathbb{Q}(\zeta)$ é

$$D(\mathbb{Q}(\zeta)) = (\mathbb{Q}(\xi))^{\varphi(m)} (\mathbb{Q}(\eta))^{\varphi(p^k)} = (-1)^{\frac{\varphi(p^k)\varphi(m)}{2}} \frac{(p^k)^{\varphi(p^k)\varphi(m)}}{p^{p^k-1}\varphi(m)} \cdot (-1)^{(s-1)\varphi(m)\varphi(p^k)/2} \frac{m^{\varphi(m)\varphi(p^k)}}{\prod_{q|m} q^{\varphi(m)\varphi(p^k)/(q-1)}} \quad (3.36)$$

e como $\varphi(p^k)\varphi(m) = \varphi(p^k m) = \varphi(n)$ (veja proposição 1.2.7) então

$$D(\mathbb{Q}(\zeta)) = (-1)^{s\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{q|m} q^{\varphi(n)/(q-1)}}. \quad (3.37)$$

Isto prova o item (b). Por fim, também devido à proposição 2.7.10, segue que $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathcal{O}_{\mathbb{Q}(\xi)}\mathcal{O}_{\mathbb{Q}(\eta)} = \mathbb{Z}[\xi]\mathbb{Z}[\eta] = \mathbb{Z}[\xi, \eta] = \mathbb{Z}[\zeta]$. Isto prova o item (a). $\square$

Antes de encerrarmos essa seção, faremos uma importante proposição que nos informa sobre primos ramificados em um corpo ciclotômico.

Proposição 3.2.8. *Se ζ é uma raiz n -ésima primitiva da unidade então nenhum número primo que não divide n se ramifica em $\mathbb{Q}(\zeta_n)$.*

Demonstração. Pelo teorema 3.2.1, os únicos divisores possíveis de $D(\mathbb{Q}(\zeta))$ são os divisores de n . Pelo teorema 2.6.2, um ideal primo p de $\mathbb{Z}$ se ramifica em $\mathcal{O}_{\mathbb{Q}(\zeta)}$ se, e somente se, $p \mid D(\mathbb{Q}(\zeta))$. Logo, os únicos primos que podem se ramificar em $\mathbb{Q}(\zeta)$ são os divisores de n . $\square$

3.3 Subcorpos ciclotômicos

Na seção anterior, estudamos sobre o corpo ciclotômico $\mathbb{Q}(\zeta_n)$, em que ζ_n é uma raiz n -ésima primitiva de unidade e $n \geq 2$. Vimos que $\mathbb{Z}[\zeta_n]$ é o seu anel de inteiros e expressamos o seu discriminante. Nesta seção, discutiremos sobre subcorpos de $\mathbb{Q}(\zeta_n)$. Em especial, estudaremos o subcorpo maximal real $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Todo subcorpo do corpo ciclotômico $\mathbb{Q}(\zeta_n)$ será chamado de **subcorpo ciclotômico**. Como vimos, $\mathbb{Q}(\zeta_n)$ é uma extensão galoisiana de $\mathbb{Q}$. Além disso, $\mathbb{Z}_n^* \simeq \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ e, portanto, $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ é um grupo abeliano. Neste caso, podemos dizer que $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ é uma extensão abeliana. Neste caso especial, podemos falar que $\mathbb{Q}(\zeta_n)$ é um corpo de números abeliano.

É claro que se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_n)$ então $\mathbb{K}$ é um corpo de números abeliano, pois $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ é abeliano. Uma interessante pergunta que se pode fazer é sobre a recíproca: se $\mathbb{K}$ é um corpo de números abeliano, então $\mathbb{K}$ é subcorpo de um corpo ciclotômico? Essa resposta é dada pelo Teorema de Kronecker-Weber:

Teorema 3.3.1. *Se $\mathbb{Q} \subset \mathbb{K}$ é uma extensão finita abeliana então existe $n \in \mathbb{N}$ tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$.*

Kronecker foi o primeiro a fazer essa afirmação em 1853, mas sua demonstração estava incompleta. Em particular, havia uma dificuldade em tratar extensões cujo grau é uma potência de 2. Weber foi o primeiro, em 1886, a dar uma prova deste teorema, mesmo ainda deixando lacunas. Ambos usaram

a teoria dos resolventes de Lagrange para provar o teorema. Em 1896, Hilbert deu outra prova deste teorema fundamentada na análise dos grupos de ramificação. Usualmente, este teorema é provado utilizando a teoria de corpos de classe (veja [28], seção 15.2). Para ver outras demonstrações deste teorema, consulte [28] (seção 15.1) ou [34] (seção 14).

Definição 3.3.1. *Seja $\mathbb{Q} \subset \mathbb{K}$ uma extensão finita abeliana. O menor inteiro positivo n tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$ é chamado de **condutor de $\mathbb{K}$** .*

A seguir discutiremos sobre o subcorpo maximal real de um corpo ciclotômico. Se ζ_n é uma raiz n -ésima primitiva da unidade então $\zeta_n + \zeta_n^{-1}$ é um número real ($n > 2$). De fato, como ζ_n^{-1} é o conjugado complexo de ζ_n em $\mathbb{C}$ então $\zeta_n + \zeta_n^{-1}$ é igual a duas vezes a parte real de ζ_n . Portanto, $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é um subcorpo de $\mathbb{Q}(\zeta_n)$ que está contido em $\mathbb{R}$. Por isso:

Definição 3.3.2. *O subcorpo $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ de $\mathbb{Q}(\zeta_n)$ é chamado de **subcorpo maximal real**. Este subcorpo é denotado por $\mathbb{Q}(\zeta_n)^+$.*

Como ζ_n não é real ($n > 2$), então o polinômio $p(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1$ é irredutível em $\mathbb{Q}(\zeta_n)^+$ e tem ζ_n como raiz. Logo, $p(x)$ é o polinômio minimal de ζ_n sobre $\mathbb{Q}(\zeta_n)^+$. Portanto, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] = 2$.

Proposição 3.3.1. *Se ζ_n é uma raiz n -ésima primitiva da unidade então $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é o anel de inteiros de $\mathbb{Q}(\zeta_n)^+$.*

Demonstração. Por um lado, como ζ_n é um inteiro algébrico então $\mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subset A$, onde $A = \mathcal{O}_{\mathbb{Q}(\zeta_n)^+}$. Por outro lado, veja inicialmente que $\mathcal{B} = \{1, \zeta_n + \zeta_n^{-1}, \dots, (\zeta_n + \zeta_n^{-1})^{\varphi(n)/2-1}\}$ é uma base de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. De fato, $\mathcal{B}$ tem $N = [\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}]$ elementos que geram o $\mathbb{Q}$ -espaço vetorial $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Então, seja $x = a_0 + a_1(\zeta_n + \zeta_n^{-1}) + \dots + a_N(\zeta_n + \zeta_n^{-1})^N \in A$, em que cada $a_i \in \mathbb{Q}$ e $N \leq \varphi(n)/2 - 1$. Se $a_N \in \mathbb{Z}$, então ao invés de x considere o elemento $x - a_N(\zeta_n + \zeta_n^{-1})^N = a_0 + a_1(\zeta_n + \zeta_n^{-1}) + \dots + a_{N-1}(\zeta_n + \zeta_n^{-1})^{N-1} \in A$. Se $a_{N-1} \in \mathbb{Z}$, repita o processo. Se $a_i \in \mathbb{Z}$ para todo $i \in \{0, 1, \dots, N\}$ então o resultado está demonstrado. Suponha que exista um índice a_i não pertencente a $\mathbb{Z}$. Suponhamos, sem perda de generalidade, $i = N$. Então, multiplique x por ζ_n^N e expanda a expressão como um polinômio em ζ_n . Teremos: $\zeta_n^N x = a_N + g(\zeta_n) + a_N \zeta_n^{2N}$, em que $g(x)$ é um polinômio com grau máximo $2N - 1$ sobre $\mathbb{Q}$ e tal que $g(0) = 0$. Como $\zeta_n^N x$ é um inteiro algébrico em $\mathbb{Q}(\zeta_n)$ então esse elemento está em $\mathbb{Z}[\zeta_n]$. Como $2N \leq \varphi(n) - 2 \leq \varphi(n) - 1$ então $\{1, \zeta_n, \dots, \zeta_n^{2N}\}$ é um subconjunto da $\mathbb{Z}$ -base $\{1, \zeta_n, \dots, \zeta_n^{\varphi(n)}\}$ de $\mathbb{Z}[\zeta_n]$. Logo, $a_N \in \mathbb{Z}$, contrariando o que foi suposto. Portanto, $x \in \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, concluindo que $A \subset \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. $\square$

A seguir, veremos dois teoremas que nos apresentam mais dois casos especiais de subcorpos ciclotômicos. Além disso, nesses casos, calcularemos também o valor do discriminante dos corpos de números envolvidos. Se m é um número inteiro positivo, para simplificar a notação, considere $\mathbb{Q}^{(m)}$ o corpo ciclotômico $\mathbb{Q}(\zeta_m)$, em que $\zeta_m = e^{(2\pi i)/m}$ é uma raiz m -ésima primitiva da unidade.

Lema 3.3.1. *Sejam τ e σ dois $\mathbb{Q}$ -automorfismos de $\mathbb{Q}^{(m)}$ tais que $\sigma(\zeta_m) = \zeta_m^5$ e $\tau(\zeta_m) = \overline{\zeta_m} = \zeta_m^{-1}$, em que $m = 2^n \geq 8$. Considere $s = m/4 = 2^{n-2}$. Assim, os corpos fixos de $\langle \sigma^{s/2} \rangle$ e $\langle \tau \rangle$ são, respectivamente, $\mathbb{Q}^{(m/2)}$ e $\mathbb{Q}(\zeta_m)^+$.*

Demonstração. Como $\langle \sigma \rangle$ tem ordem s então $\langle \sigma^{s/2} \rangle$ tem ordem 2. O grupo $\langle \tau \rangle$ e, conseqüentemente, $\langle \sigma^{s/2} \tau \rangle$ também tem ordem 2. Considere $\mathbb{L}$ o corpo fixo de $\langle \sigma^{s/2} \rangle$. Mostremos que $\mathbb{L} = \mathbb{Q}^{(m/2)}$. De fato, pelo Teorema de Euler ([31], teorema 2.13), $\zeta_{m/2}^{5^{m/8}} = \zeta_{m/2}$ e, assim, $\sigma^{s/2}(\zeta_{m/2}) = \zeta_{m/2}^{5^{m/8}} = \zeta_{m/2}$. Portanto, $\zeta_{m/2} \in \mathbb{L}$, pois $\mathbb{L}$ é o corpo fixo de $\sigma^{s/2}$. Logo, $\mathbb{Q}^{(m/2)} \subset \mathbb{L} \subset \mathbb{Q}^{(m)}$. Como $[\mathbb{Q}^{(m)} : \mathbb{Q}^{(m/2)}] = 2$ então $\mathbb{L} = \mathbb{Q}^{(m/2)}$. Isso significa que $\mathbb{Q}^{(m/2)}$ é o corpo fixo de $\langle \sigma^{s/2} \rangle$. Agora, desconsidere a notação anterior de $\mathbb{L}$ e tome $\mathbb{L}$ igual ao corpo fixo de τ . Mostremos que $\mathbb{L} = \mathbb{Q}(\zeta_m)^+$. Com efeito, $\tau(\zeta_m + \zeta_m^{-1}) = \tau(\zeta_m^{-1}) + \tau(\zeta_m) = \zeta_m + \zeta_m^{-1}$. Portanto, $\zeta_m + \zeta_m^{-1} \in \mathbb{L}$. Então, $\mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subset \mathbb{L} \subset \mathbb{Q}(\zeta_m)$ e daí, como $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m + \zeta_m^{-1})] = 2$, segue que $\mathbb{L} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. Logo, o corpo fixo de $\langle \tau \rangle$ é $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$. $\square$

Teorema 3.3.2. *Considere $m = 2^n$, $n \geq 3$, e $\mathbb{K}$ o subcorpo imaginário de $\mathbb{Q}^{(m)} = \mathbb{Q}(\zeta_m)$ distinto de $\mathbb{Q}^{(m/2)} = \mathbb{Q}(\zeta_{m/2})$ tal que $[\mathbb{Q}^{(m)} : \mathbb{K}] = 2$. Então:*

- (a) *o corpo $\mathbb{K}$ é $\mathbb{Q}(\eta)$, em que $\eta = \zeta_m - \zeta_m^{-1}$ é o período de Gauss;*
- (b) *o valor absoluto do discriminante do corpo $\mathbb{K}$ é igual a $2^{(n-1)\varphi(2^n-1)-1}$;*
- (c) *o anel de inteiros de $\mathbb{K}$ é $\mathbb{Z}[\eta]$.*

Demonstração. Seja $G = \text{Gal}(\mathbb{Q}^{(m)} : \mathbb{Q})$. Como $\mathbb{Q}^{(m)}$ é um corpo ciclotômico, sabemos que G é isomorfo a $\mathbb{Z}_m^* = \mathbb{Z}_{2^n}^*$. Da proposição 1.2.10 inferimos que $G \simeq \langle -1 \rangle \times \langle 5 \rangle$, ou seja, existem $\mathbb{Q}$ -automorfismos τ e σ de $\mathbb{Q}^{(m)}$ tais que $G = \langle \tau \rangle \langle \sigma \rangle$, em que $\tau(\zeta_m) = \overline{\zeta_m} = \zeta_m^{-1}$ (aqui, $\bar{x}$ representa a conjugação complexa de x) e $\sigma(\zeta_m) = \zeta_m^5$. É importante notar que G é, de fato como foi denotado, um produto interno, pois $\langle \tau \rangle \cap \langle \sigma \rangle = \{e\}$. Com efeito,

$$\tau(\zeta_m) = \sigma^i(\zeta_m) \iff -1 \equiv 5^i \pmod{2^n} \iff 5^i + 1 \equiv 0 \pmod{2^n} \quad (3.38)$$

mas como 4 não divide $5^i + 1$, pois $5^i + 1 \equiv (4 + 1)^i + 1 \equiv 1 + 1 \equiv 2 \pmod{4}$ então não pode ocorrer $5^i + 1 \equiv 0 \pmod{2^n}$, comprovando que a intersecção entre os subgrupos fatores de G é a identidade, donde segue que o produto direto é interno. Denotando por s o valor $\varphi(2^n)/2 = 2^{n-2}$, vê-se que

$\tau^2 = \sigma^s = e$, em que e é o automorfismo identidade. Como $\langle \sigma \rangle$ é um grupo de ordem s , então $\langle \sigma^{s/2} \rangle$, $\langle \tau \rangle$ e $H \triangleq \langle \sigma^{s/2} \tau \rangle$ são subgrupos de G de ordem 2. Mais do que isso, esses três subgrupos são os únicos subgrupos de G cuja ordem é 2. Com efeito, suponha que exista outro subgrupo G' de G cuja ordem seja 2. Então $G' = \{1, \theta\}$, para algum $\theta \in G$ tal que $\theta^2 = e$. Como $\tau^2 = e$, a existência de outro elemento de G cuja ordem é 2 só seria possível se existisse um inteiro k tal que $0 < k < s/2$ e $(\sigma^k)^2 = e$. Porém, isso não ocorre, já que a ordem de σ é s . Por hipótese, $[\mathbb{Q}^{(m)} : \mathbb{K}] = 2$. Logo, a extensão $\mathbb{K} \subset \mathbb{Q}^{(m)}$ é normal e, portanto, é Galois, já que para subcorpos complexos toda extensão é separável. Assim, a ordem do subgrupo $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K})$ de G é 2 e $\mathbb{K}$ é o corpo fixo de $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K})$. Por isso, $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K})$ só pode ser $\langle \sigma^{s/2} \rangle$, $\langle \tau \rangle$ ou $H = \langle \sigma^{s/2} \tau \rangle$. Analisemos cada caso:

- Pelo lema 3.3.1, o corpo fixo de $\langle \sigma^{s/2} \rangle$ é $\mathbb{Q}^{(m/2)}$. Porém, por hipótese, $\mathbb{K}$ não é $\mathbb{Q}^{(m/2)}$. Logo, $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K}) \neq \langle \sigma^{s/2} \rangle$.
- Também pelo lema 3.3.1, o corpo fixo de $\langle \tau \rangle$ é $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, que é um subcorpo real. No entanto, a hipótese também não permite que isso aconteça, pois $\mathbb{K}$ é suposto um subcorpo imaginário. Portanto, $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K}) \neq \langle \tau \rangle$.
- Como os dois primeiros casos não foram verificados, por exclusão concluímos que $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K}) = H = \langle \sigma^{s/2} \tau \rangle$. Portanto, $\mathbb{K}$ é o corpo fixo de H .

Agora, vamos mostrar que $\mathbb{K} = \mathbb{Q}(\eta)$, em que $\eta = \zeta_m - \zeta_m^{-1}$ é o período de Gauss. Pelo fato de $\mathbb{K}$ ser o corpo fixo de H , temos $\mathbb{K} = \{\alpha \in \mathbb{Q}^{(m)} : (\sigma^{s/2} \tau)(\alpha) = \alpha\}$. Mostremos que $\eta \in \mathbb{K}$. Como $\sigma^{s/2}(\zeta_m) = -\zeta_m$, pois, $\sigma^{s/2}(\zeta_m) = \zeta_m^{5^{2^{n-3}}} = \zeta_m \zeta_m^{2^{n-1}} = \zeta_m \zeta_m^{m/2} = -\zeta_m$ então

$$(\sigma^{s/2} \tau)(\eta) = (\sigma^{s/2} \tau)(\zeta_m - \zeta_m^{-1}) = \sigma^{s/2}(\tau(\zeta_m) - \tau(\zeta_m^{-1})) = \sigma^{s/2}(\zeta_m^{-1} - \zeta_m) = -\zeta_m^{-1} + \zeta_m. \quad (3.39)$$

Logo, $\eta \in \mathbb{K}$ e, então, $\mathbb{Q}(\eta) \subset \mathbb{K}$. Assim, $\mathbb{Q}(\eta) \subset \mathbb{K} \subset \mathbb{Q}^{(m)}$ e, daí, $[\mathbb{Q}^{(m)} : \mathbb{Q}(\eta)] \geq 2$. Além disso, ζ_m tem grau 2 sobre $\mathbb{Q}(\eta)$, já que é raiz do polinômio minimal $x^2 - \eta x - 1 \in \mathbb{Q}(\eta)[x]$. Logo, $[\mathbb{Q}^{(m)} : \mathbb{Q}(\eta)] = 2 = [\mathbb{Q}^{(m)} : \mathbb{K}]$ e, portanto, $\mathbb{K} = \mathbb{Q}(\eta)$, como afirmamos no item (a).

Como $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z} \subset \mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{Q}^{(m)}}$ e $\mathcal{O}_{\mathbb{Q}^{(m)}} = \mathbb{Z}[\zeta_m]$, então a adjunção de ζ_m a esses anéis causa $\mathbb{Z}[\zeta_m] \subset \mathcal{O}_{\mathbb{K}}[\zeta_m] \subset \mathbb{Z}[\zeta_m][\zeta_m] = \mathbb{Z}[\zeta_m]$, donde segue que $\mathcal{O}_{\mathbb{Q}^{(m)}} = \mathbb{Z}[\zeta_m] = \mathcal{O}_{\mathbb{K}}[\zeta_m]$. Logo, pela proposição 2.7.3, o diferente $\mathfrak{d}_{\mathbb{Q}^{(m)}:\mathbb{K}}$ é dado por $(G'(\zeta_m))\mathcal{O}_{\mathbb{Q}^{(m)}}$, em que G é o polinômio minimal de ζ_m sobre $\mathbb{K}$ e G' denota a derivada do polinômio G . Como $\zeta_m \notin \mathbb{K}$ e ζ_m é raiz de $x^2 - \eta x - 1 \in \mathbb{K}$, segue que este polinômio é o seu minimal G . Assim,

$$\mathfrak{d}_{\mathbb{Q}^{(m)}:\mathbb{K}} = (G'(\zeta_m))\mathcal{O}_{\mathbb{Q}^{(m)}} = (\zeta_m + \zeta_m^{-1})\mathcal{O}_{\mathbb{Q}^{(m)}} \quad (3.40)$$

Seja $\mathfrak{P} = (1 - \zeta_m)\mathcal{O}_{\mathbb{Q}(m)}$ o ideal primo de $\mathbb{Q}^{(m)}$ sobre 2. Sabemos que a norma de $\mathfrak{P}$ é 2 e $2\mathcal{O}_{\mathbb{Q}(m)} = \mathfrak{P}^{2^{n-1}}$. Pelo lema 3.2.1, como $\text{mdc}(2s+1, m) = \text{mdc}(1, m) = 1$, então $(1 - \zeta_m^{2s+1})/(1 - \zeta_m)$ é uma unidade de $\mathcal{O}_{\mathbb{Q}(m)}$ e, daí, $(1 - \zeta_m^{2s+1})\mathcal{O}_{\mathbb{Q}(m)} = (1 - \zeta_m)\mathcal{O}_{\mathbb{Q}(m)}$. Disso e da igualdade $\zeta_m^{2s} = -1$ segue que

$$(1 + \zeta_m)\mathcal{O}_{\mathbb{Q}(m)} = (1 - \zeta_m)\mathcal{O}_{\mathbb{Q}(m)} \implies (1 - \zeta_m^2)\mathcal{O}_{\mathbb{Q}(m)} = (1 - \zeta_m)^2\mathcal{O}_{\mathbb{Q}(m)} = \mathfrak{P}^2 \quad (3.41)$$

Também de $\zeta_m^{2s} = -1$ obtemos $1 + \zeta_m^2 = (1 - \zeta_m^{s+1})(1 + \zeta_m^{s+1}) = (1 - \zeta_m^{s+1})(1 - \zeta_m^{3s+1})$. De modo análogo, $1 + \zeta_m = 1 - \zeta_m^{2s+1}$. Daí, como $\text{mdc}(3s+1, m) = \text{mdc}(2s+1, m) = 1$, temos $(1 - \zeta_m^{3s+1})\mathcal{O}_{\mathbb{Q}(m)} = (1 + \zeta_m)\mathcal{O}_{\mathbb{Q}(m)}$. Analogamente, $\text{mdc}(1, m) = \text{mdc}(s+1, m) = 1$ implica $(1 - \zeta_m^{s+1})\mathcal{O}_{\mathbb{Q}(m)} = (1 - \zeta_m)\mathcal{O}_{\mathbb{Q}(m)}$. Logo,

$$(1 + \zeta_m^2)\mathcal{O}_{\mathbb{Q}(m)} = (1 - \zeta_m^{s+1})\mathcal{O}_{\mathbb{Q}(m)}(1 - \zeta_m^{3s+1})\mathcal{O}_{\mathbb{Q}(m)} = (1 + \zeta_m)\mathcal{O}_{\mathbb{Q}(m)}(1 - \zeta_m)\mathcal{O}_{\mathbb{Q}(m)} = (1 - \zeta_m^2)\mathcal{O}_{\mathbb{Q}(m)}. \quad (3.42)$$

Como ζ_m^{-1} é uma unidade de $\mathcal{O}_{\mathbb{Q}(m)}$, obtemos $(1 + \zeta_m^2)\mathcal{O}_{\mathbb{Q}(m)} = (\zeta_m + \zeta_m^{-1})\mathcal{O}_{\mathbb{Q}(m)}$. Deste fato e das equações 3.40, 3.41 e 3.42 temos

$$\mathfrak{d}_{\mathbb{Q}(m):\mathbb{K}} = (\zeta_m + \zeta_m^{-1})\mathcal{O}_{\mathbb{Q}(m)} = (1 - \zeta_m^2)\mathcal{O}_{\mathbb{Q}(m)} = \mathfrak{P}^2 \quad (3.43)$$

Da proposição 2.6.4 e das inclusões $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{Q}^{(m)}$ obtemos

$$D(\mathbb{Q}^{(m)}) = D(\mathbb{K})^{[\mathbb{Q}^{(m)}:\mathbb{K}]} N_{\mathbb{K}:\mathbb{Q}}(\delta_{\mathbb{Q}(m):\mathbb{K}}) \quad (3.44)$$

e da proposição 2.7.6 segue que

$$D(\mathbb{Q}^{(m)}) = D(\mathbb{K})^{[\mathbb{Q}^{(m)}:\mathbb{K}]} N_{\mathbb{K}:\mathbb{Q}}(N_{\mathbb{Q}(m):\mathbb{K}}(\mathfrak{d}_{\mathbb{Q}(m):\mathbb{K}})) = D(\mathbb{K})^{[\mathbb{Q}^{(m)}:\mathbb{K}]} N_{\mathbb{Q}(m)}(\mathfrak{P}^2). \quad (3.45)$$

Portanto, $D(\mathbb{K}) = \sqrt{D(\mathbb{Q}^{(m)})/N_{\mathbb{Q}(m)}(\mathfrak{d}_{\mathbb{Q}(m):\mathbb{K}})}$. Pelo teorema 3.2.1, $|D(\mathbb{Q}^{(m)})| = 2^{2^{n-1}(2n-n-1)} = 2^{2s(n-1)}$ e, como $N_{\mathbb{Q}(m)}(\mathfrak{P}^2) = N_{\mathbb{Q}(m)}(\mathfrak{P})^2 = 2^2$, obtemos que o discriminante do corpo $\mathbb{K}$ é

$$|D(\mathbb{K})| = \sqrt{|D(\mathbb{Q}^{(m)})|/2^2} = 2^{s(n-1)-1} \quad (3.46)$$

o que comprova a afirmação (b). Nosso objetivo agora é mostrar que a base de potências $\mathcal{B} = \{1, \eta, \dots, \eta^{m/4-1}\}$ é uma base integral para o anel $\mathcal{O}_{\mathbb{K}}$, pois, daí, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\eta]$. Para isso, devemos verificar que o discriminante de $\mathcal{B}$ coincide com o discriminante do corpo $\mathbb{K}$. Para $i = 0, 1$ e $j = 0, 1, \dots, s-1$, $\tau^i \sigma^j H = \{\tau^i \sigma^j, \tau^{i+1} \sigma^{j+s/2}\}$. Como $\sigma^j H = \{\sigma^{j+s/2} \tau, \sigma^j\}$ e $\tau \sigma^j H = \sigma^{j+s/2} H$ para todo $j = 0, 1, \dots, s-1$, segue que todo $\tau^i \sigma^j H$ pode ser representado como $\sigma^k H$, para algum $k = 0, 1, \dots, s-1$. Além disso, o Teorema de Lagrange nos afirma que G/H deve ter s elementos.

Logo, $G/H = \{\sigma^j H : 0 \leq j < s\}$.

Assim, podemos calcular o diferente $\mathfrak{d}_{\mathbb{K}}(\eta)$ do elemento η :

$$\mathfrak{d}_{\mathbb{K}}(\eta) = \prod_{j=1}^{s-1} (\eta - \sigma^j(\eta)) = \prod_{j=1}^{s-1} \{\zeta_m(1 - \sigma^j(\zeta_m)\zeta_m^{-1})(1 + \sigma^j(\zeta_m)^{-1}\zeta_m^{-1})\}. \quad (3.47)$$

Pelo fato de existir uma relação biunívoca entre σ^i e $\sigma^{i+s/2}$ para todo $i = 0, 1, \dots, s-1$, então

$$\{\zeta_m^j : 0 < j < m, \text{mdc}(j, m) = 1\} = \{\psi(\zeta_m) : \psi \in \text{Gal}(\mathbb{Q}^{(m)} : \mathbb{Q})\} = \{\sigma^i(\zeta_m), \tau\sigma^i(\zeta_m) : 0 \leq i < s\} \quad (3.48)$$

donde segue que

$$\{\zeta_m^i : 0 < i < m \text{ e } \text{mdc}(i, m) = 1\} = \{\sigma^i(\zeta_m), -\sigma^i(\zeta_m)^{-1} : 0 \leq i < s\} \quad (3.49)$$

Ao multiplicar os elementos deste último conjunto por ζ_m^{-1} e pelo fato de $j = i + 1$ ser um número par para cada i , obtemos:

$$\{\zeta_m^j : 0 \leq j < m \text{ e } \text{mdc}(j, m) \neq 1\} = \{\sigma^i(\zeta_m)\zeta_m^{-1}, -\sigma^i(\zeta_m)^{-1}\zeta_m^{-1} : 0 \leq i < s\}. \quad (3.50)$$

Portanto, vale a identidade de polinômios

$$f(x) \triangleq \prod_{\substack{j=0 \\ \text{mdc}(j, m) \neq 1}}^m (x - \zeta_m^j) = \prod_{j=1}^{s-1} \{(x - \sigma^j(\zeta_m)\zeta_m^{-1})(x + \sigma^j(\zeta_m)^{-1}\zeta_m^{-1})\}. \quad (3.51)$$

Assim, sendo Φ_m o m -ésimo polinômio ciclotômico, temos

$$x^m - 1 = \Phi_m(x)(x - 1)(x + \zeta_m^{-2})f(x). \quad (3.52)$$

Pondo $x = 1$, temos $\Phi_m(1) = 1 + 1^{2^{n-1}} = 2$. Além disso, devido à igualdade $(x^m - 1)/(x - 1) = x^{m-1} + \dots + x + 1$ e à equação 3.52, obtemos

$$m = 2(1 + \zeta_m^{-2})f(1). \quad (3.53)$$

Observe que $\mathfrak{d}_{\mathbb{K}}(\eta) = \zeta_m^s f(1)$ e, assim, vale a igualdade de ideais $\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)} = f(1)\mathcal{O}_{\mathbb{Q}(m)}$, pois ζ_m^s é uma unidade do anel. Das equações 3.43, 3.53 e da igualdade dos ideais principais gerados por $1 + \zeta_m^{-2}$ e $\zeta_m + \zeta_m^{-1}$ em $\mathcal{O}_{\mathbb{Q}(m)}$, obtemos

$$m/2 = 2^{n-1} = (1 + \zeta_m^{-2})f(1) \implies 2^{n-1}\mathcal{O}_{\mathbb{Q}(m)} = \mathfrak{P}^2(f(1))\mathcal{O}_{\mathbb{Q}(m)} \implies f(1)\mathcal{O}_{\mathbb{Q}(m)} = \mathfrak{P}^{-2}2^{n-1}\mathcal{O}_{\mathbb{Q}(m)}. \quad (3.54)$$

Portanto, $\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)} = \mathfrak{P}^{-2}2^{n-1}\mathcal{O}_{\mathbb{Q}(m)}$. Aplicando a norma, temos primeiramente

$$N_{\mathbb{Q}(m):\mathbb{Q}}(\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)}) = N_{\mathbb{K}:\mathbb{Q}}(N_{\mathbb{Q}(m):\mathbb{K}}(\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)})) = N_{\mathbb{K}:\mathbb{Q}}(\mathfrak{d}_{\mathbb{K}}(\eta))^2 \quad (3.55)$$

e, daí, o valor absoluto do discriminante $D_{\mathbb{K}}(\eta)$ de $\mathcal{B}$, segundo as proposições 2.3.4 e 2.7.8, é

$$\begin{aligned} |D_{\mathbb{K}}(\eta)| &= N_{\mathbb{K}:\mathbb{Q}}(\mathfrak{d}_{\mathbb{K}}(\eta)) = \sqrt{N_{\mathbb{Q}(m):\mathbb{Q}}(\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)})} = \sqrt{N_{\mathbb{Q}(m):\mathbb{Q}}(\mathfrak{P}^{-2}2^{n-1}\mathcal{O}_{\mathbb{Q}(m)})} = \\ &= \sqrt{N_{\mathbb{Q}(m):\mathbb{Q}}(2\mathcal{O}_{\mathbb{Q}(m)})^{n-1}N_{\mathbb{Q}(m):\mathbb{Q}}(\mathfrak{P})^{-2}} = \sqrt{2^{2s(n-1)}2^{-2}} = 2^{s(n-1)-1} \end{aligned} \quad (3.56)$$

donde segue finalmente que $|D_{\mathbb{K}}(\eta)| = |D(\mathbb{K})|$ e, portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\eta]$. $\square$

Lema 3.3.2. *Considere p um primo ímpar, n um número inteiro positivo e $k = 3$ ou $k = 4$ (se $k = 3$, então $p > 3$). Sejam ξ_k e ξ_{p^n} raízes k -ésima e p^n -ésima primitivas da unidade, respectivamente, de modo que $\zeta_m = \xi_k \xi_{p^n}$. Considere também os $\mathbb{Q}$ -automorfismos de $\mathbb{Q}(\zeta_m)$ dados por $\tau(\xi_k) = \xi_k^{-1}$, $\tau(\xi_{p^n}) = \xi_{p^n}$, $\sigma(\xi_k) = \xi_k$ e $\sigma(\xi_{p^n}) = \xi_{p^n}^{\bar{r}}$, em que $\bar{r}$ é o gerador do grupo multiplicativo $\mathbb{Z}_{p^n}^*$ (ou seja, r é uma raiz primitiva módulo p^n e tem ordem $\varphi(p^n)$). Nessas condições,*

$$\text{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \simeq \langle \tau \rangle \times \langle \sigma \rangle \simeq \langle \tau \rangle \langle \sigma \rangle \triangleq H. \quad (3.57)$$

Demonstração. De fato, sob as condições do enunciado, note que $\langle \tau \rangle \cap \langle \sigma \rangle = \{e\}$ (neste caso, e é o elemento identidade), pois, como r tem ordem $\varphi(p^n)$,

$$\tau(\xi_{p^n}) = \xi_{p^n} \neq \xi_{p^n}^{r^i} = \sigma^i(\xi_{p^n}), \quad \forall i \in \{0, 1, \dots, \varphi(p^n) - 1\} \quad (3.58)$$

comprovando que $\tau \neq \sigma^i$, para todo $i = 0, 1, \dots, \varphi(p^n) - 1$, donde segue imediatamente a asserção feita inicialmente. Assim, $H = \langle \tau \rangle \langle \sigma \rangle = \{\tau^i \sigma^j \mid i = 0, 1; j = 0, 1, \dots, \varphi(p^n) - 1\}$ é um produto interno de grupos e, portanto, é isomorfo ao produto externo $\langle \tau \rangle \times \langle \sigma \rangle$.

Considere τ' a restrição do $\mathbb{Q}$ -automorfismo de $\mathbb{Q}(\zeta_m)$ τ ao corpo $\mathbb{Q}(\xi_k)$ e σ' a restrição de σ a $\mathbb{Q}(\xi_{p^n})$. Assim, $\langle \tau' \rangle \simeq \langle \tau \rangle$ e $\langle \sigma' \rangle \simeq \langle \sigma \rangle$. Pela proposição 1.2.7, obtemos $\mathbb{Z}_{kp^n}^* \simeq \mathbb{Z}_k^* \times \mathbb{Z}_{p^n}^*$. Além disso, $\mathbb{Z}_k^* = \langle -1 \rangle$ e $\mathbb{Z}_{p^n}^* = \langle \bar{r} \rangle$. É conhecido que existem isomorfismos $\mathbb{Z}_k^* \simeq \text{Gal}(\mathbb{Q}^{(k)} : \mathbb{Q})$ e $\mathbb{Z}_{p^n}^* \simeq \text{Gal}(\mathbb{Q}^{(p^n)} : \mathbb{Q})$ dados, respectivamente, pelas leis $\overline{-1}^i \mapsto (\tau')^i$, $i = 0, 1$, e $\bar{r}^i \mapsto (\sigma')^i$, $i = 0, \dots, \varphi(p^n) - 1$. Logo, $\text{Gal}(\mathbb{Q}^{(k)} : \mathbb{Q}) \simeq \langle \tau' \rangle$ e $\text{Gal}(\mathbb{Q}^{(p^n)} : \mathbb{Q}) \simeq \langle \sigma' \rangle$. Então, de toda a discussão acima, sintetizamos a seguinte composição de isomorfismos:

$$\text{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \simeq \mathbb{Z}_{kp^n}^* \simeq \mathbb{Z}_k^* \times \mathbb{Z}_{p^n}^* \simeq \text{Gal}(\mathbb{Q}^{(k)} : \mathbb{Q}) \times \text{Gal}(\mathbb{Q}^{(p^n)} : \mathbb{Q}) \simeq \langle \tau' \rangle \times \langle \sigma' \rangle \simeq \langle \tau \rangle \times \langle \sigma \rangle \simeq \langle \tau \rangle \langle \sigma \rangle \quad (3.59)$$

ou seja, $\text{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \simeq H$, como queríamos demonstrar. $\square$

Lema 3.3.3. *Considere p um primo ímpar, n um inteiro positivo, $k = 3$ ou $k = 4$ (se $k = 3$, então $p > 3$), ξ_k uma raiz k -ésima primitiva da unidade e ξ_{p^n} uma raiz p^n -ésima primitiva da unidade tais*

que $\zeta_m = \xi_k \xi_{p^n}$. Sejam τ e σ dois $\mathbb{Q}$ -automorfismos de $\mathbb{Q}(\zeta_m)$ dados por $\tau(\xi_k) = \xi_k^{-1}$, $\tau(\xi_{p^n}) = \xi_{p^n}$, $\sigma(\xi_k) = \xi_k$ e $\sigma(\xi_{p^n}) = \xi_{p^n}^r$, onde r é uma raiz primitiva módulo p^n e tem ordem $\varphi(p^n)$. Sendo $s = \varphi(p^n)/2$, então:

$$(a) \sigma^s(\xi_{p^n}) = \xi_{p^n}^{-1}.$$

(b) os corpos fixos de $\langle \tau \rangle$ e $\langle \sigma^s \tau \rangle$ são, respectivamente, $\mathbb{Q}(p^n)$ e $\mathbb{Q}(\zeta_m + \zeta_m^+)$.

Demonstração. Mostremos inicialmente que o item (a) é válido. Por hipótese, $r^{\varphi(p^n)} \equiv 1 \pmod{p^n}$ e $r^i \not\equiv 1 \pmod{p^n}$ para todo $0 < i < \varphi(p^n)$. Então

$$r^{\varphi(p^n)} - 1 \equiv (r^{\varphi(p^n)/2} - 1)(r^{\varphi(p^n)/2} + 1) \equiv (r^s - 1)(r^s + 1) \equiv 0 \pmod{p^n} \quad (3.60)$$

e, como $p \mid p^n$, então $p \mid (r^s - 1)(r^s + 1)$, e daí, $p \mid r^s - 1$ ou $p \mid r^s + 1$. Se p dividisse simultaneamente $a = r^s - 1$ e $b = r^s + 1$, então p dividiria $a - b$, ou seja, $p \mid -2$, o que não ocorre, pois p é um primo ímpar. Por esse motivo, $p^n \mid a$ ou $p^n \mid b$. Como p^n não divide $r^s - 1$ (já que a ordem de r é $\varphi(p^n)$ módulo p^n), então $p^n \mid r^s + 1$, isto é, $r^s \equiv -1 \pmod{p^n}$. Assim, $\xi_{p^n}^s = \xi_{p^n}^{-1}$, o que conclui a verificação do item (a). Agora, mostremos que o item (b) é válido. Primeiramente, seja $\mathbb{L} = \{\alpha \in \mathbb{Q}(\zeta_m) : \tau(\alpha) = \alpha\}$ o corpo fixo de $\langle \tau \rangle$, o qual mostraremos que é igual a $\mathbb{Q}(\xi_{p^n})$. Para isso, note que $\xi_{p^n} \in \mathbb{L}$, pois $\tau(\xi_{p^n}) = \xi_{p^n}$ (por definição). Logo, $\mathbb{Q} \subset \mathbb{Q}(\xi_{p^n}) \subset \mathbb{L}$. Como a extensão $L \subset \mathbb{Q}(\zeta_m)$ é Galois, segue que $[\mathbb{Q}(\zeta_m) : \mathbb{L}]$ é igual à ordem do grupo $\langle \tau \rangle$, pois $\mathbb{L}$ é corpo fixo deste grupo. Portanto, $[\mathbb{Q}(\zeta_m) : \mathbb{L}] = 2$. Logo,

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] / [\mathbb{Q}(\zeta_m) : \mathbb{L}] = \varphi(m)/2 = 2\varphi(p^n)/2 = \varphi(p^n) = [\mathbb{Q}(\xi_{p^n}) : \mathbb{Q}] \quad (3.61)$$

donde concluímos que $\mathbb{Q}(\xi_{p^n}) = \mathbb{L}$, pois $\mathbb{Q} \subset \mathbb{Q}(\xi_{p^n}) \subset \mathbb{L}$. Portanto, o corpo fixo de $\langle \tau \rangle$ é $\mathbb{Q}(p^n)$.

Para completar a prova, seja $M = \{\alpha \in \mathbb{Q}(\zeta_m) : \sigma^s \tau(\alpha) = \alpha\}$ o corpo fixo de $\langle \sigma^s \tau \rangle$. Note que $\zeta_m + \zeta_m^{-1} \in M$, pois, utilizando o item (a),

$$\sigma^s \tau(\zeta_m + \zeta_m^{-1}) = \sigma^s(\xi_k^{-1} \xi_{p^n} + \xi_k \xi_{p^n}^{-1}) = \xi_k^{-1} \xi_{p^n}^{-1} + \xi_k \xi_{p^n} = \zeta_m^{-1} + \zeta_m = \zeta_m + \zeta_m^{-1}. \quad (3.62)$$

Logo, $\mathbb{Q} \subset \mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subset M$. Analogamente ao que foi feito no caso anterior desta demonstração mostra-se que $[\mathbb{Q}(\zeta_m + \zeta_m^{-1}) : \mathbb{Q}] = [M : \mathbb{Q}] = \varphi(p^n)$ e, portanto, o corpo fixo de $\langle \sigma^s \tau \rangle$ é $\mathbb{Q}(\zeta_m + \zeta_m^+)$, comprovando o item (b). $\square$

Lema 3.3.4. Se ξ_{p^n} é uma raiz p^n -ésima primitiva da unidade e Φ_{p^n} é o p^n -ésimo polinômio ciclotômico, então $p^n \xi_{p^n}^{2(p^n-1)} / \Phi'_{p^n}(\xi_{p^n}^2) = \xi_p^2 - 1$.

Demonstração. Sendo $\Psi(x) = x^{p^{n-1}} - 1$ um polinômio e $\Phi_{p^n}(x) = x^{p^{n-1}(p-1)} + \dots + x^{p^{n-1}} + 1$ o p^n -ésimo polinômio ciclotômico, então $x^{p^n} - 1 = \Psi(x)\Phi(x)$. Derivando essa expressão, obtemos $p^n x^{p^n-1} =$

$\Psi'(x)\Phi_{p^n}(x) + \Psi(x)\Phi'_{p^n}(x)$. Como $\xi_{p^n}^2$ é raiz de $\Phi_{p^n}(x)$ (pois $\text{mdc}(2, p) = 1$), então $p^n \zeta_{p^n}^{2(p^n-1)} = \Psi(\zeta_{p^n}^2)\Phi'(\zeta_{p^n}^2)$. Por fim, a igualdade $\Psi(\zeta_{p^n}) = \zeta_{p^n}^{2p^{n-1}} - 1 = \zeta_p^2 - 1$ acarreta $p^n \xi_{p^n}^{2(p^n-1)} / \Phi'_{p^n}(\xi_{p^n}^2) = \zeta_p^2 - 1$. $\square$

Teorema 3.3.3. *Considere $m = 4p^n$, em que p é um número primo ímpar e n um inteiro positivo, e $\mathbb{K}$ o subcorpo imaginário de $\mathbb{Q}^{(m)}$ distinto de $\mathbb{Q}^{(m/4)} = \mathbb{Q}(\zeta_{p^n})$ tal que $[\mathbb{Q}^{(m)} : \mathbb{K}] = 2$. Então:*

- (a) *o corpo $\mathbb{K}$ é $\mathbb{Q}(\eta)$, em que $\eta = \zeta_m - \zeta_m^{-1}$ é o período de Gauss;*
- (b) *o valor absoluto do discriminante do corpo $\mathbb{K}$ é igual a $2^{\varphi(p^n)} p^{n\varphi(p^n) - p^{n-1} - 1}$;*
- (c) *o anel de inteiros de $\mathbb{K}$ é $\mathbb{Z}[\eta]$.*

Demonstração. Inicialmente, a identidade de Bezout garante a existência de a e b inteiros tais que $4a + p^n b = 1$, pois $\text{mdc}(4, p^n) = 1$. Assim, $\text{mdc}(p^n, a) = \text{mdc}(4, b) = 1$ e, então, $\xi_4 \triangleq \zeta_4^b$ e $\xi_{p^n} \triangleq \zeta_{p^n}^a$ são raízes 4-ésima e p^n -ésima primitivas da unidade, respectivamente. Assim, $\zeta_m = \xi_4 \xi_{p^n}$. Observe ainda que $\xi_4 = -\xi_4^{-1}$. Pelo lema 3.3.2, sabemos que o grupo de Galois de $\mathbb{Q}(\zeta_m)$, denotado por G , é o produto interno $\langle \tau \rangle \langle \sigma \rangle$, em que $\tau(\xi_4) = \xi_4^{-1}$, $\tau(\xi_{p^n}) = \xi_{p^n}$, $\sigma(\xi_4) = \xi_4$ e $\sigma(\xi_{p^n}) = \xi_{p^n}^r$, onde r é uma raiz primitiva módulo p^n e tem ordem $\varphi(p^n)$. Note que $\tau(\zeta_m) = \xi_4^{-1} \xi_{p^n}$ e que $\sigma(\zeta_m) = \xi_4 \xi_{p^n}^r$. Aplicando o mesmo raciocínio feito na demonstração do teorema 3.3.2 podemos concluir que os únicos subgrupos de G de ordem 2 são $\langle \tau \rangle$, $\langle \sigma^s \tau \rangle$ e $H \triangleq \langle \sigma^s \rangle$, em que $s = \varphi(p^n)/2$. Como $[\mathbb{Q}^{(m)} : \mathbb{K}] = 2$, então a extensão $\mathbb{K} \subset \mathbb{Q}^{(m)}$ é Galois (pois é normal e separável). Logo, a ordem do subgrupo $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K})$ de G é 2 e $\mathbb{K}$ é o corpo fixo de $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K})$, ou seja, $\mathbb{K}$ é o corpo fixo de um dos três subgrupos: $\langle \tau \rangle$, $\langle \sigma^s \tau \rangle$ ou $H = \langle \sigma^s \rangle$. Analisemos cada caso:

- Pelo lema 3.3.3, o corpo fixo de $\langle \tau \rangle$ é $\mathbb{Q}^{(p^n)}$. Porém, a hipótese não permite que ocorra igualdade entre $\mathbb{K}$ e $\mathbb{Q}^{(p^n)}$. Logo, $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K}) \neq \langle \tau \rangle$.
- Pelo mesmo lema 3.3.3, o corpo fixo de $\langle \sigma^s \tau \rangle$ é $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, que é um subcorpo real de $\mathbb{Q}^{(m)}$. Por isso, a hipótese também não permite $\mathbb{K} = (\mathbb{Q}^{(m)})^+$. Logo, $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K}) \neq \langle \sigma^s \tau \rangle$.
- Por exclusão, concluímos que $\text{Gal}(\mathbb{Q}^{(m)} : \mathbb{K}) = H = \langle \sigma^s \rangle$ e, então, $\mathbb{K}$ é o corpo fixo de H .

Seja $\eta = \sum_{\rho \in H} \rho(\zeta_m) = \zeta_m - \zeta_m^{-1} = \xi_4(\xi_{p^n} + \xi_{p^n}^{-1})$ o período de Gauss. Mostremos que $\mathbb{K} = \mathbb{Q}(\eta)$. Primeiramente, note que $\eta \in \mathbb{K}$, pois $\sigma^s(\eta) = \sigma^s(\xi_4(\xi_{p^n} + \xi_{p^n}^{-1})) = \xi_4(\xi_{p^n}^{-1} + \xi_{p^n}) = -\xi_4^{-1} \xi_{p^n}^{-1} + \xi_4 \xi_{p^n} = \zeta_m - \zeta_m^{-1}$. Assim, $\mathbb{Q} \subset \mathbb{Q}(\eta) \subset \mathbb{K} \subset \mathbb{Q}(\zeta_m)$. Por um lado, $[\mathbb{Q}(\zeta_m) : \mathbb{K}] = 2$ implica $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\eta)] \geq 2$ e $\zeta_m \notin \mathbb{Q}(\eta)$. Por outro lado, ζ_m é raiz de $F(x) = x^2 - \eta x - 1 \in \mathbb{Q}(\eta)[x]$, que é, então, seu polinômio minimal sobre $\mathbb{Q}(\eta)$. Logo, $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\eta)] = 2$, donde segue que $\mathbb{K} = \mathbb{Q}(\eta)$. Além disso, $\mathbb{Z} \subset \mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{Q}^{(m)}}$ implica que $\mathcal{O}_{\mathbb{Q}^{(m)}} = \mathbb{Z}[\zeta_m] \subset \mathcal{O}_{\mathbb{K}}[\zeta_m] \subset \mathcal{O}_{\mathbb{Q}^{(m)}}[\zeta_m] = \mathcal{O}_{\mathbb{Q}^{(m)}}$. Logo, $\mathcal{O}_{\mathbb{Q}^{(m)}} = \mathcal{O}_{\mathbb{K}}[\zeta_m]$.

Por isso e pela proposição 2.7.3, o diferente $\mathfrak{d}_{\mathbb{Q}(m):\mathbb{K}}$ é dado por $(G'(\zeta_m))\mathcal{O}_{\mathbb{Q}(m)}$, em que G é o polinômio minimal de ζ_m sobre $\mathbb{K}$ e G' denota a derivada do polinômio G . Como $\zeta_m \notin \mathbb{K}$ e ζ_m é raiz de $x^2 - \eta x - 1 \in \mathbb{K}$, segue que este polinômio é o seu minimal G . Assim,

$$\mathfrak{d}_{\mathbb{Q}(m):\mathbb{K}} = (G'(\zeta_m))\mathcal{O}_{\mathbb{Q}(m)} = (\zeta_m + \zeta_m^{-1})\mathcal{O}_{\mathbb{Q}(m)} = \xi_4(\xi_{p^n} - \xi_{p^n}^{-1})\mathcal{O}_{\mathbb{Q}(m)} \quad (3.63)$$

Considere $\mathfrak{P} = (1 - \xi_{p^n})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})}$ o ideal primo ramificado de $\mathbb{Q}(\xi_{p^n})$ sobre p , ou seja, $p\mathcal{O}_{\mathbb{Q}(\xi_{p^n})} = \mathfrak{P}^{\varphi(p^n)}$ e a norma de $\mathfrak{P}$ é p . Em $\mathcal{O}_{\mathbb{Q}(\xi_{p^n})}$, como $\text{mdc}(1, p^n) = \text{mdc}(p^n, p^n - 1) = 1$, vale a igualdade dos ideais

$$(1 - \xi_{p^n})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})} = (1 - \xi_{p^n}^{p^n-1})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})} = (1 - \xi_{p^n}^{-1})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})}. \quad (3.64)$$

Multiplicando por $(1 + \xi_{p^n})$, obtemos:

$$(1 - \xi_{p^n}^2)\mathcal{O}_{\mathbb{Q}(\xi_{p^n})} = (1 + \xi_{p^n})(1 - \xi_{p^n}^{-1})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})} = (\xi_{p^n} - \xi_{p^n}^{-1})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})}. \quad (3.65)$$

Pelo fato de $\text{mdc}(2, p^n) = \text{mdc}(1, p^n) = 1$, também temos:

$$(1 - \xi_{p^n})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})} = (1 - \xi_{p^n}^2)\mathcal{O}_{\mathbb{Q}(\xi_{p^n})}. \quad (3.66)$$

De 3.65 e 3.66, concluimos que $\mathfrak{P} = (1 - \xi_{p^n})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})} = (\xi_{p^n} - \xi_{p^n}^{-1})\mathcal{O}_{\mathbb{Q}(\xi_{p^n})}$. Estendendo estes ideais para $\mathcal{O}_{\mathbb{Q}(m)}$, obtemos

$$\mathfrak{P}\mathcal{O}_{\mathbb{Q}(m)} = (\xi_{p^n} - \xi_{p^n}^{-1})\mathcal{O}_{\mathbb{Q}(m)}. \quad (3.67)$$

Por fim, das equações 3.63 e 3.67, como ξ_4 é unidade de $\mathcal{O}_{\mathbb{Q}(m)}$, implica-se que

$$\mathfrak{d}_{\mathbb{Q}(m):\mathbb{K}} = (\zeta_m + \zeta_m^{-1})\mathcal{O}_{\mathbb{Q}(m)} = \xi_4(\xi_{p^n} - \xi_{p^n}^{-1})\mathcal{O}_{\mathbb{Q}(m)} = \mathfrak{P}\mathcal{O}_{\mathbb{Q}(m)}. \quad (3.68)$$

De maneira análoga ao que foi feito na demonstração do teorema 3.3.2, mostra-se que $D(\mathbb{K}) = \sqrt{(D(\mathbb{Q}(m)))/N_{\mathbb{Q}(m)}(\mathfrak{d}_{\mathbb{Q}(m):\mathbb{K}})}$. Do teorema 3.2.1,

$$|D(\mathbb{Q}(m))| = \frac{(4p^n)^{4s}}{2^{4s}p^{2p^n-1}} = 2^{4s}p^{4ns-2p^n-1} \quad (3.69)$$

e, como

$$N_{\mathbb{Q}(m)}(\mathfrak{d}_{\mathbb{Q}(m):\mathbb{K}}) = N_{\mathbb{Q}(m)}(\mathfrak{P}\mathcal{O}_{\mathbb{Q}(m)}) = N_{\mathbb{Q}(p^n)}(N_{\mathbb{Q}(m):\mathbb{Q}(p^n)}(\mathfrak{P}\mathcal{O}_{\mathbb{Q}(m)})) = N_{\mathbb{Q}(p^n)}(\mathfrak{P}^2) = (N_{\mathbb{Q}(p^n)}(\mathfrak{P}))^2 = p^2 \quad (3.70)$$

então o valor absoluto do discriminante do corpo $\mathbb{K}$ é

$$|D(\mathbb{K})| = \sqrt{|D(\mathbb{Q}(m))|/p^2} = 2^{2s}p^{2ns-p^n-1} \quad (3.71)$$

confirmando a assertiva (b), já que $\varphi(p^n) = 2s$. Agora, para $j = s, s+1, \dots, 2s-1$, temos $\sigma^j H = \sigma^{i+s} H$, em que $i = 0, 1, \dots, s-1$ é tal que $i = s-j$. Assim, $\sigma^j H = \sigma^{i+s} H = \{\sigma^{i+s}, \sigma^{i+2s}\} = \{\sigma^{i+s}, \sigma^i\} = \sigma^i H$. Logo, para todo $j = s, s+1, \dots, 2s-1$, existe $i = 0, 1, \dots, s-1$ tal que $\sigma^j H = \sigma^i H$. Analogamente, segue que para todo $j = s, s+1, \dots, 2s-1$, existe $i = 0, 1, \dots, s-1$ tal que $\sigma^j \tau H = \sigma^i \tau H$. Daí, como a ordem de G/H deve ser igual à razão entre a ordem de G e a de H , ou seja, a ordem de G/H é $\varphi(p^n) = 2s$, segue que $G/H = \{\sigma^i H, \sigma^i \tau H : 0 \leq i < s\}$. Dessa forma, podemos calcular o diferente $\mathfrak{d}_{\mathbb{K}}(\eta)$ do elemento η :

$$\mathfrak{d}_{\mathbb{K}}(\eta) = \prod_{\psi \in (G/H) \setminus \{e\}} (\eta - \psi(\eta)) = \prod_{j=0}^{s-1} \{(\eta - \sigma^j(\eta))(\eta - \sigma^j \tau(\eta))\} = (\eta - \tau(\eta)) \prod_{j=1}^{s-1} \{(\eta - \sigma^j(\eta))(\eta - \sigma^j \tau(\eta))\}. \quad (3.72)$$

Como $\eta - \tau(\eta) = 2\xi_4(\xi_{p^n} + \xi_{p^n}^{-1})$ e

$$\begin{aligned} (\eta - \sigma^j(\eta))(\eta - \sigma^j \tau(\eta)) &= \xi_4(\xi_{p^n} - \xi_{p^n}^{r^j} + \xi_{p^n}^{-1} - \xi_{p^n}^{-r^j}) \xi_4(\xi_{p^n} + \xi_{p^n}^{-1} + \xi_{p^n}^{r^j} + \xi_{p^n}^{-r^j}) = \\ &= \xi_4^2((\xi_{p^n} + \xi_{p^n}^{-1})^2 - (\xi_{p^n}^{r^j} + \xi_{p^n}^{-r^j})^2) = \xi_4^2 \xi_{p^n}^{-2} [(\xi_{p^n}^2 - \xi_{p^n}^{2r^j})(\xi_{p^n}^2 - \xi_{p^n}^{2r^j})] \end{aligned} \quad (3.73)$$

então

$$\mathfrak{d}_{\mathbb{K}}(\eta) = (\xi_4/\xi_{p^n})^{2(s-1)} 2\xi_4(\xi_{p^n} + \xi_{p^n}^{-1}) \prod_{j=1}^{s-1} \{(\xi_{p^n}^2 - \sigma^j(\xi_{p^n}^2))(\xi_{p^n}^2 - \sigma^j(\xi_{p^n}^{-2}))\}. \quad (3.74)$$

Pelo fato de que para todo $j = 1, \dots, p^n$ tal que $\text{mdc}(j, p^n) = 1$ existe $i \in \{1, 2, \dots, p^n\}$ tal que $\text{mdc}(i, p^n) = 1$ e $\xi_{p^n}^{2j} = \xi_{p^n}^i$ então

$$\{\xi_{p^n}^{2j} : 0 < j < p^n, \text{mdc}(j, p^n) = 1\} \subset \{\xi_{p^n}^i : 0 < i < p^n, \text{mdc}(i, p^n) = 1\}. \quad (3.75)$$

Mais ainda, esses conjuntos são iguais, pois o segundo possui $\varphi(p^n)$ elementos (claro) e o primeiro também possui $\varphi(p^n)$ elementos, já que $\xi_{p^n}^{2j} = \xi_{p^n}^{2k}$ implica $j = k$ para $0 < j, k < p^n$ tais que $\text{mdc}(j, p^n) = \text{mdc}(k, p^n) = 1$. Assim,

$$\begin{aligned} \{\xi_{p^n}^i : 0 < i < p^n, \text{mdc}(i, p^n) = 1\} &= \{\xi_{p^n}^{2j} : 0 < j < p^n, \text{mdc}(j, p^n) = 1\} = \{\psi(\xi_{p^n}^2) : \psi \in \text{Gal}(\mathbb{Q}^{(p^n)} : \mathbb{Q})\} = \\ &= \{\sigma^j(\xi_{p^n}^2), \sigma^{j+s}(\xi_{p^n}^2) : j = 0, 1, \dots, s-1\} = \{\sigma^j(\xi_{p^n}^2), \sigma^j(\xi_{p^n}^{-2}) : j = 0, 1, \dots, s-1\} \end{aligned} \quad (3.76)$$

donde segue que $\{\sigma^j(\xi_{p^n}^2), \sigma^j(\xi_{p^n}^{-2}) : j = 0, 1, \dots, s-1\} = \{\xi_{p^n}^j : 0 < j < p^n, \text{mdc}(j, p^n) = 1\}$. Logo, o p^n -ésimo polinômio ciclotômico, Φ_{p^n} , é dado por

$$\Phi_{p^n}(x) = \prod_{\substack{j=0 \\ \text{mdc}(j, p^n)=1}}^{p^n} (x - \xi_{p^n}^j) = (x - \xi_{p^n}^2)(x - \xi_{p^n}^{-2})f(x) \quad (3.77)$$

em que $f(x) = \prod_{j=1}^{s-1} \{(x - \sigma^j(\xi_{p^n}^2))(x - \sigma^j(\xi_{p^n}^{-2}))\}$. Como $\Phi'_{p^n}(x) = (\xi_{p^n}^2 - \xi_{p^n}^{-2})f(\xi_{p^n}^2) + (x - \xi_{p^n}^{-2})f(x) + (x - \xi_{p^n}^2)f'(x)$, então

$$f(\xi_{p^n}^2) = \Phi'_{p^n}(\xi_{p^n}^2)/(\xi_{p^n}^2 - \xi_{p^n}^{-2}). \quad (3.78)$$

Note, da equação 3.74, que $\mathfrak{d}_{\mathbb{K}}(\eta) = (\xi_4/\xi_{p^n})^{2(s-1)}2\xi_4(\xi_{p^n} + \xi_{p^n}^{-1})f(\xi_{p^n}^2)$. Como ξ_4 , ξ_{p^n} e $\xi_{p^n}^{-1}$ são unidades de $\mathcal{O}_{\mathbb{Q}(m)}$, então $\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)} = 2(\xi_{p^n} + \xi_{p^n}^{-1})f(\xi_{p^n}^2)\mathcal{O}_{\mathbb{Q}(m)}$ e, como $(\xi_{p^n} + \xi_{p^n}^{-1})(\xi_{p^n} - \xi_{p^n}^{-1}) = \xi_{p^n}^2 - \xi_{p^n}^{-2}$, segue da igualdade de ideais anterior e da equação 3.78 que

$$\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)} = 2\Phi'_{p^n}(\xi_{p^n}^2)/(\xi_{p^n}^2 - \xi_{p^n}^{-2})\mathcal{O}_{\mathbb{Q}(m)}. \quad (3.79)$$

Por fim, pelo lema 3.3.4, $p^n \xi_{p^n}^{2(p^n-1)}/\Phi'_{p^n}(\xi_{p^n}^2) = \xi_p^2 - 1$ e, então

$$\Phi'_{p^n}(\xi_{p^n}^2)\mathcal{O}_{\mathbb{Q}(p^n)} = p^n/(\xi_p^2 - 1)\mathcal{O}_{\mathbb{Q}(p^n)} = p^n/(\xi_p - 1)\mathcal{O}_{\mathbb{Q}(p^n)}. \quad (3.80)$$

A última igualdade seguiu porque $\text{mdc}(2, p) = \text{mdc}(1, p) = 1$ e, daí, $(\xi_p^2 - 1)\mathcal{O}_{\mathbb{Q}(p^n)} = (\xi_p - 1)\mathcal{O}_{\mathbb{Q}(p^n)}$. Logo, $\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)} = 2p^n(1 - \xi_p)^{-1}(1 - \xi_{p^n})^{-1}\mathcal{O}_{\mathbb{Q}(m)}$. Utilizando esta última igualdade e notando que

$$N_{\mathbb{Q}(m)}((\xi_p - 1)\mathcal{O}_{\mathbb{Q}(m)}) = N_{\mathbb{Q}(p)}(N_{\mathbb{Q}(m):\mathbb{Q}(p)}((\xi_p - 1)\mathcal{O}_{\mathbb{Q}(m)})) = N_{\mathbb{Q}(p)}((\xi_p - 1)^{\varphi(m)/(p-1)}) = p^{\frac{\varphi(m)}{p-1}} = p^{2p^{n-1}} \quad (3.81)$$

inferimos que

$$\begin{aligned} N_{\mathbb{Q}(m)}(\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)}) &= N_{\mathbb{Q}(m)}(2p^n(1 - \xi_p)^{-1}(1 - \xi_{p^n})^{-1}\mathcal{O}_{\mathbb{Q}(m)}) = p^{-2p^{n-1}}N_{\mathbb{Q}(m)}(2p^n(1 - \xi_{p^n})^{-1}\mathcal{O}_{\mathbb{Q}(m)}) = \\ &= p^{-2p^{n-1}}N_{\mathbb{K}}(N_{\mathbb{Q}(m):\mathbb{K}}(2p^n(1 - \xi_{p^n})^{-1}\mathcal{O}_{\mathbb{Q}(m)})) = p^{-2p^{n-1}}2^{4s}p^{4ns}p^{-2} = 2^{4s}p^{4ns-2p^{n-1}-2} \end{aligned} \quad (3.82)$$

e, assim, o valor absoluto do discriminante de $\mathcal{B} = \{1, \eta, \dots, \eta^{2\varphi(p^n)}\}$ é

$$|D_{\mathbb{K}}(\eta)| = N_{\mathbb{K}}(\mathfrak{d}_{\mathbb{K}}(\eta)) = \sqrt{N_{\mathbb{Q}(m)}(\mathfrak{d}_{\mathbb{K}}(\eta)\mathcal{O}_{\mathbb{Q}(m)})} = \sqrt{2^{4s}p^{4ns-2p^{n-1}-2}} = 2^{2s}p^{2ns-p^{n-1}-1}. \quad (3.83)$$

Portanto, $|D_{\mathbb{K}}(\eta)| = |D(\mathbb{K})|$, donde concluímos que o anel de inteiros de $\mathbb{K}$ admite base integral de potências, ou seja, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\eta]$, como queríamos demonstrar. $\square$

Por fim, faremos um breve comentário sobre alguns subcorpos de $\mathbb{Q}(\zeta_p)$, em que p é um número primo. Seja g uma raiz primitiva módulo p , isto é, g satisfaz $x^{p-1} \equiv 1 \pmod{p}$ e não satisfaz $x^i \equiv 1 \pmod{p}$ se $1 \leq i \leq p-2$. Fixe um divisor e de $p-1$ e tome $f = (p-1)/e$ (apesar da notação similar, não há relação dela com índices de ramificação nem grau de inércia). Defina

$$\eta_i = \sum_{j=0}^{f-1} \zeta_p^{g^{ej+i}}, \quad i = 0, 1, \dots, e-1. \quad (3.84)$$

Cada um desses η_i é chamado **período** e sua importância é exemplificada a seguir. Seja σ um $\mathbb{Q}$ -automorfismo de $\mathbb{Q}(\zeta_p)$ tal que $\sigma(\zeta_p) = \zeta_p^g$. Como g é uma raiz primitiva, então σ gera o grupo de Galois. O subgrupo de ordem f é $H = \{1, \sigma^e, \dots, \sigma^{e(f-1)}\}$, que corresponde a $\{1, g^e, \dots, g^{e(f-1)}\} \subset \mathbb{Z}_p^*$. Consequentemente, $\{g^{ej+i} : 0 \leq j \leq f-1\}$ é uma classe lateral deste grupo. Verifica-se que H fixa η_i . Além disso, $\sigma(\eta_i) = \eta_{i+1}$, para $0 \leq i \leq e-2$, e $\sigma(\eta_{e-1}) = \eta_0$. Então η_i tem exatamente e conjugados por $\text{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Disso segue que, para qualquer i , η_i gera um subcorpo de $\mathbb{Q}(\zeta_p)$ de grau e sobre $\mathbb{Q}$. Por exemplo, o elemento $\zeta_p + \zeta_p^{-1}$ que gera o subcorpo maximal real de $\mathbb{Q}(\zeta_p)$ é um período. Neste caso, $f = 2$ e $e = (p-1)/2$.

No próximo capítulo, entre outros assuntos, iremos querer responder à seguinte pergunta: $\mathbb{Z}[\eta_i]$ é o anel de inteiros de $\mathbb{Q}(\eta_i)$? Como vimos, se $f = 2$ e $\eta_i = \zeta_p$ então isso é verdade (proposição 3.3.1). Porém, se $f > 2$, veremos que isso nem sempre ocorre.

Conclusão

Na primeira seção deste capítulo, mostramos que o anel de inteiros de um corpo quadrático $\mathbb{Q}(\sqrt{d})$ é $\mathbb{Z}[\sqrt{d}]$ ou $\mathbb{Z}[1/2 + 1/2\sqrt{d}]$, dependendo do resto de d na divisão por 4, e explicitamos o discriminante desse corpo. Na segunda seção, desenvolvemos a teoria básica sobre as raízes da unidade e os corpos ciclotômicos, mostramos que o anel de inteiros de um corpo ciclotômico $\mathbb{Q}(\zeta_m)$ é $\mathbb{Z}[\zeta_m]$ e apresentamos o discriminante desse corpo. Na última seção, enunciamos o Teorema de Kronecker-Weber, vimos que o anel de inteiros do subcorpo maximal real $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ é $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$ e provamos que o anel de inteiros dos subcorpos $\mathbb{Q}(\eta) \subset \mathbb{Q}(\zeta_m)$ é $\mathbb{Z}[\eta]$, em que $\eta = \zeta_m - \zeta_m^{-1}$, $m = 2^n$ ou $m = 4p^n$ ($p > 2$ primo), além de explicitar seu discriminante. Os teoremas 3.3.2 e 3.3.3, que provam este último fato, têm demonstrações bem elaboradas e mereceram um minucioso desenvolvimento.

Capítulo 4

Bases integrais normais e potentes

Na Álgebra Linear é notável a importância das bases para os espaços vetoriais, pois seus elementos são geradores desses espaços. Por esse motivo, é importante o conhecimento da base de uma extensão finita de corpos. Há alguns tipos de bases que são mais interessantes como, por exemplo, as bases potentes e as bases normais, as quais serão objetos de nosso estudo neste capítulo. Além disso, também estudaremos as bases potentes e as bases normais para anéis de inteiros de corpos de números sobre $\mathbb{Z}$.

4.1 Bases normais e bases potentes

Inicialmente, vamos discutir sobre bases potentes de um corpo de números. Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos de números, a qual é, então, finita e separável. Pelo Teorema do Elemento Primitivo (proposição 1.1.1) vimos que existe $u \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(u)$. Este elemento u chama-se elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$. O grau do polinômio minimal de u coincide com o grau da extensão $[\mathbb{L} : \mathbb{K}]$ e, portanto, $\{1, u, \dots, u^{[\mathbb{L}:\mathbb{K}]-1}\}$ é uma base do $\mathbb{K}$ -espaço vetorial $\mathbb{L}$.

Definição 4.1.1. Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão de corpos de números de grau n e $\mathcal{B} = \{1, u, \dots, u^{n-1}\}$ é uma $\mathbb{K}$ -base do espaço vetorial $\mathbb{L}$ então $\mathcal{B}$ é chamada **base de potências** (ou **base potente**) de $\mathbb{L}$ sobre $\mathbb{K}$. Se $\mathbb{K} = \mathbb{Q}$, podemos dizer simplesmente que $\mathcal{B}$ é uma base de potências de $\mathbb{L}$.

Como corolário imediato do Teorema do Elemento Primitivo e pela discussão que fizemos inicialmente, temos a seguinte proposição:

Proposição 4.1.1. Toda extensão de corpos de números admite uma base de potências. □

Exemplo 4.1.1. Se $\zeta_5 = e^{\frac{2\pi i}{5}}$, o conjunto $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ é uma base de potências do corpo ciclotômico $\mathbb{Q}(\zeta_5)$ (sobre $\mathbb{Q}$).

Agora, discutiremos sobre bases normais. Como vimos na definição 1.3.6, se A é um anel com unidade e G é um grupo, então $A[G]$ é um anel de grupo, cujos elementos são da forma $\sum_{g \in G} a_g g$ (soma finita), com cada $a_g \in A$. Se G é o grupo de Galois de alguma extensão de corpos de números $\mathbb{K} \subset \mathbb{L}$ galoisiana (então G é finito) e $\alpha \in \mathbb{L}$, então definimos

$$A[G]\alpha = \left\{ \sum_{\sigma \in G} a_\sigma \sigma(\alpha) : a_\sigma \in A \right\}. \quad (4.1)$$

Definição 4.1.2. Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana finita de grau n e $G = \text{Gal}(\mathbb{L} : \mathbb{K}) = \{\sigma_i : 1 \leq i \leq n\}$. Se existe $\alpha \in \mathbb{L}$ tal que $\mathcal{B} = \{\sigma_i(\alpha) : 1 \leq i \leq n\}$ é uma base do $\mathbb{K}$ -espaço vetorial $\mathbb{L}$, dizemos que $\mathcal{B}$ é uma **base normal** de $\mathbb{L}$ sobre $\mathbb{K}$. Isso é equivalente a dizer que existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}[G]\alpha$.

Exemplo 4.1.2. Considere a extensão galoisiana $\mathbb{Q} \subset \mathbb{Q}(i)$ de grau 2, em que $i = \sqrt{-1}$. Assim, $G = \text{Gal}(\mathbb{Q}(i) : \mathbb{Q}) = \{id, \sigma\}$, em que $\sigma(i) = -i$. Tome $\alpha = 1 + i$. Então $\beta = \sigma(\alpha) = 1 - i$. Considere $\mathcal{B} = \{\alpha, \sigma(\alpha)\} = \{\alpha, \beta\} = \{1 + i, 1 - i\}$. O conjunto $\mathcal{B}$ gera $\mathbb{Q}(i)$ sobre $\mathbb{Q}$, pois, para qualquer $a + bi \in \mathbb{Q}(i)$ ($a, b \in \mathbb{Q}$), tem-se que

$$a + bi = \frac{a+b}{2}\alpha + \frac{a-b}{2}\beta. \quad (4.2)$$

Logo, como $\mathbb{Q}(i)$ é um $\mathbb{Q}$ -espaço vetorial de dimensão dois e $\mathcal{B}$ tem dois elementos que geram $\mathbb{Q}(i)$ então $\mathcal{B}$ é uma base normal de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$.

Nosso objetivo a seguir é mostrar que toda extensão galoisiana finita admite base normal.

Lema 4.1.1 (Lema de Dedekind). *Seja $\mathbb{L}$ um corpo. Distintos automorfismos de um corpo $\mathbb{L}$ são linearmente independentes sobre $\mathbb{L}$.*

Demonstração. Suponhamos que um conjunto $S = \{\sigma_1, \dots, \sigma_n\}$ de automorfismos de $\mathbb{L}$ seja linearmente dependente sobre $\mathbb{L}$. Logo, existem $a_i \in \mathbb{L}$ ($1 \leq i \leq n$) não todos nulos tais que $a_1\sigma_1 + a_2\sigma_2 + \dots + a_n\sigma_n = 0$. Logo,

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \dots + a_n\sigma_n(x) = 0, \quad \forall x \in \mathbb{L}. \quad (4.3)$$

Suponhamos, sem perda de generalidade, que $a_i \neq 0$ para todo i e que n seja o menor possível (senão, retire os elementos em excesso). Se $n = 1$ então $a_1\sigma_1(x) = 0$, para todo $x \in \mathbb{L}$. Logo, $a_1 = 0$, o que é

um absurdo. Agora, sendo n qualquer, como $\sigma_1 \neq \sigma_n$ então existe $c \in \mathbb{L}$ tal que $\sigma_1(c) \neq \sigma_n(c)$. Pelo fato de cx pertencer a $\mathbb{L}$ para todo $x \in \mathbb{L}$, segue que $a_1\sigma_1(cx) + a_2\sigma_2(cx) + \dots + a_n\sigma_n(cx) = 0$. Logo,

$$a_1\sigma_1(c)\sigma_1(x) + a_2\sigma_2(c)\sigma_2(x) + \dots + a_n\sigma_n(c)\sigma_n(x) = 0, \quad \forall x \in \mathbb{L}. \quad (4.4)$$

Multiplicando a equação 4.3 por $\sigma_1(c)$ e subtraindo a expressão obtida de 4.4, obtém-se

$$a_2(\sigma_2(c) - \sigma_1(c))\sigma_2(x) + \dots + a_n(\sigma_n(c) - \sigma_1(c))\sigma_n(x) = 0, \forall x \in \mathbb{L} \quad (4.5)$$

com o termo $a_n(\sigma_n(c) - \sigma_1(c)) \neq 0$ para todo $x \in G$, o que é um absurdo devido ao fato de termos assumido n o menor número de elementos não nulos na combinação dos σ_i com coeficientes em $\mathbb{L}$. Logo, S é linearmente independente. $\square$

A seguir mostraremos um caso especial do que queremos: se uma extensão galoisiana é cíclica então essa extensão admite base normal.

Proposição 4.1.2. *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana de grau n com grupo de Galois cíclico $G = \text{Gal}(\mathbb{L} : \mathbb{K}) = \langle \sigma \rangle$. Então existe $\alpha \in \mathbb{L}$ tal que $\{\alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)\}$ é uma base para o $\mathbb{K}$ -espaço vetorial $\mathbb{L}$.*

Demonstração. Seja $\sigma : \mathbb{L} \rightarrow \mathbb{L}$ um $\mathbb{K}$ -automorfismo de $\mathbb{L}$, o qual pode ser considerado uma transformação linear do $\mathbb{K}$ -espaço vetorial $\mathbb{L}$. Seja $m_\sigma(x)$ o polinômio mônico de menor grau tal que $m_\sigma(\sigma) = 0$ (isto é, o polinômio minimal de σ). Como σ é raiz de $x^n - 1$, pois $\sigma^n = \text{id}$, então $m_\sigma(x)$ divide $x^n - 1$. No entanto, os n elementos σ^i ($0 \leq i \leq n-1$) são distintos e, devido ao lema 4.1.1, são linearmente independentes sobre $\mathbb{K}$. Portanto, não existe um polinômio de grau menor do que n que tenha σ como raiz. Dessa forma, o polinômio minimal de σ deve ter grau maior ou igual a n . Como $x^n - 1$ admite σ como raiz e é mônico, então $m_\sigma(x) = x^n - 1$. Como o polinômio característico de uma transformação linear (no caso, σ) é divisível pelo seu polinômio minimal, é mônico e tem grau igual a $[\mathbb{L} : \mathbb{K}] = n$, concluímos que o polinômio característico e o polinômio minimal de σ são iguais a $x^n - 1$. Devido a resultados de Álgebra Linear¹, segue que existe $\alpha \in \mathbb{L}$ tal que $\{\alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)\}$ é uma base para o $\mathbb{K}$ -espaço vetorial $\mathbb{L}$. $\square$

Lema 4.1.2. *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana finita de grau n com grupo de Galois $G = \{\sigma_i : 1 \leq i \leq n\}$. Então $\{a_1, \dots, a_n\}$ é uma base para o $\mathbb{K}$ -espaço vetorial $\mathbb{L}$ se, e só se, $\det(\sigma_i(a_j)) \neq 0$.*

¹ Consulte a definição de vetor cíclico e o segundo corolário do teorema 3 no capítulo 7 de [14].

Demonstração. Seja $A = [\sigma_i(a_j)]$. Por um lado, se $\{a_1, \dots, a_n\}$ não é uma $\mathbb{K}$ -base para $\mathbb{L}$ então existem $c_1, \dots, c_n \in \mathbb{K}$, não todos nulos, tais que $c_1 a_1 + \dots + c_n a_n = 0$. Assim, $Ac^T = 0$, em que $c = (c_1, \dots, c_n)$, donde segue que $\det(A) \neq 0$, pois o sistema em questão possui uma solução não nula. Por outro lado, suponha que $\{a_1, \dots, a_n\}$ seja uma base para o espaço vetorial $\mathbb{L}$ sobre $\mathbb{K}$ e que $\det(A) = 0$. Assim, existe $d = (d_1, \dots, d_n) \in \mathbb{L}^n$ não nulo tal que $d_1 \sigma_1(a_i) + \dots + d_n \sigma_n(a_i) = 0$, para todo $i \in \{1, 2, \dots, n\}$. Por linearidade, como $\{a_1, \dots, a_n\}$ é base, tem-se que $d_1 \sigma_1(x) + \dots + d_n \sigma_n(x) = 0$, para todo $x \in \mathbb{L}$, o que contradiz o lema 4.1.1. Logo, $\det(A) \neq 0$. $\square$

A proposição seguinte é conhecida como Independência Algébrica dos Automorfismos.

Proposição 4.1.3. *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana finita de grau n com grupo de Galois $G = \{\sigma_1, \dots, \sigma_n\}$. Suponha que $\mathbb{K}$ seja um corpo infinito. Se $f \in \mathbb{L}[x_1, \dots, x_n]$ é um polinômio de n variáveis tal que $f(\sigma_1(x), \dots, \sigma_n(x)) = 0$, para todo $x \in \mathbb{L}$, então f é o polinômio nulo.*

Demonstração. Sejam $\{a_1, \dots, a_n\}$ uma $\mathbb{K}$ -base para $\mathbb{L}$ e $A = [\sigma_i(a_j)]$. Para todo $x \in \mathbb{L}$, tem-se que $x = y_1 a_1 + \dots + y_n a_n$, com $y_1, \dots, y_n \in \mathbb{K}$. Então, se $y = (y_1, \dots, y_n)$ então $f(\sigma_1(x), \dots, \sigma_n(x)) = f(Ay) = g(y_1, \dots, y_n)$, para algum $g \in \mathbb{L}[x_1, \dots, x_n]$. Daí, $g(y_1, \dots, y_n) = 0$ em $\mathbb{K}^n$ e, assim, $g \equiv 0$. Disso, segue que f também é identicamente nulo. $\square$

Finalmente, o teorema a seguir garante que toda extensão finita galoisiana admite base normal.

Teorema 4.1.1 (Teorema da Base Normal). *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana finita tal que $G = \text{Gal}(\mathbb{L} : \mathbb{K})$. Então, existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}[G]\alpha$, isto é, $\mathbb{L}$ admite uma $\mathbb{K}$ -base normal gerada por α .*

Demonstração. Se $\mathbb{K}$ e $\mathbb{L}$ são corpos finitos então a proposição 4.1.2 garante o resultado. Caso contrário, consideremos que $\mathbb{K}$ é infinito. Suponha que $G = \{\sigma_1, \dots, \sigma_n\}$ e que $x_i = x_{\sigma_i}$. Considere $f(x_1, \dots, x_n) = \det(x_{\sigma_i \sigma_j})$. Dessa forma, $f(1, 0, \dots, 0)$ é o determinante de uma matriz de permutação e, portanto, é não nulo. Assim, f não é identicamente nulo e, devido à proposição 4.1.3, existe $\alpha \in \mathbb{L}$ tal que $f(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) = \det(\sigma_i(\sigma_j(\alpha))) \neq 0$. Por isso, o lema 4.1.2 garante que $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$ é uma base para $\mathbb{L}$ sobre $\mathbb{K}$. $\square$

4.2 Bases integrais normais

Na seção anterior discutimos sobre bases normais. O Teorema da Base Normal (teorema 4.1.1) nos garantiu que toda extensão galoisiana finita admite base normal. Nosso interesse agora é estudar

bases *integrais* de extensões de corpos de números. Daremos uma condição necessária e suficiente para que um corpo de números *abeliano* possua base integral normal sobre $\mathbb{Q}$, mesmo não sendo possível fazer a mesma afirmação do Teorema da Base Normal para bases integrais em geral. O resultado que objetivamos demonstrar é o Teorema de Hilbert-Speiser.

Definição 4.2.1. *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana (finita) de corpos de números cujo grupo de Galois é $G = \{\sigma_1, \dots, \sigma_n\}$. Dizemos que a extensão $\mathbb{K} \subset \mathbb{L}$ possui uma base integral normal (BIN) se existe um elemento $\alpha \in \mathcal{O}_{\mathbb{L}}$ tal que $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$ é uma base para $\mathcal{O}_{\mathbb{L}}$ sobre $\mathcal{O}_{\mathbb{K}}$, isto é, se $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[G]\alpha$. Neste caso, dizemos que α gera uma base integral normal para $\mathbb{K} \subset \mathbb{L}$.*

Proposição 4.2.1. *Seja $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ uma extensão de corpos de números tal que $\mathbb{K} \subset \mathbb{L}$ e $\mathbb{K} \subset \mathbb{F}$ são galoisianas. Se α gera uma BIN para $\mathbb{K} \subset \mathbb{L}$ então $Tr_{\mathbb{L}:\mathbb{F}}(\alpha)$ gera uma BIN para $\mathbb{K} \subset \mathbb{F}$.*

Demonstração. Estabeleçamos as seguintes notações: $G = Gal(\mathbb{L} : \mathbb{K})$, $H = Gal(\mathbb{L} : \mathbb{F})$ e $\bar{G} = Gal(\mathbb{F} : \mathbb{K}) \simeq G/H$. Por hipótese, existe $\alpha \in \mathbb{L}$ tal que $\{g(\alpha)\}_{g \in G}$ é uma BIN para $\mathbb{K} \subset \mathbb{L}$. Para qualquer $x \in \mathcal{O}_{\mathbb{F}}$ (então $x \in \mathcal{O}_{\mathbb{L}}$), existem únicos elementos $c(g) \in \mathcal{O}_{\mathbb{K}}$ tais que $x = \sum_{g \in G} c(g)g(\alpha)$. Como $x \in \mathbb{F}$ então $h(x) = x$, para todo $h \in H$. Temos:

$$h(x) = \sum_{g \in G} c(g)(h \circ g)(\alpha) = \sum_{g \in G} c(h^{-1} \circ g)(h^{-1} \circ h \circ g)(\alpha) = \sum_{g \in G} c(h^{-1} \circ g)g(\alpha). \quad (4.6)$$

Devido à unicidade de $c(g)$ e ao fato de que $h(x) = x$, tem-se que $c(h^{-1}g) = c(g)$ para todo $g \in G$ e $h \in H$ (ou seja, $c(h \circ g) = c(g)$). Para cada $\sigma \in \bar{G}$, existe $\tilde{\sigma} \in G$ tal que $\tilde{\sigma}H = \sigma$. Assim,

$$\begin{aligned} x &= \sum_{g \in G} c(g)g(\alpha) = \sum_{\sigma \in \bar{G}} \sum_{h \in H} c(h \circ \tilde{\sigma})(h \circ \tilde{\sigma})(\alpha) = \sum_{\sigma \in \bar{G}} c(\tilde{\sigma}) \sum_{h \in H} (h \circ \tilde{\sigma})(\alpha) = \\ &= \sum_{\sigma \in \bar{G}} c(\tilde{\sigma})\tilde{\sigma}(Tr_{\mathbb{L}:\mathbb{F}}(\alpha)) = \sum_{\sigma \in \bar{G}} c(\tilde{\sigma})\sigma(Tr_{\mathbb{L}:\mathbb{F}}(\alpha)). \end{aligned} \quad (4.7)$$

(note que na penúltima igualdade foi usado o fato de que H é normal em G). Portanto, $\mathcal{O}_{\mathbb{F}}$ admite uma $\mathcal{O}_{\mathbb{K}}$ -base normal gerada por $Tr_{\mathbb{L}:\mathbb{F}}(\alpha)$. $\square$

Corolário 4.2.1. *Se $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ é uma extensão galoisiana de corpos de números e $\mathbb{K} \subset \mathbb{L}$ tem BIN, então $Tr_{\mathbb{L}:\mathbb{F}}(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{F}}$.*

Demonstração. Por um lado, o corolário 2.2.2 garante que $Tr_{\mathbb{L}:\mathbb{F}}(\mathcal{O}_{\mathbb{L}}) \subset \mathcal{O}_{\mathbb{F}}$. Por outro lado, se $x \in \mathcal{O}_{\mathbb{F}}$ então (mantendo as notações da demonstração da proposição anterior) a fórmula 4.7 acarreta

$$x = \sum_{\sigma \in \bar{G}} c(\tilde{\sigma}) \sum_{h \in H} (h \circ \tilde{\sigma})(\alpha) = \sum_{\sigma \in \bar{G}} c(\tilde{\sigma})Tr_{\mathbb{L}:\mathbb{F}}(\tilde{\sigma}(\alpha)) = Tr_{\mathbb{L}:\mathbb{F}}\left(\sum_{\sigma \in \bar{G}} c(\tilde{\sigma})\tilde{\sigma}(\alpha)\right). \quad (4.8)$$

Como $\sum_{\sigma \in \bar{G}} c(\tilde{\sigma}) \tilde{\sigma}(\alpha)$ pertence a $\mathcal{O}_{\mathbb{L}}$ então $x \in \text{Tr}_{\mathbb{L}:\mathbb{F}}(\mathcal{O}_{\mathbb{L}})$, donde segue finalmente que $\mathcal{O}_{\mathbb{F}} \subset \text{Tr}_{\mathbb{L}:\mathbb{F}}(\mathcal{O}_{\mathbb{L}})$. $\square$

Corolário 4.2.2. *Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão galoisiana de corpos de números que admite BIN então $\text{Tr}_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{K}}$.*

Demonstração. Segue imediatamente do corolário 4.2.1. $\square$

Nós mostramos que se $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ é uma extensão de corpos de números tal que $\mathbb{K} \subset \mathbb{L}$ e $\mathbb{K} \subset \mathbb{F}$ são galoisianas e se $\mathbb{K} \subset \mathbb{L}$ tem BIN então $\mathbb{F} \subset \mathbb{L}$ tem BIN. No entanto, se $\mathbb{K} \subset \mathbb{L}$ tem BIN num caso mais geral, não é sempre verdade que $\mathbb{F} \subset \mathbb{L}$ também tem BIN. Por exemplo, se $\mathbb{K} = \mathbb{Q}$, $\mathbb{F} = \mathbb{Q}(\sqrt{-7})$ e $\mathbb{L} = \mathbb{Q}(\zeta_7)$ então ζ_7 gera uma base integral normal para $\mathbb{K} \subset \mathbb{L}$, mas $\mathbb{F} \subset \mathbb{L}$ não tem BIN (veja [4]).

Proposição 4.2.2. *Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ dois corpos de números de graus n e m , respectivamente, e tais que $\delta_{\mathbb{K}_1:\mathbb{Q}}$ e $\delta_{\mathbb{K}_2:\mathbb{Q}}$ são relativamente primos. Suponha que $\mathbb{Q} \subset \mathbb{K}_1$ é galoisiana com grupo de Galois $G = \{\sigma_i\}_{1 \leq i \leq n}$. Então:*

(a) *Se $\mathbb{K}_1$ tem BIN dada por $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$, $\alpha \in \mathcal{O}_{\mathbb{K}_1}$, então $\mathcal{O}_{\mathbb{K}_1\mathbb{K}_2}$ admite BIN sobre $\mathcal{O}_{\mathbb{K}_2}$ dada por $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$. Em outras palavras, se $\mathcal{O}_{\mathbb{K}_1} = \mathbb{Z}[G]\alpha$ então $\mathcal{O}_{\mathbb{K}_1\mathbb{K}_2} = \mathcal{O}_{\mathbb{K}_2}[G]\alpha$.*

(b) *Além disso, se $\mathbb{Q} \subset \mathbb{K}_2$ é galoisiana com grupo de Galois $H = \{\tau_i\}_{1 \leq i \leq m}$ e se existe $\beta \in \mathcal{O}_{\mathbb{K}_2}$ tal que $\{\tau_1(\beta), \dots, \tau_m(\beta)\}$ é BIN de $\mathbb{K}_2$ sobre $\mathbb{Q}$ então $\{\sigma_i\tau_j(\alpha\beta)\}_{1 \leq i,j \leq n}$ também é BIN para $\mathbb{K}_1\mathbb{K}_2$ sobre $\mathbb{Q}$. Em outras palavras, se $\mathcal{O}_{\mathbb{K}_1} = \mathbb{Z}[G]\alpha$ e $\mathcal{O}_{\mathbb{K}_2} = \mathbb{Z}[H]\beta$ então $\mathcal{O}_{\mathbb{K}_1\mathbb{K}_2} = \mathbb{Z}[G \times H](\alpha\beta)$.*

Demonstração. (a) Por hipótese e devido à proposição 2.7.10, temos

$$\mathcal{O}_{\mathbb{K}_1\mathbb{K}_2} = \mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2} = \mathcal{O}_{\mathbb{K}_2}\mathbb{Z}[G]\alpha. \quad (4.9)$$

Como $\mathbb{Z} \subset \mathcal{O}_{\mathbb{K}_2}$ e como $\mathcal{O}_{\mathbb{K}_2}$ tem base normal sobre $\mathbb{Z}$ então, por fim, $\mathcal{O}_{\mathbb{K}_2}\mathbb{Z}[G]\alpha = \mathcal{O}_{\mathbb{K}_2}[G]\alpha$.

(b) Por hipótese e devido à proposição 2.7.10, temos

$$\mathcal{O}_{\mathbb{K}_1\mathbb{K}_2} = \mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2} = \mathbb{Z}[G]\alpha\mathbb{Z}[H]\beta. \quad (4.10)$$

Além disso, para $a_{ij} \in \mathbb{Z}$,

$$x \in \mathbb{Z}[G]\alpha\mathbb{Z}[H]\beta \iff x = \sum_{i=1}^n \sum_{j=1}^m a_{ij} \sigma_i(\alpha) \tau_j(\beta) \iff x = \sum_{i=1}^n \sum_{j=1}^m a_{ij} (\sigma_i \tau_j)(\alpha\beta). \quad (4.11)$$

Logo, $\mathbb{Z}[G]\alpha\mathbb{Z}[H]\beta = \mathbb{Z}[G \times H](\alpha\beta)$, completando a prova. $\square$

Nas condições acima, se $\mathbb{Q} \subset \mathbb{K}_1\mathbb{K}_2$ admite BIN então a proposição 4.2.1 garante que $\mathbb{Q} \subset \mathbb{K}_1$ e $\mathbb{Q} \subset \mathbb{K}_2$ também têm BIN. Portanto, o item (b) da proposição anterior é a recíproca deste fato. No

entanto, a recíproca do item (a) não ocorre sempre, ou seja, mesmo que $\mathbb{K}_2 \subset \mathbb{K}_1\mathbb{K}_2$ tenha BIN não se pode afirmar que $\mathbb{Q} \subset \mathbb{K}_1$ tem BIN.

Proposição 4.2.3. *Seja n um número inteiro positivo ímpar e livre de quadrados tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$, em que $\mathbb{K}$ é um corpo de números. Então $\mathbb{Q} \subset \mathbb{K}$ tem BIN gerada por $\text{Tr}_{\mathbb{Q}(\zeta_n):\mathbb{K}}(\zeta_n)$.*

Demonstração. Seja p um número primo ímpar e livre de quadrados. Denote por ζ uma raiz p -ésima primitiva da unidade. Devido ao teorema 3.2.1, $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$. Assim, $\{1, \zeta, \dots, \zeta^{p-2}\}$ é $\mathbb{Z}$ -base para $\mathcal{O}_{\mathbb{Q}(\zeta)}$. Como ζ é um elemento invertível nesse anel então $\zeta\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]$, donde segue que $\{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$ também é $\mathbb{Z}$ -base para $\mathcal{O}_{\mathbb{Q}(\zeta)}$. Assim, como $\text{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) = \langle \sigma \rangle$ (cíclico), em que $\sigma(\zeta) = \zeta^z$, em que z é um elemento primitivo módulo p , então $\{\sigma^i(\zeta)\}_{1 \leq i \leq p-1} = \{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$ é uma base normal para $\mathcal{O}_{\mathbb{Q}(\zeta)}$. Agora, seja n um número inteiro positivo ímpar e livre de quadrados. Vamos mostrar que ζ_n gera uma BIN para $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$. Se n é primo, o parágrafo anterior demonstra que $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ admite BIN. Caso contrário, existem um primo p e um inteiro positivo ímpar e livre de quadrados m relativamente primo a p tais que $n = pm$. Pelo visto acima, $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ tem BIN gerada por ζ_p . Suponhamos, por indução, que $\mathbb{Q} \subset \mathbb{Q}(\zeta_m)$ também tem BIN gerada por ζ_m . Pelo teorema 3.2.1, segue que os discriminantes de $\mathbb{Q}(\zeta_p)$ e de $\mathbb{Q}(\zeta_m)$ são relativamente primos. Pela proposição 4.2.2, $\zeta_p\zeta_m$ gera uma BIN para $\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_m)$. Agora, como p e m são relativamente primos então n é uma combinação linear sobre $\mathbb{Z}$ de p e m , donde segue que $\zeta'_n = \zeta_p\zeta_m$ é uma raiz n -ésima primitiva da unidade. Assim, $\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta'_n) = \mathbb{Q}(\zeta_n)$. Logo, ζ'_n é uma raiz n -ésima primitiva da unidade que gera uma base normal para $\mathbb{Q} \subset \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta'_n)$. Por fim, a proposição 4.2.1 garante que $\text{Tr}_{\mathbb{Q}(\zeta_n):\mathbb{K}}(\zeta'_n)$ gera uma BIN para $\mathbb{K} \subset \mathbb{Q}$. Podemos trocar ζ'_n por ζ_n , já que eles são conjugados, o que garante a tese. $\square$

A seguir, definiremos alguns conceitos necessários adiante envolvendo ramificação de ideais primos em corpos de números.

Definição 4.2.2. *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão finita de corpos de números, P um ideal primo (maximal) de $\mathcal{O}_{\mathbb{K}}$ e $P\mathcal{O}_{\mathbb{L}} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_g^{e_g}$ a ramificação de P em primos de $\mathcal{O}_{\mathbb{L}}$ (se a extensão for galoisiana, $e_1 = \dots = e_g$). Considere ainda p a característica do corpo $\mathcal{O}_{\mathbb{K}}/P$.*

(a) Dizemos que $\mathfrak{P}_i$ é **severamente ramificado** em $\mathbb{K} \subset \mathbb{L}$ se $p \mid e_i$. Caso contrário, dizemos que $\mathfrak{P}_i$ é **brandamente ramificado**.

(b) Dizemos que P é **severamente ramificado** em $\mathbb{K} \subset \mathbb{L}$ se algum dos $\mathfrak{P}_i$ é severamente ramificado. Caso contrário, dizemos que P é **brandamente ramificado**.

(c) Dizemos que $\mathbb{K} \subset \mathbb{L}$ é **brandamente ramificado** se todo ideal maximal de $\mathcal{O}_{\mathbb{K}}$ é brandamente ramificado em $\mathbb{K} \subset \mathbb{L}$.

Antes da seguinte proposição, é preciso observar que se $\mathbb{K} \subset \mathbb{L}$ é uma extensão de corpos de números finita então $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}})$ é um ideal de $\mathcal{O}_{\mathbb{K}}$. De fato, se $a \in \mathcal{O}_{\mathbb{K}}$ e $x, y \in \mathcal{O}_{\mathbb{L}}$ então $aTr_{\mathbb{L}:\mathbb{K}}(x) + Tr_{\mathbb{L}:\mathbb{K}}(y) = Tr_{\mathbb{L}:\mathbb{K}}(ax + y) \in Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}})$, devido à proposição 2.2.2.

Proposição 4.2.4. *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos de números galoisiana e P um ideal maximal de $\mathcal{O}_{\mathbb{K}}$. Então P divide $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}})$ se, e somente se, P é severamente ramificado em $\mathbb{L} \subset \mathbb{K}$.*

Demonstração. Como $\mathbb{K} \subset \mathbb{L}$ é uma extensão galoisiana então $P\mathcal{O}_{\mathbb{L}} = (\mathfrak{P}_1\mathfrak{P}_2\ldots\mathfrak{P}_g)^e$ (proposição 2.6.3). Estabeleçamos as seguintes notações: $\overline{\mathbb{L}}_i = \mathcal{O}_{\mathbb{L}}/\mathfrak{P}_i$, $\overline{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}/\mathfrak{P}_i$ e $p = \text{car}(\overline{\mathbb{L}}_i) = \text{car}(\overline{\mathbb{K}})$.

Tome $\alpha \in \mathcal{O}_{\mathbb{L}}$. A aplicação multiplicação por α , $m_{\alpha} : \mathcal{O}_{\mathbb{L}} \rightarrow \mathcal{O}_{\mathbb{L}}$, induz as seguintes $\overline{\mathbb{K}}$ -transformações lineares: $m_{\overline{\alpha}} : \mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \rightarrow \mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ e $m_{\overline{\alpha}_i} : \overline{\mathbb{L}}_i \rightarrow \overline{\mathbb{L}}_i$, em que $\overline{\alpha} = \alpha + P\mathcal{O}_{\mathbb{L}}$ e $\overline{\alpha}_i = \alpha + \mathfrak{P}_i\mathcal{O}_{\mathbb{L}}$. Considerados como $\overline{\mathbb{L}}_i$ -espaços vetoriais, é possível mostrar que

$$\overline{\mathbb{L}}_i = \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i} \simeq \frac{\mathfrak{P}_i}{\mathfrak{P}_i^2} \simeq \ldots \simeq \frac{\mathfrak{P}_i^{e-1}}{\mathfrak{P}_i^e}. \quad (4.12)$$

Escolha uma $\overline{\mathbb{K}}$ -base $\mathbf{B}_i$ se $\mathcal{O}_{\mathbb{L}}/\mathfrak{P}_i^e$ como segue: escolha uma base de $\mathfrak{P}_i^{e-1}/\mathfrak{P}_i^e$, estenda-a para $\mathfrak{P}_i^{e-2}/\mathfrak{P}_i^e$ e repita esse processo recursivamente.

Existe um isomorfismo canônico $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \simeq \oplus \mathcal{O}_{\mathbb{L}}/\mathfrak{P}_i^e$ (veja o Teorema Chinês do Resto; teorema 2.25 de [15]). Identificando essas duas $\overline{\mathbb{K}}$ -álgebras, temos que $\cup_{i=1}^g \mathbf{B}_i$ é uma $\overline{\mathbb{K}}$ -base de $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$. Em relação a essa base, a matriz de $m_{\overline{\alpha}}$ é diagonal superior em blocos, em que cada um dos *eg* blocos correspondem aos endomorfismos $m_{\overline{\alpha}_i}$ em $\overline{\mathbb{L}}_i \simeq \mathfrak{P}_i^{j-1}/\mathfrak{P}_i^j$, para algum $i \in \{1, \dots, g\}$ e para algum $j \in \{1, \dots, e\}$. Portanto, em $\overline{\mathbb{K}}$, temos:

$$\overline{Tr_{\mathbb{L}:\mathbb{K}}(\alpha)} = e \sum_{i=1}^g Tr_{\overline{\mathbb{L}}_i:\overline{\mathbb{K}}}(\overline{\alpha}_i). \quad (4.13)$$

Por um lado, se P é severamente ramificado em $\mathbb{K} \subset \mathbb{L}$, ou seja, $p \mid e$, então a equação anterior garante que $\overline{Tr_{\mathbb{L}:\mathbb{K}}(\alpha)} = 0$ em $\overline{\mathbb{K}}$, para qualquer $\alpha \in \mathcal{O}_{\mathbb{L}}$ (devido à característica de $\overline{\mathbb{K}}$ ser p). Logo, $P \mid Tr_{\mathbb{L}:\mathbb{K}}(\alpha)\mathcal{O}_{\mathbb{K}}$. Portanto, $p \mid Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}})$. Por outro lado, suponha que P é brandamente ramificado, ou seja, p não divide e . Como $\overline{\mathbb{K}} \subset \overline{\mathbb{L}}_i$ é separável então existe $\overline{\beta}_1$ tal que $Tr_{\overline{\mathbb{L}}_i:\overline{\mathbb{K}}}(\overline{\beta}_1) \neq 0$. Novamente, o citado Teorema Chinês do Resto nos permite escolher $\beta \in \mathcal{O}_{\mathbb{L}}$ tal que $\beta \equiv \overline{\beta}_1 \pmod{\mathfrak{P}_1}$ e $\beta \equiv 0 \pmod{\mathfrak{P}_i}$, para $i \neq 1$. Logo, $\overline{Tr_{\mathbb{L}:\mathbb{K}}(\beta)} = eTr_{\overline{\mathbb{L}}_1:\overline{\mathbb{K}}}(\overline{\beta}_1) \neq 0$ em $\overline{\mathbb{K}}$. Portanto, P não divide $Tr_{\mathbb{L}:\mathbb{K}}(\beta)\mathcal{O}_{\mathbb{K}}$ e, daí, P não divide $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}})$. Isso completa a prova. $\square$

Corolário 4.2.3. *Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão galoisiana de corpos de números então $\mathbb{K} \subset \mathbb{L}$ é brandamente ramificada se, e somente se, $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{K}}$.*

Demonstração. Por um lado, se $\mathbb{K} \subset \mathbb{L}$ é uma extensão brandamente ramificada então todos os ideais maximais de $\mathcal{O}_{\mathbb{K}}$ são brandamente ramificados em $\mathbb{K} \subset \mathbb{L}$. Logo, a proposição 4.2.4 garante que não existe ideal maximal (primo) de $\mathbb{K}$ que divide o ideal $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}})$ (definição de ideal maximal). Logo, $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{K}}$. Por outro lado, do mesmo modo, se $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{K}}$, então não existe ideal maximal que divide $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}})$. Pela proposição 4.2.4, nenhum ideal maximal deve ser severamente ramificado, donde concluímos que todo ideal maximal de $\mathcal{O}_{\mathbb{K}}$ é brandamente ramificado. $\square$

O corolário a seguir combina a teoria de ramificação desenvolvida acima com a teoria de bases integrais normais.

Corolário 4.2.4. *Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão galoisiana de corpos de números que tem BIN então $\mathbb{K} \subset \mathbb{L}$ é brandamente ramificada.*

Demonstração. O corolário 4.2.2 nos mostra que $Tr_{\mathbb{L}:\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{K}}$. Por sua vez, do corolário 4.2.3 tem-se que $\mathbb{K} \subset \mathbb{L}$ é brandamente ramificada. $\square$

Finalmente, provaremos a seguir o Teorema de Hilbert-Speiser, que nos dá condições necessárias e suficientes para que um corpo de números abeliano admita BIN.

Teorema 4.2.1 (Teorema de Hilbert-Speiser). *Seja $\mathbb{K}$ um corpo de números abeliano de condutor n . São equivalentes:*

- (a) $\mathbb{Q} \subset \mathbb{K}$ admite BIN;
- (b) $\mathbb{Q} \subset \mathbb{K}$ é uma extensão brandamente ramificada;
- (c) n é ímpar e livre de quadrados.

Neste caso, $Tr_{\mathbb{Q}(\zeta_n):\mathbb{K}}(\zeta_n)$ é o gerador da base normal.

Demonstração. A proposição 4.2.3 garante que (c) implica (a) e que $Tr_{\mathbb{Q}(\zeta_n):\mathbb{K}}(\zeta_n)$ é o gerador da base normal. O corolário 4.2.3 garante que (a) implica (b). Falta mostrar que (b) implica (c). Para isso, suponha que $\mathbb{Q} \subset \mathbb{K}$ é uma extensão brandamente ramificada. Seja p um número primo ímpar que divide n e considere $n = mp^r$, em que $\text{mdc}(m, p) = 1$. Pela proposição 3.2.8, o primo p não se ramifica em $\mathbb{Q}(\zeta_m)$. Assim, $\mathbb{N} = \mathbb{K} \cap \mathbb{Q}(\zeta_m)$ é o subcorpo maximal de $\mathbb{K}$ em que p é não ramificado. O corpo $\mathbb{N}$ é também o corpo fixo do grupo de inércia I_p de qualquer primo de $\mathcal{O}_K$ acima de p . Portanto, $[\mathbb{K} : \mathbb{N}] = \#(I_p)$. Como p não divide e (pois a extensão é brandamente ramificada) e $\#(I_p) = e$ (proposição 2.6.5), então p não divide $[\mathbb{K} : \mathbb{N}]$. Então $\mathbb{K}$ está contido no p -subgrupo de

Sylow de $Gal(\mathbb{Q}(\zeta_n) : \mathbb{N})$. Se $r > 1$ então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{pm})] = p^{r-1}$ e, então, $\mathbb{K}$ está contido em $\mathbb{Q}(\zeta_{pm})$ e p^2 não divide n . Da mesma forma mostra-se que o grupo de inércia dos primos acima de 2 é um 2-grupo e, portanto, n é ímpar. $\square$

4.3 Bases integrais potentes

Vimos na proposição 4.1.1 que toda extensão de corpos de números admite uma base de potências. A pergunta que responderemos nesta seção é: todo corpo de números admite base *integral* de potências?

Tendo em vista os exemplos concretos que já apresentamos neste texto, alguém poderia pensar que a resposta à questão acima é positiva. De fato, já vimos que $\mathbb{Z}[\sqrt{d}]$ ou $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ é o anel de inteiros de um corpo quadrático $\mathbb{Q}(\sqrt{d})$, que $\mathbb{Z}[\zeta]$ é o anel de inteiros de um corpo ciclotômico $\mathbb{Q}(\zeta)$ e que $\mathbb{Z}[\zeta + \zeta^{-1}]$ é o anel de inteiros do subcorpo ciclotômico maximal real $\mathbb{Q}(\zeta + \zeta^{-1})$. Além disso, os teoremas 3.3.2 e 3.3.3 nos mostraram que os subcorpos $\mathbb{Q}(\eta)$, em que $\eta = \zeta_m - \zeta_m^{-1}$ para $m = 2^n \geq 8$ e $m = 4p^n$ (p primo ímpar), também admitem base integral de potências.

No entanto, nosso objetivo nesta seção é apresentar uma classe de contraexemplos afirmando que a resposta à questão introdutória desta seção é negativa.

Definição 4.3.1. *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos de números. Dizemos que $\mathbb{K} \subset \mathbb{L}$ **admite base integral de potências (BIP)** se existe $\theta \in \mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$. Isso é equivalente a dizer que $\{1, \theta, \dots, \theta^{[\mathbb{L}:\mathbb{K}]-1}\}$ é uma $\mathcal{O}_{\mathbb{K}}$ -base para $\mathcal{O}_{\mathbb{L}}$.*

*Se $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L}$ é um corpo de números, dizemos que $\mathcal{O}_{\mathbb{L}}$ é um **anel de inteiros monogênico** quando $\mathbb{Q} \subset \mathbb{L}$ admite BIP. Caso contrário, diremos que $\mathcal{O}_{\mathbb{L}}$ é **anel de inteiros não monogênico**.*

Adiante, sendo m um número inteiro positivo, denotemos por $\mathbb{Q}^{(m)}$ o corpo ciclotômico $\mathbb{Q}(\zeta_m)$, em que $\zeta_m = e^{(2\pi i)/m}$ é uma raiz m -ésima primitiva da unidade. O teorema que demonstraremos nos dá uma classe especial de corpos que são não monogênicos, isto é, que não admitem BIP. As ferramentas utilizadas e as ideias por trás da demonstração são similares às utilizadas para demonstrar os teoremas 3.3.2 e 3.3.3.

Teorema 4.3.1. *Seja $m = 3p^n$ em que $p > 3$ é um número primo e n é um inteiro positivo. Se $\mathbb{K}$ é um subcorpo imaginário de $\mathbb{Q}^{(m)} = \mathbb{Q}(\zeta_m)$ distinto de $\mathbb{Q}^{(p^n)}$ tal que $[\mathbb{Q}^{(m)} : \mathbb{K}] = 2$, então:*

- (a) *o corpo $\mathbb{K}$ é $\mathbb{Q}(\eta)$, em que $\eta = \zeta_m - \zeta_m^{-1}$ é o período de Gauss;*
- (b) *o valor absoluto do discriminante do corpo $\mathbb{K}$ é igual a $3^{\varphi(p^n)/2} p^{n\varphi(p^n) - (m/3p) - 1}$;*

(c) não existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{O}_{\mathbb{K}}$ seja da forma $\mathbb{Z}[\alpha]$, ou seja, $\mathcal{O}_{\mathbb{K}}$ não é um anel de inteiros monogênico.

Demonstração. Seja $\zeta_m = e^{2\pi i/m}$ uma raiz m -ésima primitiva da unidade. Como $\text{mdc}(3, p^n) = 1$, existem $a, b \in \mathbb{Z}$ tais que $3a + bp^n = 1$. Logo, existem $\omega \triangleq \zeta_3^b = e^{\frac{2\pi ib}{3}}$ e $\xi \triangleq \zeta_{p^n}^a = e^{\frac{2\pi ia}{p^n}}$ raízes 3-ésima e p^n -ésima primitivas da unidade, respectivamente, que satisfazem $\zeta_m = \omega\xi$. Pelo lema 3.3.2 da seção anterior, garantimos a existência de $\mathbb{Q}$ -automorfismos τ e σ em $\mathbb{Q}^{(m)}$ dados por $\tau(\omega) = \bar{\omega} = \omega^{-1}$, $\tau(\xi) = \xi$, $\sigma(\omega) = \omega$ e $\sigma(\xi) = \xi^r$ de modo que $G \triangleq \text{Gal}(\mathbb{Q}^{(m)} : \mathbb{Q}) = \langle \tau \rangle \langle \sigma \rangle$. Observe que $\tau^2 = \text{id}$ e que $\tau(\zeta_m) = \omega^{-1}\xi$ e $\sigma(\zeta_m) = \omega\xi^r$. Considere $s = \varphi(p^n)/2 = p^{n-1}(p-1)/2$. Assim, os subgrupos de ordem 2 de G são $\langle \tau \rangle$, $\langle \tau\sigma^s \rangle$ e $H \triangleq \langle \sigma^s \rangle$. Pelo lema 3.3.3, os corpos fixos de $\langle \tau \rangle$ e $\langle \sigma^s \tau \rangle$ são, respectivamente, $\mathbb{Q}^{(p^n)}$ e $(\mathbb{Q}^{(m)})^+$. Logo, por exclusão, o corpo fixo de $\langle \sigma^s \rangle$ é $\mathbb{K}$. Portanto, $\mathbb{K} = \{\alpha \in \mathbb{Q}^{(m)} : \sigma^s(\alpha) = \alpha\}$. Seja $\eta = \sum_{\rho \in H} \zeta_m^\rho$ o período de Gauss, isto é, $\eta = \sigma^s(\zeta_m) + \sigma^{2s}(\zeta_m) = \omega(\xi + \xi^{-1})$. Assim, analogamente ao que foi feito na demonstração do teorema 3.3.3, vê-se que $\mathbb{K} = \mathbb{Q}(\eta)$ (comprovando o item (a) deste teorema) e que $\mathcal{O}_{\mathbb{Q}^{(m)}} = \mathcal{O}_{\mathbb{K}}[\zeta_m]$. Por isso e pela proposição 2.7.3, o diferente $\mathfrak{d}_{\mathbb{Q}^{(m)}:\mathbb{K}}$ é dado por $(G'(\zeta_m))\mathcal{O}_{\mathbb{Q}^{(m)}}$, em que G é o polinômio minimal de ζ_m sobre $\mathbb{K}$ e G' denota a derivada do polinômio G . Como $\zeta_m \notin \mathbb{K}$ e ζ_m é raiz de $x^2 - \eta x - 1 \in \mathbb{K}[x]$, segue que este polinômio é o seu minimal G . Assim,

$$\mathfrak{d}_{\mathbb{Q}^{(m)}:\mathbb{K}} = (G'(\zeta_m))\mathcal{O}_{\mathbb{Q}^{(m)}} = (\zeta_m + \zeta_m^{-1})\mathcal{O}_{\mathbb{Q}^{(m)}} = \omega(\xi - \xi^{-1})\mathcal{O}_{\mathbb{Q}^{(m)}} \quad (4.14)$$

Considere $\mathfrak{P} = (1 - \xi)\mathcal{O}_{\mathbb{Q}^{(p^n)}}$ o ideal primo ramificado de $\mathbb{Q}^{(p^n)}$ sobre p . Neste caso, a norma de $\mathfrak{P}$ é p . Novamente, de maneira similar à demonstração do teorema 3.3.3 nas equações 3.65, 3.66 e 3.67, podemos concluir que

$$\mathfrak{d}_{\mathbb{Q}^{(m)}:\mathbb{K}} = \omega(\xi - \xi^{-1})\mathcal{O}_{\mathbb{Q}^{(m)}} = \mathfrak{P}\mathcal{O}_{\mathbb{Q}^{(m)}}. \quad (4.15)$$

e que

$$D(\mathbb{K}) = \sqrt{D(\mathbb{Q}^{(m)})/N_{\mathbb{Q}^{(m)}}(\mathfrak{d}_{\mathbb{Q}^{(m)}:\mathbb{K}})}. \quad (4.16)$$

Pelo teorema 3.2.1, temos

$$|D(\mathbb{Q}^{(m)})| = \frac{(3p^n)^{4s}}{3^{4s/2}p^{2p^{n-1}}} = 3^{2s}p^{4ns-2p^{n-1}} \quad (4.17)$$

e

$$N_{\mathbb{Q}^{(m)}}(\mathfrak{d}_{\mathbb{Q}^{(m)}:\mathbb{K}}) = N_{\mathbb{Q}^{(m)}}(\mathfrak{P}\mathcal{O}_{\mathbb{Q}^{(m)}}) = N_{\mathbb{Q}^{(p^n)}}(N_{\mathbb{Q}^{(m)}:\mathbb{Q}^{(p^n)}}(\mathfrak{P}\mathcal{O}_{\mathbb{Q}^{(m)}})) = N_{\mathbb{Q}^{(p^n)}}(\mathfrak{P}^2) = (N_{\mathbb{Q}^{(p^n)}}(\mathfrak{P}))^2 = p^2 \quad (4.18)$$

donde segue que o valor absoluto do discriminante do corpo $\mathbb{K}$ é

$$|D(\mathbb{K})| = \sqrt{|D(\mathbb{Q}^{(m)})|/p^2} = 3^s p^{2ns-p^{n-1}-1} \quad (4.19)$$

demonstrando a afirmação (b), já que $\varphi(p^n) = 2s$. Por fim, demonstremos que o anel de inteiros de $\mathbb{K}$ não é monogênico. Adotemos a notação $\gamma \triangleq \xi + \xi^{-1} \in \mathbb{R}$. Como $\eta = \omega(\xi + \xi^{-1}) = \omega\gamma$ e $\mathbb{Q}(\omega) \cap \mathbb{Q}(\gamma) = \mathbb{Q}$ então $\mathbb{K} = \mathbb{Q}(\eta) = \mathbb{Q}(\omega\gamma) = \mathbb{Q}(\omega)\mathbb{Q}(\gamma)$ e, daí, $\mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{Q}(\omega)}\mathcal{O}_{\mathbb{Q}(\gamma)} = \mathbb{Z}[\omega]\mathbb{Z}[\gamma]$. Como o discriminante da base $\{\omega, \omega^2\}$ de $\mathbb{Q}(\omega)$ sobre $\mathbb{Q}$ é igual a -3 , que é livre de quadrados, segue da proposição 2.5.7 que esta base é uma base integral para $\mathbb{Z}[\omega]$. Logo, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\omega]\mathbb{Z}[\gamma] = \omega\mathbb{Z}[\gamma] + \omega^2\mathbb{Z}[\gamma]$. Daí, para todo $\alpha \in \mathcal{O}_{\mathbb{K}}$, existem $R, S \in \mathbb{Z}[\gamma]$ tais que $\alpha = \omega R + \omega^2 S$. Sabendo que $G/H = \{\sigma^j H, \sigma^j \tau H : 0 \leq j < s\}$, podemos calcular o diferente de α :

$$\mathfrak{d}_{\mathbb{K}}(\alpha) = (\alpha - \tau(\alpha)) \prod_{j=1}^{s-1} (\alpha - \sigma^j(\alpha))(\alpha - \tau\sigma^j(\alpha)). \quad (4.20)$$

Substituindo $\alpha - \tau(\alpha) = (\omega - \omega^2)(R - S)$ e $\sigma^j(\alpha) = \omega(R - \sigma^j(R)) + \omega^2(S - \sigma^j(S))$ na equação anterior, obtemos:

$$\mathfrak{d}_{\mathbb{K}}(\alpha) = (\omega - \omega^2)(R - S) \prod_{j=1}^{s-1} (\alpha - \sigma^j \tau(\alpha)) \prod_{j=1}^{s-1} \{\omega(R - \sigma^j(R)) + \omega^2(S - \sigma^j(S))\}. \quad (4.21)$$

Para quaisquer $T \in \mathbb{Z}[\gamma]$ e $\rho \in G$, é verdade que $T - \rho(T)$ é divisível por $\gamma - \rho(\gamma)$ em $\mathbb{Z}[\gamma]$. De fato, para cada $i = 1, \dots, m$, existe $x_i = \gamma^{i-1} + \gamma^{i-2}\rho(\gamma) + \dots + \gamma\rho(\gamma)^{i-2} + \rho(\gamma)^{i-1} \in \mathbb{Z}[\gamma]$ tal que $\gamma - \rho(\gamma)^i = (\gamma - \rho(\gamma))x_i$. Assim, sendo $T = \sum_{i=0}^m a_i \gamma^i$ com $a_i \in \mathbb{Z}$ para todo $i = 0, 1, \dots, m$, então,

$$T - \rho(T) = \sum_{i=0}^m a_i (\gamma^i - \rho(\gamma)^i) = \sum_{i=1}^m a_i (\gamma^i - \rho(\gamma)^i) = (\gamma - \rho(\gamma)) \sum_{i=1}^m a_i x_i \quad (4.22)$$

com $\sum_{i=1}^m a_i x_i \in \mathbb{Z}[\gamma]$. Além disso, $1 - \xi$ divide $\gamma - \rho(\gamma)$ em $\mathcal{O}_{\mathbb{Q}(p^n)}$. Com efeito, temos $\gamma - \rho(\gamma) = \xi - \rho(\xi) + \xi^{-1} - \rho(\xi^{-1})$, temos $\xi + \xi^{-1} = (1 - \xi)(\xi^{-1} - 1) + 2$ e temos $\rho(\xi) + \rho(\xi^{-1}) = (1 - \rho(\xi))(\rho(\xi^{-1}) - 1) + 2$. Além disso, para algum f inteiro positivo, $1 - \rho(\xi) = 1 - \xi^f = (1 - \xi)(\xi^{f-1} + \dots + \xi + 1)$. Daí, existe $\mu \in \mathcal{O}_{\mathbb{Q}(p^n)}$ tal que

$$\gamma - \rho(\gamma) = (1 - \xi)(\xi^{-1} - 1) - (1 - \rho(\xi))(\rho(\xi^{-1}) - 1) = (1 - \xi)\mu \quad (4.23)$$

confirmando a afirmação anterior de que $(1 - \xi) \mid (\gamma - \rho(\gamma))$ em $\mathcal{O}_{\mathbb{Q}(p^n)}$. Assim, seja β dado por

$$\beta = \omega(R - S) \prod_{j=1}^{s-1} (\omega a_j + \omega^2 b_j) \prod_{j=2}^{s-1} (\alpha - \sigma^j \tau(\alpha)) \quad (4.24)$$

em que $a_j, b_j \in \mathbb{Z}[\gamma]$ são tais que $R - \sigma^j(R) = (\gamma - \rho(\gamma))a_j$ e $S - \sigma^j(S) = (\gamma - \rho(\gamma))b_j$, para cada $j = 1, 2, \dots, s-1$. Nessas condições, nota-se que $\beta \in \mathcal{O}_{\mathbb{K}}$. Então, da equação 4.21, obtém-se que

$$\mathfrak{d}_{\mathbb{K}}(\alpha) = \beta(1 - \omega)(\alpha - \sigma\tau(\alpha)) \prod_{j=1}^{s-1} (\gamma - \sigma^j \tau(\gamma)) \quad (4.25)$$

com $\beta \in \mathcal{O}_{\mathbb{K}}$. Agora, por definição, o diferente de $\mathbb{Z}[\gamma]$ é $\mathfrak{d}_{\mathbb{Z}[\gamma]} = \prod_{j=1}^{s-1} (\gamma - \sigma^j \tau(\gamma))$. Logo,

$$\mathfrak{d}_{\mathbb{K}}(\alpha) = \beta(1 - \omega)(\alpha - \sigma\tau(\alpha))\mathfrak{d}_{\mathbb{Z}[\gamma]}O_{\mathbb{K}}. \quad (4.26)$$

Vamos calcular o discriminante de α em $\mathbb{K}$. Da proposição 2.7.10, obtemos

$$D(\mathbb{K}) = D(\mathbb{K}_3)^{[\mathbb{Q}(\gamma):\mathbb{Q}]}D(\mathbb{Q}(\gamma)) = 3^s N_{\mathbb{K}}(\mathfrak{d}_{\mathbb{Z}[\gamma]}). \quad (4.27)$$

Das equações 4.26 e 4.27, obtemos:

$$D_{\mathbb{K}}(\alpha) = N_{\mathbb{K}}(\mathfrak{d}_{\mathbb{K}}(\alpha)) = N_{\mathbb{K}}(\beta)3^s N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))N_{\mathbb{K}}(\mathfrak{d}_{\mathbb{Z}[\gamma]}) = N_{\mathbb{K}}(\beta)N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))D(\mathbb{K}). \quad (4.28)$$

Portanto,

$$D_{\mathbb{K}}(\alpha) \geq N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))D(\mathbb{K}). \quad (4.29)$$

Mostraremos a seguir que $N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha)) > 1$. Para fazer isso, é preciso dividir a demonstração em casos, supondo $\alpha - \sigma\tau(\alpha) \neq 0$:

- Se $R = \sigma(S)$, como $1 - \xi \mid T - \rho(T)$ para todo $T \in \mathbb{Z}[\gamma]$ e $\rho \in G$, então

$$\alpha - \sigma\tau(\alpha) = \omega^2(S - \sigma^2(S)) = \omega^2(1 - \xi)l \quad (l \in \mathcal{O}_{\mathbb{Q}(m)}) \quad (4.30)$$

e, portanto,

$$N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha)) = \sqrt{N_{\mathbb{Q}(m)}(\omega^2(1 - \xi)l)} \geq \sqrt{N_{\mathbb{Q}(m)}(1 - \xi)} = \sqrt{p} > 1. \quad (4.31)$$

- Se $S = \sigma(R)$, analogamente ao feito no item anterior mostra-se que $N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha)) > 1$.
- Se $R - \sigma(S) = S - \sigma(R)$, então

$$2(\alpha - \sigma\tau(\alpha)) = 2(\sigma(R) - S) = -(R + S) + \sigma(R + S) = (1 - \xi)l \quad (l \in \mathcal{O}_{\mathbb{Q}(m)}). \quad (4.32)$$

Calculando a norma $N_{\mathbb{Q}(m)}(\cdot)$ da expressão anterior, obtemos $|2^{\varphi(p^n)} N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))| = |p N_{\mathbb{Q}(m)}(l)|$ e, como $\text{mdc}(2, p) = 1$, $z = N_{\mathbb{Q}(m)}(l)/2^{\varphi(p^n)} \in \mathbb{Z}$ (não nulo), então

$$|N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))| = |pz| \geq |p| > 1. \quad (4.33)$$

- Se $R - \sigma(S) = \sigma(R) - S$, então $\alpha - \sigma\tau(\alpha) = \omega(R - \sigma(S))(1 - \omega)$ e, daí,

$$\begin{aligned} N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha)) &= \sqrt{N_{\mathbb{Q}(m)}(\omega(R - \sigma(S))(1 - \omega))} \geq \sqrt{N_{\mathbb{Q}(m)}(1 - \omega)} = \\ &= \sqrt{N_{\mathbb{Q}(3)}((1 - \omega)^{\varphi(p^n)})} = \sqrt{3^{\varphi(p^n)}} = 3^{p^n(p-1)/2} > 1. \end{aligned} \quad (4.34)$$

- Por fim, suponha que nenhum dos quatro casos anteriores são verificados. Primeiramente, como $\omega^2 + \omega = -1$, temos:

$$\begin{aligned}
|N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))| &= |N_{\mathbb{K}}(\omega(R - \sigma(S)) + \omega^2(S - \sigma(R)))| = \\
&= |N_{\mathbb{Q}(\gamma)}(N_{\mathbb{K}:\mathbb{Q}(\gamma)}([\omega(R - \sigma(S)) + \omega^2(S - \sigma(R))][\tau(\omega(R - \sigma(S)) + \omega^2(S - \sigma(R))]))| = \\
&= |N_{\mathbb{Q}(\gamma)}((R - \sigma(S))^2 - (R - \sigma(S))(S - \sigma(R)) + (S - \sigma(R))^2).| \quad (4.35)
\end{aligned}$$

Daí, como R, S são reais, obtemos:

$$\begin{aligned}
|N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))| &= |N_{\mathbb{Q}(\gamma)}((R - \sigma(S))^2 - (R - \sigma(S))(S - \sigma(R)) + (S - \sigma(R))^2)| > \\
&> |N_{\mathbb{Q}(\gamma)}((R - \sigma(S))(S - \sigma(R)))| \geq 1 \quad (4.36)
\end{aligned}$$

comprovando que $|N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))| > 1$.

Logo, em todo caso, $N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha)) > 1$, e, da equação 4.29, obtemos a implicação a seguir:

$$D_{\mathbb{K}}(\alpha) \geq N_{\mathbb{K}}(\alpha - \sigma\tau(\alpha))D(\mathbb{K}) \implies D_{\mathbb{K}}(\alpha) > D(\mathbb{K}). \quad (4.37)$$

Portanto, para todo $\alpha \in \mathcal{O}_{\mathbb{K}}$ com $D_{\mathbb{K}}(\alpha) \neq 0$, segue que $D_{\mathbb{K}}(\alpha) > D(\mathbb{K})$, o que impede $\mathcal{O}_{\mathbb{K}}$ de ser monogênico. $\square$

Conclusão

Neste capítulo, nos dedicamos ao estudo das bases normais e potentes tanto para corpos como para anéis de inteiros. Na primeira seção, notamos que toda extensão de corpos de números possui base de potências e mostramos que toda extensão galoisiana finita admite base normal, por meio do Teorema da Base Normal. Na segunda seção, definimos o que é uma base integral normal (BIN) e demos uma condição necessária e suficiente para que um corpo de números abeliano admita BIN, devido ao Teorema de Hilbert-Speiser. Por fim, na última seção definimos o que é uma base integral de potências (BIP) e apresentamos um exemplo de corpos de números que não possuem BIP.

Capítulo 5

Caracteres

Caractere é um homomorfismo de um grupo G (que consideraremos abeliano e finito) no grupo $\mathbb{C} - \{0\}$. Os caracteres de um grupo G são muito úteis à Teoria dos Números, como poderemos comprovar neste capítulo. Um exemplo claro disso será o Teorema do Condutor-Discriminante, que apenas enunciaremos, mas que nos permitirá calcular o discriminante de qualquer corpo de números, desde que sejam conhecidos os caracteres de seu grupo de Galois. Daremos uma atenção especial aos caracteres de $\mathbb{Z}_n^*$. Estudaremos ainda nesta seção os caracteres de Dirichlet módulo n , uma expressão para seu condutor, relações de ortogonalidade entre caracteres e a soma de Gauss.

5.1 Caracteres de grupos abelianos finitos

Em toda esta seção, considere G um grupo abeliano finito de ordem $o(G) = n$ com notação multiplicativa para sua operação. Denotemos por $\mathbb{C}^\times = \mathbb{C} - \{0\}$ o conjunto dos elementos complexos invertíveis.

Definição 5.1.1. *Uma função $\chi : G \longrightarrow \mathbb{C}^\times$ é chamada de **caractere de G** se é um homomorfismo de grupos.*

Observe imediatamente da definição acima que se χ é um caractere de G então, para quaisquer elementos a e b desse grupo, $\chi(a) \neq 0$ e $\chi(ab) = \chi(a)\chi(b)$. Além disso, considerando que e é a unidade de G , vale que $\chi(e) = 1$ e que $\chi(a)^n = \chi(a^n) = 1$, para qualquer $a \in G$. Daí, segue claramente que $\chi(G)$ é um subgrupo do grupo multiplicativo cíclico das raízes n -ésimas da unidade. Portanto, $\chi(G)$ é um grupo cíclico multiplicativo e $|\chi(a)| = 1$ para qualquer $a \in G$. Dado um caractere χ de G , definimos o **caractere conjugado** de χ por $\bar{\chi}(a) \triangleq \overline{\chi(a)}$, para todo $a \in G$. Vamos definir agora uma operação entre caracteres, a operação multiplicação. Dados χ_1 e χ_2 caracteres de G , denotamos

a operação de **multiplicação** entre esses caracteres por $\chi_1\chi_2$, que é dada por

$$(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a) \quad \forall a \in G. \quad (5.1)$$

Com essa operação, verifica-se que o conjunto dos caracteres de G é um grupo abeliano, o qual denotamos por $\widehat{G}$. Observe que o elemento unidade de $\widehat{G}$ é o caractere $\chi_0 : G \rightarrow \mathbb{C}^\times$ definido por $\chi_0(a) = 1$ para todo $a \in G$. Consequentemente, o elemento inverso de um caractere χ de G qualquer em $\widehat{G}$ é seu caractere conjugado $\overline{\chi}$. De fato, para todo $a \in G$,

$$(\chi\overline{\chi})(a) = \chi(a)\overline{\chi(a)} = |\chi(a)|^2 = 1. \quad (5.2)$$

Exemplo 5.1.1. Considere $G = \mathbb{Z}_5^* = \{1, 2, 3, 4\}$. Vamos determinar os caracteres de G : denote primeiramente por $\chi_0 = 1$ a unidade de $\widehat{\mathbb{Z}_5^*}$. Seja χ_1 o caractere de $\mathbb{Z}_5^*$ definido por

$$\chi_1(1) = 1, \quad \chi_1(2) = i, \quad \chi_1(3) = -i, \quad \chi_1(4) = -1. \quad (5.3)$$

Denote por χ_2 o caractere conjugado de χ_1 . Considere agora χ_3 o caractere de $\mathbb{Z}_5^*$ dado por

$$\chi_3(1) = 1, \quad \chi_3(2) = -1, \quad \chi_3(3) = -1, \quad \chi_3(4) = 1. \quad (5.4)$$

Como χ_3 é um caractere com imagem real, então seu caractere conjugado é o próprio χ_3 . Como veremos nesta seção, o número de caracteres de G deve ser exatamente igual à ordem de G . Assim, $\widehat{\mathbb{Z}_5^*} = \{\chi_0, \chi_1, \chi_2, \chi_3\}$.

A seguir vamos comparar grupos de caracteres de diferentes grupos, como subgrupos e grupos quocientes. Considere G_1 e G_2 grupos abelianos finitos e um homomorfismo de grupos $\varphi : G_2 \rightarrow G_1$. Então a aplicação

$$\widehat{\varphi} : \widehat{G_1} \rightarrow \widehat{G_2} \quad \text{tal que} \quad \chi \in \widehat{G_1} \mapsto \widehat{\varphi}(\chi) = \chi \circ \varphi \in \widehat{G_2} \quad (5.5)$$

também é um homomorfismo de grupos. Com efeito, se $\chi \in \widehat{G_1}$, então $\chi \circ \varphi \in \widehat{G_2}$, pois, para todo $a, b \in G_2$, $\chi \circ \varphi(a) = \chi(\varphi(a)) \neq 0$ e

$$\chi \circ \varphi(ab) = \chi(\varphi(ab)) = \chi(\varphi(a)\varphi(b)) = \chi(\varphi(a))\chi(\varphi(b)) = (\chi \circ \varphi(a))(\chi \circ \varphi(b)). \quad (5.6)$$

Além disso, o fato de ser homomorfismo é facilmente verificado, já que para todo $\chi_1, \chi_2 \in \widehat{G_1}$,

$$\widehat{\varphi}(\chi_1\chi_2) = (\chi_1\chi_2) \circ \varphi = (\chi_1 \circ \varphi)(\chi_2 \circ \varphi) = \widehat{\varphi}(\chi_1)\widehat{\varphi}(\chi_2). \quad (5.7)$$

Em particular, se G_2 é um subgrupo de G_1 e φ é a aplicação inclusão então $\widehat{\varphi}(\chi)$ é a restrição de χ ao subgrupo G_2 , pois para todo $a \in G_2$, tem-se $\widehat{\varphi}(\chi)(a) = \chi(\varphi(a)) = \chi(a)$.

Se G_1 e G_2 são grupos abelianos finitos quaisquer e $\phi : G_2 \longrightarrow G_1$ é um homomorfismo de grupos então seu núcleo é dado por

$$\ker(\widehat{\phi}) = \{\chi \in \widehat{G_1} : \chi(\phi(a)) = 1, \forall a \in G_2\}. \quad (5.8)$$

Sejam H um subgrupo do grupo abeliano finito G e $\psi : G \longrightarrow G/H$ o homomorfismo canônico que associa cada elemento $g \in G$ à sua classe $aH \in G/H$. Então seu correspondente homomorfismo é $\widehat{\psi} : \widehat{G/H} \longrightarrow \widehat{G}$, em que $\widehat{\psi}(\widetilde{\chi}) = \widetilde{\chi} \circ \psi$. Neste caso, claramente $\chi = \widetilde{\chi} \circ \psi$ é um caractere de G tal que $\chi(a) = \widetilde{\chi}(aH)$ para todo $a \in G$.

Proposição 5.1.1. *Sejam H um subgrupo do grupo abeliano finito G , $\varphi : H \longrightarrow G$ a aplicação inclusão e $\psi : G \longrightarrow G/H$ o homomorfismo canônico. Então:*

$$(a) \ker(\widehat{\varphi}) = \{\chi \in \widehat{G} : aH = bH \implies \chi(a) = \chi(b)\}.$$

$$(b) \widehat{\psi} \text{ é um homomorfismo injetor.}$$

$$(c) \widehat{\psi}(\widehat{G/H}) = \ker(\widehat{\varphi}).$$

$$(d) \text{ Estabelece-se o isomorfismo}$$

$$\frac{\widehat{G}}{\widehat{\psi}(\widehat{G/H})} \simeq \widehat{\varphi}(\widehat{G}) \subset \widehat{H}. \quad (5.9)$$

Demonstração. (a) Por um lado, se $\chi \in \ker(\widehat{\varphi})$, então 5.8 garante que $\chi(\varphi(a)) = 1$ para todo $a \in H$. Como φ é a inclusão, então $\chi(H) = 1$. Assim, se $aH = bH$ então $ab^{-1} \in H$ e

$$1 = \chi(ab^{-1}) = \chi(a)\chi(b)^{-1} \implies \chi(a) = \chi(b). \quad (5.10)$$

Por outro lado, suponha que $\chi \in \widehat{G}$ é tal que $aH = bH \implies \chi(a) = \chi(b)$. Assim, para qualquer $a \in H$, $aH = H$. Logo, $\chi(a) = \chi(1) = 1$. Assim, $\chi(\varphi(a)) = \chi(a) = 1$, donde segue o resultado pela igualdade 5.8. (b) Sejam $\widetilde{\chi} \in \widehat{G/H}$ e χ_0 a unidade de $\widehat{G}$. Então:

$$\widehat{\psi}(\widetilde{\chi}) = \chi_0 \iff \widetilde{\chi} \circ \psi(a) = 1, \forall a \in G \iff \widetilde{\chi}(aH) = 1, \forall a \in G \iff \widetilde{\chi}(aH) = 1, \forall aH \in G/H \quad (5.11)$$

e este último fato ocorre se, e somente se, $\widetilde{\chi}$ é a unidade de $\widehat{G/H}$. Logo, $\widehat{\psi}$ é um homomorfismo injetor. (c) Por um lado, considere $\chi \in \widehat{\psi}(\widehat{G/H})$, ou seja, $\chi = \widehat{\chi} \circ \psi$. Sejam $a, b \in G$ tais que $aH = bH$. Então

$$\chi(a) = \widehat{\chi} \circ \psi(a) = \widehat{\chi}(aH) = \widehat{\chi}(bH) = \widehat{\chi} \circ \psi(b) = \chi(b). \quad (5.12)$$

Portanto, $aH = bH \implies \chi(a) = \chi(b)$ e daí $\chi \in \ker(\widehat{\varphi})$ devido ao item (a). Logo, $\widehat{\psi}(\widehat{G/H}) \subset \ker(\widehat{\varphi})$. Por outro lado, tome $\chi \in \ker(\widehat{\varphi})$. Defina $\widetilde{\chi} : G/H \longrightarrow \mathbb{C}^\times$ dada por $\widetilde{\chi}(aH) = \chi(a)$ para todo $a \in G$. Primeiramente, note que $\widetilde{\chi}$ está bem definida, pois, devido ao item (a) e como $\chi \in \ker(\widehat{\varphi})$,

$$aH = bH \implies \chi(a) = \chi(b) \implies \widetilde{\chi}(aH) = \widetilde{\chi}(bH). \quad (5.13)$$

Além disso, $\tilde{\chi}$ é caractere, pois, para todo $a, b \in G$, $\tilde{\chi}(aH) = \chi(a) \neq 0$ e

$$\tilde{\chi}(aHbH) = \tilde{\chi}(abH) = \chi(ab) = \chi(a)\chi(b) = \tilde{\chi}(aH)\tilde{\chi}(bH). \quad (5.14)$$

Então $\chi = \widehat{\psi}(\tilde{\chi}) \in \widehat{\psi}(\widehat{G/H})$, donde segue que $\ker(\widehat{\varphi}) \subset \widehat{\psi}(\widehat{G/H})$, completando a prova. (d) Finalmente, o Teorema do Homomorfismo aplicado a $\widehat{\phi} : \widehat{G} \longrightarrow \widehat{H}$ e o item (c) garantem que

$$\frac{\widehat{G}}{\widehat{\psi}(\widehat{G/H})} = \frac{\widehat{G}}{\ker(\widehat{\varphi})} \simeq \widehat{\varphi}(\widehat{G}) \subset \widehat{H}. \quad (5.15)$$

□

A proposição seguinte descreve explicitamente os caracteres de um grupo abeliano finito *cíclico*.

Proposição 5.1.2. *Seja G um grupo abeliano finito cíclico de ordem n e com gerador a (isto é, $G = \langle a \rangle$). Se ζ_n denota uma raiz n -ésima primitiva da unidade, então $\widehat{G} = \{\chi_0, \chi_1, \dots, \chi_{n-1}\}$ possui n distintos elementos, em que $\chi_r(a^s) = \zeta_n^{rs}$, com $1 \leq s \leq n$ e $0 \leq r \leq n-1$.*

Demonstração. Simplifiquemos a notação considerando $\zeta = \zeta_n$. Primeiramente, cada χ_r é um caractere de G ($0 \leq r \leq n-1$), pois, para quaisquer a^s e a^t em G ,

$$\chi_r(a^s a^t) = \chi_r(a^{s+t}) = \zeta^{r(s+t)} = \zeta^{rs} \zeta^{rt} = \chi_r(a^s) \chi_r(a^t). \quad (5.16)$$

Além disso, se $0 \leq r < r' \leq n-1$, então $\chi_r \neq \chi_{r'}$. De fato,

$$\chi_r(a) = \chi_{r'}(a) \implies \zeta^r = \zeta^{r'} \implies n \mid r - r' \implies r - r' = 0 \quad (5.17)$$

o que é um absurdo pois supomos $r < r'$. Assim, mostramos que $\{\chi_r\}_{r=0}^{n-1} \subset \widehat{G}$ e que o primeiro conjunto possui n elementos distintos. Agora, se $\chi \in \widehat{G}$ então $\chi(a)^n = \chi(a^n) = 1$ e, daí, $\chi(a) = \zeta^r$ para algum r entre 0 e $n-1$. Logo, para todo $s \in \{1, 2, \dots, n\}$, temos $\chi(a^s) = \chi(a)^s = \zeta^{rs} = \chi_r(a^s)$. Portanto, $\chi = \chi_r$, donde concluimos finalmente que $\widehat{G} \subset \{\chi_r\}_{r=0}^{n-1}$. □

Corolário 5.1.1. *Se G é um grupo abeliano finito cíclico de ordem n então $G \simeq \widehat{G}$.*

Demonstração. Sendo $G = \langle a \rangle$ e ζ uma raiz n -ésima primitiva da unidade, considere $\theta : G \longrightarrow \widehat{G}$ dado por $\theta(a^r) = \chi_r$ para cada $0 \leq r \leq n-1$. A aplicação θ está bem definida, pois

$$a^r = a^t \implies n \mid r - t \implies \zeta^r = \zeta^t \implies \chi_r(a) = \chi_t(a) \implies \theta(a^r) = \chi_r = \chi_t = \theta(a^t). \quad (5.18)$$

A aplicação θ é um homomorfismo, pois

$$\theta(a^r a^t) = \theta(a^{r+t}) = \theta(a^{r+t \pmod n}) = \chi_{r+t \pmod n} = \chi_r \chi_t = \theta(a^r) \theta(a^t). \quad (5.19)$$

A aplicação é também injetora, pois

$$\theta(a^r) = \chi_0 \iff \chi_r = \chi_0 \iff \chi_r(a) = \chi_0(a) \iff \zeta^r = 1 \iff n \mid r \iff r = 0. \quad (5.20)$$

Por fim, como G e $\widehat{G}$ são grupos finitos com mesmo número de elementos (devido à proposição anterior), então θ é sobrejetora. Isso comprova que θ é um isomorfismo entre G e $\widehat{G}$. $\square$

Um fato importante da teoria dos grupos é que todo grupo abeliano finito é isomorfo ao produto cartesiano de uma quantidade finita de grupos cíclicos (proposição 1.2.12). Por isso, todo grupo G abeliano finito se enquadra na seguinte proposição:

Proposição 5.1.3. *Se $\theta : G \longrightarrow \prod_{i=1}^r G_i$ é um isomorfismo de grupos, então existe um isomorfismo de grupos $\widehat{\theta} : \widehat{G} \longrightarrow \prod_{i=1}^r \widehat{G}_i$ induzido por θ .*

Demonstração. Considere que $\theta : G \longrightarrow \prod_{i=1}^r G_i$ é dado por $\theta(g) = (g_1, g_2, \dots, g_r)$ para cada $g \in G$, tendo $g_i \in G_i$. Assim, $\theta^{-1}(g_1, g_2, \dots, g_r) = g$. Defina, para cada $i = 1, 2, \dots, r$ a aplicação $v_i : G_i \longrightarrow G$ dada por $v_i(g_i) = \theta^{-1}(1, \dots, g_i, \dots, 1)$ em que $g_i \in G_i$ ocupa a i -ésima posição da r -upla $(1, \dots, g_i, \dots, 1)$. É claro que $G_i \simeq v_i(G_i)$ é um subgrupo de G . Para cada $\chi \in \widehat{G}$ defina o caractere $\chi_i : G_i \longrightarrow \mathbb{C}^\times$ por $\chi_i = \chi \circ v_i = \widehat{v}_i(\chi)$ ($i = 1, 2, \dots, r$).

Agora, defina $\widehat{\theta} : \widehat{G} \longrightarrow \prod_{i=1}^r \widehat{G}_i$ por $\widehat{\theta}(\chi) = (\chi_1, \dots, \chi_r)$. Essa aplicação está bem definida, pois

$$\chi = \chi' \implies \chi \circ v_i = \chi' \circ v_i, \forall 1 \leq i \leq r \implies \chi_i = \chi'_i, \forall 1 \leq i \leq r \implies \widehat{\theta}(\chi) = \widehat{\theta}(\chi'). \quad (5.21)$$

A aplicação $\widehat{\theta}$ é um homomorfismo, pois

$$\widehat{\theta}(\chi\chi') = (\chi\chi' \circ v_1, \dots, \chi\chi' \circ v_r) = (\chi(v_1), \dots, \chi(v_r))(\chi'(v_1), \dots, \chi'(v_r)) = \widehat{\theta}(\chi)\widehat{\theta}(\chi'). \quad (5.22)$$

Verifiquemos que $\widehat{\theta}$ é injetora. Seja $\chi \in \widehat{G}$ tal que $\widehat{\theta}(\chi)$ é a unidade de $\prod_{i=1}^r \widehat{G}_i$, isto é, $\chi \circ v_i$ é a unidade de $\widehat{G}_i$. Então

$$\begin{aligned} \chi(g) &= \chi(\theta^{-1}(g_1, \dots, g_r)) = \chi(\theta^{-1}((g_1, 1, \dots, 1)(1, g_2, \dots, 1) \dots (1, 1, \dots, g_r))) = \\ &= \chi(\theta^{-1}(g_1, 1, \dots, 1)\theta^{-1}(1, g_2, \dots, 1) \dots \theta^{-1}(1, 1, \dots, g_r)) = \chi(v_1(g_1)v_2(g_2) \dots v_r(g_r)) = \\ &= \chi \circ v_1(g_1)\chi \circ v_2(g_2) \dots \chi \circ v_r(g_r) = 1.1 \dots 1 = 1 \end{aligned} \quad (5.23)$$

isto é, $\chi(G) = 1$. Logo, χ é a unidade de $\widehat{G}$, comprovando que $\widehat{\theta}$ é injetora.

Por fim, comprovemos que $\widehat{\theta}$ é sobrejetora. Dado $\chi_i \in \widehat{G}_i$, $1 \leq i \leq r$, considere a aplicação $\chi :$

$G \longrightarrow \mathbb{C}^\times$ dada por $\chi(g) = \chi_1(g_1)\chi_2(g_2)\dots\chi_r(g_r)$ para qualquer $g = \theta^{-1}(g_1, g_2, \dots, g_r) \in G$. Como cada χ_i é caractere, então χ está bem definida e $\chi(g) \neq 0$ para todo $g \in G$. Além disso, χ é um homomorfismo, pois, dados $g = \theta^{-1}(g_1, g_2, \dots, g_r), h = \theta^{-1}(h_1, h_2, \dots, h_r) \in G$,

$$\chi(gh) = \chi(\theta^{-1}(g_1, g_2, \dots, g_r)\theta^{-1}(h_1, h_2, \dots, h_r)) = \chi(\theta^{-1}(g_1h_1, g_2h_2, \dots, g_rh_r)) =$$

$$= \chi_1(g_1h_1)\chi_2(g_2h_2)\dots\chi_r(g_rh_r) = \chi_1(g_1)\chi_2(g_2)\dots\chi_r(g_r)\chi_1(h_1)\chi_2(h_2)\dots\chi_r(h_r) = \chi(g)\chi(h). \quad (5.24)$$

Portanto, a aplicação χ é um caractere de G . Por fim, notemos que $\widehat{\theta}(\chi) = (\chi_1, \chi_2, \dots, \chi_r)$, já que para cada $g_i \in G_i$,

$$\chi \circ v_i(g_i) = \chi(v_i(g_i)) = \chi(\theta^{-1}(1, \dots, g_i, \dots, 1)) = \chi_1(1)\dots\chi_i(g_i)\dots\chi_r(1) = \chi_i(g_i) \quad (5.25)$$

isto é, $\chi \circ v_i = \chi_i$ para cada $1 \leq i \leq r$, comprovando que $\widehat{\theta}(\chi) = (\chi \circ v_1, \chi \circ v_2, \dots, \chi \circ v_r) = (\chi_1, \chi_2, \dots, \chi_r)$. Portanto, $\widehat{\theta}$ é um isomorfismo de grupos. $\square$

Uma consequência dessa proposição é que o número de elementos de G e o número de elementos de seu grupo de caracteres associado $\widehat{G}$ é igual, como nos mostra o corolário a seguir:

Corolário 5.1.2. *Se G é um grupo finito abeliano, então $G \simeq \widehat{G}$. Consequentemente, $o(G) = o(\widehat{G})$.*

Demonstração. Como G é abeliano finito, segue da proposição 1.2.12 que $G \simeq \prod_{i=1}^r G_i$, em que cada G_i é cíclico. Da proposição 5.1.3 segue que $\widehat{G} \simeq \prod_{i=1}^r \widehat{G}_i$. Por sua vez, o corolário 5.1.1 nos permite afirmar que $\prod_{i=1}^r \widehat{G}_i \simeq \prod_{i=1}^r G_i$, e este último é isomorfo a G . Logo, usando a transitividade do isomorfismo, $\widehat{G} \simeq G$. $\square$

Vejamos a seguir outras propriedades importantes dos caracteres de grupos abelianos finitos.

Proposição 5.1.4. *Seja H um subgrupo de ordem m do grupo abeliano finito G de ordem n . Todo caractere de H admite n/m extensões para caracteres de G .*

Demonstração. Seja $\varphi : H \longrightarrow G$ o homomorfismo inclusão e $\psi : G \longrightarrow G/H$ o homomorfismo canônico. Devido ao item (d) da proposição 5.1.1, sabemos que $\frac{\widehat{G}}{\widehat{\psi(G/H)}} \simeq \widehat{\varphi(H)} \subset \widehat{H}$. Logo,

$$o(\widehat{G})/o(\widehat{\psi(G/H)}) \leq o(\widehat{H}). \quad (5.26)$$

Devido ao corolário 5.1.2, afirmamos que $o(G) = o(\widehat{G})$, $o(H) = o(\widehat{H})$ e $o(G/H) = o(\widehat{G/H})$. Além disso, como a imagem de qualquer aplicação cujo domínio é finito não pode ter mais elementos do

que o domínio, então $o(\widehat{\psi(G/H)}) \leq o(\widehat{G/H})$. Daí,

$$o(\widehat{\psi(G/H)}) \leq o(\widehat{G/H}) = o(G/H) = \frac{o(G)}{o(H)} = \frac{o(\widehat{G})}{o(\widehat{H})} \quad (5.27)$$

ou seja

$$\frac{o(\widehat{G})}{o(\widehat{\psi(G/H)})} \geq o(\widehat{H}). \quad (5.28)$$

Das equações 5.8 e 5.26 segue que $o(\widehat{G})/o(\widehat{\psi(G/H)}) = o(\widehat{H})$ e, conseqüentemente,

$$\frac{\widehat{G}}{\widehat{\psi(G/H)}} \simeq \widehat{\varphi(G)} = \widehat{H}. \quad (5.29)$$

Como $\widehat{\varphi} = \chi \circ \varphi$ é a restrição de $\chi \in \widehat{G}$ ao subgrupo H , então a igualdade de conjuntos $\widehat{\varphi(G)} = \widehat{H}$ significa que todo caractere de H é a restrição de um caractere de G (por $\widehat{\varphi}$). Sabe-se que $\ker(\widehat{\varphi}) = \widehat{\psi(G/H)}$ (item (c) da proposição 5.1.1) tem n/m elementos, pois $o(\widehat{\psi(G/H)}) = o(G)/o(H) = n/m$. Note agora que $\widehat{\varphi}(\chi_1) = \widehat{\varphi}(\chi_2)$ se, e somente se, $\chi_1 \circ \chi_2^{-1} \in \ker(\widehat{\varphi})$. Para cada caractere χ_H de H existe um caractere χ de G tal que $\widehat{\varphi}(\chi) = \chi_H$, pois $\widehat{\varphi}$ é sobrejetora. Assim, $\widehat{\varphi}(\chi') = \chi_H$ se, e somente, $\chi' \circ \chi^{-1} \in \ker(\widehat{\varphi})$, o que ocorre exatamente n/m vezes (que é o número de elementos no núcleo). Logo, cada caractere de H admite n/m extensões a caracteres de G . $\square$

Proposição 5.1.5 (Propriedade de Separação). *Sejam $a \neq b$ elementos do grupo abeliano finito G . Nessas condições, existe $\chi \in \widehat{G}$ tal que $\chi(a) \neq \chi(b)$.*

Demonstração. Seja $H = \{a \in G : \chi(a) = 1, \forall \chi \in \widehat{G}\}$. Se mostrarmos que $H = \{e\}$ podemos garantir que existe um caractere χ de G tal que $\chi(a) \neq 1$ se $a \neq e$. Façamos isso: verifiquemos inicialmente que H é um subgrupo de G . De fato, dados $a, b \in H$, $\chi(ab^{-1}) = \chi(a)\chi(b)^{-1} = 1 \cdot 1 = 1$, pois $\chi(b^{-1}) = 1 \cdot \chi(b)^{-1} = \chi(b)\chi(b)^{-1} = \chi(bb^{-1}) = \chi(1) = 1$. Logo, $ab^{-1} \in H$, ou seja, H é subgrupo de G . Para cada $\chi \in \widehat{G}$, considere a aplicação $\widetilde{\chi} : G/H \rightarrow \mathbb{C}^\times$ definida por $\widetilde{\chi}(gH) = \chi(g)$, para todo $g \in G$. Essa aplicação está bem definida, pois para cada $g_1, g_2 \in G$,

$$g_1H = g_2H \implies g_1g_2^{-1} \in H \implies \chi(g_1g_2^{-1}) = 1 \implies \chi(g_1) = \chi(g_2) \implies \widetilde{\chi}(g_1H) = \widetilde{\chi}(g_2H), \quad (5.30)$$

e é um caractere, já que $\widetilde{\chi}(g_1H) = \chi(g_1) \neq 0$ e

$$\widetilde{\chi}(g_1Hg_2H) = \widetilde{\chi}(g_1g_2H) = \chi(g_1g_2) = \chi(g_1)\chi(g_2) = \widetilde{\chi}(g_1H)\widetilde{\chi}(g_2H). \quad (5.31)$$

Portanto, dado $\chi \in \widehat{G}$, existe $\widetilde{\chi} \in \widehat{G/H}$ tal que $\widetilde{\chi}(gH) = \chi(g)$, para todo $g \in G$. Assim, $\widehat{\psi}(\widetilde{\chi}) = \widetilde{\chi} \circ \psi = \chi$, isto é, $\widehat{\psi}$ é sobrejetora. O item (b) da proposição 5.1.1 já nos informava que $\widehat{\psi}$ era

um homomorfismo injetor. Portanto, podemos agora garantir que $\widehat{\psi}$ é um isomorfismo. Assim, $\widehat{\psi}(\widehat{G/H}) \simeq \widehat{G}$ e, então,

$$o(\widehat{\psi}(\widehat{G/H})) = o(\widehat{G}). \quad (5.32)$$

Como vimos na demonstração da proposição 5.1.4, vale ainda que

$$\frac{\widehat{G}}{\widehat{\psi}(\widehat{G/H})} \simeq \widehat{\varphi}(\widehat{G}) = \widehat{H} \quad (5.33)$$

e, daí,

$$o(\widehat{G})/o(\widehat{\psi}(\widehat{G/H})) = o(\widehat{H}). \quad (5.34)$$

Logo, das igualdades 5.32 e 5.34 concluímos que $o(\widehat{H}) = o(H) = 1$. Portanto, $H = \{e\}$.

Portanto, existe um caractere χ de G tal que $\chi(a) \neq 1$ se $a \neq e$. Finalmente, tome elementos a e b distintos em G . Assim, $ab^{-1} \neq e$. Logo, existe um caractere χ de G tal que $\chi(ab^{-1}) \neq 1$, ou seja, tal que $\chi(a) \neq \chi(b)$, comprovando a tese. $\square$

Observe que a contrarrecíproca da proposição anterior nos diz que se $\chi(a) = \chi(b)$ para todo $\chi \in \widehat{G}$, então $a = b$.

Vamos analisar agora o conjunto dos caracteres de $\widehat{G}$, o qual denotaremos por $\widehat{\widehat{G}}$. Considere, para cada $a \in G$, a aplicação $\iota_a : \widehat{G} \longrightarrow \mathbb{C}^\times$ definida por

$$\iota_a(\chi) = \chi(a), \quad \forall \chi \in \widehat{G}. \quad (5.35)$$

Essa aplicação está bem definida, pois $\chi_1 = \chi_2$ implica $\chi_1(a) = \chi_2(a)$, donde segue que $\iota_a(\chi_1) = \iota_a(\chi_2)$. Além disso, ι_a é um caractere de $\widehat{G}$, pois $\iota_a(\chi) = \chi(a) \neq 0$ e

$$\iota_a(\chi_1\chi_2) = \chi_1\chi_2(a) = \chi_1(a)\chi_2(a) = \iota_a(\chi_1)\iota_a(\chi_2). \quad (5.36)$$

Dessa forma, considere a aplicação $\iota : G \longrightarrow \widehat{\widehat{G}}$ definida por

$$\iota(a) = \iota_a, \quad \forall a \in G. \quad (5.37)$$

Pela transitividade do isomorfismo, note que já podemos garantir que $G \simeq \widehat{\widehat{G}}$ e que $o(G) = o(\widehat{\widehat{G}})$. Porém, a proposição a seguir nos esclarece que ι é a aplicação que confere esse isomorfismo.

Proposição 5.1.6. *A aplicação $\iota : G \longrightarrow \widehat{\widehat{G}}$ é um isomorfismo.*

Demonstração. Mostremos inicialmente que ι é um homomorfismo: para todo $a, b \in G$, $\iota(ab) = \iota_{ab} = \iota_a\iota_b = \iota(a)\iota(b)$, pois $\iota_a(\chi)\iota_b(\chi) = \chi(ab) = \chi(a)\chi(b) = \iota_a(\chi)\iota_b(\chi)$, $\forall \chi \in \widehat{G}$. Note que, se e é a unidade de G , então ι_e é a unidade de $\widehat{\widehat{G}}$, já que $\iota_e(\chi) = \chi(e) = 1$, para todo $\chi \in \widehat{G}$. Portanto,

$$a \in \ker(\iota) \implies \iota(a) = i_e \implies \iota_a = \iota_e \implies \chi(a) = \chi(e), \quad \forall \chi \in \widehat{G} \quad (5.38)$$

e, pela contrarrecíproca da proposição 5.1.5, isso implica que $a = e$. Logo, $\ker(\iota) = \{e\}$, ou seja, ι é injetora. Como $o(G) = o(\widehat{G})$, então ι é sobrejetora e, portanto, ι é um isomorfismo. $\square$

5.2 Caracteres de $\mathbb{Z}_n^*$

Nesta seção explicitaremos os caracteres do grupo multiplicativo $(\mathbb{Z}/\mathbb{Z}n)^*$, o qual estamos denotando ao longo deste texto simplesmente por $\mathbb{Z}_n^*$. Consideraremos $n \geq 1$. Devido ao Teorema Fundamental da Aritmética, podemos escrever $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, em que p_i é primo e $\text{mdc}(p_i, p_j) = 1$, para todo $i \neq j$, $0 \leq i, j \leq r$. Para cada i , denotemos $n_i = p_i^{e_i}$. Assim, $n = n_1 n_2 \dots n_r$, com $\text{mdc}(n_i, n_j) = 1$ para cada $i \neq j$, $0 \leq i, j \leq r$.

Devido à proposição 1.2.7, existe um isomorfismo de grupos $\theta : \mathbb{Z}_n^* \longrightarrow \prod_{i=1}^r \mathbb{Z}_{n_i}^*$ que associa cada elemento $x \in \mathbb{Z}_n^*$ a $\theta(x) = (x \pmod{n_1}, x \pmod{n_2}, \dots, x \pmod{n_r})$. Utilizando a proposição 5.1.3, consideremos a aplicação $\widehat{\theta} : \widehat{\mathbb{Z}_n^*} \longrightarrow \prod_{i=1}^r \widehat{\mathbb{Z}_{n_i}^*}$ dada por $\widehat{\theta}(\chi) = (\chi_1, \chi_2, \dots, \chi_r)$, em que $\chi_i = \chi \circ v_i$ e $v_i(x_i) = \theta^{-1}(1, \dots, x_i, \dots, 1)$ (como na demonstração da referida proposição), para cada $i = 1, 2, \dots, r$. Pela proposição 5.1.3, $\widehat{\theta}$ é um isomorfismo. Portanto, o que faremos a seguir é explicitar os grupos de caracteres $\widehat{\mathbb{Z}_{p^e}^*}$ (p primo, $e \geq 1$), já que assim, pelo comentário anterior, também fica explícito o grupo $\widehat{\mathbb{Z}_n^*}$. Para realizar essa tarefa será necessário considerar dois casos: quando $p = 2$ e quando $p \neq 2$.

Caso 1: p primo ímpar ($p \neq 2$).

Neste caso, sabemos da proposição 1.2.9 (ou de sua demonstração) que $\mathbb{Z}_{p^e}^* = B \times C$, onde $B = \langle b \rangle$ é um grupo cíclico de ordem $p-1$ e $C = \langle p+1 \rangle$ é um grupo cíclico de ordem p^{e-1} . Assim, os elementos de $\mathbb{Z}_{p^e}^*$ são da forma

$$b^i(1+p)^j \quad \text{com } 0 \leq i < p-1 \text{ e } 0 \leq j < p^{e-1}. \quad (5.39)$$

Consideramos $\chi : B \longrightarrow \mathbb{C}^\times$ o caractere dado por $\chi(b) = \zeta_{p-1}$ e $\psi : C \longrightarrow \mathbb{C}^\times$ o caractere dado por $\psi(p+1) = \zeta_{p^{e-1}}$. Pela proposição 5.1.2, $\widehat{B} = \langle \chi \rangle$ e $\widehat{C} = \langle \psi \rangle$. De fato, seja χ_r um caractere de B dado por $\chi_r(b^s) = \zeta_{p-1}^{rs}$ ($0 \leq r < p-1$ e $1 \leq s \leq p-1$) conforme indicado pela proposição citada. Assim, é verdade que $\chi_r = \chi^r$ para cada $0 \leq r < p-1$, pois

$$\chi_r(b^s) = \zeta_{p-1}^{rs} = (\zeta_{p-1}^s)^r = \chi(b^s)^r = \chi^r(b^s), \quad \forall 1 \leq s \leq p-1. \quad (5.40)$$

Portanto, $\widehat{B} = \langle \chi \rangle$. Analogamente mostra-se que $\widehat{C} = \langle \psi \rangle$. Então $\widehat{\mathbb{Z}_{p^e}^*} = \langle \chi \rangle \times \langle \psi \rangle$. Assim, todo caractere de $\mathbb{Z}_{p^e}^*$ é da forma $\chi^r \psi^s$, com $0 \leq r < p-1$ e $0 \leq s < p^{e-1}$. Agora, sejam $\eta = \chi^r \psi^s$ um elemento qualquer de $\widehat{\mathbb{Z}_{p^e}^*}$ e $a = b^i(1+p)^j$ um elemento qualquer de $\mathbb{Z}_{p^e}^*$. Então

$$\eta(a) = \chi^r \psi^s(a) = \chi^r(b^i) \psi^s((1+p)^j) = \zeta_{p-1}^{ir} \zeta_{p^{e-1}}^{js} \quad (5.41)$$

é a descrição explícita de um caractere qualquer de $\widehat{\mathbb{Z}_{p^e}^*}$.

Caso 2: $p = 2$.

Se $p = 2$ e $e = 1$ então $\widehat{\mathbb{Z}_2^*} = \{\chi_0\}$, em que $\chi_0 \equiv 1$. Portanto, podemos supor $e \geq 2$. Pela proposição 1.2.10 sabe-se que $\mathbb{Z}_{2^e}^* \simeq B \times C$, onde $B = \{-1, 1\} = \langle -1 \rangle$ tem ordem 2 e $C = \{a \in \mathbb{Z}_{2^e}^* : a \equiv 1 \pmod{4}\} = \langle 5 \rangle$ tem ordem 2^{e-2} , isto é, $\mathbb{Z}_{2^e}^* \simeq \langle -1 \rangle \times \langle 5 \rangle$. Logo, todo elemento de $\mathbb{Z}_{2^e}^*$ é da forma

$$(-1)^i 5^j \quad \text{com } i = 0, 1 \text{ e } 0 \leq j < 2^{e-2}. \quad (5.42)$$

Defina $\chi : B \rightarrow \mathbb{C}^*$ por $\chi(-1) = -1$ e $\psi : C \rightarrow \mathbb{C}^*$ por $\psi(5) = \zeta_{2^{e-2}}$. Devido à proposição 5.1.2 e de maneira análoga ao que foi feito no caso p ímpar verifica-se que $\widehat{B} = \{1, \chi\} = \langle \chi \rangle$ e que $\widehat{C} = \langle \psi \rangle$. Como $\mathbb{Z}_{2^e}^* \simeq B \times C$ então $\widehat{\mathbb{Z}_{2^e}^*} \simeq \widehat{B} \times \widehat{C}$, ou seja, $\widehat{\mathbb{Z}_{2^e}^*} = \langle \chi \rangle \times \langle \psi \rangle$. Portanto, todo caractere de $\mathbb{Z}_{2^e}^*$ é da forma $\chi^r \psi^s$, com $r = 0, 1$ e $0 \leq s < 2^{e-2}$. Tomando $\eta = \chi^r \psi^s$ um elemento qualquer de $\widehat{\mathbb{Z}_{2^e}^*}$ e $a = (-1)^i 5^j$ um elemento qualquer de $\mathbb{Z}_{2^e}^*$, então

$$\eta(a) = \chi^r \psi^s(a) = \chi^r((-1)^i) \psi^s(5^j) = (-1)^{ir} \zeta_{2^{e-2}}^{js} \quad (5.43)$$

é a descrição explícita de um caractere qualquer de $\widehat{\mathbb{Z}_{2^e}^*}$.

5.3 Relações de ortogonalidade entre caracteres

Seja G um grupo abeliano finito de ordem n . Considere

$$V = \{f : G \rightarrow \mathbb{C} ; f \text{ é função}\} \quad (5.44)$$

o conjunto das funções complexas definidas em G . O conjunto V é um espaço vetorial sobre $\mathbb{C}$. Além disso, a dimensão de V sobre $\mathbb{C}$ é $o(G) = n$. De fato, V é espaço vetorial, pois $(f+g)(a) = f(a)+g(a)$, $(\alpha f)(a) = \alpha f(a)$ para quaisquer $f, g \in V$, $a \in G$, $\alpha \in \mathbb{C}$, e verificam-se todas as propriedades da definição de um espaço vetorial. Para mostrar que V tem dimensão n considere $G = \{g_1, g_2, \dots, g_n\}$

e tome o conjunto $\mathcal{B} = \{f_1, f_2, \dots, f_n\} \subset V$ tal que cada função f_i é definida por

$$f_i(g_j) = \begin{cases} 1, & i = j; \\ 0, & i \neq j; \end{cases} \quad (5.45)$$

Mostremos que $\mathcal{B}$ é base para V . Com efeito, se $\alpha_i \in \mathbb{C}$,

$$\sum_{i=1}^n \alpha_i f_i = 0 \implies \sum_{i=1}^n \alpha_i f_i(g_j) = 0 \implies \alpha_j = \alpha_j f_j(g_j) = 0 \quad (5.46)$$

para todo $j \in \{1, 2, \dots, n\}$. Logo, $\mathcal{B}$ é um conjunto linearmente independente sobre os números complexos. Além disso, se $f \in V$, defina $c_i \triangleq f(g_i) \in \mathbb{C}$. Assim, $f(x) = \sum_{i=1}^n c_i f_i(x)$ para todo $x \in G$. Logo, $\mathcal{B}$ gera V e, portanto, V tem dimensão n sobre $\mathbb{C}$. A base $\mathcal{B}$ é chamada de **base canônica** de V .

A expressão

$$\langle f, g \rangle = \frac{1}{n} \sum_{a \in G} f(a) \overline{g(a)}, \quad f, g \in V \quad (5.47)$$

define um produto interno em V . Em geral, se f e g são elementos de V tais que $\langle f, g \rangle = 0$, dizemos que f e g são ortogonais. Esse produto vetorial induz uma norma, $\|f\| = \langle f, f \rangle^{1/2}$. Se $\|f\| = 1$, dizemos que f é unitário.

Seja o conjunto dos caracteres de G dado por $\widehat{G} = \{\chi_0, \chi_1, \dots, \chi_{n-1}\}$, em que χ_0 é o caractere trivial. Veremos na proposição seguinte que esse conjunto forma uma base ortonormal de V .

Proposição 5.3.1. *Consideradas as notações acima:*

- (a) $\|\chi_i\| = 1, 0 \leq i \leq n-1$;
- (b) $\langle \chi_i, \chi_j \rangle = 0$, se $i \neq j$;
- (c) Para $0 \leq j \leq n-1$ e $\alpha_i \in \mathbb{C}$, tem-se $\langle \sum_{i=0}^{n-1} \alpha_i \chi_i, \chi_j \rangle = \alpha_j$.
- (d) O conjunto $\widehat{G} = \{\chi_0, \chi_1, \dots, \chi_{n-1}\}$ é base de V .

Demonstração. Seja $\alpha = \langle \chi_i, \chi_0 \rangle = \frac{1}{n} \sum_{a \in G} \chi_i(a)$. Se $\chi_i = \chi_0$, então $\langle \chi_i, \chi_0 \rangle = \frac{1}{n} \sum_{a \in G} 1 = \frac{n}{n} = 1$. Caso $\chi_i \neq \chi_0$, deve existir $b \in G$ tal que $\chi_i(b) \neq 1$. Logo,

$$\alpha \chi_i(b) = \frac{1}{n} \sum_{a \in G} \chi_i(a) \chi_i(b) = \frac{1}{n} \sum_{a \in G} \chi_i(ab) = \frac{1}{n} \sum_{c \in G} \chi_i(c) = \alpha \quad (5.48)$$

do que segue que $\alpha \chi_i(b) = \alpha$ e, portanto, $\alpha = 0$. Logo, $\langle \chi_i, \chi_0 \rangle = 0$ se $i \neq 0$. Para quaisquer $\chi_j, \chi_k \in \widehat{G}$, considere $\chi_i = \chi_j \overline{\chi_k} \in \widehat{G}$. Pelo que provamos acima,

$$\langle \chi_j, \chi_k \rangle = \frac{1}{n} \sum_{a \in G} \chi_j(a) \overline{\chi_k(a)} = \frac{1}{n} \sum_{a \in G} \chi_i(a) = \alpha \quad (5.49)$$

donde segue que se $j \neq k$ então $\langle \chi_j, \chi_k \rangle = 0$ e se $j = k$ então $\langle \chi_j, \chi_k \rangle = 1$, o que comprova os itens (a) e (b). O item (c) é imediato devido à linearidade do primeiro termo do produto interno e devido aos itens (a) e (b). Por fim, verifiquemos que vale o item (d). Se $\alpha_i \in \mathbb{C}$, $1 \leq i \leq n$, a combinação linear $\sum_{i=0}^{n-1} \alpha_i \chi_i = 0$ implica, pelo item (c), que $\alpha_j = \langle \sum_{i=0}^{n-1} \alpha_i \chi_i, \chi_j \rangle = \langle 0, \chi_j \rangle = 0$, para todo $0 \leq j \leq n-1$. Portanto, $\widehat{G}$ é linearmente independente sobre $\mathbb{C}$ e, como $\widehat{G}$ tem mesma dimensão de V , então o conjunto dos caracteres de G forma uma base para V , completando a prova. $\square$

Como corolário desta proposição, seguem as relações de ortogonalidade entre caracteres de um grupo abeliano finito G :

Corolário 5.3.1 (Relações de ortogonalidade entre caracteres). *Se $\widehat{G} = \{\chi_0, \chi_1, \dots, \chi_{n-1}\}$, χ_0 é o caractere trivial de G e e é o elemento identidade de G , então:*

$$\begin{aligned} (a) \sum_{a \in G} \chi_i(a) &= \begin{cases} n, & i = 0; \\ 0, & i \neq 0; \end{cases} \\ (b) \sum_{a \in G} \chi_i(a) \overline{\chi_j(a)} &= \begin{cases} n, & i = j; \\ 0, & i \neq j; \end{cases} \\ (c) \text{ Se } a \in G, \sum_{i=0}^{n-1} \chi_i(a) &= \begin{cases} n, & a = e; \\ 0, & a \neq e; \end{cases} \\ (d) \text{ Se } a, b \in G, \sum_{i=0}^{n-1} \chi_i(a) \overline{\chi_i(b)} &= \begin{cases} n, & a = b; \\ 0, & a \neq b; \end{cases} \end{aligned}$$

Demonstração. (a) Como $\chi_0(a) = 1$ para todo $a \in G$, então $\sum_{a \in G} \chi_0(a) = n$. Caso $\chi_i \neq \chi_0$, então pela proposição 5.3.1, $0 = \langle \chi_i, \chi_0 \rangle = \frac{1}{n} \sum_{a \in G} \chi_i(a)$, donde segue que $\sum_{a \in G} \chi_i(a) = 0$. (b) Se $i = j$, então $\chi_i = \chi_j$ e, pela proposição 5.3.1, $1 = \langle \chi_i, \chi_i \rangle = \frac{1}{n} \sum_{a \in G} \chi_i(a) \overline{\chi_i(a)}$, donde segue que $\sum_{a \in G} \chi_i(a) \overline{\chi_i(a)} = n$. Se $i \neq j$, então $0 = \langle \chi_i, \chi_j \rangle = \frac{1}{n} \sum_{a \in G} \chi_i(a) \overline{\chi_j(a)}$, o que implica $\sum_{a \in G} \chi_i(a) \overline{\chi_j(a)} = 0$. (c) No item (a), trocando o conjunto G por $\widehat{G}$ e utilizando a aplicação ι_a definida na fórmula 5.35 tem-se que

$$\sum_{i=0}^{n-1} \chi_i(a) = \sum_{\chi_i \in \widehat{G}} \iota_a(\chi_i) = \begin{cases} n, & \iota_a = \iota_e; \\ 0, & \iota_a \neq \iota_e; \end{cases} = \begin{cases} n, & a = e; \\ 0, & a \neq e; \end{cases} \quad (5.50)$$

(d) Se $a = b$, então $\iota_a = \iota_b$ e, daí,

$$n = n \langle \iota_a \iota_b^{-1}, \iota_e \rangle = n \frac{1}{n} \sum_{i=0}^{n-1} \iota_a(\chi_i) \iota_b^{-1}(\chi_i) = \sum_{i=0}^{n-1} \chi_i(a) \overline{\chi_i(b)}. \quad (5.51)$$

Se $a \neq b$, do item (c) segue que $0 = \sum_{i=0}^{n-1} \chi_i(ab^{-1}) = \sum_{i=0}^{n-1} \chi_i(a) \overline{\chi_i(b)}$. $\square$

Terminaremos esta seção estudando alguns operadores lineares de V . Para cada $a \in G$, defina $S_a : V \rightarrow V$ uma aplicação tal que, para cada $f \in V$, $S_a(f)$ seja uma função de G dada por

$$S_a(f)(b) = f(ab), \quad \forall b \in G. \quad (5.52)$$

Essa aplicação S_a é uma transformação linear de V em V e é chamada de **operador de mudança**.

Para todo elemento $f \in V$, considere

$$S_f \triangleq \sum_{a \in G} f(a) S_a \quad (5.53)$$

uma nova transformação linear de V em V .

Note que se χ é um caractere de G qualquer, então $S_a(\chi)(b) = \chi(ab) = \chi(a)\chi(b)$, para todo $b \in G$. Logo, $S_a(\chi) = \chi(a)\chi$, o que nos mostra que todo caractere de G é um autovetor de S_a , cujo autovalor associado é $\chi(a)$. Da mesma forma, dado $f \in V$,

$$S_f(\chi)(b) = \sum_{a \in G} f(a) S_a(\chi)(b) = \left[\sum_{a \in G} f(a) \chi(a) \chi \right] (b), \quad \forall b \in G, \quad (5.54)$$

donde conclui-se que $S_f(\chi) = (\sum_{a \in G} f(a) \chi(a)) \chi$. Portanto, todo caractere χ é um autovetor de S_f , cujo autovalor associado é $\sum_{a \in G} f(a) \chi(a)$. Isso nos leva à seguinte proposição:

Proposição 5.3.2. *Se $f \in V$ então*

$$\prod_{\chi \in \widehat{G}} \left(\sum_{a \in G} f(a) \chi(a) \right) = \det(f(ba^{-1}))_{a \in G, b \in G}. \quad (5.55)$$

Demonstração. Considere a matriz $n \times n$ dada por $M = [f(ba^{-1})]_{a \in G, b \in G}$. Seja $S = S_f = \sum_{a \in G} f(a) S_a$. Por um lado, como $\widehat{G} = \{\chi_0, \chi_1, \dots, \chi_{n-1}\}$ é base de V que consiste de autovetores de S e $\sum_{a \in G} f(a) \chi(a)$ são os autovalores relacionados a esses autovetores, então $\det(S) = \prod_{i=0}^{n-1} (\sum_{a \in G} f(a) \chi_i(a))$.

Por outro lado, seja $\mathcal{B} = \{f_a\}_{a \in G}$ a base canônica de V , isto é, $f_a(b) = 1$ se $b = a$ e $f_a(b) = 0$ se $b \neq a$, para quaisquer $a, b \in G$. Temos, para cada $b, c \in G$,

$$S(f_b)(c) = \sum_{a \in G} f(a) S_a(f_b)(c) = \sum_{a \in G} f(a) f_b(ac) = f(bc^{-1}) = \left(\sum_{a \in G} f(ba^{-1}) f_a \right) (c). \quad (5.56)$$

Então, $S(f_b) = \sum_{a \in G} f(ba^{-1}) f_a$, para todo $b \in G$. Logo, a matriz de S com relação à base $\mathcal{B}$ tem entradas $f(ba^{-1})$ na linha a e coluna b , ou seja, a matriz de S é M . Daí, $\det(S) = \det(M)$. Portanto,

$$\det(M) = \det(S) = \prod_{i=0}^{n-1} \left(\sum_{a \in G} f(a) \chi_i(a) \right). \quad (5.57)$$

□

5.4 Caracteres de Dirichlet

Os caracteres que definiremos nesta seção podem ser relacionados com os caracteres anteriormente estudados. Porém, o domínio do caractere agora considerado não é mais um grupo finito, mas sim o anel $\mathbb{Z}$. Ao longo dessa seção, considere $n > 1$ um número inteiro.

Definição 5.4.1. *Uma função $\chi : \mathbb{Z} \rightarrow \mathbb{C}$ é chamada de **caractere de Dirichlet módulo n** (ou **caractere modular módulo n**) quando satisfaz as seguintes condições:*

- (a) $\chi(a) = 0 \iff \text{mdc}(a, n) \neq 1$;
- (b) $a \equiv b \pmod{n} \implies \chi(a) = \chi(b)$;
- (c) $\chi(ab) = \chi(a)\chi(b)$.

Se χ é um caractere de Dirichlet módulo n então o conjunto dos elementos de $\mathbb{Z}$ que são relativamente primos a n é chamado de **suporte** de χ . Note que $\chi(a) = 1$ para todo $a \equiv 1 \pmod{n}$. Em particular, definimos o caractere χ_0 tal que $\chi_0(a) = 1$ se $\text{mdc}(a, n) = 1$ e $\chi_0(a) = 0$ caso contrário, o qual chamamos de **caractere trivial módulo n** .

Observe também que $\chi((-1))^2 = \chi((-1)^2) = \chi(1) = 1$. Assim, $\chi(-1) = \pm 1$. Consequentemente, para qualquer inteiro a , $\chi(-a) = \chi(-1)\chi(a) = \pm\chi(a)$. Dessa forma, todo caractere de Dirichlet módulo n pode ser classificado da seguinte maneira:

- se $\chi(-a) = \chi(a)$ para todo a relativamente primo a n , χ é chamado **caractere par**;
- se $\chi(-a) = -\chi(a)$ para todo a relativamente primo a n , χ é chamado **caractere ímpar**.

A primeira proposição desta seção compara os caracteres de grupos abelianos finitos com os caracteres de Dirichlet:

Proposição 5.4.1. *Existe uma correspondência biunívoca entre os caracteres de $\mathbb{Z}_n^*$ e os caracteres de Dirichlet módulo n .*

Demonstração. Seja χ um caractere módulo n . Defina $\tilde{\chi} : \mathbb{Z}_n^* \rightarrow \mathbb{C}^\times$ uma aplicação tal que $\tilde{\chi}(\bar{a}) = \chi(a)$, para cada $\bar{a} \in \mathbb{Z}_n^*$. Note que $\tilde{\chi}$ está bem definida e é um homomorfismo, pois χ está bem definida e é um homomorfismo. Como $\tilde{\chi}(\bar{a}) = \chi(a) \neq 0$ para todo $\bar{a} \in \mathbb{Z}_n^*$, então $\tilde{\chi}$ é um caractere de $\mathbb{Z}_n^*$. Considere agora a função $\varphi : \{\text{caracteres de Dirichlet mod } n\} \rightarrow \widehat{\mathbb{Z}_n^*}$ definida por $\varphi(\chi) = \tilde{\chi}$, a qual está claramente bem definida. Além disso, φ é injetora. De fato, se $\varphi(\chi_1) = \varphi(\chi_2)$, então $\widehat{\chi_1} = \widehat{\chi_2}$. Daí, $\chi_1(a) = \chi_2(a)$ sempre que $\text{mdc}(a, n) = 1$. Caso $\text{mdc}(a, n) \neq 1$, como χ_1 e χ_2 são caracteres de Dirichlet módulo n , então $\chi_1(a) = \chi_2(a) = 0$. Logo, $\chi_1 = \chi_2$ e φ é injetora. A função

φ é sobrejetora, pois, dado $\rho \in \widehat{\mathbb{Z}_n^*}$, considere $\chi : \mathbb{Z} \rightarrow \mathbb{C}$ tal que $\chi(a) = 0$ se $\text{mdc}(a, n) \neq 1$ e $\chi(a) = \rho(\bar{a})$ se $\text{mdc}(a, n) = 1$. Assim definida, a aplicação χ é um caractere de Dirichlet módulo n tal que $\varphi(\chi) = \rho$. Portanto φ é bijetora, o que comprova que existe uma relação biunívoca entre os caracteres de Dirichlet módulo n e os caracteres de $\mathbb{Z}_n^*$. $\square$

Observação 5.4.1. Considerando χ_1 e χ_2 dois caracteres de Dirichlet módulo n , podemos definir o produto $\chi_1\chi_2$ por $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$, para cada $a \in \mathbb{Z}$. Assim, $\varphi(\chi_1\chi_2) = \varphi(\chi_1)\varphi(\chi_2)$. Logo, podemos considerar que o conjunto dos caracteres de Dirichlet módulo n é um grupo isomorfo a $\widehat{\mathbb{Z}_n^*}$. Isso nos permite, sempre que conveniente, considerar o conjunto dos caracteres de Dirichlet módulo n como sendo o conjunto $\widehat{\mathbb{Z}_n^*}$, com relação dada de maneira natural.

Seja χ um caractere de Dirichlet módulo n . Considere o conjunto

$$M_\chi = \{m \in \mathbb{N} - \{0\} : \text{mdc}(a, n) = \text{mdc}(b, n) \text{ e } a \equiv b \pmod{m} \implies \chi(a) = \chi(b)\}. \quad (5.58)$$

Cada elemento de M_χ é chamado de **definidor modular de χ** . Note que $n \in M_\chi$ devido ao item (b) da definição de caractere de Dirichlet módulo n (definição 5.4.1). Além disso, se $m_1 \in M_\chi$ e $m_1 \mid m_2$ então $m_2 \in M_\chi$. De fato, como $a \equiv b \pmod{m_2}$ implica $a \equiv b \pmod{m_1}$, então para quaisquer a e b tais que $a \equiv b \pmod{m_2}$ e $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$ segue que $\chi(a) = \chi(b)$, pois $m_1 \in M_\chi$. Logo, $m_2 \in M_\chi$.

O Princípio da Boa Ordem nos garante que o conjunto M_χ possui um menor elemento natural positivo. Por ser muito interessante para os nossos propósitos, isso nos leva à seguinte definição:

Definição 5.4.2. Para qualquer caractere de Dirichlet χ módulo n , o menor elemento de M_χ é chamado de **condutor de χ** e é denotado por f_χ .

Note que se χ_0 é o caractere trivial módulo n , então seu condutor é $f_{\chi_0} = 1$, pois se $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$, como $a \equiv b \pmod{1}$, então $\chi_0(a) = 1 = \chi_0(b)$.

As próximas proposições fazem importantes observações acerca do condutor de um caractere de Dirichlet. Antes, demonstraremos um lema que será útil na demonstração da próxima proposição.

Lema 5.4.1. Sejam a, b, m_1, m_2, n e d inteiros tais que $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$, $d = \text{mdc}(m_1, m_2)$ e $a \equiv b \pmod{d}$. Considere m_0 o produto dos primos que dividem n e que não dividem m_2 . Então existe um inteiro x tal que $x \equiv a \pmod{m_0 m_1}$, $x \equiv b \pmod{m_2}$ e $\text{mdc}(x, n) = 1$.

Demonstração. Por hipótese, $d = \text{mdc}(m_1, m_2)$. Logo, pela Relação de Bezóut existem inteiros r e s tais que $d = rm_0 m_1 + sm_2$. Tome $x = sm_2[(a - b)/d] + b = a - m_0 m_1 r[(a - b)/d]$. Então existe x

tal que $x \equiv b \pmod{m_2}$ e $x \equiv a \pmod{m_0 m_1}$. Por consequência, $\text{mdc}(x, n) = 1$. De fato, suponha que exista p primo que divida x e n . Então p não pode dividir m_2 , pois se $p \mid m_2$ então $p \mid (x - b)$, donde $p \mid b$ (pois $p \mid x$) e $p \mid n$, o que é uma contradição do fato de b e n serem relativamente primos. Portanto, como p divide n e p não divide m_2 , segue da definição de m_0 que $p \mid m_0$. Logo $p \mid m_0 m_1$ e $p \mid x$, donde segue que $p \mid a$ e $p \mid n$, o que é um absurdo do fato de a e n serem relativamente primos. Portanto, a existência do primo p é um absurdo e $\text{mdc}(x, n) = 1$. $\square$

Proposição 5.4.2. *Seja χ um caractere de Dirichlet módulo n . Então M_χ consiste de todos os múltiplos positivos de f_χ .*

Demonstração. Primeiramente, mostremos que se $m_1, m_2 \in M_\chi$, então $d = \text{mdc}(m_1, m_2) \in M_\chi$. Suponha que a e b sejam inteiros tais que $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$ e $a \equiv b \pmod{d}$. Considere m o produto dos primos que dividem n e que não dividem m_2 . Então ainda vale $d = \text{mdc}(mm_1, m_2)$. Pelo lema 5.4.1 é garantida a existência de x tal que $x \equiv b \pmod{m_2}$, $x \equiv a \pmod{mm_1}$ e $\text{mdc}(x, n) = 1$. Como $m_1 \in M_\chi$ e $m_1 \mid mm_1$ então $mm_1 \in M_\chi$. Assim, $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$, $x \equiv a \pmod{mm_1}$ e $x \equiv b \pmod{m_2}$. Pela definição de M_χ , como $mm_1, m_2 \in M_\chi$, segue que $\chi(a) = \chi(x) = \chi(b)$. Logo, se $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$ e $a \equiv b \pmod{d}$, obtém-se $\chi(a) = \chi(b)$. Portanto, $d \in M_\chi$. Agora, seja $m' \in M_\chi$ qualquer. Como $f_\chi \in M_\chi$, segue do que foi provado acima que $d = \text{mdc}(f_\chi, m') \in M_\chi$. Por um lado $d \mid f_\chi$ implica que $d \leq f_\chi$. Por outro lado, $d \in M_\chi$ implica $d \geq f_\chi$. Logo, $d = f_\chi$. Assim, o fato de d dividir m' acarreta que f_χ divide m' , para qualquer $m' \in M_\chi$. $\square$

Proposição 5.4.3. *Não existe caractere de Dirichlet com condutor $2m$, onde m é um número ímpar.*

Demonstração. Seja χ um caractere de Dirichlet módulo n tal que $f_\chi = 2m$, com m ímpar. Como $n \in M_\chi$, pela proposição 5.4.2 tem-se que $f_\chi \mid n$. Logo $2 \mid n$, ou seja, n é par. Por definição de M_χ , se a e b são inteiros que satisfazem $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$ e $a \equiv b \pmod{2m}$ então $\chi(a) = \chi(b)$. Suponha que a e b sejam inteiros quaisquer tais que $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$ e $a \equiv b \pmod{m}$. Como n é par, então a e b devem ser ímpares. Além disso, $a \equiv b \pmod{m}$ acarreta $a \equiv b \pmod{2m}$ e, do que foi suposto, $\chi(a) = \chi(b)$. Portanto, $m \in M_\chi$, o que é um absurdo do fato de $2m$ ser o menor elemento desse conjunto. Portanto, não pode existir um caractere de Dirichlet χ com condutor da forma $2m$, com m ímpar. $\square$

Lema 5.4.2. *Sejam d um divisor de n e a um número inteiro relativamente primo com d . Então existe x relativamente primo a n tal que $x \equiv a \pmod{d}$.*

Demonstração. Seja m o produto dos primos distintos que dividem n e que não dividem d . Assim, $\text{mdc}(m, d) = 1$. Pelo Teorema do Resto Chinês, segue que existe x inteiro tal que $x \equiv a \pmod{d}$ e $x \equiv 1 \pmod{m}$. Mostremos que $\text{mdc}(x, n) = 1$. Suponha que exista p primo que divida x e n . Como $p \mid n$, então $p \mid d$ ou $p \mid m$. Se p dividisse d , então p dividiria $x - a$ e, como $p \mid x$, então $p \mid a$, o que é um absurdo por $\text{mdc}(a, d) = 1$. No outro caso, se $p \mid m$, então $p \mid x - 1$, donde segue que $p \mid 1$, pois $p \mid x$, o que novamente é um absurdo. Portanto, a existência de p não é verificada. Logo, $\text{mdc}(x, n) = 1$. $\square$

Trocando em miúdos, a próxima proposição nos permite “reduzir” o suporte de cada caractere de Dirichlet à sua forma mínima, ou seja, nos garante que cada caractere pode ser considerado com módulo dado pelo seu condutor.

Proposição 5.4.4. *Se χ é um caractere de Dirichlet módulo n com condutor f , então existe um único caractere ψ módulo f de condutor f tal que*

$$\text{mdc}(a, n) = 1 \implies \psi(a) = \chi(a). \quad (5.59)$$

Demonstração. Sabemos da proposição 5.4.2 que $f \mid n$. Logo, como $\text{mdc}(a, n) = 1$, então $\text{mdc}(a, f) = 1$. Pelo lema 5.4.2, se $\text{mdc}(a, f) = 1$ então existe x inteiro tal que $x \equiv a \pmod{f}$, $x \equiv 1 \pmod{m_0}$ e $\text{mdc}(x, m) = 1$, em que m_0 é o produto dos primos distintos que dividem n e que não dividem f . Seja y um inteiro tal que $\text{mdc}(y, n) = 1 = \text{mdc}(x, n)$ e $y \equiv x \equiv a \pmod{f}$. Como $f \in M_\chi$, então isso garante que $\chi(y) = \chi(x) = \chi(a)$. Defina $\psi : \mathbb{Z} \rightarrow \mathbb{C}$ por $\psi(a) = \chi(x)$ se $\text{mdc}(a, f) = 1$ e por $\psi(a) = 0$ caso contrário. Como χ é um caractere de Dirichlet, então ψ também é um caractere de Dirichlet. Mais ainda: ψ é um caractere de Dirichlet módulo f . De fato, se $a \equiv y \pmod{f}$ então $y \equiv x \equiv a \pmod{f}$ e, daí, $\psi(a) = \chi(x)$ e $\psi(y) = \chi(x)$, ou seja, $\psi(a) = \psi(y)$. Além disso, se $\text{mdc}(a, n) = 1$, então $\psi(a) = \chi(a)$, pois como $\text{mdc}(a, n) = \text{mdc}(x, n) = 1$ e $f \in M_\chi$, então

$$a \equiv x \pmod{f} \implies \chi(a) = \chi(x) = \psi(a). \quad (5.60)$$

O condutor de ψ é f , já que se $d \in M_\psi$ é o condutor de ψ , como $f \in M_\psi$, então $d \mid f$ (pela proposição 5.4.2). Porém, nesse caso, como $\text{mdc}(a, n) = \text{mdc}(b, n) = 1$ e $a \equiv b \pmod{d}$ então $\psi(a) = \psi(b)$, pois $d \in M_\psi$, e então $\chi(a) = \chi(b)$. Logo, $d \in M_\chi$ e, então, como f é mínimo nesse conjunto, obtém-se $d = f$. Por fim, verifiquemos que ψ é o único caractere que satisfaz as propriedades citadas. Suponha que ψ' seja outro caractere de Dirichlet módulo f com condutor f tal que se $\text{mdc}(a, n) = 1$ então $\psi'(a) = \chi(a)$. Mostremos que $\psi = \psi'$: se $\text{mdc}(a, f) = 1$, como $x \equiv a \pmod{f}$, ψ' tem módulo f e $\text{mdc}(x, n) = 1$, então $\psi'(a) = \psi'(x) = \chi(x) = \psi(a)$; caso contrário, se $\text{mdc}(a, f) \neq 1$, então

$\psi'(a) = 0 = \psi(a)$, pois ψ também é um caractere módulo f . Logo, $\psi = \psi'$ e a unicidade de ψ é garantida. $\square$

Da proposição anterior, podemos concluir que existe um único caractere de Dirichlet módulo f com condutor f , para cada f possível de ser condutor de um caractere de Dirichlet. Um caractere definido módulo seu condutor é chamado **caractere de Dirichlet primitivo**.

Proposição 5.4.5. *Um caractere de Dirichlet χ módulo n tem condutor n se, e somente se, para todo divisor d de n , $1 < d < n$, existir $a \in \mathbb{Z}$ relativamente primo com n , $a \equiv 1 \pmod{d}$ e $\chi(a) \neq 1$.*

Demonstração. ($\Leftarrow$) Seja χ um caractere módulo n com condutor d tal que $1 < d < n$. Logo $d \mid n$ (pela proposição 5.4.2) e, devido à proposição 5.4.4, existe um único caractere ψ módulo d com condutor d tal que

$$mdc(x, n) = 1 \implies \psi(x) = \chi(x). \quad (5.61)$$

Por hipótese, considere a um inteiro tal que $mdc(a, n) = 1$, $a \equiv 1 \pmod{d}$ e $\chi(a) \neq 1$. Devido à fórmula 5.61 tem-se que $\psi(a) = \chi(a) \neq 1$. Porém, como $a \equiv 1 \pmod{d}$ e ψ é um caractere módulo d , então $\psi(a) = \psi(1) = 1$, o que é um absurdo. Logo, o condutor de χ é 1 ou n . No entanto, a existência de um elemento a tal que $\chi(a) \neq 1$ nos permite dizer que χ não é trivial. Portanto, o condutor de χ é n . ($\Rightarrow$) Seja χ um caractere de Dirichlet módulo n com condutor n . Suponhamos, por absurdo, que exista um divisor d de n , $1 < d < n$, tal que para cada inteiro a relativamente primo a n e congruente a 1 módulo d infira-se que $\chi(a) = 1$. Pela lema 5.4.2, se b é um inteiro tal que $mdc(b, d) = 1$ então existe $x \in \mathbb{Z}$ tal que $mdc(x, n) = 1$ e $x \equiv b \pmod{d}$. Claramente, se $mdc(b, n) = 1$, podemos tomar $x = b$. Seja $\psi : \mathbb{Z} \rightarrow \mathbb{C}$ uma aplicação dada por $\psi(b) = \chi(x)$ ($\neq 0$) se $mdc(b, d) = 1$ e $\psi(b) = 0$ caso contrário. Esta aplicação está bem definida. Com efeito, se $c = b$ são inteiros tais que $mdc(b, d) = mdc(c, d) = 1$, então existem x e y tais que $x \equiv c \equiv b \equiv y \pmod{d}$, $mdc(x, n) = mdc(y, n) = 1$ e $\psi(b) = \chi(y)$ e $\psi(c) = \chi(x)$. Considere o inteiro a tal que $ax \equiv y \pmod{n}$ (de fato, existe solução para esta congruência linear). Então $a \equiv 1 \pmod{d}$, pois

$$d \mid m \text{ e } m \mid ax - y \implies d \mid ax - y \implies ax \equiv y \equiv x \pmod{d} \implies a \equiv 1 \pmod{d} \quad (5.62)$$

já que $mdc(x, n) = 1$ e, conseqüentemente, $mdc(x, d) = 1$. Além disso, $mdc(a, n) = 1$, pois se existisse um primo p que dividisse a e n , então p dividiria $ax - y$ e, então, dividiria y , o que é um absurdo, pois $mdc(y, n) = 1$. Logo, por hipótese, tem-se que $\chi(a) = 1$. Daí,

$$\psi(b) = \chi(y) = \chi(ax) = \chi(a)\chi(x) = \chi(x) = \psi(c). \quad (5.63)$$

O caso em que $b = c$ não é primo com d é óbvio. Portanto, ψ está bem definida. Além disso, ψ é um caractere de Dirichlet módulo d . De fato, ψ é um homomorfismo multiplicativo de anéis porque χ é. Por definição tem-se claramente que $\psi(a) = \chi(x) = 0$ se, e somente se, $\text{mdc}(x, d) \neq 1$. Por fim, se b e c são inteiros relativamente primos a d tais que $b \equiv c \pmod{d}$, então existem x e y tais que $\text{mdc}(x, n) = \text{mdc}(y, n) = 1$, $x \equiv c \equiv b \equiv y \pmod{d}$ e $\psi(b) = \chi(y)$ e $\psi(c) = \chi(x)$. Analogamente, existe a inteiro tal que $ax \equiv y \pmod{n}$ e $\psi(b) = \chi(y) = \chi(ax) = \psi(c)$. Portanto, ψ é um caractere de Dirichlet módulo d . Por fim, como podemos tomar $x = b$ quando $\text{mdc}(b, n) = 1$, então nesse caso $\chi(b) = \psi(b)$. Como $d < n$, isso significa que χ tem condutor menor do que n , pois coincide com o caractere ψ de condutor menor ou igual a d no seu suporte. Isso é uma contradição de termos suposto que χ tem condutor n , o que conclui a demonstração. $\square$

A última proposição desta seção nos mostra uma maneira interessante de decompor caracteres de Dirichlet em outros caracteres de modo que o seu condutor coincida com o produto dos condutores dos caracteres da decomposição.

Proposição 5.4.6. *Seja $n = \prod_{i=1}^r n_i > 1$ um número inteiro positivo, em que $\text{mdc}(n_i, n_j) = 1$ para todo $i \neq j$ (na verdade, n_i é a maior potência de um primo p_i na decomposição de n pelo Teorema Fundamental da Aritmética). Assim, todo caractere de Dirichlet χ módulo n pode ser escrito de maneira única como $\chi = \prod_{i=1}^r \chi_i$, em que χ_i é um caractere módulo n_i . Além disso, $f_\chi = \prod_{i=1}^r f_{\chi_i}$. Mais ainda, se χ é primitivo, então cada χ_i também é primitivo.*

Demonstração. Pelo Teorema Chinês do Resto, se a é um inteiro tal que $\text{mdc}(a, n_i) = 1$ para todo $1 \leq i \leq r$, então existem inteiros a_i tais que $a_i \equiv a \pmod{n_i}$ e $a_i \equiv 1 \pmod{n_j}$ se $j \neq i$, de modo que a_i seja solução única para a congruência $X \equiv a \pmod{n}$ em X (pois $n = \prod_{i=1}^r n_i$). Além disso, da mesma forma como fizemos na demonstração do lema 5.4.2, mostra-se que $\text{mdc}(a_i, n) = 1$ para todo $1 \leq i \leq r$. Defina cada aplicação $\chi_i : \mathbb{Z} \rightarrow \mathbb{C}$ por $\chi_i(a) = \chi(a)$, se $\text{mdc}(a, n_i) = 1$, e $\chi_i(a) = 0$ caso contrário, $1 \leq i \leq r$. Mostremos que χ_i está bem definida: para cada a e b , existem a_i e b_i tais que $a_i \equiv a \pmod{n_i}$ e $b_i \equiv b \pmod{n_i}$. Assim, $a_i \equiv a \equiv b \equiv b_i \pmod{n}$, $\chi(a_i) = \chi(b_i)$ e, consequentemente, $\chi_i(a) = \chi_i(b)$. Cada χ_i é um homomorfismo de anéis, pois, se a e b são inteiros relativamente primos a n_i , então $\text{mdc}(ab, n_i) = 1$ e $\chi_i(ab) = \chi(a_i b_i) = \chi(a_i) \chi(b_i) = \chi_i(a) \chi_i(b)$. No caso em que a ou b não é primo com n_i a conclusão de que χ_i é um caractere de Dirichlet é óbvia. Além disso, pela definição da aplicação vê-se que χ_i é um caractere de Dirichlet módulo n_i .

Vejamos que $\chi = \prod_{i=1}^r \chi_i$. Dado um inteiro a relativamente primo a n , então existem a_i ($1 \leq i \leq r$) tais que $a_i \equiv a \pmod{n_i}$ e $a_i \equiv 1 \pmod{n_j}$ se $j \neq i$. Das propriedades de congruência, é claro que

$\prod_{i=1}^r a_i \equiv 1 \dots a \dots 1 \equiv a \pmod{n_i}$ para todo $1 \leq i \leq r$. Logo, $\prod_{i=1}^r a_i \equiv a \pmod{n}$ e, daí,

$$\chi(a) = \chi\left(\prod_{i=1}^r a_i\right) = \prod_{i=1}^r \chi(a_i) = \prod_{i=1}^r \chi_i(a) \quad (5.64)$$

para todo a relativamente primo a n . O caso em que $\text{mdc}(a, n) \neq 1$ é trivial. Logo, $\chi = \prod_{i=1}^r \chi_i$.

Essa representação é única, pois, seja $\chi = \prod_{i=1}^r \chi'_i$ outra decomposição de χ em um produto de caracteres de Dirichlet módulo n_i . Para cada $a \in \mathbb{Z}$ primo com n sejam a_i , $1 \leq i \leq r$, inteiros como definidos no início da demonstração. Assim, para cada $1 \leq i \leq r$,

$$\chi'_i(a) = \chi'_i(a_i) = \prod_{j=1}^r \chi'_j(a_i) = 1 \dots \chi(a_i) \dots 1 = \chi(a_i) = \chi_i(a) \quad (5.65)$$

donde somos levados a concluir que a representação $\chi = \prod_{i=1}^r \chi_i$ é única. Agora, mostremos que $f_\chi = \prod_{i=1}^r f_{\chi_i}$. Inicialmente, se $d_i \in M_{\chi_i}$ para todo $1 \leq i \leq r$ então $d = \prod_{i=1}^r d_i \in M_\chi$. De fato, sejam a e b inteiros relativamente primos a n tais que $a \equiv b \pmod{d}$. Daí, $\text{mdc}(a, n_i) = \text{mdc}(b, n_i) = 1$ e $a \equiv b \pmod{d_i}$. Logo, por hipótese, $\chi_i(a) = \chi_i(b)$ para todo $1 \leq i \leq r$. Logo, a igualdade $\chi = \prod_{i=1}^r \chi_i$ acarreta $\chi(a) = \prod_{i=1}^r \chi_i(a) = \prod_{i=1}^r \chi_i(b) = \chi(b)$. Portanto, $d \in M_\chi$. Afirmamos que se $d \in M_\chi$ satisfaz $d \leq n$ (ou seja, $d \mid n$) então $d = \prod_{i=1}^r d_i$, em que $d_i = \text{mdc}(d, n_i) \in M_{\chi_i}$. Com efeito, como cada n_i é a potência máxima de um primo p_i na fatoração de n , $\text{mdc}(n_i, n_j) = 1$ para $i \neq j$ e $d \mid n$ então verifica-se o produto $d = \prod_{i=1}^r d_i$. Falta mostrar que $d_i = \text{mdc}(d, n_i) \in M_{\chi_i}$, $1 \leq i \leq r$. Para isso, sejam a e b inteiros positivos relativamente primos a n_i tais que $a \equiv b \pmod{d_i}$. Vamos mostrar que $\chi_i(a) = \chi_i(b)$. De fato, sejam a_i e b_i números inteiros que satisfazem $\text{mdc}(a_i, n) = \text{mdc}(b_i, n) = 1$, $a_i \equiv a \pmod{n_i}$, $b_i \equiv b \pmod{n_i}$, $a_i \equiv 1 \pmod{n_j}$, $b_i \equiv 1 \pmod{n_j}$ para $i \neq j$, $\chi_i(a) = \chi(a_i)$ e $\chi_i(b) = \chi(b_i)$. Como $d_i = \text{mdc}(d, n_i) \mid n_i$ então $a_i \equiv a \pmod{d_i}$ e $b_i \equiv b \pmod{d_i}$, donde segue que $a_i \equiv b_i \pmod{d_i}$. Das outras congruências, analogamente mostra-se que $a_i \equiv b_i \pmod{d_j}$ se $i \neq j$. Daí, devido ao fato de d_i e d_j serem primos entre si quando $i \neq j$ conclui-se que $a_i \equiv b_i \pmod{d}$. Por hipótese, $d \in M_\chi$. Assim, $a_i \equiv b_i \pmod{d}$ e $\text{mdc}(a_i, n) = \text{mdc}(b_i, n) = 1$ implicam que $\chi_i(a) = \chi(a_i) = \chi(b_i) = \chi_i(b)$. Portanto, $d_i \in M_{\chi_i}$ se $1 \leq i \leq r$. Em suma, o que mostramos foi:

$$d = \prod_{i=1}^r d_i \in M_\chi \iff d_i \in M_{\chi_i}, \quad 1 \leq i \leq r. \quad (5.66)$$

Daí, como f_{χ_i} é o menor elemento do conjunto M_{χ_i} , $1 \leq i \leq r$, então $\prod_{i=1}^r f_{\chi_i}$ é o menor elemento de M_χ . De fato, suponha que exista $d < \prod_{i=1}^r f_{\chi_i} \in M_\chi$ e tome $d_i = \text{mdc}(d, n_i) \in M_{\chi_i}$ para cada $1 \leq i \leq r$. Assim, $d = \prod_{i=1}^r d_i$ e $f_{\chi_i} \mid d_i$. Logo, $\prod_{i=1}^r f_{\chi_i} \mid \prod_{i=1}^r d_i = d$, o que é um absurdo por termos suposto $d < \prod_{i=1}^r f_{\chi_i}$. Portanto, $f_\chi = \prod_{i=1}^r f_{\chi_i}$. Por fim, dessa igualdade segue que se χ for um caractere módulo $f_\chi = \prod_{i=1}^r f_{\chi_i}$ (note que esta é a fatoração de f_χ em um produto de elementos

primos entre si) com condutor f_χ , então decompomos $\chi = \prod_{i=1}^r \chi_i$, em que cada caractere χ_i tem módulo e caractere f_{χ_i} , o que demonstra o fato de que se χ é um caractere primitivo então cada χ_i , $1 \leq i \leq r$, também é um caractere primitivo. Isso conclui a demonstração. $\square$

Por fim, citamos o importante teorema a seguir, que nos dá o discriminante de um corpo de números em função dos condutores dos caracteres associados ao corpo:

Teorema 5.4.1 (Teorema do Condutor-Discriminante). *Sejam $\mathbb{K}$ um corpo de números e $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$. Considere X o grupo dos caracteres de Dirichlet associados a $\mathbb{K}$, isto é, $X \simeq \widehat{G}$. Então o discriminante de $\mathbb{K}$ é dado por*

$$D(\mathbb{K}) = \pm \prod_{\chi \in X} f_\chi. \quad (5.67)$$

Demonstração. Consulte [34], capítulos 3 (teorema 3.11) e 4 (após teorema 4.5). $\square$

5.5 Condutores dos caracteres de Dirichlet

Nosso objetivo nesta seção é determinar uma fórmula para os condutores dos caracteres de Dirichlet módulo n . Antes disso, faremos algumas considerações acerca do conjunto de caracteres de Dirichlet módulo n .

Sejam n um número inteiro positivo e ζ_n uma raiz n -ésima primitiva da unidade. Pelo corolário 3.2.3, $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \simeq \mathbb{Z}_n^*$, o que é dado pelo isomorfismo ϕ que associa cada $k \in \mathbb{Z}_n^*$ a $\phi(k) = \sigma_k \in \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$, em que $\sigma_k(\zeta_n) = \zeta_n^k$. Para simplificar a notação, denotemos por $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta_n)$ o n -ésimo corpo ciclotômico e por $G^{(n)} = \text{Gal}(\mathbb{Q}^{(n)} : \mathbb{Q})$ seu grupo de Galois. Como $\mathbb{Z}_n^*$ é um grupo finito abeliano, o corolário 5.1.2 nos mostra que $\widehat{\mathbb{Z}_n^*} \simeq \mathbb{Z}_n^* \simeq G^{(n)}$. Devido à proposição 5.4.1, garantimos a existência de uma relação bijetora entre os caracteres de $\mathbb{Z}_n^*$ e os caracteres de Dirichlet módulo n , o qual denotaremos por $X^{(n)}$. Evidentemente, os caracteres de Dirichlet de $X^{(n)}$ são aqueles que podem ser definidos módulo n , ou seja, que têm condutor dividindo n , ou seja,

$$X^{(n)} = \{\chi : \mathbb{Z} \longrightarrow \mathbb{C}^\times \text{ caractere de Dirichlet} : f_\chi \mid n\}. \quad (5.68)$$

Pela observação 5.4.1, podemos considerar $X^{(n)} \simeq \widehat{\mathbb{Z}_n^*}$.

Observação 5.5.1. *Devido à relação $\mathbb{Z}_n^* \simeq G^{(n)}$, podemos identificar $\chi(\sigma_k) = \chi(k)$ para todo $k \in \mathbb{Z}_n^*$. Assim, em suma,*

$$X^{(n)} \simeq \widehat{\mathbb{Z}_n^*} \simeq \mathbb{Z}_n^* \simeq G^{(n)} \simeq \widehat{G^{(n)}}. \quad (5.69)$$

Devido à proposição 5.4.3, se n é ímpar então $X^{(2n)} = X^{(n)}$. Por isso daqui em diante podemos assumir que n não é da forma $2m$, com m ímpar, isto é, que $n \not\equiv 2 \pmod{4}$.

Pelo Teorema Fundamental da Aritmética, $n = \prod_{i=1}^r p_i^{e_i}$, em que cada p_i é primo e e_i é um inteiro positivo, $1 \leq i \leq r$, de modo que $p_i \neq p_j$ se $i \neq j$. Devido à proposição 5.4.6 tem-se que $X^{(n)} = \prod_{i=1}^r X^{(p_i^{e_i})}$, o que significa que todo caractere de Dirichlet χ módulo n pode ser escrito de maneira única como um produto de caracteres χ_i módulo $p_i^{e_i}$. Além disso, $f_\chi = \prod_{i=1}^r f_{\chi_i}$. Portanto, para conhecer o condutor de um caractere módulo n basta conhecer o condutor de cada um de seus fatores módulo $p_i^{e_i}$. Por esse motivo, estudaremos a seguir os condutores dos caracteres de Dirichlet módulo p^e , em que p é um primo e e é um inteiro positivo. No entanto, será necessário dividir esse estudo em dois casos: se $p = 2$ ou se $p \neq 2$.

Caso $p=2$

Primeiramente, supondo $p = 2$, temos que supor também que $e \geq 2$. De fato, pelo que observamos anteriormente, não existe caractere com condutor igual a 2^1 e assumimos $n \not\equiv 2 \pmod{4}$. Como $X^{(2^e)} \simeq \widehat{\mathbb{Z}_{2^e}^*}$ (com um pouco de abuso, consideraremos essa relação uma igualdade), as discussões da seção 5.2 nos lembram que

$$X^{(2^e)} = \langle \omega_2 \rangle \times \langle \psi_2 \rangle \quad (5.70)$$

em que $\omega_2((-1)^i) = (-1)^i$, $\psi_2(5^j) = \zeta_{2^{e-2}}^j$, $\langle \omega_2 \rangle$ tem ordem 2 e $\langle \psi_2 \rangle$ tem ordem 2^{e-2} . Assim, para todo $\chi \in X^{(2^e)}$ e para todo $a = (-1)^i 5^j \in \mathbb{Z}_{2^e}^*$ (proposição 1.2.10) existem $0 \leq r < 2$ e $0 \leq s < 2^{e-2}$ tais que

$$\chi(a) = \omega_2^r((-1)^i) \psi_2^s(5^j) = (-1)^{ir} \zeta_{2^{e-2}}^{js}. \quad (5.71)$$

Para $q, m \in \mathbb{Z}$ denotemos por $v_q(m)$ o inteiro x tal que q^x divide m e q^{x+1} não divide m , ao qual chamaremos de **valorização** de m por q . Note que $v_q(m)$ representa a maior potência de q que divide m .

Proposição 5.5.1. *Seja $\chi = \omega_2^r \psi_2^s \in X^{(2^e)}$, com $0 \leq r < 2$ e $0 \leq s < 2^{e-2}$. Então*

$$f_\chi = \begin{cases} 2^{e-v_2(s)}, & \text{se } s > 0; \\ 4, & \text{se } s = 0 \text{ e } r = 1; \\ 1, & \text{se } s = r = 0 \text{ } (\chi \text{ trivial}). \end{cases} \quad (5.72)$$

Demonstração. O caractere $\chi \equiv 1$ é o trivial. Portanto, para $s = r = 0$ tem-se que $f_\chi = 1$. Suponha $s = 0$ e $r = 1$, ou seja, $\chi = \omega_2$, em módulo 2^e . Mostremos que $f_\chi = 4$. Primeiramente, mostremos que

$4 \in M_\chi$. Sejam $a, b \in \mathbb{Z}_{2^e}^*$ (o que é equivalente a afirmar que a e b são inteiros relativamente primos a 2^e) tais que $a \equiv b \pmod{4}$. Escrevendo $a = (-1)^{i_a} 5^{j_a}$ e $b = (-1)^{i_b} 5^{j_b}$, como $5^j \equiv 1 \pmod{4}$ para todo j inteiro, então $a \equiv b \pmod{4}$ implica $(-1)^{i_a} \equiv (-1)^{i_b} \pmod{4}$, donde segue que $i_a = i_b$. Então $\chi(a) = \omega_2(a) = \zeta_2^{i_a} = \zeta_2^{i_b} = \omega_2(b) = \chi(b)$, o que acarreta $4 \in M_\chi$. Logo $f_\chi \mid 4$ e, consequentemente, $f_\chi = 4$, já que não existe caractere com condutor 2 e χ não é trivial. Agora, seja $0 < s < 2^{e-2}$. Claramente, $s = 2^{v_2(s)} q$, com q ímpar e $0 \leq v_2(s) < e - 2$. Mostremos que $2^{e-v_2(s)} \in M_\chi$: sejam $a = (-1)^{i_a} 5^{j_a}$ e $b = (-1)^{i_b} 5^{j_b}$ elementos relativamente primos a 2^e tais que $a \equiv b \pmod{2^{e-v_2(s)}}$. Como $e - v_2(s) > 2$ então $a \equiv b \pmod{4}$, o que implica que $i_a = i_b$ pelo que já vimos. Logo, $5^{j_a-j_b} \equiv 1 \pmod{2^{e-v_2(s)}}$. Como a ordem de 5 em $\mathbb{Z}_{2^m}^*$ (m inteiro positivo qualquer) é 2^{m-2} , então tomando $m = e - v_2(s)$ tem-se que $2^{e-v_2(s)-2} \mid j_a - j_b$, donde segue que $2^{e-2} \mid s(j_a - j_b)$. Assim, $\chi(a) = (-1)^{i_a} \zeta_{2^{e-2}}^{j_a s} = (-1)^{i_b} \zeta_{2^{e-2}}^{j_b s} = \chi(b)$. Portanto, $2^{e-v_2(s)} \in M_\chi$. Assim, como χ não é trivial, $f_\chi = 2^{e-v_2(s)-k}$, com $0 \leq k < e - v_2(s) - 1$. Suponha $k > 0$. Considere $a = 5^{2^{e-v_2(s)-k-2}}$ e $b = 1$ em $\mathbb{Z}_{2^e}^*$. Assim, $a \equiv b \pmod{2^{e-v_2(s)-k}}$ e $\chi(a) = \chi(b)$, donde $\zeta_2^{0,r} \zeta_{2^{e-2}}^{(2^{e-v_2(s)-k-2})s} = \zeta_2^{0,r} \zeta_{2^{e-2}}^{0,s}$. Então $2^{e-2} \mid s \cdot 2^{e-v_2(s)-k-2}$ e, daí, $2^{v_2(s)+k} \mid s$, o que é um absurdo, pois $k > 0$ e $2^{v_2(s)+1}$ não divide s . Portanto, $f_\chi = 2^{e-v_2(s)}$. $\square$

Caso $p \neq 2$

Analogamente ao que foi feito no caso anterior, como $X^{(p^e)} \simeq \widehat{\mathbb{Z}_{2^e}^*}$ (novamente, com um pouco de abuso, consideraremos essa relação uma igualdade), na seção 5.2 vimos que

$$X^{(p^e)} = \langle \omega_p \rangle \times \langle \psi_p \rangle \quad (5.73)$$

em que $\omega_p(b^i) = \zeta_{p-1}^i$, $\psi_p((1+p)^j) = \zeta_{p^{e-1}}^j$, $\langle \omega_p \rangle$ tem ordem $p-1$ e $\langle \psi_p \rangle$ tem ordem p^{e-1} . Assim, para todo $\chi \in X^{(p^e)}$ e para todo $a = b^i(1+p)^j \in \mathbb{Z}_{p^e}^*$ (proposição 1.2.9) existem $0 \leq r < p-1$ e $0 \leq s < p^{e-1}$ tais que

$$\chi(a) = \omega_p^r(b^i) \psi_p^s((1+p)^j) = \zeta_{p-1}^{ir} \zeta_{p^{e-1}}^{js}. \quad (5.74)$$

Proposição 5.5.2. *Seja $\chi = \omega_p^r \psi_p^s \in X^{(p^e)}$, com $0 \leq r < p-1$ e $0 \leq s < p^{e-1}$. Então*

$$f_\chi = \begin{cases} p^{e-v_p(s)}, & \text{se } s > 0; \\ p, & \text{se } s = 0 \text{ e } r > 0; \\ 1, & \text{se } s = r = 0 \text{ } (\chi \text{ trivial}). \end{cases} \quad (5.75)$$

Demonstração. Já vimos que se $\chi \equiv 1$ é o caractere trivial, então $f_\chi = 1$. Suponha $s = 0$ e $r > 0$. Desta forma, $\chi = \omega_p^r$. Mostremos que $f_\chi = p$. Sejam $x, y \in \mathbb{Z}_{p^e}^*$ tais que $x \equiv y \pmod{p}$. Tomando

$x = b^{i_x}(1+p)^{j_x}$ e $y = b^{i_y}(1+p)^{j_y}$, como $(1+p)^j \equiv 1 \pmod{p}$ para todo j inteiro, então $x \equiv y \pmod{p}$ implica $b^{i_x} \equiv b^{i_y} \pmod{p}$, donde segue que $i_x = i_y$. Então $\chi(x) = \omega_p(x) = \zeta_{p-1}^{i_x} = \zeta_{p-1}^{i_y} = \omega_p(y) = \chi(y)$, o que acarreta $p \in M_\chi$. Como χ não é trivial, então $f_\chi = p$. Para o último caso, suponha $0 < s < p^{e-1}$. Note que $v_p(s) < e - 1$. Mostremos que $p^{e-v_p(s)} \in M_\chi$: sejam $x = b^{i_x}(1+p)^{j_x}$ e $y = b^{i_y}(1+p)^{j_y}$ elementos de $\mathbb{Z}_{p^e}^*$ tais que $x \equiv y \pmod{p^{e-v_p(s)}}$. Como $e - v_p(s) > 1$ então $x \equiv y \pmod{p}$, o que implica que $i_x = i_y$. Logo, $(1+p)^{j_x-j_y} \equiv 1 \pmod{p^{e-v_p(s)}}$. Como a ordem de $1+p$ em $\mathbb{Z}_{p^m}^*$ (m inteiro positivo qualquer) é p^{m-1} , então tomando $m = e - v_p(s)$ tem-se que $p^{e-v_p(s)-1} \mid j_x - j_y$, donde segue que $p^{e-1} \mid s(j_x - j_y)$. Daí, $\chi(x) = \zeta_{p-1}^{i_x r} \zeta_{p^{e-1}}^{j_x s} = \zeta_{p-1}^{i_y r} \zeta_{p^{e-1}}^{j_y s} = \chi(y)$. Portanto, $p^{e-v_p(s)} \in M_\chi$. Assim, como χ não é trivial, $f_\chi = p^{e-v_p(s)-k}$, com $0 \leq k < e - v_p(s)$. Suponha $k > 0$. Considere $x = (1+p)^{p^{e-v_p(s)-k-1}}$ e $b = 1$ em $\mathbb{Z}_{p^e}^*$. Assim, $x \equiv y \pmod{p^{e-v_p(s)-k}}$ e $\chi(x) = \chi(y)$, donde tem-se $\zeta_{p-1}^{0.r} \zeta_{p^{e-1}}^{(p^{e-v_p(s)-k-1})s} = \zeta_{p-1}^{0.r} \zeta_{p^{e-1}}^{0.s}$. Então $p^{e-1} \mid s.p^{e-v_p(s)-k-1}$ e, daí, $p^{v_p(s)+k} \mid s$, o que é um absurdo, pois $k > 0$ e $2^{v_p(s)+1}$ não divide s . Portanto, $f_\chi = p^{e-v_p(s)}$. $\square$

5.6 Soma de Gauss

Nesta seção definiremos a soma de Gauss de um caractere de Dirichlet. Na seção 6.2, adiante, utilizaremos os conhecimentos aqui adquiridos para definir e estudar os *caracteres coordenados de Dirichlet*. Em toda esta seção, considere $m \geq 2$ um inteiro positivo e $\zeta_m = e^{\frac{2\pi i}{m}}$ uma raiz m -ésima primitiva da unidade.

Definição 5.6.1. *Seja χ um caractere de Dirichlet módulo m . Para cada $i \in \{0, 1, 2, \dots, m-1\}$, a i -ésima soma de Gauss de χ , denotada por $\tau_i(\chi)$, é definida por*

$$\tau_i(\chi) \triangleq \sum_{k=1}^n \chi(k) \zeta_m^{ik}. \quad (5.76)$$

Quando $i = 1$, diremos simplesmente **soma de Gauss** ao valor τ_1 , que será denotado por τ .

Note na definição da soma de Gauss que as parcelas $\chi(k) \zeta_n^{ik}$ não aparecem quando $\text{mdc}(k, n) \neq 1$, pois, neste caso, $\chi(k) = 0$.

Proposição 5.6.1. *Se χ é um caractere primitivo módulo m (ou seja, $f_\chi = m$) e $1 \leq i < m$, então:*
(a) *sendo χ_0 o caractere trivial e φ a função de Euler,*

$$\tau_0(\chi) = \begin{cases} \varphi(m), & \text{se } \chi = \chi_0 \\ 0, & \text{se } \chi \neq \chi_0. \end{cases} \quad (5.77)$$

(b) $\tau_i(\chi) = \chi(i)^{-1}\tau(\chi)$, se $\text{mdc}(i, m) = 1$;

(c) $\tau_i(\chi) = 0$, se $\text{mdc}(i, m) \neq 1$.

Demonstração. Como $\tau_0(\chi) = \sum_{k=0}^m \chi(k)$, então o item (a) deste lema segue imediatamente como corolário do item (a) da proposição 5.3.1 tomando $G = \mathbb{Z}_m^*$. Se $\text{mdc}(i, m) = 1$, a aplicação $f : \mathbb{Z}_m^* \rightarrow \mathbb{Z}_m^*$ definida por $f(x) = ix$ para cada $x \in \mathbb{Z}_m^*$ é bijetora. Então, para cada $k \in \mathbb{Z}_m^*$, existe um único $a \in \mathbb{Z}_m^*$ tal que $a = ik$. Assim,

$$\chi(i)\tau_i(\chi) = \sum_{k=1}^m \chi(i)\chi(k)\zeta_m^{ik} = \sum_{a=1}^m \chi(a)\zeta_m^a = \tau(\chi) \quad (5.78)$$

o que demonstra o item (b). Por fim, suponha $\text{mdc}(i, m) \neq 1$ e tome $d = \text{mdc}(i, m)$. Então $1 < d \leq i < m$ e existe um inteiro m' , $1 < m' < m$, tal que $m = dm'$. Como χ é um caractere módulo $f_\chi = m$, pela proposição 5.4.5 é garantida a existência de um inteiro b tal que $\text{mdc}(b, m) = 1$, $b \equiv 1 \pmod{m'}$ e $\chi(b) \neq 1$. Daí $\zeta_{m'} = \zeta_m^b$ e,

$$\zeta_m^i = \zeta_{m'd}^i = \zeta_{m'}^{i/d} = \zeta_{m'}^{bi/d} = \zeta_{dm'}^{bi} = \zeta_m^{bi}. \quad (5.79)$$

Como $\text{mdc}(b, m) = 1$, a aplicação $g : \mathbb{Z}_m^* \rightarrow \mathbb{Z}_m^*$ definida por $g(x) = bx$ para cada $x \in \mathbb{Z}_m^*$ também é bijetora. Assim, para cada $a \in \mathbb{Z}_m^*$ existe um único $k \in \mathbb{Z}_m^*$ tal que $k = ba$ e

$$\tau_i(\chi) = \sum_{k=1}^m \chi(k)\zeta_m^{ik} = \sum_{a=1}^m \chi(b)\chi(a)\zeta_m^{iba} = \chi(b) \sum_{a=1}^m \chi(a)\zeta_m^{ia} = \chi(b)\tau_k(\chi). \quad (5.80)$$

Como $\chi(b) \neq 1$, então $\tau_k(\chi) = 0$, completando a prova. $\square$

Seja χ um caractere módulo $m = \prod_{i=1}^r m_i$, em que $\text{mdc}(m_i, m_j) = 1$ se $i \neq j$. Assim, devido à proposição 5.4.6, para cada $i \in \{1, 2, \dots, r\}$ existe um caractere χ_i módulo m_i tal que $\chi = \prod_{i=1}^r \chi_i$. Considere ainda, para cada $i \in \{1, 2, \dots, r\}$, o número inteiro $m'_i = m/m_i$.

Lema 5.6.1. *Nas condições acima, vale a seguinte igualdade:*

$$\tau(\chi) = \prod_{i=1}^r \chi_i(m'_i) \prod_{i=1}^r \tau(\chi_i). \quad (5.81)$$

Demonstração. Para cada $k \in \mathbb{Z}_m^*$, a demonstração da proposição 5.4.6 nos garante que existem $k_i \in \mathbb{Z}$, $i \in \{1, 2, \dots, r\}$, tais que $k \equiv \prod_{i=1}^r k_i \pmod{m}$, $\text{mdc}(k_i, m_i) = 1$, $k \equiv k_i \pmod{m_i}$, $k \equiv 1 \pmod{m'_i}$ e $\chi(k) = \prod_{i=1}^r \chi_i(k_i)$. Como $\text{mdc}(m'_i, m_i) = 1$ então existe um inteiro b_i tal que $b_i m'_i \equiv 1 \pmod{m_i}$, para cada $i \in \{1, 2, \dots, r\}$. Além disso, se $i \neq j$, como $\text{mdc}(m_j, m_i) = 1$ então $m_j \mid m'_i$ e $b_i m'_i \equiv 0 \pmod{m_j}$. Logo, $k \equiv \sum_{i=1}^r b_i m'_i k_i \pmod{m}$. Assim,

$$\zeta_m^k = \zeta_m^{\sum_{i=1}^r b_i m'_i k_i} = \prod_{i=1}^r \zeta_m^{b_i m'_i k_i} = \zeta_{m/m'_i}^{b_i k_i} = \zeta_{m_i}^{b_i k_i}. \quad (5.82)$$

Isso acarreta

$$\tau(\chi) = \sum_{k=1}^m \chi(k) \zeta_m^k = \prod_{i=1}^r \left(\sum_{k_i=1}^{m_i} \chi_i(k_i) \zeta_{m_i}^{b_i k_i} \right) \quad (5.83)$$

Além disso, como $\chi_i(b_i) \chi_i(m'_i) = \chi_i(b_i m'_i) = \chi_i(1) = 1$, então

$$\sum_{k_i=1}^{m_i} \chi_i(k_i) \zeta_{m_i}^{b_i k_i} = \chi_i(b_i)^{-1} \sum_{k_i=1}^{m_i} \chi_i(b_i k_i) \zeta_{m_i}^{b_i k_i} = \chi_i(m'_i) \tau(\chi_i). \quad (5.84)$$

Logo,

$$\tau(\chi) = \prod_{i=1}^r \left(\sum_{k_i=1}^{m_i} \chi_i(k_i) \zeta_{m_i}^{b_i k_i} \right) = \prod_{i=1}^r (\chi_i(m'_i) \tau(\chi_i)) = \prod_{i=1}^r \chi_i(m'_i) \prod_{i=1}^r \tau(\chi_i) \quad (5.85)$$

como queríamos demonstrar. $\square$

Proposição 5.6.2. *Se χ é um caractere de Dirichlet cujo módulo f é igual a seu condutor então $|\tau(\chi)|^2 = f$.*

Demonstração. Inicialmente, suponha $f = p^e$, em que p é primo e $e \geq 1$. Seja χ um caractere módulo f com condutor f (primitivo). Assim, utilizando a definição da soma de Gauss, temos:

$$|\tau(\chi)|^2 = \overline{\tau(\chi)} \tau(\chi) = \left(\prod_{k=0}^{p^e-1} \overline{\chi(k)} \zeta_{p^e}^{-k} \right) \left(\prod_{i=0}^{p^e-1} \chi(i) \zeta_{p^e}^i \right) = \sum_{k=1}^{p^e} \sum_{i=1}^{p^e} \chi(k)^{-1} \chi(i) \zeta_{p^e}^{i-k} \quad (5.86)$$

Como já foi observado, as parcelas em que $\text{mdc}(k, p) \neq 1$ ou $\text{mdc}(i, p) \neq 1$ não aparecem. Logo, podemos reescrever a fórmula anterior como:

$$|\tau(\chi)|^2 = \sum_{\substack{k=1, \\ \text{mdc}(k,p)=1}}^{p^e} \sum_{\substack{i=1, \\ \text{mdc}(i,p)=1}}^{p^e} \chi(k)^{-1} \chi(i) \zeta_{p^e}^{i-k}. \quad (5.87)$$

Tomando i e k tais que $\text{mdc}(i, p) = \text{mdc}(k, p) = 1$, é garantido que existe $t \in \mathbb{Z}_{p^e}^*$ tal que $kt \equiv i \pmod{p^e}$. Fazendo essa mudança de variável, como $\chi(i) = \chi(k) \chi(t)$, tem-se

$$|\tau(\chi)|^2 = \sum_{\substack{k=1, \\ \text{mdc}(k,p)=1}}^{p^e} \sum_{\substack{t=1, \\ \text{mdc}(t,p)=1}}^{p^e} \chi(t) \zeta_{p^e}^{k(t-1)} = \sum_{\substack{t=1, \\ \text{mdc}(t,p)=1}}^{p^e} \chi(t) \left(\sum_{\substack{k=1, \\ \text{mdc}(k,p)=1}}^{p^e} \zeta_{p^e}^{k(t-1)} \right). \quad (5.88)$$

Note que para $k \in \{1, 2, \dots, p^e\}$, $\text{mdc}(k, p) = 1$ se, e somente se, $k = cp$ ($c \in \{1, 2, \dots, p^{e-1}\}$). Logo,

$$\sum_{\substack{k=1, \\ \text{mdc}(k,p)=1}}^{p^e} \zeta_{p^e}^{k(t-1)} = \sum_{k=1}^{p^e} \zeta_{p^e}^{k(t-1)} - \sum_{c=1}^{p^{e-1}} \zeta_{p^e}^{cp(t-1)}. \quad (5.89)$$

Usando a identidade $1 + x + x^2 + \dots + x^{n-1} = \frac{x^n - 1}{x - 1}$ para quaisquer $x \neq 1$, vê-se que

$$\sum_{k=1}^{p^e} \zeta_{p^e}^{k(t-1)} = \begin{cases} p^e, & \text{se } t = 1, \\ 0, & \text{se } t \neq 1 \end{cases} \quad (5.90)$$

e

$$\sum_{c=1}^{p^{e-1}} \zeta_{p^e}^{cp(t-1)} = \begin{cases} p^{e-1}, & \text{se } t \equiv 1 \pmod{p^{e-1}}, \\ 0, & \text{se } t \not\equiv 1 \pmod{p^{e-1}}. \end{cases} \quad (5.91)$$

Então,

$$|\tau(\chi)|^2 = \sum_{\substack{t=1, \\ mdc(t,p)=1}}^{p^e} \chi(t) \left(\sum_{k=1}^{p^e} \zeta_{p^e}^{k(t-1)} \right) - \sum_{\substack{t=1, \\ mdc(t,p)=1}}^{p^e} \chi(t) \left(\sum_{c=1}^{p^{e-1}} \zeta_{p^e}^{cp(t-1)} \right) = p^e - p^{e-1} \left(\sum_{\substack{t=1, mdc(t,p)=1 \\ t \equiv 1 \pmod{p^{e-1}}}}^{p^e} \chi(t) \right). \quad (5.92)$$

Vamos analisar esta última soma. Sabemos que se $p \neq 2$, como $mdc(t, p) = 1$ e $1 \leq t \leq p^e$, tem-se que $t \equiv b^{\alpha'}(1+p)^{\alpha''} \pmod{p^e}$, em que $0 \leq \alpha' < p-1$, $0 \leq \alpha'' < p^{e-1}$ e $\chi(t) = \zeta_{p-1}^{\alpha'} \zeta_{p^{e-1}}^{\alpha''}$. Então $t \equiv 1 \pmod{p^{e-1}}$ se, e somente se, $\alpha' = 0$ e $\alpha'' = sp^{e-2}$, $0 \leq s \leq p-1$. Assim, $\chi(t) = \zeta_{p^{e-1}}^{sp^{e-2}} = \zeta_p^s$ e, então,

$$\sum_{\substack{t=1, mdc(t,p)=1 \\ t \equiv 1 \pmod{p^{e-1}}}}^{p^e} \chi(t) = \sum_{s=0}^{p-1} \zeta_p^s = 0. \quad (5.93)$$

Se $p = 2$ e $e \geq 3$, sabemos que para cada t relativamente primo a p , $1 \leq t \leq p^e$, tem-se que $t = (-1)^{\alpha'} 5^{\alpha''}$ em que $\alpha' = 0$ ou 1 , $0 \leq \alpha'' < 2^{e-2}$ e $\chi(t) = (-1)^{\alpha'} \zeta_{2^{e-2}}^{\alpha''}$. Então $t \equiv 1 \pmod{2^{e-1}}$ se, e somente se, $\alpha' = 0$ e $\alpha'' = 0$ ou 2^{e-3} . Daí,

$$\sum_{\substack{t=1, mdc(t,2)=1 \\ t \equiv 1 \pmod{2^{e-1}}}}^{2^e} \chi(t) = 1 + \zeta_{2^{e-2}}^{2^{e-3}} = 1 - 1 = 0. \quad (5.94)$$

Por último, se $p = 2$ e $e = 2$, então $\sum_{\substack{t=1, mdc(t,2)=1 \\ t \equiv 1 \pmod{2^{e-1}}}}^4 \chi(t) = \chi(1) + \chi(3) = 0$. Como $p = 2$ e $e = 1$ não se aplica, então todos os casos possíveis para p e e já foram tratados. Logo, em todos os casos, $|\tau(\chi)|^2 = p^e$. Agora, considere geralmente $f = \prod_{i=1}^r p_i^{e_i}$, em que $p_1, \dots, p_r$ são primos distintos e $e_i \geq 1$. Seja $\chi = \prod_{i=1}^r \chi_i$ a decomposição de χ em caracteres de módulo e condutor $p_i^{e_i}$. Denotando $f_i = f/p_i^{e_i}$, tem-se que $mdc(f_i, f) = 1$ e, pelo lema 5.6.1,

$$|\tau(\chi)|^2 = \overline{\tau(\chi)} \tau(\chi) = \prod_{i=1}^r \overline{\chi_i(f_i)} \prod_{i=1}^r \tau(\chi_i) \prod_{i=1}^r \chi_i(f_i) \prod_{i=1}^r \tau(\chi_i) = \quad (5.95)$$

$$= \prod_{i=1}^r \overline{\chi_i(f_i)} \chi_i(f_i) \prod_{i=1}^r \overline{\tau(\chi_i)} \tau(\chi_i) = 1 \cdot \prod_{i=1}^r \overline{\tau(\chi_i)} \tau(\chi_i) = \prod_{i=1}^r p_i^{e_i} = f, \quad (5.96)$$

como queríamos demonstrar. □

Definição 5.6.2. Se χ é um caractere módulo m com condutor f , a soma de Gauss **primitiva** é

$$\tau(\chi) = \sum_{k=1}^f \chi(k) \zeta_f^k. \quad (5.97)$$

Observação 5.6.1. Note que na definição 5.6.2, acima, a raiz primitiva da unidade não é m -ésima, mas sim f -ésima.

Proposição 5.6.3. Sejam χ um caractere módulo m com condutor f , $\tau(\chi) = \sum_{k=1}^f \chi(k) \zeta_f^{ik}$ a soma de Gauss primitiva de χ e $\tau_i(\chi) = \sum_{k=1}^n \chi(k) \zeta_m^{ik}$ a i -ésima soma de Gauss de χ . Considere ainda m_0 e i_0 números naturais tais que $\zeta_m^i = \zeta_{m_0}^{i_0}$ e $\text{mdc}(m_0, i_0) = 1$. Então a soma primitiva e a soma i -ésima se relacionam pela fórmula

$$\tau_i(\chi) = \frac{\varphi(m)}{\varphi(m_0)} \mu\left(\frac{m_0}{f}\right) \chi\left(\frac{m_0}{f}\right) \overline{\chi}(i_0) \tau(\chi). \quad (5.98)$$

em que μ denota a função de Möbius (veja a equação 1.1). Além disso, $\tau_i(\chi) \neq 0$ se, e somente se, $f \mid m_0$ e m_0/f é livre de quadrados.

Demonstração. Consulte [13], §20.1.IV. □

Conclusão

Inicialmente, estudamos noções gerais de caracteres em um grupo. Na primeira seção, mostramos que um grupo e seu grupo de caracteres associado são isomorfos. Na segunda seção descrevemos os caracteres do grupo $\mathbb{Z}_n^*$. Vimos na seção 3 que é possível estabelecer relações de ortogonalidade entre caracteres ao definir um produto interno entre dois deles. Posteriormente, no quarto capítulo, apresentamos noções básicas sobre caracteres de Dirichlet, provamos um resultado sobre decomposição de caracteres e enunciamos a Fórmula do Condutor-Discriminante. Na quinta seção, apresentamos fórmulas que permitem calcular o condutor de caracteres de Dirichlet. Por fim, na sexta seção, estudamos noções básicas envolvendo soma de Gauss.

Capítulo 6

Anéis de inteiros de corpos de números abelianos

Neste capítulo, que é o principal desta dissertação, temos por objetivo demonstrar o Teorema de Leopoldt-Letl, que fornece o anel de inteiros de qualquer corpo de números abeliano. A seguir, detalharemos o artigo [20] a fim de apresentar uma demonstração completa do mencionado teorema, que é mais conhecido como Teorema de Leopoldt ([19], 1959), sob o enfoque e a teoria desenvolvida por Günter Letl ([20], 1990).

6.1 Classes de ramos

Nesta seção, conceituaremos e demonstraremos alguns resultados técnicos sobre classes de ramos. Tais conjuntos serão utilizados adiante na demonstração do teorema de Leopoldt. Ao longo deste texto, consideremos $\mathbb{K}$ um corpo de números abeliano contido em um corpo ciclotômico $\mathbb{Q}^{(n)} \triangleq \mathbb{Q}(\zeta_n)$, em que ζ_n é uma raiz n -ésima primitiva da unidade e n é o condutor de $\mathbb{K}$ (teorema 3.3.1). Assumamos também as seguintes notações: $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$ e $G^{(n)} = \text{Gal}(\mathbb{Q}^{(n)} : \mathbb{Q})$. Note que G é um subgrupo de $G^{(n)}$.

Assim como fizemos na seção 5.5, considere a relação bijetora entre os caracteres de $\mathbb{Z}_n^* \simeq G^{(n)}$ e os caracteres de Dirichlet módulo n (proposição 5.4.1). Continuaremos denotando por $X^{(n)}$ ao conjunto dos caracteres de Dirichlet módulo n . Evidentemente, os caracteres de Dirichlet de $X^{(n)}$ são aqueles que podem ser definidos módulo n , ou seja, que têm condutor dividindo n , ou seja,

$$X^{(n)} = \{\chi : \mathbb{Z} \longrightarrow \mathbb{C}^\times \text{ caractere de Dirichlet} : f_\chi \mid n\}. \quad (6.1)$$

Devido à relação $\mathbb{Z}_n^* \simeq G^{(n)}$, podemos identificar $\chi(\sigma_k) = \chi(k)$ para todo $k \in \mathbb{Z}_n^*$. Temos:

$$X^{(n)} \simeq \widehat{\mathbb{Z}_n^*} \simeq \mathbb{Z}_n^* \simeq G^{(n)} \simeq \widehat{G^{(n)}}. \quad (6.2)$$

Se a fatoração de primos de n é dada por $n = \prod_{i=1}^r p_i^{e_i}$, $e_i > 0$, a proposição 5.4.6 garante que

$$X^{(n)} = \prod_{i=1}^r X^{(p_i^{e_i})}. \quad (6.3)$$

Além disso, para cada primo p cuja potência na fatoração de n é $e > 0$, vimos na seção 5.2 que

$$X^{(p^e)} = \langle \omega_p \rangle \times \langle \psi_p \rangle. \quad (6.4)$$

Decompondo $\chi \in X^{(p^e)}$ como

$$\chi = \omega_p^a \psi_p^b \quad (6.5)$$

(se $p = 2$ então $0 \leq a \leq 1$ e $0 \leq b < 2^{e-2}$, mas se $p \neq 2$ então $0 \leq a < p-1$ e $0 \leq b < p^{e-1}$), os resultados da seção 5.5 nos afirmam que o condutor de χ é dado por

$$f_\chi = \begin{cases} p^{e-v_p(b)}, & \text{se } b > 0; \\ p, & \text{se } b = 0, a > 0 \text{ e } p \neq 2; \\ 4, & \text{se } b = 0, a > 0 \text{ e } p = 2; \\ 1, & \text{se } b = a = 0 \text{ } (\chi \text{ trivial}). \end{cases} \quad (6.6)$$

Juntando as fórmulas 6.4 e 6.6, temos que $X^{(n)} = \Omega^{(n)} \times \Psi^{(n)}$, em que $\Omega^{(n)} = \prod_{i=1}^r \langle \omega_{p_i} \rangle$ é o grupo de caracteres de Dirichlet de primeiro tipo módulo n e $\Psi^{(n)} = \prod_{i=1}^r \langle \psi_{p_i} \rangle$ é o grupo de caracteres de Dirichlet de segundo tipo módulo n .

Observação 6.1.1. Como G é um subgrupo de $G^{(n)}$, e este último está associado a $X^{(n)}$, então existe um subgrupo $X \simeq \widehat{G}$ de $X^{(n)}$ biunivocamente associado a G . Devido ao teorema 1.1.1, há também uma correspondência biunívoca entre os subcorpos de $\mathbb{Q}^{(n)}$ e os subgrupos de $G^{(n)}$, pois $G^{(n)}$ é abeliano. Por transitividade, cada subcorpo de $\mathbb{Q}^{(n)}$ está associado de maneira biunívoca a um subgrupo de $X^{(n)}$.

Proposição 6.1.1. O condutor de $\mathbb{K}$ é igual a $\text{mmc}\{f_\chi : \chi \in X\}$.

Demonstração. Sejam n o condutor de $\mathbb{K}$ e $n' = \text{mmc}\{f_\chi : \chi \in X\}$. Considere G o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$ e $G^{(n)}$ o grupo de Galois de $\mathbb{Q}^{(n)}$. Então existe $X < X^{(n)}$ tal que $X \simeq \widehat{G}$, ou seja, tal que X está associado a G e a $\mathbb{K}$ (observação 6.1.1). Se $\chi \in X$ então $f_\chi \mid n$, pois $X \subset X^{(n)}$. Logo, $n' \mid n$ e, então, $X^{(n')} \subset X^{(n)}$. Como $f_\chi \mid n'$ para todo $\chi \in X$ (por definição), segue que

$X \subset X^{(n')}$. Assim, temos a seguinte cadeia: $X \subset X^{(n')} \subset X^{(n)}$. Pela observação 6.1.1, essa relação implica que $\mathbb{K} \subset \mathbb{Q}^{(n')} \subset \mathbb{Q}^{(n)}$, donde segue que $n = n'$, pois n é o condutor de $\mathbb{K}$. Isso mostra que $n = mmc\{f_\chi : \chi \in X\}$. $\square$

Definição 6.1.1. Para cada $n \in \mathbb{N}$, definimos o conjunto

$$\mathcal{D}(n) = \{d \in \mathbb{N} : P_n \mid d, d \mid n \text{ e } d \not\equiv 2 \pmod{4}\} \quad (6.7)$$

em que P_n é o produto dos primos distintos de n que são diferentes de 2.

Na definição do conjunto $\mathcal{D}(n)$, note que um elemento d deste conjunto deve satisfazer à condição $d \not\equiv 2 \pmod{4}$. Isto é equivalente a dizer que d não é da forma $2m$, em que m é um número ímpar. Note que se n não é da forma $2m$, com m ímpar, então $\mathcal{D}(n) \neq \emptyset$, pois $n \in \mathcal{D}(n)$.

Definição 6.1.2. Considere a função aritmética $q : \mathbb{N} \longrightarrow \mathbb{N}$ que a cada número natural $n = \prod_{i=1}^r p_i^{e_i}$ (sendo p_i primos distintos e $e_i > 0$) associa um outro natural $n' = \prod_{i=1}^r p_i^{f_i}$ tal que $f_j = e_j$ se $e_j \geq 2$ e $f_j = 0$ se $e_j = 1$, ou seja, definida por

$$q(n) = \prod_{\substack{i=1 \\ v_{p_i}(n) \geq 2}}^r p_i^{v_{p_i}(n)}. \quad (6.8)$$

Essa função é chamada de **função parte potente** e a imagem $q(n)$ é chamada de **parte potente de n** .

Proposição 6.1.2. A função parte potente q é uma função aritmética multiplicativa, isto é, $q(mn) = q(m)q(n)$ se $\text{mdc}(m, n) = 1$.

Demonstração. Considere p_1 e p_2 dois primos distintos. Assim, $q(p_1 p_2) = 1 = q(p_1)q(p_2)$. Se $e \geq 2$, $q(p_1^e p_2) = p_1^e = q(p_1^e)q(p_2)$ e $q(p_1 p_2^e) = p_2^e = q(p_1)q(p_2^e)$. Por fim, se $e \geq 2$ e $f \geq 2$, $q(p_1^e p_2^f) = p_1^e p_2^f = q(p_1^e)q(p_2^f)$. Por indução sobre o número de primos nas fatorações de m e de n , verifica-se facilmente que $q(mn) = q(m)q(n)$ se $\text{mdc}(m, n) = 1$. $\square$

Lema 6.1.1. Seja $B(n)$ o conjunto das possíveis partes potentes dos condutores de todos os χ em $X^{(n)}$. Assim, a restrição da função parte potente $q : \mathcal{D}(n) \longrightarrow B(n)$ é bijetora. Em outras palavras, existe uma correspondência biunívoca entre os elementos de $\mathcal{D}(n)$ e as possíveis partes potentes dos condutores dos $\chi \in X^{(n)}$.

Demonstração. Suponha que a fatora  o de n seja dada por $n = 2^{e_0} p_1^{e_1} \dots p_m^{e_m}$, em que p_i s  o primos   mpares distintos, $e_i \geq 1$ e $e_0 \geq 0$. Por defini  o,

$$\mathcal{D}(n) = \left\{ 2^x \prod_{i=1}^m p_i^{x_i} : 1 \leq x_i \leq e_i, 0 \leq x \leq e_0, x \neq 1 \right\}. \quad (6.9)$$

Portanto, $\#(\mathcal{D}(n)) = e_0 e_1 \dots e_m$. Al  m disso,

$$A(n) \triangleq \left\{ 2^x \prod_{i=1}^m p_i^{x_i} : 0 \leq x \leq e_0, 0 \leq x_i \leq e_i, x \neq 1, x_i \neq i \right\} = \{q(d) : d \in \mathcal{D}(n)\}. \quad (6.10)$$

Agora, para todo $\chi \in X^{(n)}$, tem-se que $f_\chi \mid n$. Como n  o existe condutor da forma $2m$, com m   mpar, ent  o $f_\chi = 2^x p_1^{x_1} \dots p_m^{x_m}$, em que $0 \leq x \leq e_0$, $x \neq 1$ e $0 \leq x_i \leq e_i$. Portanto, por um lado, $B(n) = \{q(f_\chi) : \chi \in X^{(n)}\} \subset A(n)$. Por outro lado, variando a e b na equa  o 6.5 e utilizando a f  rmula 6.6, v  -se que $A(n) \subset B(n)$. Portanto, $A(n) = B(n)$. Assim, a fun  o $q : \mathcal{D}(n) \longrightarrow A(n)$ tal que $q(2^x \prod_{i=1}^m p_i^{x_i}) = 2^x \prod_{i=1}^m p_i^{y_i}$, em que $y_i = 0$ se $x_i = 1$ e $y_i = x_i$ se $x_i \geq 2$,    a fun  o parte potente restrita a $\mathcal{D}(n)$. Claramente, por defini  o de $\mathcal{D}(n)$ verifica-se que q    sobrejetora. Por contagem dos elementos, como $\#(A(n)) = e_0 e_1 \dots e_m = \#(\mathcal{D}(n))$, ent  o a aplica  o    bijetora. $\square$

Defini  o 6.1.3. *Seja X um grupo finito de caracteres de Dirichlet, $n = mmc\{f_\chi : \chi \in X\}$ e $d \in \mathcal{D}(n)$. Chama-se **classe de ramo** **d** em X ao conjunto*

$$\Phi_d = \{\chi \in X : q(f_\chi) = q(d)\}. \quad (6.11)$$

Proposi  o 6.1.3. *Nas condi  o  es da defini  o anterior,*

$$X = \bigcup_{d \in \mathcal{D}(n)} \Phi_d \quad (6.12)$$

isto   , as classes de ramos de X particionam X em subconjuntos disjuntos.

Demonstr  o. Seja $\chi \in X$. Como $X \subset X^{(n)}$ ent  o existe $d \in \mathcal{D}(n)$ tal que $q(d) = q(f_\chi)$ (lema 6.1.1). Portanto, $\chi \in \Phi_d$. Logo, $X \subset \bigcup_{d \in \mathcal{D}(n)} \Phi_d$. A igualdade vem do fato   bvio de que $\Phi_d \subset X$. Falta ver que a uni  o    disjunta. Suponha que $\Phi_{d_1} \neq \emptyset$ e $\Phi_{d_2} \neq \emptyset$ s  o tais que existe $\chi \in \Phi_{d_1} \cap \Phi_{d_2}$. Ent  o $q(d_1) = q(f_\chi) = q(d_2)$. Como $d_1, d_2 \in \mathcal{D}(n)$ ent  o os primos da fatora  o de n aparecem na fatora  o de d_1 e de d_2 . Assim, se $n = \prod_{i=1}^r p_i^{\alpha_i}$ ($\alpha_i \geq 1$, p_i primos distintos) ent  o $d_1 = \prod_{i=1}^r p_i^{e_i}$ e $d_2 = \prod_{i=1}^r p_i^{f_i}$, em que $1 \leq e_i, f_i \leq \alpha_i$ se $p_i \neq 2$. Se $p_i = 2$ ent  o e_i ou f_i podem ser zero e n  o podem ser iguais a um. Em todo caso, como $q(d_1) = q(d_2)$ ent  o $e_i = f_i$ se $e_i \geq 2$. Caso p_i seja primo   mpar e $e_i = 1$ ent  o $f_i = 1$ (sen  o $f_i \geq 2$ acarretaria diferen  a entre $q(d_1)$ e $q(d_2)$). Se $p_i = 2$ e $e_i = 0$ ent  o

$f_i = 0$ ($f_i = 1$ não pode ocorrer por definição de $\mathcal{D}(n)$ e $f_i \geq 2$ acarretaria diferença entre $q(d_1)$ e $q(d_2)$). Analogamente, se $p_i = 2$ e $f_i = 0$ então $e_i = 0$. Em todo caso, portanto, $e_i = f_i$ para todo i . Logo, $d_1 = d_2$. Assim, a união $\bigcup_{d \in \mathcal{D}(n)} \Phi_d$ é comprovadamente disjunta. $\square$

No que segue, se $d \in \mathbb{N}$ é divisível por um número primo p então $q(d)|_p$ denotará o valor p^e , em que $e = v_p(q(d))$. Pelo fato de q ser uma função aritmética multiplicativa (proposição 6.1.2), concluímos que

$$q(d) = q\left(\prod_{p|n} p^e\right) = \prod_{p|n} q(p^e) = \prod_{p|n} q(d)|_p. \quad (6.13)$$

Seja $\chi = \prod_{p|n} \chi_p$ a fatoração de $\chi \in X^{(n)}$ em caracteres de $X^{(p^e)}$. Logo, $f_\chi = \prod_{p|n} f_{\chi_p}$ (proposição 5.4.6). Então

$$q(f_\chi) = q\left(\prod_{p|n} f_{\chi_p}\right) = \prod_{p|n} q(f_{\chi_p}). \quad (6.14)$$

Das fórmulas 6.13 e 6.14, concluímos que

$$q(d) = q(f_\chi) \iff q(d)|_p = q(f_{\chi_p}), \quad \forall p | n \text{ (} p \text{ primo)}. \quad (6.15)$$

A seguir, sejam X um grupo de caracteres de Dirichlet e $n = \text{mmc}\{f_\chi : \chi \in X\}$.

Lema 6.1.2. *Se p é um número primo divisor de n então a projeção $\pi : X \longrightarrow \langle \psi_p \rangle$ é sobrejetora.*

Demonstração. Mostremos que existe $\chi_0 \in X$ tal que $\pi(\chi_0) = \psi_p$. Seja $e = v_p(n)$. Assim, $p^e | n$ e p^{e+1} não divide n . Como $n = \text{mmc}\{f_\chi : \chi \in X\}$, existe $\chi \in X$ tal que $f_\chi = p^e q$, com $\text{mdc}(q, p) = 1$. Logo, $\chi = \omega_p^a \psi_p^b \prod_{p_i \neq p} \omega_{p_i}^{e_i} \psi_{p_i}^{f_i}$, em que $v_p(b) = 0$, pois $e = e - v_p(b)$ (equação 6.6). Logo, p não divide b e, portanto, $\text{mdc}(b, p) = 1$. Como a ordem de $H = \langle \psi_p \rangle$ é p^{e-1} se $p \neq 2$ e é p^{e-2} se $p = 2$ então $\text{mdc}(b, o(H)) = 1$. Portanto, $\langle \psi_p \rangle = \langle \psi_p^b \rangle$. Por isso, existe $\alpha \in \mathbb{Z}$ tal que $\psi_p = \psi_p^{\alpha b}$. Portanto, tome $\chi_0 = \chi^\alpha$. Neste caso, $\chi_0 = \omega_p^{a\alpha} \psi_p^{\alpha b} \prod_{p_i \neq p} \omega_{p_i}^{\alpha e_i} \psi_{p_i}^{\alpha f_i}$. Logo, $\pi(\chi_0) = \psi_p$. Então, para cada $\psi_p^r \in \langle \psi_p \rangle$, existe $\chi_r = \chi_0^r \in X$ tal que $\pi(\chi_r) = \psi_p^r$. Isso comprova que a projeção $\pi : X \longrightarrow \langle \psi_p \rangle$ é sobrejetora. $\square$

Lema 6.1.3. *Se $n \equiv 4 \pmod{8}$ (ou seja, $n = 4x$, em que x é ímpar) então a projeção $\pi : X \longrightarrow \langle \omega_2 \rangle$ é sobrejetora.*

Demonstração. Note que $\langle \omega_2 \rangle = \{1, \omega_2\}$. Como $\pi(1) = 1$ e $1 \in X$, falta só mostrar existe $\chi \in X$ tal que $\pi(\chi) = \omega_2$. Como $n = 4x$, com x ímpar, e como $n = \text{mmc}\{f_\chi : \chi \in X\}$, existe $\chi \in X$ tal que $4 | f_\chi$ e 2^y não divide f_χ se $y > 2$. Então, da equação 6.6, segue que $a = 1$ e $b = 0$. De fato, se $b \neq 0$

então $f_{\chi_2} = 2^{e-v_2(b)}$, donde segue que $2^{e-2} \mid b$, o que é um absurdo, pois $0 < b < 2^{e-2}$. Portanto, $b = 0$ e $a = 1$. Logo, $\chi = \omega_2 \prod_{p_i \neq 2} \omega_{p_i}^{e_i} \psi_{p_i}^{f_i}$. Daí, $\pi(\chi) = \omega_2$. $\square$

A proposição a seguir nos mostra quando uma classe de ramo Φ_d é não vazia.

Proposição 6.1.4. *Mantidas as notações anteriores para X e n , tem-se que:*

- (a) $\Phi_n \neq \emptyset$;
- (b) $d \not\equiv 4 \pmod{8} \implies \Phi_d \neq \emptyset$;
- (c) Se $d \equiv 4 \pmod{8}$ então $\Phi_d \neq \emptyset \iff \exists \chi_0 \in X$ tal que $q(f_{\chi_0}) = 4$.

Demonstração. (a) Se n não tem parte potente então $q(n) = 1$ e $\chi \equiv 1$ satisfaz $q(f_\chi) = 1 = q(n)$. Agora, suponha que n é ímpar. Então podemos fatorar esse número natural como $n = \prod_i p_i^{\alpha_i} \prod_j q_j$, em que p_i e q_j são primos e $\alpha_i \geq 2$. Assim, $q(n) = \prod_i p_i^{\alpha_i}$. O lema 6.1.2 nos diz que para cada $p_i^{\alpha_i}$, a projeção $\pi : X \longrightarrow \prod_{p_i} \langle \psi_{p_i} \rangle$ é sobrejetora, já que os componentes do produto são dois a dois relativamente primos. Por isso, existe $\chi \in X$ tal que $\pi(\chi) = \prod_{p_i} \psi_{p_i}$. Assim, pondo $b = 1$ na equação 6.6 para cada primo p_i tem-se que $f_{\chi_{p_i}} = p_i^{\alpha_i}$. Portanto, $q(f_{\chi_{p_i}}) = q(n)|_{p_i}$, para todo p_i que divide $q(n)$. Devido à equivalência 6.15, segue que $q(f_\chi) = q(n)$, ou seja, que $\chi \in \Phi_n$. Agora, suponhamos que $n = 4x$, com x ímpar. Como fizemos anteriormente, podemos fatorar n como $n = 2^2 \prod_i p_i^{\alpha_i} \prod_j q_j$, em que p_i e q_j são primos diferentes de 2 e $\alpha_i \geq 2$. Assim, $q(n) = 2^2 \prod_i p_i^{\alpha_i}$. Acima, vimos que $q(f_{\chi_{p_i}}) = q(n)|_{p_i}$, para todo p_i diferente de 2 que divide $q(n)$. Falta analisar o fator 2^2 . Pelos lemas 6.1.2 e 6.1.3, a projeção $\pi : X \longrightarrow \langle \omega_2 \rangle \prod_{p_i} \langle \psi_{p_i} \rangle$ é sobrejetora, já que os componentes do produto são dois a dois relativamente primos. Logo, existe $\chi \in X$ tal que $\pi(\chi) = \omega_2 \prod_{p_i} \psi_{p_i}$ (note que não aparece o termo ψ_2). Assim, pela igualdade 6.6, $f_{\chi_2} = 4$ e, portanto, $q(f_{\chi_2}) = 4 = q(n)|_2$. Portanto, $q(f_\chi) = q(n)$, donde segue que $\chi \in \Phi_n$. No último caso, suponha que $n = 8x$ (ou seja, $n \not\equiv 4 \pmod{8}$). Nesse caso, supondo $n = 2^\alpha \prod_i p_i^{\alpha_i} \prod_j q_j$, em que p_i e q_j são primos diferentes de 2, $\alpha_i \geq 2$ e $\alpha \geq 3$, tem-se que $q(n) = 2^\alpha \prod_i p_i^{\alpha_i}$. Pelo lema 6.1.2, a projeção $\pi : X \longrightarrow \langle \psi_2 \rangle \prod_{p_i} \langle \psi_{p_i} \rangle$ é sobrejetora, pois os componentes do produto são dois a dois relativamente primos. Por isso, existe $\chi \in X$ tal que $\pi(\chi) = \psi_2 \prod_{p_i} \psi_{p_i}$. Tomando $b = 1$ na equação 6.6 para o primo 2, tem-se que $q(f_{\chi_2}) = 2^\alpha$. Assim, $q(f_{\chi_2}) = q(n)|_2$. Como $q(f_{\chi_{p_i}}) = q(n)|_{p_i}$, para todo p_i diferente de 2 que divide $q(n)$ (visto acima), inferimos da equivalência 6.15 que $q(f_\chi) = q(n)$. Portanto, $\chi \in \Phi_n$. (b) Suponha que d seja um elemento de $\mathcal{D}(n)$ tal que $d \not\equiv 4 \pmod{8}$. Assim, d é ímpar ou $d = 8x$, em que x é inteiro. Consideremos a fatoração de d em primos dada por $d = \prod_i p_i^{\alpha_i} \prod_j q_j$, em que p_i e q_j são primos distintos e $\alpha_i \geq 2$ (pelas restrições impostas, permite-se que algum p_i seja 2, mas não se permite que algum q_i seja 2). Portanto, $q(d) = \prod_i p_i^{\alpha_i}$. Como $\pi : X \longrightarrow \prod_{p_i} \langle \psi_{p_i} \rangle$ é uma projeção sobrejetora,

então existe $\chi \in X$ tal que $\pi(\chi) = \prod_{p_i} \psi_{p_i}$. Para cada p_i , a fórmula 6.6 acarreta $q(f_{\chi_{p_i}}) = p_i^{\alpha_i}$. Por raciocínio análogo ao já feito anteriormente, tem-se que $q(f_\chi) = q(d)$, donde segue que $\chi \in \Phi_d$. (c) Suponha que $d = 4x$, em que x é ímpar. Podemos fatorar d como $d = 2^2 \prod_i p_i^{\alpha_i} \prod_j q_j$, em que p_i e q_j são primos ímpares e $\alpha_i \geq 2$. Assim, $q(d) = 4 \prod_i p_i^{\alpha_i}$. A projeção $\pi : X \longrightarrow \langle \omega_2 \rangle \prod_{p_i} \langle \psi_{p_i} \rangle$ é sobrejetora se, e somente se, $\pi_2 : X \longrightarrow \langle \omega_2 \rangle$ é sobrejetora, já que $o(\langle \omega_2 \rangle) = 2$ é relativamente prima com $o(\langle \psi_{p_i} \rangle)$. Isso ocorre se, e somente se, existe $\chi_0 \in X$ tal que $\pi_2(\chi_0) = \omega_2$, ou seja, se 4 é a potência de 2 na fatoração de f_{χ_0} . Portanto, $q(f_{(\chi_0)_2}) = 4$ se, e somente se, $\pi : X \longrightarrow \langle \omega_2 \rangle \prod_{p_i} \langle \psi_{p_i} \rangle$ é sobrejetora. Neste caso, existe $\chi \in X$ tal que $\pi(\chi) = \omega_2 \prod_{p_i} \psi_{p_i}$ e, portanto, $q(f_\chi) = 4p_i^{\alpha_i} = q(d)$, donde segue que $\chi \in \Phi_d$. $\square$

Proposição 6.1.5. *Considere as notações anteriores para X e n e a projeção $\pi : X \longrightarrow \Psi^{(n)} \times Z$, em que $Z = \langle \omega_2 \rangle$ se $n \equiv 4 \pmod{8}$ ou $Z = \langle 1 \rangle$ se $n \not\equiv 4 \pmod{8}$. Então π é sobrejetora e $\langle \Phi_n \rangle = X$.*

Demonstração. O fato da projeção π ser sobrejetora segue dos lemas 6.1.2 e 6.1.3, já que $\Psi^{(n)} \times Z$ é um produto de grupos cíclicos com ordens relativamente primas entre si duas a duas. Por definição, $\Phi_n \subset X$. Assim, $\langle \Phi_n \rangle \subset X$. Mostremos a outra inclusão. Seja $\chi \in X$. Faremos a demonstração em quatro passos:

1º passo: Mostremos que $\pi(\langle \Phi_n \rangle) = \Psi^{(n)} \times Z$. Sabemos que existe $\chi_0 \in \Phi_n$ tal que $\pi(\chi_0) = \omega \prod_p \psi_p$, em que ω é o gerador de Z . Denotemos $\psi = \pi(\chi_0)$. Como $\Psi^{(n)} \times Z$ é um produto de grupos cíclicos com ordens relativamente primas entre si duas a duas, então $\Psi^{(n)} \times Z$ é cíclico e tem gerador ψ . Assim, dado $\psi_1 = \psi^m \in \Psi^{(n)} \times Z$, garante-se a existência de $\chi_0^m \in \langle \Phi_n \rangle$ tal que

$$\pi(\chi_0^m) = \pi(\chi_0)^m = \psi^m = \psi_1. \quad (6.16)$$

Portanto, $\Psi^{(n)} \times Z \subset \pi(\langle \Phi_n \rangle)$. Como $\langle \Phi_n \rangle \subset X$ então $\pi(\langle \Phi_n \rangle) \subset \Psi^{(n)} \times Z$ e, daí, $\pi(\langle \Phi_n \rangle) = \Psi^{(n)} \times Z$.

2º passo: Existe $\chi' \in \langle \Phi_n \rangle$ tal que $\pi(\chi\chi')$ gera $\Psi^{(n)} \times Z$.

De fato, denote $\psi' = \pi(\chi) \in \Psi^{(n)} \times Z$. Pelo 1º passo, existe $\chi_1 \in \langle \Phi_n \rangle$ tal que $\pi(\chi_1) = \psi'$. Assim, $\pi(\chi) = \pi(\chi_1)$ implica que $\pi(\chi\chi_1^{-1}) = 1$. Seja $\chi' = \chi_1^{-1}\chi \in \langle \Phi_n \rangle$. Então

$$\pi(\chi\chi') = \pi(\chi\chi_1^{-1}\chi_0) = \pi(\chi\chi_1^{-1})\pi(\chi_0) = \pi(\chi_0) = \psi. \quad (6.17)$$

Portanto, $\pi(\chi\chi')$ gera $\Psi^{(n)} \times Z$.

3º passo: $\chi\chi' \in \Phi_n$.

Com efeito, como $\pi(\chi\chi') = \psi = \omega \prod_p \psi_p$, então o mesmo raciocínio utilizado na demonstração do item (a) da proposição 6.1.4 mostra que $\chi\chi' \in \Phi_n$.

4º passo: Finalmente, verifiquemos que $X \subset \langle \Phi_n \rangle$.

Se $\chi' \in \langle \Phi_n \rangle$ então $\chi'^{-1} \in \langle \Phi_n \rangle$. Assim, $\chi\chi' = \chi'' \in \Phi_n$, donde segue que $\chi = \chi''(\chi')^{-1} \in \langle \Phi_n \rangle$. Portanto, $\chi \in \langle \Phi_n \rangle$, comprovando que $X \subset \langle \Phi_n \rangle$. Isso conclui a demonstração. $\square$

As classes de ramos que são não vazias apresentam propriedades relatadas na proposição seguinte.

Proposição 6.1.6. *Mantendo as notações anteriores, se $d \in \mathcal{D}(n)$ e se $\Phi_d \neq \emptyset$ então*

$$\langle \Phi_d \rangle = X \cap X^{(d)} = \{\chi \in X : f_\chi \mid d\} \quad (6.18)$$

e a projeção

$$\pi : \langle \Phi_d \rangle \longrightarrow \Psi^{(d)} \times Z \quad (6.19)$$

é sobrejetora, em que $Z = \langle \omega_2 \rangle$ se $d \equiv 4 \pmod{8}$ ou $Z = \langle 1 \rangle$ se $d \not\equiv 4 \pmod{8}$.

Demonstração. Seja $d' = \text{mmc}\{f_\chi : \chi \in X \cap X^{(d)}\}$. Tomando $n = d'$ nas proposições anteriores, sabemos que a projeção $\pi : X \cap X^{(d)} \longrightarrow \Psi^{(d')} \times Z$ é sobrejetora, em que $Z = \langle \omega_2 \rangle$ se $d' \equiv 4 \pmod{8}$ ou $Z = \langle 1 \rangle$ se $d' \not\equiv 4 \pmod{8}$. Como $d' = \text{mmc}\{f_\chi : \chi \in X \text{ e } f_\chi \mid d\}$ então $d' \mid d$. Por definição, $\Phi_d = \{\chi \in X : q(d) = q(f_\chi)\} \neq \emptyset$. Considere

$$A_d = \{\chi \in X : q(d) = q(f_\chi) \text{ e } f_\chi \mid d\}. \quad (6.20)$$

Por um lado, é claro que $A_d \subset \Phi_d$. Por outro lado, se $\chi \in \Phi_d$ então $q(d) = q(f_\chi)$. Como $f_\chi \not\equiv 2 \pmod{4}$ então f_χ é ímpar ou $f_\chi = 4x$, com x ímpar. Podemos supor, sem perda de generalidade, que $f_\chi = 4 \prod_i p_i^{e_i} \prod_j q_j$, em que p_i e q_j são primos ímpares distintos e $e_i \geq 2$, donde segue que $q(f_\chi) = 4 \prod_i p_i^{e_i}$. Pelo fato de esse valor coincidir com $q(d)$, tem-se que $d = 4 \prod_i p_i^{e_i} \prod_j r_j$, com r_j primos ímpares distintos de p_i e distintos entre si. Como r_i e p_i formam o conjunto de todos os primos ímpares distintos divisores de n (pois $d \in \mathcal{D}(n)$) e como $q_j \mid n$, segue que os todos os fatores q_j são particulares dos r_i . Logo, $f_\chi \mid d$, donde segue que $\Phi_d \subset A_d$. Portanto, $\Phi_d = A_d$. Por isso,

$$\Phi_d = \{\chi \in X : q(d) = q(f_\chi) \text{ e } f_\chi \mid d\} = \{\chi \in X \cap X^{(d)} : q(d) = q(f_\chi)\}. \quad (6.21)$$

A seguir, mostremos que $q(d) \mid d'$:

$$\Phi_d \neq \emptyset \implies \exists \chi \in \Phi_d \implies q(f_\chi) = q(d) \text{ e } f_\chi \mid d \implies q(d) \mid f_\chi \text{ e } f_\chi \mid d \implies q(d) \mid f_\chi \text{ e } \chi \in X \cap X^{(d)} \implies$$

$$\implies q(d) \mid f_\chi \text{ e } f_\chi \mid \text{mmc}\{f_\chi : \chi \in X \cap X^{(d)}\} \implies q(d) \mid f_\chi \text{ e } f_\chi \mid d' \implies q(d) \mid d'. \quad (6.22)$$

Como $q(d) \mid d'$ e $d' \mid d$ então $d/d' = \prod_i q_i$, em que q_i são primos distintos (não relacionados com os q_i anteriores). Note que se houvesse um primo divisor de d cujo expoente m na fatoração de d/d'

fosse maior do que 1, então teríamos que q_i^m deveria dividir $q(d)$, um divisor de d' , donde seguiria que q_i não pode aparecer na fatoração de d/d' . Portanto, $q(d) = q(d')$. Observe que d e d' só diferem possivelmente em primos ímpares divisores de n que aparecem com expoente 1 na fatoração de d e que não aparecem na fatoração de d' . Logo, $\Psi^{(d)} = \Psi^{(d')} \times \prod_i \langle \Psi_{q_i} \rangle$, em que os q_i são primos divisores de d com expoente $e = 1$ na sua fatoração. Logo, $o(\langle \Psi_{q_i} \rangle) = q_i^{e-1} = 1$, ou seja, $\Psi^{(d)} = \Psi^{(d')} \times \prod_i 1$. Agora, observe que $d \equiv 4 \pmod{8}$ se, e somente se, $d' \equiv 4 \pmod{8}$. De fato,

$$\begin{aligned} d \equiv 4 \pmod{8} &\iff d = 4x, \text{ mdc}(2, x) = 1 \iff 4 \mid q(d) = q(d') \text{ e } 8 \nmid q(d) = q(d') \iff \\ &\iff d' = 4y, \text{ mdc}(2, y) = 1 \iff d' \equiv 4 \pmod{8} \end{aligned} \quad (6.23)$$

Portanto, devido à afirmação do primeiro parágrafo desta demonstração, concluímos que $\pi : \langle \Phi_d \rangle \longrightarrow \Psi^{(d)} \times Z$ é uma projeção sobrejetora, em que $Z = \langle \omega_2 \rangle$ se $d \equiv 4 \pmod{8}$ ou $Z = \langle 1 \rangle$ se $d \not\equiv 4 \pmod{8}$. Além disso, sendo $\widetilde{\Phi}_{d'} = \{\chi \in X \cap X^{(d)} : q(f_\chi) = q(d')\}$, a proposição 6.1.5 nos informa que $\langle \widetilde{\Phi}_{d'} \rangle = X \cap X^{(d)}$. Porém, a fórmula 6.21 nos garante que

$$\widetilde{\Phi}_{d'} = \{\chi \in X \cap X^{(d)} : q(f_\chi) = q(d') = q(d)\} = \Phi_d. \quad (6.24)$$

Portanto, $\langle \Phi_d \rangle = \langle \widetilde{\Phi}_{d'} \rangle = X \cap X^{(d)}$. □

6.2 Caracteres coordenados de Leopoldt

Estudaremos agora idempotentes ortogonais em anéis de grupo e caracteres coordenados de Leopoldt. Esses elementos serão úteis nas justificativas da seção seguinte, em que demonstraremos o Teorema de Leopoldt. Os caracteres coordenados de Leopoldt foram introduzidos por esse matemático em [19] e a maioria das demonstrações aqui feitas são encontradas de maneira sintética e não tão detalhada no primeiro capítulo do referido artigo.

Ao longo desta seção, considere $\mathbb{K}$ um corpo de números abeliano com anel de inteiros $\mathcal{O}_{\mathbb{K}}$, denote por $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$ o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$ e por X o grupo de caracteres de Dirichlet associado a $\mathbb{K}$. Devemos lembrar que X pode ser identificado com o grupo de caracteres de G .

Dado $\chi \in X$, definimos o elemento ϵ_χ do anel de grupo $\mathbb{C}[G]$ pela expressão

$$\epsilon_\chi \triangleq \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma. \quad (6.25)$$

Proposição 6.2.1. *São válidas as propriedades:*

- (a) $\sum_{\chi \in X} \epsilon_\chi = 1$ (identidade de $\mathbb{C}[G]$);
- (b) Se $\chi \neq \psi$ são elementos de X , então $\epsilon_\chi \epsilon_\psi = 0$;
- (c) Se $\chi \in X$, então $\epsilon_\chi^2 = \epsilon_\chi$.

Demonstração. O corolário 5.3.1 garante que

$$\sum_{i=0}^{n-1} \chi_i(\sigma) = \begin{cases} n & \text{se } \sigma = id \\ 0 & \text{se } \sigma \neq id \end{cases} \quad (6.26)$$

onde $n = [\mathbb{K} : \mathbb{Q}]$. Logo, denotando por $id = 1.id$ a unidade de $\mathbb{C}[G]$,

$$\sum_{\chi \in X} \epsilon_\chi = \sum_{i=0}^{n-1} \frac{1}{n} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma = \sum_{\sigma \in G} \left(\sum_{i=0}^{n-1} \frac{\overline{\chi(\sigma)}}{n} \right) \sigma = \frac{n}{n} id + \sum_{id \neq \sigma \in G} 0 \cdot \sigma = id \quad (6.27)$$

o que completa a prova do item (a). Para provar os itens (b) e (c), observe que

$$\epsilon_\chi \epsilon_\psi = \frac{1}{[\mathbb{K} : \mathbb{Q}]^2} \left(\sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma \right) \left(\sum_{\sigma \in G} \overline{\psi(\sigma)} \sigma \right) = \frac{1}{[\mathbb{K} : \mathbb{Q}]^2} \sum_{\sigma \in G} \left(\sum_{\sigma_1 \sigma_2 = \sigma} \overline{\chi(\sigma_1) \psi(\sigma_2)} \right) \sigma. \quad (6.28)$$

Se $\sigma \in G$ for fixado, então $\sigma_2 = \sigma \sigma_1$ percorrerá todos os elementos de G fazendo σ_1 assumir cada elemento de G . Além disso, como $\overline{\chi(\sigma_1)} = \chi(\sigma_1^{-1})$ então

$$\begin{aligned} \sum_{\sigma_1 \sigma_2 = \sigma} \overline{\chi(\sigma_1) \psi(\sigma_2)} &= \sum_{\sigma_1 \sigma_2 = \sigma} \chi(\sigma_1^{-1}) \overline{\psi(\sigma_2)} = \sum_{\sigma_1^{-1} \sigma_2 = \sigma} \chi(\sigma_1) \overline{\psi(\sigma_2)} = \sum_{\sigma_2 = \sigma \sigma_1} \chi(\sigma_1) \overline{\psi(\sigma_2)} = \\ &= \sum_{\sigma_1 \in G} \chi(\sigma_1) \overline{\psi(\sigma_1 \sigma)} = \overline{\psi(\sigma)} \sum_{\sigma_1 \in G} \chi(\sigma_1) \overline{\psi(\sigma_1)}. \end{aligned} \quad (6.29)$$

Do corolário 5.3.1 é possível afirmar que

$$\sum_{\sigma_1 \in G} \chi(\sigma_1) \overline{\psi(\sigma_1)} = \begin{cases} 0 & \text{se } \chi \neq \psi \\ n & \text{se } \chi = \psi \end{cases} \quad (6.30)$$

donde segue finalmente que

$$\sum_{\sigma_1 \sigma_2 = \sigma} \overline{\chi(\sigma_1) \psi(\sigma_2)} = \begin{cases} 0 & \text{se } \chi \neq \psi \\ \overline{\psi(\sigma)} n & \text{se } \chi = \psi \end{cases} \quad (6.31)$$

Utilizando a igualdade acima e voltando à equação 6.28, concluímos que se $\chi \neq \psi$ então $\epsilon_\chi \epsilon_\psi = 0$.

No caso em que $\chi = \psi$, tem-se

$$\epsilon_\chi^2 = \epsilon_\chi \epsilon_\psi = \frac{n}{n^2} \sum_{\sigma \in G} \overline{\psi(\sigma)} \sigma = \frac{1}{n} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma = \epsilon_\chi. \quad (6.32)$$

Isso demonstra os itens (b) e (c). □

Devido a isso, os elementos ϵ_χ são chamados de **idempotentes ortogonais** de $\mathbb{C}[G]$.

Definição 6.2.1 (Caractere coordenado de Leopoldt). *Sejam $a \in \mathbb{K}$ e $\chi \in X$. Definimos o **caractere coordenado de Leopoldt** pela expressão*

$$y_{\mathbb{K}}(\chi|a) \triangleq \frac{1}{\tau(\chi)} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma(a) \quad (6.33)$$

em que $\tau(\chi) = \sum_{k=1}^{f_\chi} \chi(k) \zeta_{f_\chi}^k$ é a soma primitiva de Gauss de χ e $\zeta_{f_\chi} = e^{\frac{2\pi i}{f_\chi}}$ é uma raiz f_χ -ésima primitiva da unidade.

Para qualquer $\chi \in X$, defina $\mathbb{Q}(\chi) \triangleq \mathbb{Q}(\{\chi(\sigma) : \sigma \in G\})$ o menor corpo que contém $\mathbb{Q}$ e as imagens de χ .

Proposição 6.2.2. *Seja $\chi \in X$. Então $\mathbb{Q}(\chi) = \mathbb{Q}(\zeta_{ord(\chi)})$.*

Demonstração. Por um lado, para qualquer $\sigma \in G$, $\chi(\sigma)^{ord(\chi)} = \chi^{ord(\chi)}(\sigma) = 1$. Assim, $\mathbb{Q}(\chi) \subset \mathbb{Q}(\zeta_{ord(\chi)})$. Por outro lado, sabemos que $\chi(G) = \{\chi(\sigma) : \sigma \in G\}$ é um grupo cíclico, pois é um subgrupo do grupo (cíclico) multiplicativo das raízes $o(G)$ -ésimas da unidade. Portanto, existe $\rho \in G$ tal que $\chi(G) = \langle \chi(\rho) \rangle$. Afirmamos que $ord(\chi) = ord(\chi(\rho))$. De fato, denotando $h = ord(\chi(\rho))$, temos $\chi(\rho)^h = 1$ e $\chi(\rho)^m \neq 1$ para $0 < m < h$. Além disso, para todo $\sigma \in G$, existe um inteiro e tal que $\chi(\sigma)^h = (\chi(\rho)^e)^h = (\chi(\rho)^h)^e = 1^e = 1$ e, para $0 < m < h$, $\chi^m(\sigma) = \chi(\sigma)^m \neq 1$. Portanto, $ord(\chi) = ord(\chi(\rho))$.

Logo, concluímos que $\chi(\rho)$ é uma raiz $ord(\chi)$ -ésima primitiva da unidade. Assim, para todo $\sigma \in G$, existe um inteiro e tal que $\chi(\sigma) = (\chi(\rho))^e \in \mathbb{Q}(\zeta_{ord(\chi)})$. Portanto, $\mathbb{Q}(\chi(G)) \subset \mathbb{Q}(\zeta_{ord(\chi)})$, concluindo a demonstração. $\square$

Assim, para qualquer $\chi \in X$ e para qualquer $a \in \mathbb{K}$, observe que $y_{\mathbb{K}}(\chi|a) \in \mathbb{K}\mathbb{Q}(\chi)$. Estendendo a operação de $\mathbb{Q}[G]$ à estrutura aditiva de $\mathbb{K}$ por linearidade, obtém-se

$$\epsilon_\chi(a) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma(a) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} y_{\mathbb{K}}(\chi|a) \overline{\tau(\chi)} \quad (6.34)$$

A seguir faremos uma sequência de resultados técnicos sobre caracteres coordenados de Leopoldt.

Proposição 6.2.3. *Todo $a \in \mathbb{K}$ pode ser representado como*

$$a = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in X} y_{\mathbb{K}}(\chi|a) \overline{\tau(\chi)}. \quad (6.35)$$

Demonstração. Devido à proposição 6.2.1, sabemos que $\sum_{\chi \in X} \epsilon_\chi = 1_{\mathbb{C}[G]} = 1.id$ (unidade do anel de grupo). Assim, $\sum_{\chi \in X} \epsilon_\chi(a) = 1.id(a) = a$. Logo, pela igualdade 6.34, tem-se

$$a = \sum_{\chi \in X} \epsilon_\chi(a) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in X} y_{\mathbb{K}}(\chi|a) \overline{\tau(\chi)}. \quad (6.36)$$

□

A próxima proposição relaciona o caractere coordenado aplicado a um elemento $a \in \mathbb{K}$ e sua imagem por um elemento de G . Esse resultado pode ser chamado de primeira propriedade de invariância dos caracteres coordenados de Leopoldt.

Proposição 6.2.4. *Para todo $\rho \in G$, $y_{\mathbb{K}}(\chi|\rho(a)) = \chi(\rho)y_{\mathbb{K}}(\chi|a)$.*

Demonstração. Como, para qualquer $\sigma \in G$, $\chi(\sigma \circ \rho) = \chi(\sigma)\chi(\rho)$, então

$$y_{\mathbb{K}}(\chi|\rho(a)) = \frac{1}{\tau(\chi)} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma(\rho(a)) = \frac{1}{\tau(\chi)} \sum_{\sigma \in G} \frac{\overline{\chi(\sigma \circ \rho)}}{\chi(\rho)} (\sigma \circ \rho)(a). \quad (6.37)$$

Fazendo variar $\sigma \in G$, como G é um grupo, $\sigma \circ \rho$ varia entre todos os elementos de G . Logo, podemos reindexar o somatória anterior e obter o seguinte:

$$y_{\mathbb{K}}(\chi|\rho(a)) = \frac{1}{\tau(\chi)\chi(\rho)} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma(a) = \frac{1}{\chi(\rho)} y_{\mathbb{K}}(\chi|a). \quad (6.38)$$

Como $\overline{\chi(\rho)} = \chi(\rho)^{-1}$ e $\chi(\rho)\overline{\chi(\rho)} = |\chi(\rho)| = 1$, finalmente concluímos que $y_{\mathbb{K}}(\chi|\rho(a)) = \chi(\rho)y_{\mathbb{K}}(\chi|a)$.

□

Como já vimos, existe uma correspondência biunívoca entre grupos de caracteres de Dirichlet e grupos abelianos finitos. Devido ao Teorema da Correspondência de Galois podemos, por transitividade, garantir que existe uma correspondência biunívoca entre corpos intermediários de $\mathbb{K}$ e grupos de caracteres de Dirichlet. Portanto, seja $\mathbb{K}_\chi$ o subcorpo de $\mathbb{K}$ associado ao grupo de caractere $\langle \chi \rangle$, para qualquer $\chi \in X$.

Proposição 6.2.5. *Se $a \in \mathbb{K}$, $\chi \in X$ e $f = f_\chi$ é o condutor de χ , então*

$$y_{\mathbb{K}}(\chi|a) = \frac{1}{f} \sum_{\sigma \in Gal(\mathbb{K}_\chi : \mathbb{Q})} \overline{\chi(\sigma)} Tr_{\mathbb{K}_\chi : \mathbb{Q}}[(Tr_{\mathbb{Q}(\zeta_f) : \mathbb{K}_\chi}(\zeta_f))\sigma(Tr_{\mathbb{K} : \mathbb{K}_\chi}(a))]. \quad (6.39)$$

Demonstração. Desde o início desta seção estamos considerando $G = Gal(\mathbb{K} : \mathbb{Q})$. Seja também $H = Gal(\mathbb{K} : \mathbb{K}_\chi) = \{\tau_1, \tau_2, \dots, \tau_m\} < G$ e $G/H \simeq Gal(\mathbb{K}_\chi : \mathbb{Q}) = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ (devido ao Teorema da Correspondência de Galois, pois G é abeliano). Dessa forma, $G = \{\sigma_i \tau_j : 1 \leq i \leq m \text{ e } 1 \leq j \leq n\}$.

Note ainda que se $\mathbb{K}_\chi$ é o subcorpo de $\mathbb{K}$ associado a $\langle \chi \rangle$, então $\mathbb{K}_\chi$ é o corpo fixo de $Gal(\mathbb{K} : \mathbb{K}_\chi) = H$. Porém, o fato de G/H estar associado a $\mathbb{K}_\chi$ significa que χ pode ser definido restrito a G/H , ou seja, todo elemento de G que não está em G/H é levado na unidade de G , ou ainda,

$$\tau \in Gal(\mathbb{K} : \mathbb{K}_\chi) \iff \chi(\tau) = 1 \iff \tau \in ker(\chi). \quad (6.40)$$

Portanto, $ker(\chi) = H$ (nessa igualdade, permite-se estar embutido um isomorfismo). Logo, $\chi(\tau_j) = 1$, para todo $1 \leq j \leq n$. Considere $G' = Gal(\mathbb{Q}(\zeta_f) : \mathbb{Q})$. Como $\mathbb{K}_\chi \subset \mathbb{Q}(\zeta_f)$, podemos tomar $G'/(G/H) = Gal(\mathbb{Q}(\zeta_f) : \mathbb{K}_\chi) = \{\psi_1, \psi_2, \dots, \psi_r\}$. Logo, $G' \simeq \{\sigma_i \psi_j : 1 \leq i \leq n \text{ e } 1 \leq j \leq r\}$. De maneira análoga ao que foi comentado acima, é claro que $\chi(\psi_j) = 1$ para todo $1 \leq j \leq r$. Agora, como $\mathbb{Z}_f^* \simeq Gal(\mathbb{Q}(\zeta_f) : \mathbb{Q})$, podemos escrever a soma de Gauss de maneira diferente da definida inicialmente (ressaltando que o “produto” dos automorfismo abaixo é, na verdade, uma composição):

$$\tau(\chi) = \sum_{k=1}^f \chi(k) \zeta_f^k = \sum_{\sigma_i \psi_j \in Gal(\mathbb{Q}(\zeta_f) : \mathbb{Q})} \chi(\sigma_i \psi_j)(\zeta_f) = \sum_{i=1}^n \sum_{j=1}^r \chi(\sigma_i \psi_j)(\zeta_f). \quad (6.41)$$

Como $\chi(\psi_j) = 1$ para todo $1 \leq j \leq r$, segue que

$$\tau(\chi) = \sum_{i=1}^n \chi(\sigma_i) \sigma_i \left(\sum_{j=1}^r \psi_j(\zeta_f) \right) = \sum_{i=1}^n \chi(\sigma_i) \sigma_i (Tr_{\mathbb{Q}(\zeta_f) : \mathbb{K}_\chi}(\zeta_f)) \quad (6.42)$$

Para simplificar a notação, denotemos $B = Tr_{\mathbb{Q}(\zeta_f) : \mathbb{K}_\chi}(\zeta_f)$. Assim, $\tau(\chi) = \sum_{i=1}^n \chi(\sigma_i) \sigma_i(B)$. De posse dessas informações, segue que

$$\begin{aligned} \tau(\chi) \sum_{\sigma_i \tau_j \in G} \overline{\chi(\sigma_i \tau_j)} \sigma_i \tau_j(a) &= \sum_{i=1}^n \chi(\sigma_i) \sigma_i(B) \sum_{k=1}^n \sum_{j=1}^m \overline{\chi(\sigma_k \tau_j)} \sigma_k \tau_j(a) = \\ &= \sum_{i=1}^n \sum_{k=1}^n \sum_{j=1}^m \chi(\sigma_i \sigma_k^{-1} \tau_j^{-1}) \sigma_i(B) \sigma_k \tau_j(a). \end{aligned} \quad (6.43)$$

Como G é grupo, podemos trocar os elementos σ_k por elementos $\sigma_i \sigma_l$, $1 \leq l \leq n$, reindexando o somatório anterior da seguinte forma:

$$\tau(\chi) \sum_{\sigma_i \tau_j \in G} \overline{\chi(\sigma_i \tau_j)} \sigma_i \tau_j(a) = \sum_{i=1}^n \sum_{l=1}^n \sum_{j=1}^m \chi(\sigma_i \sigma_l^{-1} \tau_j^{-1}) \sigma_i(B) \sigma_i \sigma_l \tau_j(a). \quad (6.44)$$

Como $\chi(\tau_j) = \chi(\tau_j^{-1}) = 1$, podemos simplificar o somatório anterior e seguir os cálculos:

$$\begin{aligned} \tau(\chi) \sum_{\sigma_i \tau_j \in G} \overline{\chi(\sigma_i \tau_j)} \sigma_i \tau_j(a) &= \sum_{i=1}^n \sum_{l=1}^n \sum_{j=1}^m \overline{\chi(\sigma_l)} \sigma_i (B \cdot \sigma_l(\tau_j(a))) = \\ &= \sum_{l=1}^n \overline{\chi(\sigma_l)} \sum_{i=1}^n \sigma_i \left(B \cdot \sigma_l \left(\sum_{j=1}^m \tau_j(a) \right) \right) = \sum_{l=1}^n \overline{\chi(\sigma_l)} Tr_{\mathbb{K}_\chi : \mathbb{Q}}(B \cdot \sigma_l(Tr_{\mathbb{K} : \mathbb{K}_\chi}(a))). \end{aligned} \quad (6.45)$$

Portanto, simplificando as notações, substituindo B por sua expressão definidora e utilizando a definição dos caracteres coordenados de Leopoldt, temos:

$$\tau(\chi)\overline{\tau(\chi)}y_{\mathbb{K}}(\chi|a) = \tau(\chi)\sum_{\sigma \in G}\overline{\chi(\sigma)}\sigma(a) = \sum_{\sigma \in \text{Gal}(\mathbb{K}_{\chi}:\mathbb{Q})}\overline{\chi(\sigma)}Tr_{\mathbb{K}_{\chi}:\mathbb{Q}}\left(Tr_{\mathbb{Q}(\zeta_f):\mathbb{K}_{\chi}}(\zeta_f)\sigma(Tr_{\mathbb{K}:\mathbb{K}_{\chi}}(a))\right). \quad (6.46)$$

Por fim, a igualdade $\tau(\chi)\overline{\tau(\chi)} = |\tau(\chi)|^2 = f$ dada pela proposição 5.6.2 finaliza a demonstração. $\square$

Corolário 6.2.1. *Para quaisquer $a \in \mathbb{K}$ e $\chi \in X$, tem-se $y_{\mathbb{K}}(\chi|a) \in \mathbb{Q}(\chi)$.*

Demonstração. Como $1/f \in \mathbb{Q}$ e $Tr_{\mathbb{K}_{\chi}:\mathbb{Q}}(x) \in \mathbb{Q}$ para qualquer $x \in \mathbb{K}_{\chi}$ então o resultado segue imediatamente da proposição anterior. $\square$

Lema 6.2.1. *Se $\chi \in X$ e r é um inteiro positivo tal que $\text{mdc}(r, \text{ord}(\chi)) = 1$, então $\langle \chi \rangle = \langle \chi^r \rangle$ e $f_{\chi} = f_{\chi^r}$.*

Demonstração. Seja $m = \text{ord}(\chi)$. Como $\text{mdc}(r, m) = 1$, então existem inteiros a e b tais que $ra + mb = 1$. Assim, para qualquer $\chi^e \in \langle \chi \rangle$, temos $\chi^e = \chi^{rae+mbe} = (\chi^r)^{ae}(\chi^m)^{be} = (\chi^r)^{ae} \in \langle \chi^r \rangle$. Portanto, $\langle \chi \rangle = \langle \chi^r \rangle$, já que obviamente $\langle \chi^r \rangle \subset \langle \chi \rangle$. Mostremos que $f_{\chi} = f_{\chi^r}$. Como $\langle \chi \rangle = \langle \chi^r \rangle$, então existe um inteiro s tal que $\text{mdc}(s, m) = 1$ e $\chi^{rs} = \chi$. Daí, para quaisquer $a, b \in G$,

$$\chi(a) = \chi(b) \implies \chi(a)^r = \chi(b)^r \implies \chi^r(a) = \chi^r(b) \quad (6.47)$$

e também

$$\chi^r(a) = \chi^r(b) \implies \chi(a)^{rs} = \chi(b)^{rs} \implies \chi(a) = \chi(b). \quad (6.48)$$

Em suma, $\chi(a) = \chi(b)$ se, e somente se, $\chi^r(a) = \chi^r(b)$. Como χ e χ^r podem ser definidos sob o mesmo módulo, note que $M_{\chi} = M_{\chi^r}$ (veja a definição desse conjunto na seção 5.4). Portanto, $f_{\chi} = f_{\chi^r}$. $\square$

Proposição 6.2.6. *Se $\text{mdc}(r, \text{ord}(\chi)) = 1$ e $\sigma_r \in \text{Gal}(\mathbb{Q}(\zeta_{\text{ord}(\chi)}) : \mathbb{Q})$ é o automorfismo definido por $\sigma_r(\zeta_{\text{ord}(\chi)}) = \zeta_{\text{ord}(\chi)}^r$, então $y_{\mathbb{K}}(\chi^r|a) = \sigma_r(y_{\mathbb{K}}(\chi|a))$.*

Demonstração. Seja $m = \text{ord}(\chi)$. Pela proposição 6.2.2, $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\chi)$. Em particular, como $\mathbb{K}_{\chi} \subset \mathbb{K}$, segue que para todo $\sigma \in H \triangleq \text{Gal}(\mathbb{K}_{\chi} : \mathbb{Q})$ tem-se $\chi(\sigma) = \zeta_m^e$. Então, $\sigma_r(\chi(\sigma)) = \sigma_r(\zeta_m^e) = (\zeta_m^r)^e = \chi(\sigma)^r = \chi^r(\sigma)$. Portanto, $\sigma_r(\chi(\sigma)) = \chi^r(\sigma)$ para qualquer $\sigma \in H$. Pelo lema 6.2.1, sabemos que $\langle \chi \rangle = \langle \chi^r \rangle$, ou seja, $\mathbb{K}_{\chi} = \mathbb{K}_{\chi^r}$, e que $f_{\chi^r} = f_{\chi}$. Assim, para qualquer $\sigma \in H$,

$$C_{\sigma} \triangleq Tr_{\mathbb{K}_{\chi}:\mathbb{Q}}\left(Tr_{\mathbb{Q}(\zeta_{f_{\chi}}):\mathbb{K}_{\chi}}(\zeta_{f_{\chi}})\sigma(Tr_{\mathbb{K}:\mathbb{K}_{\chi}}(a))\right) = Tr_{\mathbb{K}_{\chi^r}:\mathbb{Q}}\left(Tr_{\mathbb{Q}(\zeta_{f_{\chi^r}}):\mathbb{K}_{\chi^r}}(\zeta_{f_{\chi^r}})\sigma(Tr_{\mathbb{K}:\mathbb{K}_{\chi^r}}(a))\right). \quad (6.49)$$

Note que $C_\sigma \in \mathbb{Q}$. Logo, pela proposição 6.2.5 e como $\sigma_r(\chi(\sigma)) = \chi^r(\sigma)$ para qualquer $\sigma \in H$, temos $y_{\mathbb{K}}(\chi|a) = 1/f_\chi \sum_{\sigma \in H} \overline{\chi(\sigma)} C$ e, consequentemente,

$$\sigma_r(y_{\mathbb{K}}(\chi|a)) = \frac{1}{f_\chi} \sum_{\sigma \in H} \sigma_r(\overline{\chi(\sigma)}) C = \frac{1}{f_{\chi^r}} \sum_{\sigma \in H} \overline{\chi^r(\sigma)} C = y_{\mathbb{K}}(\chi^r|a). \quad (6.50)$$

□

A próxima proposição pode ser chamada de segunda propriedade de invariância, pois nos mostra como calcular o caractere coordenado de Dirichlet $y_{\mathbb{F}}(\chi|a)$ em um subcorpo $\mathbb{F}$ de $\mathbb{K}$ que define completamente o caractere χ .

Proposição 6.2.7. *Seja $\mathbb{F}$ um corpo tal que $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{K}$. Se χ é um caractere de $\text{Gal}(\mathbb{F} : \mathbb{Q})$, ou seja, $\chi(\rho) = 1$ para qualquer $\rho \in \text{Gal}(\mathbb{K} : \mathbb{F})$, então*

$$y_{\mathbb{K}}(\chi|a) = y_{\mathbb{F}}(\chi|Tr_{\mathbb{K}:\mathbb{F}}(a)). \quad (6.51)$$

Demonstração. Sejam $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$, $H = \text{Gal}(\mathbb{K} : \mathbb{F})$ e $G/H \simeq \text{Gal}(\mathbb{F} : \mathbb{Q})$. Por definição de caractere coordenado de Dirichlet, como a soma de Gauss independe do elemento a do corpo $\mathbb{K}$ nas condições consideradas, então

$$y_{\mathbb{F}}(\chi|Tr_{\mathbb{K}:\mathbb{F}}(a)) = \frac{1}{\tau(\chi)} \sum_{\psi \in G/H} \overline{\chi(\psi)} \psi \left(\sum_{\rho \in H} \rho(a) \right) = \frac{1}{\tau(\chi)} \sum_{\psi \in G/H} \overline{\chi(\psi)} \sum_{\rho \in H} (\psi \circ \rho)(a) \quad (6.52)$$

Por hipótese, $\chi(\rho) = 1$ para todo $\rho \in H$. Logo,

$$\begin{aligned} y_{\mathbb{F}}(\chi|Tr_{\mathbb{K}:\mathbb{F}}(a)) &= \frac{1}{\tau(\chi)} \sum_{\psi \in G/H} \sum_{\rho \in H} \overline{\chi(\psi)\chi(\rho)} (\psi \circ \rho)(a) = \\ &= \frac{1}{\tau(\chi)} \sum_{\psi \in G/H, \rho \in H} \overline{\chi(\psi \circ \rho)} (\psi \circ \rho)(a) = \frac{1}{\tau(\chi)} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma(a) = y_{\mathbb{K}}(\chi|a). \end{aligned} \quad (6.53)$$

□

A seguir, utilizaremos a notação $[A : B]$ para dois $\mathbb{Z}$ -módulos livres de posto igual ao grau de $\mathbb{K}$ (vistos como grupo aditivos), mesmo que B não esteja contido em A . De acordo com a definição estabelecida em [21] (§4, capítulo 2), se C é um $\mathbb{Z}$ -módulo livre também de posto igual ao grau de $\mathbb{K}$ então

$$[A : B] \triangleq \frac{[C : B]}{[C : A]}. \quad (6.54)$$

Esse valor é chamado de **índice generalizado**. Não há problema na definição, pois tal valor independe da escolha de C . Se B está contido em A , então o índice generalizado coincide com o índice usual de grupos aditivos.

A próxima proposição nos diz quando o $\mathbb{Z}$ -módulo $\mathbb{Z}[G]a$ tem posto máximo, para algum $a \in \mathbb{K}$.

Proposição 6.2.8. *Seja $a \in \mathbb{K}$.*

(i) *Se $D(\mathbb{K})$ denota o discriminante de $\mathbb{K}$ então*

$$D_{\mathbb{K}:\mathbb{Q}}(\sigma(a) : \sigma \in G) = \left(\prod_{\chi \in X} y_{\mathbb{K}}(\chi|a) \right)^2 D(\mathbb{K}). \quad (6.55)$$

(ii) *$\mathbb{Z}[G]a$ tem rank maximal $[\mathbb{K} : \mathbb{Q}]$ se, e somente se, $y_{\mathbb{K}}(\chi|a) \neq 0$, para todo $\chi \in X$. Neste caso,*

$$[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[G]a] = \left| \prod_{\chi \in X} y_{\mathbb{K}}(\chi|a) \right| \quad (6.56)$$

Demonstração. (i) Seja $f : G \rightarrow \mathbb{C}$ a aplicação dada por $f(\sigma) = \sigma^{-1}(a)$, para todo $\sigma \in G$. Devido à proposição 5.3.2, temos

$$\det[\sigma'(\sigma(a))]_{\sigma' \in G, \sigma \in G} = \prod_{\chi \in X} \left(\sum_{\sigma \in G} \chi(\sigma) \sigma^{-1}(a) \right) \quad (6.57)$$

Pela proposição 2.3.3, note que

$$D_{\mathbb{K}:\mathbb{Q}}(\sigma(a) : \sigma \in G) = (\det[\sigma'(\sigma(a))]_{\sigma' \in G, \sigma \in G})^2 \quad (6.58)$$

Por definição, sabemos que $\overline{\tau(\chi)} y_{\mathbb{K}}(\chi|a) = \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma(a) = \sum_{\sigma \in G} \chi(\sigma) \sigma^{-1}(a)$. Disso e das equações 6.57 e 6.58, temos

$$D_{\mathbb{K}:\mathbb{Q}}(\sigma(a) : \sigma \in G) = \prod_{\chi \in X} \left(\sum_{\sigma \in G} \chi(\sigma) \sigma^{-1}(a) \right)^2 = \prod_{\chi \in X} \left(\overline{\tau(\chi)} y_{\mathbb{K}}(\chi|a) \right)^2 = \prod_{\chi \in X} y_{\mathbb{K}}(\chi|a)^2 \prod_{\chi \in X} \tau(\chi) \overline{\tau(\chi)}. \quad (6.59)$$

Note que, para a última igualdade, associou-se um elemento $\tau(\chi)$ indexado em χ ao correspondente $\overline{\chi}$. Como $|\tau(\chi)|^2 = \tau(\chi) \overline{\tau(\chi)} = f_{\chi}$ (proposição 5.6.2) então

$$D_{\mathbb{K}:\mathbb{Q}}(\sigma(a) : \sigma \in G) = \prod_{\chi \in X} f_{\chi} \prod_{\chi \in X} y_{\mathbb{K}}(\chi|a)^2 = D(\mathbb{K}) \prod_{\chi \in X} y_{\mathbb{K}}(\chi|a)^2 \quad (6.60)$$

em que a última igualdade advém da Fórmula do Condutor-Discriminante (teorema 5.4.1). (ii) Pelo item (i), $y_{\mathbb{K}}(\chi|a) \neq 0$ para todo $\chi \in X$ se, e somente se, $D_{\mathbb{K}:\mathbb{Q}}(\sigma(a) : \sigma \in G) \neq 0$. Devido à proposição 2.3.5, isso ocorre se, e somente se, $\{\sigma(a) : \sigma \in G\}$ é uma $\mathbb{Q}$ -base para $\mathbb{K}$ (ou seja, é linearmente independente sobre $\mathbb{Q}$). Isso é equivalente a dizer que $\{\sigma(a) : \sigma \in G\}$ é linearmente independente sobre $\mathbb{Z}$, ou seja, que $\mathbb{Z}[G]a = \sum_{\sigma \in G} \mathbb{Z}\sigma(a)$ tem posto maximal $[\mathbb{K} : \mathbb{Q}]$. Portanto, $y_{\mathbb{K}}(\chi|a) \neq 0$ para todo $\chi \in X$ se, e somente se, $\mathbb{Z}[G]a$ tem posto maximal $[\mathbb{K} : \mathbb{Q}]$. Neste caso, tem-se que $D_{\mathbb{K}:\mathbb{Q}}(\sigma(a) : \sigma \in G) = [\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[G]a]^2 D(\mathbb{K})$. Comparando com a igualdade do item (i), conclui-se que $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[G]a] = \left| \prod_{\chi \in X} y_{\mathbb{K}}(\chi|a) \right|$. $\square$

Na próxima proposição, calculamos os caracteres coordenados das raízes da unidade.

Proposição 6.2.9. *Sejam $k, n \in \mathbb{N}$ tais que $\zeta_n^k = \zeta_{n_0}^{k_0}$, em que $k_0, n_0 \in \mathbb{N}$ e $\text{mdc}(k_0, n_0) = 1$. Então, para qualquer $\chi \in X^{(n)}$, temos:*

$$y_{\mathbb{Q}(n)}(\chi|\zeta_n^k) = \begin{cases} 0, & \text{se } f \text{ não divide } n_0 \text{ ou } q(f) \neq q(n_0) \\ \frac{\varphi(n)}{\varphi(n_0)} \mu\left(\frac{n_0}{f}\right) \bar{\chi}\left(-\frac{n_0}{f}\right) \chi(k_0) \neq 0, & \text{se } f \mid n_0 \text{ e } q(f) = q(n_0) \end{cases} \quad (6.61)$$

em que μ denota função de Möbius (veja a equação 1.1) e f denota o condutor de χ .

Demonstração. Por definição, temos

$$y_{\mathbb{Q}(n)}(\chi|\zeta_n^k) = \frac{1}{\tau(\chi)} \sum_{\sigma \in G^{(n)}} \overline{\chi(\sigma)} \sigma(\zeta_n^k) = \frac{1}{\tau(\chi)} \sum_{j=1}^n \overline{\chi(j)} \zeta_n^{kj} = \frac{\overline{\tau_k(\chi)}}{\tau(\chi)} \quad (6.62)$$

em que $\tau(\chi)$ é a soma primitiva de Gauss e $\tau_k(\chi)$ é a soma de Gauss (geral). Pela proposição 5.6.3, tem-se então que

$$y_{\mathbb{Q}(n)}(\chi|\zeta_n^k) = \frac{\varphi(n)}{\varphi(n_0)} \mu\left(\frac{n_0}{f}\right) \bar{\chi}\left(-\frac{n_0}{f}\right) \chi(k_0) \quad (6.63)$$

a qual é diferente de zero se, e somente se, $f \mid n_0$ e n_0/f for livre de quadrados. Porém, essa última condição é válida somente quando $q(f) = q(n_0)$. Isso conclui a prova. $\square$

6.3 Teorema de Leopoldt-Lettl

Nesta seção demonstraremos o principal resultado desta dissertação: o Teorema de Leopoldt-Lettl. Esse teorema nos fornece o anel de inteiros de qualquer corpo de números abeliano.

O matemático alemão Heinrich-Wolfgang Leopoldt (1927-2011) demonstrou esse resultado originalmente em 1959, no seu artigo [19]. Ele mostrou que se $\mathbb{K}$ é um corpo de números abeliano e $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$ então $\mathcal{O}_{\mathbb{K}} = R_{\mathbb{K}} T_{\mathbb{K}}$, em que $R_{\mathbb{K}}$ é uma ordem em $\mathbb{Q}[G]$ e $T_{\mathbb{K}}$ é um inteiro algébrico de $\mathbb{K}$ chamado de **Basiszahl** de Leopoldt. Por conta da origem do teorema ser devida a Leopoldt, usualmente o teorema principal desta seção é conhecido como **Teorema de Leopoldt**.

Em suas notas ([16]), Henri Johnston explicita esse teorema da seguinte forma: seja $\mathbb{K}$ um corpo de números abeliano com grupo de Galois $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$; então $\mathcal{O}_{\mathbb{K}}$ é um $\mathcal{A}_{\mathbb{K}:\mathbb{Q}}$ -módulo livre de posto um, em que $\mathcal{A}_{\mathbb{K}:\mathbb{Q}} = \{x \in \mathbb{Q}[G] : x\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{K}}\}$ é uma $\mathbb{Z}$ -ordem em $\mathbb{Q}[G]$, chamada de **ordem associada** da extensão $\mathbb{Q} \subset \mathbb{K}$. Henri ressalta ainda que é possível explicitar um gerador $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{O}_{\mathbb{K}} = \mathcal{A}_{\mathbb{K}:\mathbb{Q}}\alpha$ (teorema 1.8 de [16]). No texto, Johnston demonstra esse resultado para os casos em que $\mathbb{K}$ tem condutor n ímpar ou quando $i = \sqrt{-1} \in \mathbb{K}$ (teorema 12.9 de [16]), mas faz comentários acerca da demonstração geral.

Por sua vez, Günter Lettl deu outra demonstração do Teorema de Leopoldt em 1990, no seu artigo [20], no qual mostrou de maneira um pouco mais elementar do que a original que $\mathcal{O}_{\mathbb{K}} = R_{\mathbb{K}}T$, em que $R_{\mathbb{K}}$ é uma ordem em $\mathbb{Q}[G]$ e T é um inteiro algébrico do corpo de números abeliano $\mathbb{K}$. Além disso, Lettl foi mais específico e demonstrou também que, se n é o condutor de $\mathbb{K}$, então $\mathcal{O}_{\mathbb{K}} = \oplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d$, em que $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$ e η_d é um elemento de $\mathbb{K} \cap \mathbb{Q}(\zeta_d)$. Nesta seção, citaremos o Teorema de Leopoldt da maneira como foi enunciado e demonstrado por Lettl no capítulo 4 de [20]. Por isso, chamaremos esse importante resultado de **Teorema de Leopoldt-Lettl**.

Em toda esta seção, considere $\mathbb{K}$ um corpo de números abeliano com condutor n , $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$, $\mathbb{Q}^{(m)} \triangleq \mathbb{Q}(\zeta_m)$, em que $\zeta_m = e^{\frac{2\pi i}{m}}$ é uma raiz m -ésima primitiva da unidade, para qualquer $m > 1$ natural, e X o grupo de caracteres de Dirichlet associado a G . Para qualquer $d \in \mathcal{D}(n)$ (definição 6.1.1), assumamos ainda as seguintes notações:

$$\mathbb{K}_d \triangleq \mathbb{K} \cap \mathbb{Q}^{(d)} \quad e \quad \eta_d \triangleq \text{Tr}_{\mathbb{Q}^{(d)} : \mathbb{K}_d} \zeta_d. \quad (6.64)$$

A seguir, faremos uma série de resultados que nos levarão ao Teorema de Leopoldt-Lettl. O lema seguinte é provado em cursos de Teoria de Galois e está enunciado abaixo porque será utilizado na prova do lema posterior.

Lema 6.3.1 ([22], capítulo 6, teorema 1.12.). *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana de corpos e $\mathbb{K} \subset \mathbb{M}$ uma extensão de corpos arbitrária, ambas contidas em um mesmo corpo Ω . Considere $H = \text{Gal}(\mathbb{L}\mathbb{M} : \mathbb{M})$. Então:*

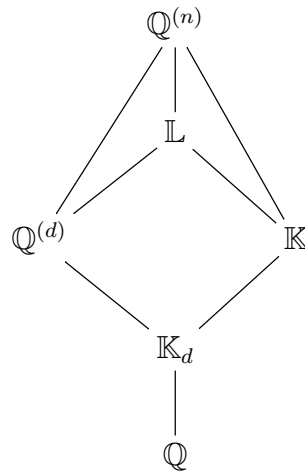
- (a) *O corpo composto $\mathbb{M}\mathbb{L}$ é Galois sobre $\mathbb{M}$, enquanto $\mathbb{L}$ é Galois sobre $\mathbb{L} \cap \mathbb{M}$.*
- (b) *Se $\sigma \in H$ então $\sigma|_{\mathbb{L}} \in \text{Gal}(\mathbb{L} : \mathbb{K})$.*
- (c) *A aplicação $\psi : H \rightarrow \text{Gal}(\mathbb{L} : \mathbb{L} \cap \mathbb{M})$ dada por $\psi(\sigma) = \sigma|_{\mathbb{L}}$, para qualquer $\sigma \in H$, é um isomorfismo.*

Lema 6.3.2. *Com as notações já estabelecidas, se $\chi \in X$ e $d \in \mathcal{D}(n)$,*

$$y_{\mathbb{K}}(\chi|\eta_d) = \frac{[\mathbb{K} : \mathbb{K}_d]}{[\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}]} y_{\mathbb{Q}^{(n)}}(\chi|\zeta_d). \quad (6.65)$$

Demonstração. Como n é o condutor de $\mathbb{K}$ então $\mathbb{K} \subset \mathbb{Q}^{(n)}$ e, como $d \mid n$, então $\mathbb{Q}^{(d)} \subset \mathbb{Q}^{(n)}$.

Considere o corpo composto $\mathbb{L} = \mathbb{Q}^{(d)}\mathbb{K}$. Considere o seguinte diagrama de corpos:



Como $\mathbb{Q} \subset \mathbb{Q}^{(d)}$ é uma extensão galoisiana, os itens (a) e (c) do lema 6.3.1 nos garantem que

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{Q}^{(d)} : \mathbb{K}_d] = \frac{[\mathbb{Q}^{(n)} : \mathbb{K}_d]}{[\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}]}. \quad (6.66)$$

Vamos mostrar que

$$Tr_{\mathbb{Q}^{(n)}:\mathbb{K}}\zeta_d = \frac{[\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}]}{[\mathbb{K} : \mathbb{K}_d]}\eta_d \quad (6.67)$$

De fato, novamente pelo lema 6.3.1, tem-se que

$$\eta_d = Tr_{\mathbb{Q}^{(d)}:\mathbb{K}_d}\zeta_d = Tr_{\mathbb{L}:\mathbb{K}}\zeta_d = Tr_{\mathbb{L}:\mathbb{K}}\left(\zeta_d \frac{[\mathbb{Q}^{(n)} : \mathbb{L}]}{[\mathbb{Q}^{(n)} : \mathbb{L}]}\right) = \frac{1}{[\mathbb{Q}^{(n)} : \mathbb{L}]}Tr_{\mathbb{L}:\mathbb{K}}(Tr_{\mathbb{Q}^{(n)}:\mathbb{L}}\zeta_d) \quad (6.68)$$

em que a última igualdade segue do fato de que $\zeta_d \in \mathbb{L}$. Pela transitividade do traço (proposição 2.2.4), obtém-se que

$$Tr_{\mathbb{Q}^{(n)}:\mathbb{K}}\zeta_d = [\mathbb{Q}^{(n)} : \mathbb{L}]\eta_d. \quad (6.69)$$

Além disso,

$$[\mathbb{Q}^{(n)} : \mathbb{L}] = \frac{[\mathbb{Q}^{(n)} : \mathbb{K}]}{[\mathbb{L} : \mathbb{K}]} = \frac{[\mathbb{Q}^{(n)} : \mathbb{K}_d]}{[\mathbb{K} : \mathbb{K}_d]} \frac{[\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}]}{[\mathbb{Q}^{(n)} : \mathbb{K}_d]} = \frac{[\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}]}{[\mathbb{K} : \mathbb{K}_d]}. \quad (6.70)$$

Juntando as equações 6.69 e 6.70, finalmente vê-se que a equação 6.67 é verdadeira. Assim, devido também à proposição 6.2.7, temos finalmente

$$y_{\mathbb{Q}^{(n)}}(\chi|\zeta_d) = y_{\mathbb{K}}(\chi|Tr_{\mathbb{Q}^{(n)}:\mathbb{K}}\zeta_d) = \frac{[\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}]}{[\mathbb{K} : \mathbb{K}_d]}y_{\mathbb{K}}(\chi|\eta_d) \quad (6.71)$$

donde segue o resultado. $\square$

Lema 6.3.3. Com as notações anteriores, se $\chi \in X$ e $d \in \mathcal{D}(n)$ então

$$y_{\mathbb{K}}(\chi|\eta_d) \neq 0 \iff q(d) \mid f_{\chi} \text{ e } f_{\chi} \mid d \iff \chi \in \Phi_d \quad (6.72)$$

em que Φ_d é classe de ramo d de X .

Demonstração. Pelo lema 6.3.2, $y_{\mathbb{K}}(\chi|\eta_d) \neq 0$ se, e somente se, $y_{\mathbb{Q}(n)}(\chi|\zeta_d) \neq 0$. Pela proposição 6.2.9, isso ocorre se, e somente se, $f_{\chi} \mid d$ e $q(f_{\chi}) = q(d)$. Assim, por um lado, $y_{\mathbb{K}}(\chi|\eta_d) \neq 0$ implica que $\chi \in \Phi_d$. Por outro lado, seja $\chi \in \Phi_d$. Então $q(f_{\chi}) = q(d)$ e, como $q(d) \mid d$, tem-se que $q(f_{\chi}) \mid d$. Como $f_{\chi} \not\equiv 2 \pmod{4}$ então f_{χ} é ímpar ou é da forma $4x$, para algum inteiro x . No primeiro caso, podemos fatorar $f_{\chi} = \prod_i p_i^{e_i} \prod_j q_j$, em que p_i e q_j são primos ímpares distintos e $e_i > 1$. Como $f_{\chi} \mid n$ e todos os primos ímpares de n dividem d então $\prod_i p_i \prod_j q_j \mid d$. Além disso, a hipótese de que $q(f_{\chi}) = q(d)$ acarreta $\prod_i p_i^{e_i} \mid d$. Logo, $\prod_i p_i^{e_i} \prod_j q_j \mid d$ e, portanto, $f_{\chi} \mid d$. Logo, $f_{\chi} \mid d$ e $q(f_{\chi}) = q(d)$. Pela equivalência estabelecida no início, conclui-se que $y_{\mathbb{Q}(n)}(\chi|\zeta_d) \neq 0$. Por fim, mostremos que $f_{\chi} \mid d$ e $q(f_{\chi}) = q(d)$ é equivalente a dizer que $f_{\chi} \mid d$ e $q(d) \mid f_{\chi}$. De fato, por um lado, como $q(f_{\chi}) \mid f_{\chi}$ então $q(d) = q(f_{\chi}) \mid f_{\chi}$. Por outro lado, suponha $f_{\chi} \mid d$ e $q(d) \mid f_{\chi}$. Obviamente, $q(d) \mid q(f_{\chi})$. Além disso, seja $q(f_{\chi}) = \prod_i p_i^{e_i}$ a fatoração de $q(f_{\chi})$ em primos, com $e_i > 1$. Dessa forma, $f_{\chi} = \prod_i p_i^{e_i} \prod_j q_j$, em que q_j também são primos dividindo f_{χ} . Como $f_{\chi} \mid d$ então a fatoração de primos de d é dada $d = \prod_i p_i^{e_i + \alpha_i} \prod_j r_j^{\beta_j}$, em que parte dos r_j é formada pelos q_j . Assim, $q(f_{\chi}) \mid q(d)$. Portanto, $q(f_{\chi}) = q(d)$. Isso completa a prova. $\square$

Lema 6.3.4. *Com as notações anteriores, se $\chi \in X$ e $d \in \mathcal{D}(n)$ então*

$$\eta_d = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in \Phi_d} [\mathbb{K} : \mathbb{K}_d] \mu\left(\frac{d}{f_{\chi}}\right) \bar{\chi}\left(\frac{-d}{f_{\chi}}\right) \overline{\tau(\chi)}. \quad (6.73)$$

Demonstração. Tome $k = n/d \in \mathbb{Z}$. Assim, $\zeta_n^k = \zeta_n^{n/d} = \zeta_d$. Aplicando a proposição 6.2.9, quando $y_{\mathbb{Q}(n)}(\chi|\zeta_d) \neq 0$ tem-se que

$$y_{\mathbb{Q}(n)}(\chi|\zeta_d) = \frac{\varphi(n)}{\varphi(d)} \mu\left(\frac{d}{f_{\chi}}\right) \bar{\chi}\left(-\frac{d}{f_{\chi}}\right). \quad (6.74)$$

Como $[\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}] = [\mathbb{Q}^{(n)} : \mathbb{Q}] / [\mathbb{Q}^{(d)} : \mathbb{Q}] = \varphi(n)/\varphi(d)$, segue do lema 6.3.2 que

$$y_{\mathbb{K}}(\chi|\eta_d) = \frac{[\mathbb{K} : \mathbb{K}_d]}{\varphi(n)/\varphi(d)} \frac{\varphi(n)}{\varphi(d)} \mu\left(\frac{d}{f_{\chi}}\right) \bar{\chi}\left(-\frac{d}{f_{\chi}}\right) = [\mathbb{K} : \mathbb{K}_d] \mu\left(\frac{d}{f_{\chi}}\right) \bar{\chi}\left(-\frac{d}{f_{\chi}}\right). \quad (6.75)$$

A proposição 6.2.3 e o lema 6.3.3 acarretam

$$\eta_d = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in X} y_{\mathbb{K}}(\chi|\eta_d) \overline{\tau(\chi)} = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in \Phi_d} y_{\mathbb{K}}(\chi|\eta_d) \overline{\tau(\chi)}. \quad (6.76)$$

Finalmente, substituindo a igualdade 6.75 na expressão 6.76 tem-se a expressão 6.73 que queríamos demonstrar. $\square$

O lema 6.3.4 nos permite ver claramente que se $\Phi_d = \emptyset$ então $\eta_d = 0$. Reciprocamente, se $\eta_d = 0$ então $y_{\mathbb{K}}(\chi|\eta_d) = y_{\mathbb{K}}(\chi|0) = 1/\overline{\tau(\chi)} \sum_{\sigma \in G} \overline{\chi(\sigma)} \sigma(0) = 0$, para todo $\chi \in X$. Disso e do lema 6.3.3

podemos concluir que $\chi \notin \Phi_d$, para todo $\chi \in X$, ou seja, que $\Phi_d = \emptyset$. Portanto, para cada $d \in \mathcal{D}(n)$,

$$\eta_d = 0 \iff \Phi_d = \emptyset \quad (6.77)$$

Devido à proposição 6.1.4, isso só pode ocorrer quando $d \equiv 4 \pmod{8}$.

Mantidas as notações acima, definimos

$$T \triangleq \sum_{d \in \mathcal{D}(n)} \eta_d = \sum_{d \in \mathcal{D}(n)} \text{Tr}_{\mathbb{Q}^{(d)} : \mathbb{K}_d} \zeta_d. \quad (6.78)$$

Esse elemento é similar ao já comentando “Basiszahl” definido por Leopoldt em [19].

Lema 6.3.5. *Mantidas as notações anteriores, $y_{\mathbb{K}}(\chi|T) \neq 0$, para qualquer $\chi \in X$.*

Demonstração. Seja $\chi \in X$ qualquer. Como o caractere coordenado de Leopoldt preserva a soma,

$$y_{\mathbb{K}}(\chi|T) = y_{\mathbb{K}}\left(\chi \left| \sum_{d \in \mathcal{D}(n)} \eta_d \right.\right) = \sum_{d \in \mathcal{D}(n)} y_{\mathbb{K}}(\chi|\eta_d). \quad (6.79)$$

Pela proposição 6.1.3, $X = \bigcup_{d \in \mathcal{D}(n)} \Phi_d$, sendo esta união disjunta. Logo, existe um único $d_0 \in \mathcal{D}(n)$ tal que $\chi \in \Phi_{d_0}$. Assim, o lema 6.3.3 garante que $y_{\mathbb{K}}(\chi|\eta_{d_0}) \neq 0$ e $y_{\mathbb{K}}(\chi|\eta_d) = 0$ se $d \neq d_0$. Da equação 6.79, obtemos finalmente que $y_{\mathbb{K}}(\chi|T) = y_{\mathbb{K}}(\chi|\eta_{d_0}) \neq 0$. $\square$

Portanto, o lema 6.3.5 e a proposição 6.2.8 nos garantem que $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[G]T] = \left| \prod_{\chi \in X} y_{\mathbb{K}}(\chi|T) \right|$ é um índice finito.

O resultado a seguir é interessante, pois nos mostra que T gera uma base normal para a extensão de corpos $\mathbb{Q} \subset \mathbb{K}$.

Proposição 6.3.1. *Com as notações anteriores, $\mathbb{K} = \mathbb{Q}[G]T$.*

Demonstração. Seja $G = \text{Gal}(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \dots, \sigma_m\}$. Pelo lema 6.3.5, $y_{\mathbb{K}}(\chi|T) \neq 0$, para todo $\chi \in X$. Devido ao que foi mostrado na proposição 6.2.8, isso significa que $\mathbb{Z}[G]T$ tem posto maximal $m = [\mathbb{K} : \mathbb{Q}]$. Neste caso, vimos ainda que $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[G]T] = \left| \prod_{\chi \in X} y_{\mathbb{K}}(\chi|T) \right|$ é um índice finito.

Por um lado, é claro que $\mathbb{Q}[G]T \subset \mathbb{K}$, pois $T \in \mathbb{K}$. Por outro lado, seja $\mathcal{B} = \{x_1, \dots, x_m\}$ uma $\mathbb{Z}$ -base para o $\mathbb{Z}$ -módulo $\mathbb{Z}[G]T$. Como $\mathcal{B}$ é linearmente independente sobre $\mathbb{Z}$ então é também linearmente independente sobre $\mathbb{Q}$. Além disso, $\mathcal{B}$ gera $\mathbb{Q}[G]T$, pois gera $\mathbb{Z}[G]T$. Portanto, $\mathcal{B}$ é uma base para $\mathbb{Q}[G]T$ sobre $\mathbb{Q}$. Assim, $[\mathbb{Q}[G]T : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}]$ e, como $\mathbb{Q}[G]T \subset \mathbb{K}$, então $\mathbb{Q}[G]T = \mathbb{K}$. $\square$

Agora, para cada $d \in \mathcal{D}(n)$, defina

$$\epsilon_d \triangleq \sum_{\chi \in \Phi_d} \epsilon_{\chi} \quad (6.80)$$

em que cada ϵ_χ é o idempotente ortogonal de χ definido na seção 6.2. Como $f_\chi = f_{\bar{\chi}}$ então Φ_d é fechado para a conjugação de caracteres. Por isso, o texto [20] afirma que ϵ_d é um elemento do anel de grupo $\mathbb{Q}[G]$. Além disso:

Lema 6.3.6. *Com as notações anteriores,*

$$R_{\mathbb{K}} = \mathbb{Z}[G][\{\epsilon_d : d \in \mathcal{D}(n)\}] \quad (6.81)$$

é uma $\mathbb{Z}$ -ordem em $\mathbb{Q}[G]$.

Demonstração. Como $\epsilon_d \in \mathbb{Q}[G]$ e $\mathbb{Z}[G] \subset \mathbb{Q}[G]$, então $R_{\mathbb{K}}$ é um subanel de $\mathbb{Q}[G]$. Além disso, como $\sum_{d \in \mathcal{D}(n)} \epsilon_d = \sum_{\chi \in X} \epsilon_\chi = 1$ então $1 \in R_{\mathbb{K}}$. Além disso, como

$$R_{\mathbb{K}} = \mathbb{Z}[G][\{\epsilon_d : d \in \mathcal{D}(n)\}] = \left\{ \sum_{d \in \mathcal{D}(n)} \sum_{g \in G} a_g g \epsilon_d : a_g \in \mathbb{Z} \right\} \quad (6.82)$$

então $R_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo finitamente gerado por $\{g \epsilon_d : g \in G, d \in \mathcal{D}(n)\}$. Agora, obviamente $\mathbb{Q}[G] \subset \mathbb{Q}R_{\mathbb{K}}$, pois G pode ser considerado contido em $R_{\mathbb{K}}$. De fato, cada $g \in G$ pode ser escrito como $g = 1 \cdot g \cdot (\sum_{d \in \mathcal{D}(n)} \epsilon_d)$. Reciprocamente, como $\epsilon_d \in \mathbb{Q}[G]$ tem-se que $\mathbb{Q}R_{\mathbb{K}} \subset \mathbb{Q}[G]$, donde segue que $\mathbb{Q}R_{\mathbb{K}} = \mathbb{Q}[G]$. Portanto, $R_{\mathbb{K}}$ é uma $\mathbb{Z}$ -ordem em $\mathbb{Q}[G]$. $\square$

Lema 6.3.7. *Com as notações anteriores, para cada $d \in \mathcal{D}(n)$,*

$$\epsilon_d(T) = \eta_d. \quad (6.83)$$

Demonstração. Por um lado, da definição de ϵ_d e de ϵ_χ tem-se que

$$\begin{aligned} \epsilon_d(T) &= \sum_{\chi \in \Phi_d} \epsilon_\chi(T) = \sum_{\chi \in \Phi_d} \frac{y_{\mathbb{K}}(\chi|T) \overline{\tau(\chi)}}{[\mathbb{K} : \mathbb{Q}]} = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in \Phi_d} \overline{\tau(\chi)} y_{\mathbb{K}} \left(\chi \left| \sum_{c \in \mathcal{D}(n)} \eta_c \right. \right) = \\ &= \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in \Phi_d} \overline{\tau(\chi)} \sum_{c \in \mathcal{D}(n)} y_{\mathbb{K}}(\chi|\eta_c) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in \Phi_d} \overline{\tau(\chi)} y_{\mathbb{K}}(\chi|\eta_d) \end{aligned} \quad (6.84)$$

em que a última igualdade seguiu do lema 6.3.3. Por outro lado, das proposições 6.2.3 e 6.1.3,

$$\eta_d = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in X} y_{\mathbb{K}}(\chi|\eta_d) \overline{\tau(\chi)} = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{c \in \mathcal{D}(n)} \sum_{\chi \in \Phi_c} y_{\mathbb{K}}(\chi|\eta_d) \overline{\tau(\chi)} = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\chi \in \Phi_d} y_{\mathbb{K}}(\chi|\eta_d) \overline{\tau(\chi)} \quad (6.85)$$

em que a última igualdade também se deve ao lema 6.3.3. Isso comprova que $\epsilon_d(T) = \eta_d$. $\square$

Devido ao lema anterior, $\epsilon_d(T) = \eta_d$. Assim, se $rk_{\mathbb{Z}}(M)$ denota o posto do $\mathbb{Z}$ -módulo M , então

$$rk_{\mathbb{Z}}(\mathbb{Z}[G]\eta_d) = rk_{\mathbb{Z}}(\mathbb{Z}[G]\epsilon_d) = \#\Phi_d. \quad (6.86)$$

De acordo com a construção que fizemos é ainda possível explicitar $\mathbb{K}$ por meio de uma soma direta:

Proposição 6.3.2. *Com as notações anteriores,*

$$\mathbb{K} = \mathbb{Q}[G]T = \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Q}[G]\eta_d. \quad (6.87)$$

Demonstração. A primeira igualdade já foi demonstrada (proposição 6.3.1). Mostremos a outra igualdade. Considere $\mathbb{L}_d \triangleq \mathbb{Q}[G]\eta_d$. Para todo $m \in \mathbb{K}$, $m = id(m) = \sum_{\chi \in X} \epsilon_{\chi}(m) = \sum_{d \in \mathcal{D}(n)} \epsilon_d(m)$. Como $m \in \mathbb{K} = \mathbb{Q}[G]T$, então existe $\epsilon \in \mathbb{Q}[G]$ tal que $m = \epsilon(T)$. Então, pelo fato de $\mathbb{Q}[G]$ ser comutativo e pelo lema 6.3.7, $m = \sum_{d \in \mathcal{D}(n)} \epsilon_d(\epsilon(T)) = \sum_{d \in \mathcal{D}(n)} \epsilon(\epsilon_d(T)) = \sum_{d \in \mathcal{D}(n)} \epsilon(\eta_d)$. Portanto, $m \in \sum_{d \in \mathcal{D}(n)} \mathbb{L}_d$. Reciprocamente, como $\eta_d \in \mathbb{K}$, então $\sum_{d \in \mathcal{D}(n)} \mathbb{L}_d \subset \mathbb{K}$. Portanto, $\mathbb{K} = \sum_{d \in \mathcal{D}(n)} \mathbb{L}_d$. Falta mostrar que a soma é direta. Para isso, considere $\sum_{d \in \mathcal{D}(n)} \mu_d(\eta_d) = 0$, com $\mu_d \in \mathbb{Q}[G]$ e $\mu_d(\eta_d) \in \mathbb{L}_d$. Mostremos que cada parcela é zero. De fato, note que $\mu_d(\eta_d) = \mu_d(\epsilon_d(T)) = \epsilon_d(\mu_d(T))$ e, então, para cada $d \in \mathcal{D}(n)$,

$$0 = \epsilon_d(0) = \epsilon_d\left(\sum_{i \in \mathcal{D}(n)} \mu_i(\eta_i)\right) = \epsilon_d\left(\sum_{i \in \mathcal{D}(n)} \epsilon_i(\mu_i(T))\right) = \sum_{i \in \mathcal{D}(n)} \epsilon_d \circ \epsilon_i(\mu_i(T)). \quad (6.88)$$

Pela idempotência dos ϵ_i (consequência da proposição 6.2.1), então

$$0 = \sum_{i \in \mathcal{D}(n)} \epsilon_d \circ \epsilon_i(\mu_i(T)) = \epsilon_d^2(\mu_d(T)) = \epsilon_d(\mu_d(T)) = \mu_d(\eta_d). \quad (6.89)$$

Portanto, $\mu_d(\eta_d) = 0$, donde segue finalmente que a soma $\mathbb{K} = \sum_{d \in \mathcal{D}(n)} \mathbb{L}_d$ é direta. $\square$

Comparavelmente à proposição anterior, mostraremos no Teorema de Leopoldt-Letl que o anel de inteiros de um corpo de números abeliano $\mathbb{K}$ é $\bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d$ (notações anteriores mantidas). Antes de partir para a demonstração efetiva deste teorema, precisamos de mais dois lemas:

Lema 6.3.8. *Sejam $n \in \mathbb{N}$ e p um número primo. Considere ζ uma raiz np -ésima da unidade que não é uma raiz n -ésima da unidade. Considere ainda $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ e*

$$M \triangleq \{\tau \in \text{Gal}(\mathbb{Q}(\zeta_{np}) : \mathbb{Q}) : \tau|_{\mathbb{Q}(\zeta_n)} = \sigma\}. \quad (6.90)$$

Então

$$\sum_{\tau \in M} \tau(\zeta) = \begin{cases} 0, & \text{se } p \mid n; \\ -\text{Frob}(p)^{-1}\sigma(\zeta^p), & \text{se } p \text{ não divide } n \end{cases} \quad (6.91)$$

onde $\text{Frob}(p) \in \text{Gal}(\mathbb{Q}(\zeta_{np}) : \mathbb{Q})$ é tal que $\text{Frob}(p)|_{\mathbb{Q}(\zeta_n)} = \sigma_p \in \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$.

Demonstração. Como $\sigma \in G^{(n)}$, existe $k \in \mathbb{Z}_n^*$ tal que $\sigma = \sigma_k$. Suponha que $p \mid n$. Cada $\tau_i \in G^{(np)}$ é tal que $\tau_i(\zeta) = \zeta^i$, para $0 < i < np$ e $\text{mdc}(i, np) = 1$. Pela definição de M , $\tau_i \in M$ se, e somente se, $\tau_i(\zeta_n) = \sigma_k(\zeta_n) = \zeta_n^k$. Assim,

$$\tau_i(\zeta_n) = \zeta_n^k \iff \tau_i(\zeta)^p = \zeta_n^k \iff \zeta_n^i = \zeta_n^k \iff i = k + jn \quad (6.92)$$

em que $0 \leq j < p$, pois $0 < i < np$ e podemos assumir $0 < k < n$. Mais ainda, note que $\text{mdc}(i, n) = \text{mdc}(k + jn, pn) = 1$, pois $p \mid n$ e $\text{mdc}(k, n) = 1$. Portanto, $\tau_i \in M$ se, e só se, $\tau_i(\zeta) = \zeta^{k+jn}$, com $0 \leq j < p$. Além disso,

$$\sum_{j=0}^{p-1} (\zeta^n)^j = \sum_{j=0}^{p-1} \zeta_p^j = 1 + \sum_{j=1}^{p-1} \zeta_p^j = 1 + \text{Tr}(\zeta_p) = 1 - 1 = 0. \quad (6.93)$$

Logo,

$$\sum_{\tau \in M} \tau(\zeta) = \sum_{j=0}^{p-1} \zeta^{k+jn} = \zeta^k \sum_{j=0}^{p-1} (\zeta^n)^j = 0 \quad (6.94)$$

comprovando a primeira parte deste lema. Agora, suponha que p não divide n . Analogamente ao que foi feita acima, tem-se que $\tau_i \in M$ se, e só se, $i = k + jn$ e $\text{mdc}(i, pn) = \text{mdc}(k + jn, pn) = 1$, ou seja, $i = k + jn$ e $\text{mdc}(k + jn, p) = 1$ (pois p não divide n). Assim,

$$\begin{aligned} \sum_{\tau \in M} \tau(\zeta) &= \sum_{\substack{0 \leq j < p \\ k+jn \not\equiv 0 \pmod{p}}} \zeta^{k+jn} = \zeta^k \sum_{\substack{j=0 \\ k+jn \not\equiv 0 \pmod{p}}}^{p-1} (\zeta^n)^j = \zeta^k \sum_{\substack{j=0 \\ k+jn \not\equiv 0 \pmod{p}}}^{p-1} \zeta_p^j = \\ &= \zeta^k \left[\sum_{\substack{j=0 \\ k+jn \not\equiv 0 \pmod{p}}}^{p-1} \zeta_p^j + \sum_{\substack{j=0 \\ k+jn \equiv 0 \pmod{p}}}^{p-1} \zeta_p^j - \sum_{\substack{j=0 \\ k+jn \equiv 0 \pmod{p}}}^{p-1} \zeta_p^j \right] = \zeta^k \left[\text{Tr}(\zeta_p) + 1 - \sum_{\substack{j=0 \\ k+jn \equiv 0 \pmod{p}}}^{p-1} \zeta_p^j \right] = \\ &= -\zeta^k \sum_{\substack{j=0 \\ k+jn \equiv 0 \pmod{p}}}^{p-1} \zeta_p^j = - \sum_{\substack{j=0 \\ k+jn \equiv 0 \pmod{p}}}^{p-1} \zeta^{k+jn} = -\zeta^{k+j_0n} \end{aligned} \quad (6.95)$$

em que $j_0 \in \{0, 1, \dots, p-1\}$ e $k + j_0n \equiv 0 \pmod{p}$. Note que a última igualdade segue do fato de que a equação $k + xn \equiv 0 \pmod{p}$ possui única solução j_0 para $0 \leq x < p$ (consulte o teorema 2.8 de [31]). Logo $p \mid k + j_0n$ e, então, $(k + j_0n)/p \equiv kp^{-1} \pmod{n}$, donde segue que $-\zeta^{k+j_0n} = -(\zeta^p)^{kp^{-1}} = -\text{Frob}(p)^{-1}(\sigma_k(\zeta^p))$. $\square$

Lema 6.3.9. Mantidas as notações anteriores, sejam $d \in \mathcal{D}(n)$ tal que $\Phi_d \neq \emptyset$ e $U \triangleq \text{Gal}(\mathbb{Q}^{(d)} : \mathbb{K}_d)$.

Assim, existe um subconjunto $B \subset \text{Gal}(\mathbb{Q}^{(d)} : \mathbb{Q}) = G^{(d)}$ tal que $BU = B$ e $\mathbb{Z}[G^{(d)}]\zeta_d = \bigoplus_{\beta \in B} \beta(\zeta_d)\mathbb{Z}$.

Demonstração. Pela proposição 6.1.6, como $\Phi_d \neq \emptyset$ então $\langle \Phi_d \rangle = X \cap X^{(d)} = \{\chi \in X : f_\chi \mid d\}$. Devido à relação biunívoca existente entre caracteres e corpos abelianos, podemos associar o corpo $\mathbb{K}_d = \mathbb{K} \cap \mathbb{Q}(\zeta_d)$ ao grupo de caracteres $X \cap X^{(d)} = \langle \Phi_d \rangle$. Denote $d_0 = z \prod_{\substack{2 \neq p \mid n \\ p \text{ primo}}} p$, em que $z = 1$, se $v_2(d) \leq 2$, ou $z = 4$, se $v_2(d) \geq 3$ (lembrando que $v_2(d)$ denota o maior expoente x de 2 tal que $2^x \mid d$). Suponha que $d \not\equiv 4 \pmod{8}$. Pelos resultados da seção 5.5, tem-se que $X^{(p)} \simeq \widehat{\mathbb{Z}}_p^* = \langle \omega_p \rangle$. Como $d \not\equiv 4 \pmod{8}$ então d é ímpar (I) ou $d = 8x$ (II), em que $x \in \mathbb{Z}$ (pois $d \equiv 2 \pmod{4}$ não ocorre, já que $d \in \mathcal{D}(n)$). No caso (I), tem-se que d_0 é um produto de primos ímpares divisores de n . Assim, lembrando que $\Omega^{(m)}$ denota os caracteres de primeiro tipo módulo m , tem-se que $\Omega^{(d)} = \prod_{2 \neq p \mid d} \langle \omega_p \rangle = \prod_{2 \neq p \mid n} \langle \omega_p \rangle = \prod_{2 \neq p \mid d_0} \langle \omega_p \rangle = \Omega^{(d_0)}$. No caso (II), tem-se que $d_0 = 4 \prod_{2 \neq p \mid n} p$. É claro que os primos que dividem d e d_0 coincidem, pois $d \in \mathcal{D}(n)$. Portanto, $\Omega^{(d)} = \prod_{p \mid d} \langle \omega_p \rangle = \prod_{p \mid d_0} \langle \omega_p \rangle = \Omega^{(d_0)}$. Em ambos os casos (I) e (II) obtemos $\Omega^{(d)} = \Omega^{(d_0)} = X^{(d_0)}$. Logo, se $d \not\equiv 4 \pmod{8}$ então $\mathbb{Q}^{(d_0)}$ está associado a $\Omega^{(d)}$. Note também que $d_0 \mid d$ nesses casos. Suponha agora que $d \equiv 4 \pmod{8}$, ou seja, que $d = 4x$, com x ímpar. Neste caso, d_0 é o produto dos primos ímpares divisores de n . Como $d \in \mathcal{D}(n)$ então $d_0 \mid d$. Também $X^{(d_0)} = \prod_{2 \neq p \mid n} \langle \omega_p \rangle$, isto é, $\mathbb{Q}^{(d_0)}$ está associado a $\prod_{2 \neq p \mid n} \langle \omega_p \rangle$. Denotemos $G' \triangleq \text{Gal}(\mathbb{Q}^{(d)} : \mathbb{Q}^{(d_0)})$. Como $d_0 \mid d$ então a aplicação $f : \mathbb{Z}_d^* \leftarrow \mathbb{Z}_{d_0}^*$ tal que $f(x) = x \pmod{d_0}$, para qualquer $x \in \mathbb{Z}_d^*$, é sobrejetora e tem núcleo $\{x \in \mathbb{Z}_d^* : x \equiv 1 \pmod{d}\}$. Pelo Teorema do Homomorfismo e pelo Teorema Fundamental de Galois (teorema 1.1.1), tem-se que $G' \simeq G^{(d)}/G^{(d_0)} \simeq \mathbb{Z}_d^*/\mathbb{Z}_{d_0}^* \simeq \ker(f)$. Portanto,

$$G' = \text{Gal}(\mathbb{Q}^{(d)} : \mathbb{Q}^{(d_0)}) = \{\sigma_t : t \in \mathbb{Z}_d^* \text{ e } t \equiv 1 \pmod{d_0}\}. \quad (6.96)$$

Mostremos que $U \cap G' = \{id\}$, em que id é o automorfismo identidade de G' . Seja $\sigma \in U \cap G'$. Devido à proposição 5.1.5, para mostrar que $\sigma = id$, basta mostrar que $\chi(\sigma) = 1$, para qualquer $\chi \in X^{(d)}$. Seja $\chi \in X^{(d)}$. Como $\mathbb{Q}^{(d_0)}$ está associado a $\Omega^{(d)}$ ou a $\Omega^{(d)}/Z$ (Z definido como na proposição 6.1.6) então $G' \simeq \Psi(d) \times Z$. Utilizando a projeção $\pi : X^{(d)} \rightarrow \Psi^{(d)} \times Z$ e a sobrejetividade de $\pi|_{X \cap X^{(d)}}$, a proposição 6.1.6 nos leva a concluir que $\chi(\sigma) = \pi(\chi)(\sigma) = \pi(\chi_0)(\sigma) = \chi_0(\sigma)$, para algum $\chi_0 \in X \cap X^{(d)}$. Como $\sigma \in U$ e $X \cap X^{(d)}$ é trivial em U então $\chi_0(\sigma) = 1$, ou seja, $\chi(\sigma) = 1$, para todo $\chi \in X^{(d)}$. Portanto, $U \cap G' = \{id\}$. Considere $R : G^{(d)} \rightarrow G^{(d_0)}$ o homomorfismo restrição dado por $R(\sigma) = \sigma|_{\mathbb{Q}^{(d_0)}}$. Claramente $\ker(R) = G'$. Assim, $R : U \rightarrow G^{(d_0)}$ tem núcleo $G' \cap U = \{id\}$, donde segue que $R : U \rightarrow G^{(d_0)}$ é injetora. Afirmamos que existem $k_1, \dots, k_l \in G^{(d)}$ tais que $U' = \dot{\cup}_{i=1}^l k_i U$ (união disjunta). De fato, seja $H = R(U)$. Como $G^{(d_0)}$ é abeliano então H é normal nesse grupo. Portanto, $G^{(d_0)}/H = \{\tau_1, \dots, \tau_l\}$ é um grupo. Se $\tau : \mathbb{Q}^{(d_0)} \rightarrow \mathbb{Q}^{(d_0)}$ é um $\mathbb{Q}$ -automorfismo então $\tau : \mathbb{Q}^{(d_0)} \rightarrow \mathbb{Q}^{(d)}$ é um $\mathbb{Q}$ -monomorfismo ($d_0 \mid d$). Da teoria de Galois, existe um $\mathbb{Q}$ -automorfismo $\sigma : \mathbb{Q}^{(d)} \rightarrow \mathbb{Q}^{(d)}$ tal que $\sigma|_{\mathbb{Q}^{(d_0)}} = \tau$. Logo, $R(\sigma) = \tau$. Assim, $R : G^{(d)} \rightarrow$

$G^{(d_0)}$ é um homomorfismo sobrejetor. Sejam $k_1, \dots, k_l \in G^{(d)}$ tais que $R(k_i) = \tau_i$ ($1 \leq i \leq l$) e $U' = \dot{\cup}_{i=1}^l k_i U$. Inicialmente, veja que essa união é disjunta. De fato, se $\sigma \in k_i U \cap k_j U$ ($i \neq j$) então $\sigma = k_i u_1 k_j u_2$, em que $u_1, u_2 \in U$. Assim, por R estar bem definida e ser um homomorfismo segue que $\tau_i R(u_1) = R(k_i) R(u_1) = R(k_j) R(u_2) = \tau_j R(u_2) \in \tau_i R(u) \cap \tau_j R(u) = \emptyset$, o que é um absurdo. Portanto, $\sigma \in k_i U \cap k_j U$. Pela disjunção da união U' e pela definição de homomorfismo aplicada a R vê-se facilmente que $R : U' \rightarrow G^{(d_0)}$ é bijetora. Note agora que $G^{(d)} = U' G'$. De fato, isso segue do Teorema Fundamental de Galois e da afirmação anterior. Além disso, cada $\sigma \in G^{(d)}$ se escreve de maneira única como $\sigma = v\tau$, em que $v \in U'$ e $\tau \in G'$. Sejam $p_1, \dots, p_r$ os primos distintos que dividem d/d_0 e $e_i = v_{p_i}(d)$. Seja também

$$c_i = v_{p_i}(d_0) = \begin{cases} 1, & \text{se } p_i \neq 2; \\ 0, & \text{se } p_i = 2 \text{ e } v_2(d) = 1 \text{ ou } 2; \\ 2, & \text{se } p_i = 2 \text{ e } v_2(d) \geq 3. \end{cases} \quad (6.97)$$

Observe que $e_i > c_i$. Para cada $i \in \{1, \dots, r\}$, considere $H_i \triangleq \text{Gal}(\mathbb{Q}^{(p_i^{e_i})} : \mathbb{Q}^{(p_i^{c_i})})$ e $H'_i \subset H_i$ um conjunto de representantes para $\text{Gal}(\mathbb{Q}^{(p_i^{e_i-1})} : \mathbb{Q}^{(p_i^{c_i})})$. Como $G^{(d)} = \prod_{\substack{p|d \\ p \text{ primo}}} G^{(p^{v_p(d)})}$, considere a inclusão (homomorfismo injetor) $\lambda : \prod_{i=1}^r G^{(p_i^{e_i-1})} \rightarrow G^{(d)}$. Como $H_i < G^{(p_i^{e_i})}$, podemos considerar o grupo $G' = \lambda(\prod_{i=1}^r H_i)$. Considere ainda $H = \lambda(\prod_{i=1}^r H_i/H'_i)$ e $B = U'H$. Como $H \subset G^{(d)}$ e $U' \subset G^{(d)}$ então $B \subset G^{(d)}$. Pelo fato de id pertencer a U então $B \subset BU$. Agora, tomando $bu \in BU$ ($b \in B, u \in U$) vê-se que $bu \in BU'H = B$, pois, tomando algum k_i como identidade, vê-se que $u \in U'$ e $u.1 \in U'H$. Portanto, $BU = B$. Falta mostrar que $\mathbb{Z}[G^{(d)}]\zeta_d = \bigoplus_{\beta \in B} \beta(\zeta_d)\mathbb{Z}$. Devido à construção acima e considerando $\Lambda^{(d)} \triangleq \{\chi \in X^{(d)} : q(f_\chi) = q(d)\}$, tem-se que

$$\#(B) = \varphi(d_0) \prod_{i=1}^r \varphi(p_i^{e_i-c_i}) = \#(\Lambda^{(d)}) = rk_{\mathbb{Z}} \mathbb{Z}[G^{(d)}]\zeta_d \quad (6.98)$$

em que o segundo termo da igualdade não considera $p_i = 2$ se $d \equiv 4 \pmod{8}$. Portanto, resta mostrar que $\sigma(\zeta_d) \in \sum_{\beta \in B} \beta(\zeta_d)\mathbb{Z}$ para qualquer $\sigma \in G^{(d)}$. Seja $\sigma = v\lambda(\tau_1, \dots, \tau_r)$, em que $v \in U'$ e $\tau_i \in H_i$. Considere ainda

$$M_i \triangleq \begin{cases} \{\rho \in H_i : \rho|_{\mathbb{Q}^{(p_i^{e_i-1})}} = \tau_i|_{\mathbb{Q}^{(p_i^{e_i-1})}}\} - \{\tau_i\}, & \text{se } \tau_i \in H'_i; \\ \{\tau_i\}, & \text{se } \tau_i \notin H'_i. \end{cases} \quad (6.99)$$

Note que, em ambos os casos, $M_i \subset H_i/H'_i$. Seja $i \in \{1, 2, \dots, r\}$ tal que $\tau_i \in H'_i$. Do lema 6.3.8, tem-se $\sigma(\zeta_d) = -\sum_{\rho \in M_i} v\lambda(\tau_1, \dots, \rho, \dots, \tau_r)(\zeta_d)$ em que ρ ocupa a i -ésima posição da r -upla acima. Usando essa igualdade para todo i com $\tau_i \in H'_i$ e denotando por k o número de índices i entre 1 e r

tais que $\tau_i \in H'_i$, conclui-se que

$$\sigma(\zeta_d) = (-1)^k \sum_{\rho_1 \in M_1, \dots, \rho_r \in M_r} v\lambda(\rho_1, \dots, \rho_r)(\zeta_d) \in \sum_{\beta \in B} \beta(\zeta_d)\mathbb{Z}. \quad (6.100)$$

Com isso, finalmente verificamos que $\mathbb{Z}[G^{(d)}]\zeta_d = \bigoplus_{\beta \in B} \beta(\zeta_d)\mathbb{Z}$. $\square$

Enfim, abaixo enunciamos e demonstramos o Teorema de Leopoldt-Lettl:

Teorema 6.3.1 (Teorema de Leopoldt-Lettl). *Sejam $\mathbb{K}$ um corpo de números abeliano de condutor n , $G = \text{Gal}(\mathbb{K} : \mathbb{Q})$, η_d definido como na equação 6.64, T definido como na equação 6.78 e $R_{\mathbb{K}}$ a $\mathbb{Z}$ -ordem definida pela fórmula 6.81. Assim, o anel de inteiros de $\mathbb{K}$ é dado por*

$$\mathcal{O}_{\mathbb{K}} = \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d = R_{\mathbb{K}}(T). \quad (6.101)$$

Demonstração. Mostremos inicialmente que a segunda igualdade é verdadeira. Por um lado, como o conjunto $\{\epsilon_\chi : \chi \in X\}$ é uma família de idempotentes ortogonais e como $\Phi_{d_1} \cap \Phi_{d_2} = \emptyset$ se $d_1 \neq d_2$, então $\{\epsilon_d : d \in \mathcal{D}(n)\}$ também é uma família de idempotentes ortogonais. Além disso, $\sum_{d \in \mathcal{D}(n)} \epsilon_d = \sum_{\chi \in X} \epsilon_\chi = 1$ e $\epsilon_d \in \mathbb{Q}[G]$. Assim, para qualquer $x \in \sum_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d$, existem $a_d \in \mathbb{Z}[G]$ tais que $x = \sum_{d \in \mathcal{D}(n)} a_d \eta_d = \sum_{d \in \mathcal{D}(n)} a_d \epsilon_d(T) = \left(\sum_{d \in \mathcal{D}(n)} a_d \epsilon_d \right)(T)$, ou seja, $x \in R_{\mathbb{K}}(T)$. Portanto, $\sum_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d \subset R_{\mathbb{K}}(T)$. Por outro lado, considere $x \in R_{\mathbb{K}}(T)$. Como $\epsilon_d^2 = \epsilon_d$ então $\epsilon^m = \epsilon$ para qualquer natural $m \geq 2$. Assim, $x = (a + \sum_{d \in \mathcal{D}(n)} a_d \epsilon_d)(T)$, em que $a, a_d \in A$, para todo $d \in \mathcal{D}(n)$ (note que na expressão de x não aparecem outras potências de ϵ_d pelo que foi comentado antes nem produtos mistos $\epsilon_{d_1} \epsilon_{d_2}$, pois quando $d_1 \neq d_2$ tem-se que $\epsilon_{d_1} \epsilon_{d_2} = 0$). Além disso, $\sum_{d \in \mathcal{D}(n)} \epsilon_d = 1$ implica que $\left(\sum_{d \in \mathcal{D}(n)} \epsilon_d \right)(T) = T$, donde segue que $\sum_{d \in \mathcal{D}(n)} \eta_d = T$. Logo, $x = a(T) + \sum_{d \in \mathcal{D}(n)} a_d \epsilon_d(T) = a \left(\sum_{d \in \mathcal{D}(n)} \eta_d \right) + \sum_{d \in \mathcal{D}(n)} a_d \eta_d = \sum_{d \in \mathcal{D}(n)} (a + a_d) \eta_d$, donde segue que $x \in \sum_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d$. Portanto, $R_{\mathbb{K}}(T) = \sum_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d$. Para mostrar que a soma é direta, sejam $d_1 \neq d_2 \in \mathcal{D}(n)$. Se $x \in \mathbb{Z}[G]\eta_{d_1} \cap \mathbb{Z}[G]\eta_{d_2}$ então $x = a\eta_{d_1} = b\eta_{d_2}$, com $a, b \in \mathbb{Z}[G]$. Assim, $a\epsilon_{d_1}(T) = b\epsilon_{d_2}(T)$. Multiplicando por $\epsilon_{d_1}(T)$ tem-se que $a\epsilon_{d_1}(T) = a\epsilon_{d_1}^2(T) = b(\epsilon_{d_2}\epsilon_{d_1})(T) = 0$. Portanto, $x = a\epsilon_{d_1}(T) = 0$, donde segue que $\mathbb{Z}[G]\eta_{d_1} \cap \mathbb{Z}[G]\eta_{d_2} = \{0\}$ se $d_1 \neq d_2$. Em suma, comprovamos até agora que $\bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d = R_{\mathbb{K}}(T)$. Por sua vez, $\eta_d \in \mathcal{O}_{\mathbb{K}}$. De fato, como $\eta_d = \text{Tr}_{\mathbb{Q}^{(d)} : \mathbb{Q}^{(d)} \cap \mathbb{K}}(\eta_d)$ e como $\eta_d \in \mathcal{O}_{\mathbb{Q}^{(d)}}$, o corolário 2.2.2 garante que $\eta_d \in \mathcal{O}_{\mathbb{K}}$. Nessas circunstâncias, também $\sigma(\eta_d) \in \mathcal{O}_{\mathbb{K}}$, para todo $\sigma \in \text{Gal}(\mathbb{K} : \mathbb{Q})$. Logo, $\mathbb{Z}[G]\eta_d \subset \mathcal{O}_{\mathbb{K}}$, donde segue que $\bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d \subset \mathcal{O}_{\mathbb{K}}$. Falta somente mostrar que $\mathcal{O}_{\mathbb{K}} \subset \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d$. Para isso, consideraremos dois casos. No primeiro caso, suponha que $\mathbb{K}$ é um corpo ciclotômico, ou seja, que $\mathbb{K} = \mathbb{Q}^{(n)}$. Neste caso, $G = G^{(n)}$. Para cada $d \in \mathcal{D}(n)$, tem-se que $\mathbb{K}_d = \mathbb{Q}^{(n)} \cap \mathbb{Q}^{(d)} = \mathbb{Q}^{(d)}$ e que $\eta_d = \text{Tr}_{\mathbb{Q}^{(d)} : \mathbb{Q}^{(d)}} \eta_d = \eta_d$, ou seja, $\eta_d = \zeta_d$.

Mostremos que $\zeta_n^k \in \mathbb{Z}[G]\eta_d \subset \mathcal{O}_{\mathbb{K}}$ para qualquer $k \in \mathbb{N}$. Com efeito, sejam $\alpha = \text{mdc}(n, k)$, $k_0 = k/\alpha$ e $n_0 = n/\alpha$. Assim, $\text{mdc}(k_0, n_0) = \text{mdc}(k_0, n) = 1$. Então, se $n_0 \not\equiv 2 \pmod{4}$ então $\zeta_n^k = \zeta_{n_0}^{k_0}$. Caso $n_0 \equiv 2 \pmod{4}$ (n_0 ímpar) então $\zeta_n^k = \zeta_{n_0}^{k_0} = \pm \zeta_{n_0/2}^{k_0}$. Por isso, podemos assumir $n_0 \not\equiv 2 \pmod{4}$ e tomar $\zeta_n^k = \pm \zeta_{n_0}^{k_0}$. Considerando $d = q(n_0) \prod_{p|n, p \nmid 2n_0} p \in \mathcal{D}(n)$ tem-se que $n_0 \mid d$. Pelo lema 6.3.8, obtém-se que

$$\text{Tr}_{\mathbb{Q}^{(d)}:\mathbb{Q}^{(n_0)}}(\zeta_d) = \prod_{p|d/n_0} (-\text{Frob}(p)^{-1}) (\zeta_{n_0}) = \mu\left(\frac{d}{n_0}\right) \sigma_l(\zeta_{n_0}) \quad (6.102)$$

para algum $\sigma_l \in G^{(d)}$. Então $\zeta_n^k = \pm \sigma_{k_0} \sigma_l^{-1} (\text{Tr}_{\mathbb{Q}^{(d)}:\mathbb{Q}^{(n_0)}} \zeta_d) \in \mathbb{Z}[G^{(d)}]\zeta_d = \mathbb{Z}[G^{(n)}]\zeta_d$. Agora, suponha que $\mathbb{K}$ é um corpo de números abeliano qualquer de condutor n e tome $\alpha \in \mathcal{O}_{\mathbb{K}}$. Como vimos que o teorema vale para $\mathbb{Q}^{(n)}$ então $\alpha = \sum_{d \in \mathcal{D}(n)} \alpha_d$, em que $\alpha_d \in \mathbb{Z}[G^{(d)}]\zeta_d$. Como $\mathbb{Q}^{(n)} = \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Q}[G^{(d)}]\zeta_d$ então tais α_d são determinados de maneira única. Se $\Phi_d = \emptyset$ então $\alpha_d = 0$. Senão $\alpha_d = \epsilon_d(\alpha) \in \mathbb{Q}[G]\eta_d \subset \mathbb{Q}[G^{(d)}]\zeta_d$. Além disso, α_d é fixo por $\text{Gal}(\mathbb{Q}^{(d)} : \mathbb{K}_d)$. Por isso, só falta mostrar que para qualquer $d \in \mathcal{D}(n)$ tal que $\Phi_d \neq \emptyset$, se $x \in \mathbb{Z}[G^{(d)}]\zeta_d$ é fixo por $U = \text{Gal}(\mathbb{Q}^{(d)} : \mathbb{K}_d)$ então $x \in \mathbb{Z}[G]\eta_d$. Com efeito, pelo lema 6.3.9, sabemos que existe $B \subset G^{(d)}$ tal que $BU = B$ e $x = \sum_{\beta \in B} x_\beta \beta(\zeta_d)$ com x_β unicamente determinado em $\mathbb{Z}$. Para qualquer $\tau \in U$, $\tau^{-1}(x) = x$ e $BU = B$ implica que $x_{\tau\beta} = x_\beta$. Escolhendo $B' \subset B$ tal que $B = \bigcup_{\beta \in B'} \beta U$, finalmente obtém-se que

$$x = \sum_{\beta \in B'} x_\beta \left(\sum_{\tau \in U} \tau \beta(\zeta_d) \right) = \sum_{\beta \in B'} x_\beta \beta(\eta_d) \in \mathbb{Z}[G]\eta_d. \quad (6.103)$$

Isso mostra, enfim, que $\mathcal{O}_{\mathbb{K}} \subset \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d$, concluindo a prova. $\square$

Corolário 6.3.1. Com as notações anteriores, $T \in \mathcal{O}_{\mathbb{K}}$. $\square$

Exemplo 6.3.1. Seja $\mathbb{K}$ um corpo de números abeliano com condutor n , em que n é ímpar e livre de quadrados. Dessa forma, $n = \prod_{i=1}^r p_i$, sendo cada p_i um primo ímpar. Nessas condições, $\mathcal{D}(n) = \{n\}$. Além disso, $\mathbb{K}_n = \mathbb{K} \cap \mathbb{Q}^{(n)} = \mathbb{K}$ e $T = \eta_n = \text{Tr}_{\mathbb{Q}^{(n)}:\mathbb{K}}(\zeta_n)$. Portanto,

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[G]T = \mathbb{Z}[G]\text{Tr}_{\mathbb{Q}^{(n)}:\mathbb{K}}(\zeta_n) \quad (6.104)$$

isto é, $\mathbb{K}$ admite base integral normal. Note que isto fornece outra prova para a proposição 4.2.3 ou para a implicação (c) $\implies$ (a) do Teorema de Hilbert-Speiser (teorema 4.2.1).

Exemplo 6.3.2. Seja $\mathbb{K}$ um corpo de números de grau p (primo ímpar) com condutor $n = p^2 p_1 p_2 \dots p_r$, em que os p_i são primos ímpares distintos entre si e distintos de p . Neste caso, $\mathcal{D}(n) = \{pp_1 p_2 \dots p_n, n\}$. Denotemos $d = pp_1 p_2 \dots p_n$. Como o grau de $\mathbb{K}$ é primo, então $\mathbb{K}_d = \mathbb{K} \cap \mathbb{Q}^{(d)}$ deve ser $\mathbb{K}$ ou $\mathbb{Q}$. Como o condutor de $\mathbb{K}$ é n , então a primeira opção não pode ocorrer, pois, caso contrário, $\mathbb{K}$ estaria

contido em $\mathbb{Q}^{(d)}$. Dessa forma, $\mathbb{K}_d = \mathbb{Q}$. Neste caso, $\eta_d = \text{Tr}_{\mathbb{Q}^{(d)}:\mathbb{Q}}\zeta_d = -1$ (calculado na seção 3.2). Então, como $\eta_n = \text{Tr}_{\mathbb{Q}^{(n)}:\mathbb{K}}(\zeta_n)$ (exemplo 6.3.1), temos

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[G](-1) \oplus \mathbb{Z}[G]\text{Tr}_{\mathbb{Q}^{(n)}:\mathbb{K}}(\zeta_n) = \mathbb{Z} \oplus \mathbb{Z}[G]\text{Tr}_{\mathbb{Q}^{(n)}:\mathbb{K}}(\zeta_n). \quad (6.105)$$

Conclusão

Como vimos, o Teorema de Leopoldt-Lettl, apresentado e demonstrado na última seção, fornece o anel de inteiros de qualquer corpo de números abeliano como soma direta de $\mathbb{Z}$ -módulos. Nas primeiras seções, estudamos as classes de ramos e os caracteres coordenados de Leopoldt, fundamentais na prova do principal teorema deste capítulo sob o enfoque considerado. Ressaltamos que o detalhamento cuidadoso do artigo [20] foi o maior desafio vencido no processo de produção desta dissertação. Os resultados da primeira seção deste capítulo foram demonstrados no referido artigo, mas aqui tivemos o objetivo de detalhá-los ao máximo. Por sua vez, a maior parte dos resultados da segunda seção e os primeiros da terceira seção foram apenas mencionados no artigo citado e, aqui, receberam demonstrações detalhadas.

Capítulo 7

Reticulados algébricos

Neste capítulo apresentamos uma aplicação da teoria desenvolvida nesta dissertação. Reticulados são conjuntos de $\mathbb{R}^n$ atualmente muito utilizados na teoria dos Códigos Corretores de Erros e na Criptografia. Nosso objetivo nesta última parte da dissertação é definir reticulados, enunciar o problema do empacotamento esférico, descrever o que são reticulados algébricos e apresentar construções de reticulados via corpos de números em algumas dimensões. As duas últimas seções deste capítulo permitirão ao leitor compreender onde é possível aplicar a teoria desenvolvida ao longo desta dissertação.

7.1 Reticulados

Definiremos nesta seção os principais conceitos relacionados a reticulados, tais como região fundamental, matriz geradora e matriz de Gram.

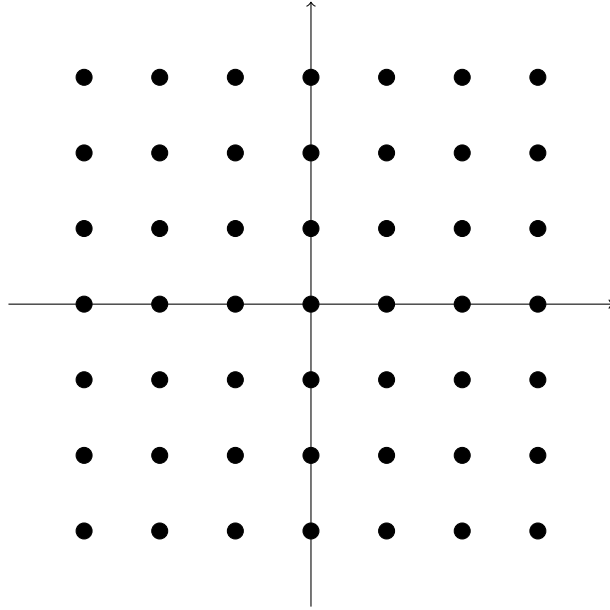
Definição 7.1.1. *Sejam $\mathbb{K}$ um corpo, $A \subset \mathbb{K}$ um anel e V um $\mathbb{K}$ -espaço vetorial de dimensão finita n . Considere ainda $\mathcal{B} = \{v_1, v_2, \dots, v_m\} \subset V$ um conjunto com m vetores linearmente independentes sobre $\mathbb{K}$ (logo, $m \leq n$). Assim, o conjunto*

$$\Lambda = \left\{ \sum_{i=1}^m a_i v_i \ : \ a_i \in A \right\} \quad (7.1)$$

*é chamado de **reticulado m -dimensional** com base $\mathcal{B}$. Se $m = n$, dizemos que Λ é um **reticulado completo**.*

Neste texto, assumiremos $\mathbb{K} = \mathbb{R}$, $V = \mathbb{R}^n$ e $A = \mathbb{Z}$. Além disso, em geral trataremos do caso em que $m = n$ e, por simplicidade, chamaremos um reticulado completo somente de reticulado.

Exemplo 7.1.1. Em $\mathbb{R}^2$, considere o reticulado $\Lambda = \{a(1,0) + b(0,1) : a, b \in \mathbb{Z}\}$, cuja base é a canônica $\{(0,1), (1,0)\}$. Assim, $\Lambda = \mathbb{Z}^2$ e, geometricamente,



em que os pontos assinalados marcam os pontos do reticulado $\mathbb{Z}^2$.

Note que um reticulado pode ter mais do que uma base. Por exemplo, veja que $\mathcal{C} = \{(2,1), (-1,3)\}$ também é uma base para o reticulado $\mathbb{Z}^2$ do exemplo 7.1.1.

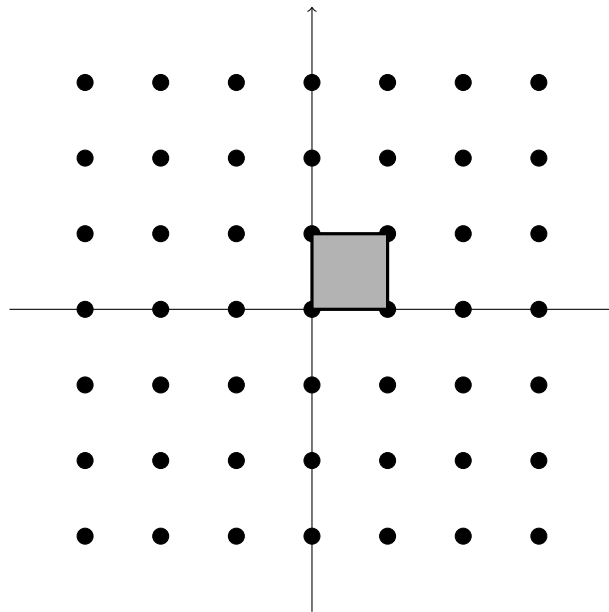
Se Λ é um reticulado de $\mathbb{R}^n$ com base $\mathcal{B}$ (com n elementos) então um conjunto linearmente independente $\mathcal{C} \subset \Lambda$ com n elementos é outra base para o reticulado Λ se, e somente se, a matriz de mudança de base de $\mathcal{B}$ para $\mathcal{C}$ é invertível (isto é, se essa matriz tem entradas inteiras e determinante ± 1).

Definição 7.1.2. Seja Λ um reticulado de $\mathbb{R}^n$ com base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$. O conjunto

$$\mathcal{P} = \left\{ \sum_{i=1}^n \lambda_i v_i : 0 \leq \lambda_i < 1 \right\} \quad (7.2)$$

é chamado de **região fundamental** do reticulado Λ .

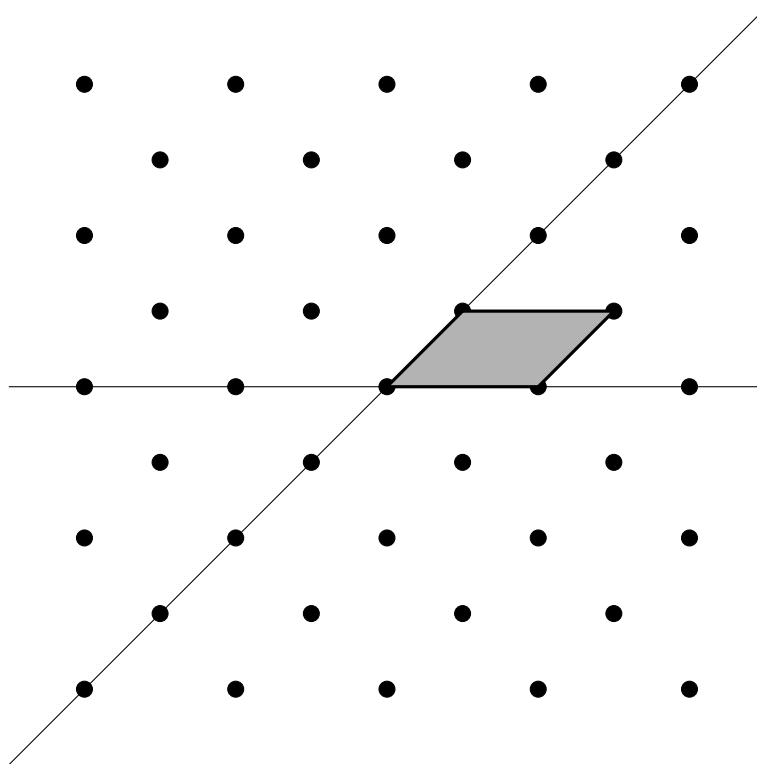
Exemplo 7.1.2. No exemplo 7.1.1, o retângulo de vértices $(0,0)$, $(0,1)$, $(1,0)$ e $(1,1)$ (hachurado abaixo) é a região fundamental do reticulado $\mathbb{Z}^2$.



Exemplo 7.1.3. Considere o reticulado de $\mathbb{R}^2$ gerado pela $\mathbb{Z}$ -base $\mathcal{B} = \{(2,0), (1,1)\}$. Explicitamente,

$$\Lambda = \{(a,b) \in \mathbb{Z}^2 : a + b \equiv 0 \pmod{2}\}. \quad (7.3)$$

Hachurando sua região fundamental, geometricamente esse reticulado é o seguinte:



A região fundamental $\mathcal{P}$ de um reticulado Λ pode ser transladada pelo espaço $\mathbb{R}^n$. Se essa translação for feita pela adição de um elemento $l \in \Lambda$ não nulo, então essa nova região não intercepta a região fundamental. Mais ainda, a proposição a seguir nos garante que todas as translação feitas

por adição dos elementos de Λ preenchem o espaço. Isso significa que o espaço $\mathbb{R}^n$ é *ladrilhado pela região fundamental* (na verdade, por suas translações).

Proposição 7.1.1. *Seja Λ um reticulado de $\mathbb{R}^n$ com região fundamental $\mathcal{P}$. Então todo elemento de $\mathbb{R}^n$ pertence a uma única região $\mathcal{P} + l$, em que $l \in \Lambda$, isto é, $\mathbb{R}^n = \dot{\bigcup}_{l \in \Lambda} \mathcal{P} + l$.*

Demonstração. Considere $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ uma base geradora de Λ . Como é linearmente independente e tem n elementos, esse conjunto também é base para o espaço vetorial $\mathbb{R}^n$. Sendo assim, todo $x \in \mathbb{R}^n$ é escrito como $x = \sum_{i=1}^n a_i v_i$, com $a_i \in \mathbb{R}$. Escrevendo cada $a_i = b_i + \theta_i$, em que b_i é a parte inteira de a_i e $0 \leq \theta_i < 1$, tem-se que $x = \sum_{i=1}^n b_i v_i + \sum_{i=1}^n \theta_i v_i$, sendo que $\sum_{i=1}^n b_i v_i \in \Lambda$ e $\sum_{i=1}^n \theta_i v_i \in \mathcal{P}$. Portanto, cada $x \in \mathbb{R}^n$ pertence a uma classe $\mathcal{P} + l$. Para ver que cada elemento de $\mathbb{R}^n$ pertence a uma única classe dessas, suponha que exista $x \in \mathbb{R}^n$ tal que $x \in (\mathcal{P} + l_1) \cap (\mathcal{P} + l_2)$, em que $l_1 = \sum_{i=1}^n a_i v_i$ e $l_2 = \sum_{i=1}^n b_i v_i$ são elementos distintos em Λ ($a_i, b_i \in \mathbb{Z}$). Assim, $x = \sum_{i=1}^n a_i v_i + \sum_{i=1}^n \theta_i v_i = \sum_{i=1}^n b_i v_i + \sum_{i=1}^n \theta'_i v_i$, em que $0 \leq \theta_i, \theta'_i < 1$. Daí,

$$\sum_{i=1}^n (a_i - b_i) v_i = \sum_{i=1}^n (\theta_i - \theta'_i) v_i. \quad (7.4)$$

Como $\mathcal{B}$ é linearmente independente então, para cada i , $a_i - b_i = \theta_i - \theta'_i$. Pelo intervalo de definição de θ_i e de θ'_i concluímos que $-1 < \theta_i - \theta'_i < 1$. Porém, $a_i - b_i \in \mathbb{Z}$, donde obrigatoriamente segue que $\theta_i - \theta'_i = 0$, ou seja, $\theta_i = \theta'_i$. Consequentemente, $a_i = b_i$. Disso segue que $l_1 = l_2$, o que é uma contradição da suposição que fizemos. Portanto, cada elemento de $\mathbb{R}^n$ está em uma única classe $\mathcal{P} + l$. $\square$

Definição 7.1.3. *Seja $H \subset \mathbb{R}^n$ um subgrupo. Dizemos que H é um **subgrupo discreto** se para qualquer conjunto compacto $\mathbb{K} \subset \mathbb{R}^n$, $H \cap \mathbb{K}$ é finito.*

Por exemplo, o conjunto $\mathbb{Z}^n$ é um subgrupo discreto de $\mathbb{R}^n$.

Proposição 7.1.2. *O conjunto dos pontos de um reticulado $\Lambda \subset \mathbb{R}^n$ é discreto.*

Demonstração. Seja $\{v_1, v_2, \dots, v_n\}$ uma base para o reticulado Λ . Considere o sistema linear homogêneo com $n - 1$ equações e n incógnitas dado por $\langle x, v_2 \rangle, \langle x, v_3 \rangle, \dots, \langle x, v_n \rangle$. Esse sistema deve possuir uma solução x não nula. Se $\langle x, v_1 \rangle = 0$ então o vetor x seria ortogonal a todos os vetores de $\mathbb{R}^n$, o que é impossível já que $x \neq 0$. Portanto, $\langle x, v_1 \rangle \neq 0$. Agora, o vetor $s_1 = x / \langle x, v_1 \rangle$ também é ortogonal a $v_2, \dots, v_n$ e satisfaz $\langle s_1, v_1 \rangle = 1$. Generalizando, podemos dizer que, para cada $1 \leq i \leq n$, existe um vetor s_i tal que $\langle s_i, v_i \rangle = 1$ e $\langle s_i, v_j \rangle = 0$ se $i \neq j$. Seja $z = \sum_{i=1}^n a_i v_i \in \Lambda$, com $a_i \in \mathbb{Z}$, um vetor pertencente a uma bola de raio r . Assim, $a_i = \langle z, s_i \rangle$ e, pela inequação de Cauchy-Schwartz,

$\|a_i\| = \|\langle z, s_i \rangle\| \leq \|z\| \|s_i\| < r \|s_i\|$. Como $r \|s_i\|$ não depende de z então existe um número finito de possibilidades para a_i . Assim, o conjunto de todos os $z \in \Lambda$ tais que $\|z\| < r$ é finito. Isso prova que a intersecção de Λ com qualquer compacto de $\mathbb{R}^n$ é finito. $\square$

Proposição 7.1.3. *Seja $H \subset \mathbb{R}^n$ um subgrupo discreto. Então H é gerado como um $\mathbb{Z}$ -módulo por $r \leq n$ vetores linearmente independentes sobre $\mathbb{R}$.*

Demonstração. Seja $\{v_1, v_2, \dots, v_r\}$ um conjunto linearmente independente sobre $\mathbb{R}$, em que $r \leq n$ é o maior possível. Considere $\mathcal{P} = \{\sum_{i=1}^r a_i v_i : 0 \leq a_i \leq 1\}$, que é obviamente um conjunto compacto em $\mathbb{R}^n$ (pois é fechado e limitado). Por hipótese, $\mathcal{P} \cap H$ é finito. Tome $x \in H$. Da maximalidade de r , segue que $x = \sum_{i=1}^r \lambda_i v_i$, em que $\lambda_i \in \mathbb{R}$. Para $j \in \mathbb{Z}$, defina $x_j \triangleq jx - \sum_{i=1}^r [j\lambda_i] v_i$, em que o símbolo $[.]$ denota a parte inteira de um número. Assim,

$$x_j = \sum_{i=1}^r (j\lambda_i - [j\lambda_i]) v_i \quad (7.5)$$

donde segue que $x_j \in \mathcal{P}$ e, pela definição de x_j , $x_j \in \mathcal{P} \cap H$. Como $x_1 = x - \sum_{i=1}^r [\lambda_i] v_i$ então $x = x_1 + \sum_{i=1}^r [\lambda_i] v_i$. Por isso, H é gerado como um $\mathbb{Z}$ -módulo por $\mathcal{P} \cap H$, já que $x_1, v_i \in \mathcal{P} \cap H$. Dessa forma, como $\mathcal{P} \cap H$ é finito, tem-se que H é um $\mathbb{Z}$ -módulo finitamente gerado. Porém, como $\mathcal{P} \cap H$ é finito e $\mathbb{Z}$ é infinito, devem existir inteiros $j \neq k$ tais que $x_j = x_k$. Assim, da definição desses elementos vemos que $(j - k)\lambda_i = [j\lambda_i] - [k\lambda_i]$ para cada i , donde segue que cada $\lambda_i \in \mathbb{Q}$. Portanto, H é um $\mathbb{Z}$ -módulo gerado por um número finito de elementos que são $\mathbb{Q}$ -combinações lineares dos v_i . Seja $d \neq 0$ um número inteiro que seja denominador comum dos coeficientes de todos os elementos de $\mathcal{P} \cap H$. Assim, $dH \subset \sum_{i=1}^r \mathbb{Z} v_i$. Sabe-se que existem uma base $\{f_1, f_2, \dots, f_r\}$ para o $\mathbb{Z}$ -módulo $\sum_{i=1}^r \mathbb{Z} v_i$ e inteiros α_i tais que $\{\alpha_1 f_1, \alpha_2 f_2, \dots, \alpha_r f_r\}$ gera dH , ou seja, $rk(dH) \leq r$. Por outro lado, como dH e H são $\mathbb{Z}$ -módulos com mesmo posto e como $\sum_{i=1}^r \mathbb{Z} v_i \subset H$ então $rk(dH) \geq r$. Portanto, o posto de dH é r e os α_i são não nulos. Logo, os f_i também são linearmente independentes sobre $\mathbb{R}$, assim como os e_i . Disso segue que dH e, por sua vez, H são $\mathbb{Z}$ -módulos gerados por r vetores linearmente independentes sobre $\mathbb{R}$. $\square$

Corolário 7.1.1. *Seja Λ um subgrupo aditivo (visto como $\mathbb{Z}$ -módulo) de $\mathbb{R}^n$. Então, Λ é um reticulado se, e somente se, Λ é um subgrupo discreto.*

Demonstração. Segue como consequência direta das proposições 7.1.2 e 7.1.3. $\square$

A seguir, faremos uma série de definições envolvendo reticulados:

Definição 7.1.4. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$. Seja $v_j = (v_{1j}, v_{2j}, \dots, v_{nj})$ a expressão em coordenadas reais de cada vetor dessa base. A matriz $M = [v_{ij}]_{1 \leq i, j \leq n}$ é chamada de **matriz geradora de Λ** .*

Nesta seção, considere μ a medida de Lebesgue em $\mathbb{R}^n$.

Definição 7.1.5. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com região fundamental $\mathcal{P}$. O **volume do reticulado** Λ é definido como sendo*

$$\text{vol}(\Lambda) \triangleq \text{vol}(\mathcal{P}) = \mu(\mathcal{P}) = \int_{\mathcal{P}} d\mu. \quad (7.6)$$

Para que a definição anterior não admita problema, é preciso mostrar que o volume de um reticulado independe da base escolhida. Faremos isso a seguir.

Proposição 7.1.4. *Se M é uma matriz geradora de um reticulado Λ então $\text{vol}(\Lambda) = |\det(M)|$.*

Demonstração. Por definição, $\text{vol}(\Lambda) = \int_{\mathcal{P}} d\mu$. Considere a transformação linear $h : \mathbb{R}^n \rightarrow \mathbb{R}^n$ dada por $h(x) = xM^T$. Como $\det(M^T) = \det(M) \neq 0$ (pois M é matriz de uma base de Λ) então h é invertível. Portanto, h é um difeomorfismo e $h'(x) = h$, para todo $x \in \mathbb{R}^n$. Além disso, $h([0, 1]^n) = \mathcal{P}$. Pelo Teorema da Mudança de Variáveis, tem-se que

$$\int_{\mathcal{P}} d\mu = \int_{h([0, 1]^n)} dx = \int_{[0, 1]^n} |\det(M^T)| dx = |\det(M^T)| = |\det(M)|. \quad (7.7)$$

□

Corolário 7.1.2. *O volume de um reticulado $\Lambda \subset \mathbb{R}^n$ independe da escolha da base $\mathcal{B}$ desse reticulado.*

Demonstração. Considere $\mathcal{B} = \{v_1, \dots, v_n\}$ e tome $\mathcal{C} = \{u_1, \dots, u_n\}$ outra base para Λ . Então $u_i = \sum_{j=1}^n a_{ij}v_j$, $a_{ij} \in \mathbb{Z}$, para todo $1 \leq i \leq n$. Assim, $A = [a_{ij}]$ é a matriz mudança de base. Portanto, $\det(A) = \pm 1$. Denote por M a matriz geradora de Λ gerada pelas coordenadas dos vetores de $\mathcal{B}$ e por M' a matriz geradora relacionada a $\mathcal{C}$. Assim, $M' = AM$. Aplicando o determinante a esta expressão, tem-se que $|\det(M')| = |\det(A)||\det(M)| = |\det(M)|$. Da proposição 7.1.4 segue que o volume do reticulado Λ independe da base escolhida. □

Definição 7.1.6. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado cuja matriz geradora é M . A **matriz de Gram** associada a M é*

$$G = M^T M. \quad (7.8)$$

Note que a matriz de Gram é sempre uma matriz simétrica. Além disso, matrizes de Gram podem ser diferentes caso mude-se a base ou a matriz geradora de um mesmo reticulado. Por exemplo, no reticulado $\mathbb{Z}^2$, verifica-se facilmente que a matriz de Gram associada à base $\{(1, 2), (-2, 1)\}$ e a matriz de Gram associada à base $\{(2, 2), (-1, 3)\}$ são diferentes (veja [3]). Em contrapartida, vale a seguinte proposição:

Proposição 7.1.5. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com matrizes de Gram G , em relação a uma base $\mathcal{B}$, e G' , em relação a uma base $\mathcal{C}$, então $\det(G) = \det(G')$.*

Demonstração. De fato, seja A a matriz mudança de base de $\mathcal{B}$ a $\mathcal{C}$. Considere M e M' as matrizes geradoras de Λ em relação às bases $\mathcal{B}$ e $\mathcal{C}$, respectivamente. Assim, $M' = AM$ e, utilizando propriedades de determinante, como $|\det(A)| = 1$, tem-se que $\det(G') = \det(M'^T M') = \det(M^T A^T A M) = \det(M^T) \det(A^T) \det(A) \det(M) = \det(M^T) \det(M) = \det(G)$. $\square$

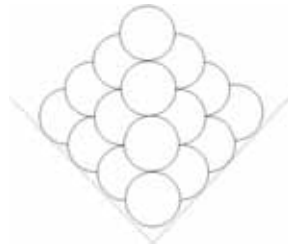
Devido à proposição anterior, justifica-se a definição a seguir:

Definição 7.1.7. *Se $\Lambda \subset \mathbb{R}^n$ é um reticulado então o **determinante** de Λ é o determinante de uma matriz de Gram de Λ . Notação: $\det(\Lambda)$.*

7.2 Empacotamento no $\mathbb{R}^n$

Um problema geométrico importante é o do empacotamento de esferas no $\mathbb{R}^n$: procura-se encontrar qual a melhor maneira, em termos de densidade, de colocar esferas idênticas maciças juntas preenchendo um espaço. Por exemplo, queremos saber quantos balões idênticos podem ser colocados em um grande galpão vazio. Se ao invés de balões colocássemos cubos idênticos, seria mais fácil notar que é possível preencher todo o espaço. Como as esferas não se juntam tal qual os cubos, haverá sempre espaço vazio entre elas. A solução do problema do empacotamento de esferas é útil para a Teoria da Informação, mas também para outras áreas como a otimização, a física, a química, a biologia, a medicina, entre outras. Um famoso exemplo de arranjos de esferas tridimensionais é dado pela figura seguinte:

O empacotamento de esferas acima é normalmente visto em feiras, na maneira como os feirantes dispõem as frutas, e em memoriais de guerra. Essas esferas ocupam aproximadamente 74,5% do espaço e cada uma toca exatamente outras doze, se o espaço não for limitado.



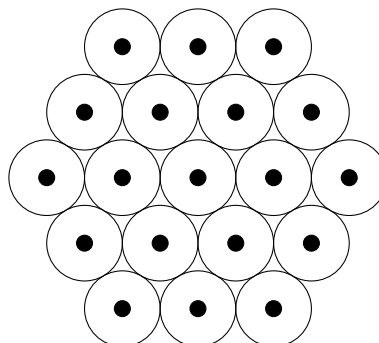
É clássica a pergunta: em uma dada dimensão, qual é a maior densidade possível que se pode alcançar empacotando o espaço com esferas maciças tangentes idênticas? Nesse caso, qual é a disposição e o raio dessas esferas? Em outras palavras, como é possível preencher o espaço utilizando esferas maciças tangentes idênticas deixando o menor espaço possível sem preenchimento?

Este é ainda um problema em aberto. Por exemplo, na dimensão 3 acredita-se que o empacotamento comentado anteriormente é o mais denso. Gauss (1831) já mostrou que isso é válido para os chamados *empacotamentos reticulados* (que estudaremos nesta seção). No entanto, não foi ainda possível mostrar que a disposição de esferas comentada é a melhor possível entre todas as possíveis disposições de esferas idênticas. Sabe-se, no entanto, que a melhor densidade é menor do que 77,9% (veja o primeiro capítulo de [5]).

Em contrapartida, sabe-se que para a dimensão $n = 1$, as esferas (intervalos) centrados nos números inteiros e de raio 0,5 cobrem toda a reta. Dessa forma, a densidade máxima de empacotamento de esferas em $\mathbb{R}$ é exatamente igual a 1. Para a dimensão $n = 2$, também já foi provado que a maior densidade possível é $\pi/12 \simeq 0,907$. Neste caso, o empacotamento de esferas máximo é atingido pelo conhecido **empacotamento reticulado hexagonal**, em que as esferas (círculos em $\mathbb{R}^2$) são inscritas em um hexágono e centradas no reticulado que tem matriz geradora

$$M = \begin{bmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{bmatrix} \quad (7.9)$$

visto na figura abaixo:



Em termos gerais, um **empacotamento esférico** no $\mathbb{R}^n$ é uma forma de dispor esferas n -dimensionais de mesmo raio de modo que elas se interceptem em apenas um ponto de modo que essa distribuição de esferas ocupe o “maior espaço possível”. Por sua vez, um empacotamento é dito **empacotamento reticulado** se o conjunto dos centros das esferas desse empacotamento forma um reticulado em $\mathbb{R}^n$. Obviamente, um empacotamento pode ser descrito apenas pelo raio e pelos centros das esferas.

Dá-se o nome de **densidade de empacotamento** à proporção do espaço coberto pelas esferas que formam um certo empacotamento. Tal valor é denotado por Δ . Se o empacotamento é reticulado, podemos observar a proporção ocupada pelas esferas na região fundamental e estendê-lo para todo o plano (proposição 7.1.1). Assim, é intuitiva a seguinte definição:

Definição 7.2.1. *A densidade do empacotamento associado a um reticulado $\Lambda \subset \mathbb{R}^n$ é dada por*

$$\Delta(\Lambda) = \frac{\text{Volume da região coberta por uma esfera}}{\text{Volume da região fundamental}} = \frac{\text{vol}(B(0, \rho))}{\text{vol}(\Lambda)} \quad (7.10)$$

em que $B(0, \rho)$ denota a esfera de centro na origem e raio ρ .

Com recursos de integração em $\mathbb{R}^n$ é possível mostrar que $\text{vol}(B(0, \rho)) = \rho^n \text{vol}(B(0, 1))$. Como $B(0, 1)$ é um valor fixo em cada dimensão n , maximizar o cálculo da densidade de um empacotamento reticulado associado a Λ é maximizar o valor de $\rho^n / \text{vol}(\Lambda)$, pois $\Delta(\Lambda) = \rho^n \text{vol}(B(0, 1)) / \text{vol}(\Lambda)$.

Definição 7.2.2. *Se $\Lambda \subset \mathbb{R}^n$ é um reticulado, a **densidade de centro** de Λ é dada por*

$$\delta(\Lambda) = \frac{\rho^n}{\text{vol}(\Lambda)} \quad (7.11)$$

em que ρ é o raio de empacotamento de Λ .

Da discussão anterior, note que $\Delta(\Lambda) = \delta(\Lambda) \text{vol}(B(0, 1))$. Por motivo já comentado, para maximizar a densidade de empacotamento de Λ basta maximizar a sua **densidade de centro**.

Além disso, outro problema é determinar o melhor raio a considerar para realizar um empacotamento reticulado. Para isso, se $\Lambda \subset \mathbb{R}^n$, considere o valor

$$\Lambda_{\min} = \min\{|\lambda| : \lambda \in \Lambda, \lambda \neq 0\}. \quad (7.12)$$

Note que tal valor existe, já que a intersecção de Λ com uma esfera compacta de centro na origem e raio $k > 0$ é um conjunto finito. Nesses termos, é claro que o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento é $\Lambda_{\min}/2$. Este valor geralmente é chamado **raio de empacotamento de Λ** .

Exemplo 7.2.1. Considere o reticulado hexagonal Λ definido pela matriz geradora da equação 7.9 e cujos pontos estão representados geometricamente na figura seguinte à matriz. A região fundamental deste reticulado é o paralelogramo de vértices $(0,0)$, $(0,5;0,5\sqrt{3})$, $(1,5;0,5\sqrt{3})$ e $(1,0)$, cuja área (noção que coincide com a de volume num espaço n -dimensional) é $\sqrt{3}/2$. Considere o raio das esferas (círculos) igual a $\rho = \Lambda_{\min}/2 = 1/2$. Assim, duas esferas quaisquer no plano ou se tangenciam ou não se tocam. No $\mathbb{R}^2$, $B(0,1) = \pi$. Assim,

$$\Delta(\Lambda) = \rho^n \text{vol}(B(0,1)) / \text{vol}(\Lambda) = (1/2)^2 \pi / (\sqrt{3}/2) = \pi / (2\sqrt{3}) = 0,9069... \quad (7.13)$$

Exemplo 7.2.2. Como comentamos, em 1831 Gauss demonstrou que a disposição das esferas em $\mathbb{R}^3$ similar à das laranjas nas feiras é a de melhor empacotamento reticulado. O reticulado que origina este empacotamento é um subconjunto de $\mathbb{Z}^3$ cujos elementos são tais que a soma de suas coordenadas é um número par, isto é,

$$\Lambda = \{(x_1, x_2, x_3) \in \mathbb{Z}^3 : x_1 + x_2 + x_3 \text{ é par}\}. \quad (7.14)$$

Tal reticulado é chamado de fcc (face - centered - cubic). Uma matriz geradora para Λ é

$$M = \begin{bmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix}. \quad (7.15)$$

Usando o raio de empacotamento $\rho = \Lambda_{\min}/2 = \sqrt{2}/2$, tem-se que a densidade de centro de Λ é $\delta = \sqrt{2}/8 \simeq 0,17678$. Isso implica que a densidade de empacotamento de Λ é $\pi/\sqrt{18} \simeq 0,741$, a qual é a melhor possível dentre os empacotamentos reticulados.

Exemplo 7.2.3 (Reticulado n -dimensional A_n). Para $n \geq 1$, o reticulado n -dimensional A_n é definido por

$$A_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1} : x_0 + x_1 + \dots + x_n = 0\}. \quad (7.16)$$

A_n é um reticulado n -dimensional e possui matriz geradora obtida de $M = [a_{ij}]_{n \times n+1}$, em que $a_{ii} = -1$ e $a_{i,i+1} = 1$ para $1 \leq i \leq n$ e $a_{ij} = 0$ nas outras entradas. O raio de empacotamento de A_n é $\rho = \sqrt{2}/2$ e a densidade de centro é $\delta = 2^{-n/2}(n+1)^{-1/2}$. Para $n = 2$, o reticulado A_2 coincide com o reticulado hexagonal do exemplo 7.2.1. A matriz geradora é obtida de

$$M = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}. \quad (7.17)$$

Por esse método, o raio de empacotamento é $\rho = 2/\sqrt{2}$ e a densidade de centro é igual a $2^{2/2}(2+1)^{-1/2} = 1/\sqrt{12} \simeq 0,28868$, o que causa $\Delta(\Lambda) = \pi/(2\sqrt{3}) = 0,9069\dots$ (de acordo com o que vimos no exemplo 7.2.1).

Exemplo 7.2.4 (Reticulado n -dimensional D_n , $n \geq 3$). Se $n \geq 3$, define-se o reticulado D_n por

$$D_n = \{(x_1, x_2, \dots, x_n) \in \mathbb{Z}^n : x_1 + x_2 + \dots + x_n \equiv 0 \pmod{2}\}. \quad (7.18)$$

Em outras palavras, D_n é obtido colorindo os pontos de $\mathbb{Z}^n$ alternadamente de preto e branco e tomando os pretos. A matriz geradora deste reticulado é dada por

$$M = \begin{bmatrix} -1 & -1 & 0 & \dots & 0 & 0 \\ 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -1 \end{bmatrix}. \quad (7.19)$$

O reticulado D_n tem raio de empacotamento $\rho = \sqrt{2}/2$ e densidade de centro igual a $2^{-(n+2)/2}$.

O reticulado fcc do exemplo 7.2.2 pode ser obtido de qualquer um dos reticulados A_3 e D_3 . Na dimensão 4, a densidade de centro de D_4 é $\delta = 1/8 = 0,125$ e é a melhor possível para empacotamentos reticulados em quarta dimensão. Na dimensão 5, a densidade de centro de D_5 é $\delta = 1/(8\sqrt{2})$, a qual é a melhor possível para empacotamentos reticulados em quinta dimensão.

Exemplo 7.2.5 (Reticulados E_8 , E_6 e E_7). O conjunto

$$E_8 = \left\{ (x_0, x_1, \dots, x_8) \in \mathbb{R}^8 : x_i \in \mathbb{Z} \text{ ou } x_i + 1/2 \in \mathbb{Z}, \sum_{i=0}^8 x_i \equiv 0 \pmod{2} \right\} \quad (7.20)$$

é o reticulado 8-dimensional que tem a melhor densidade nessa dimensão. Seu raio de empacotamento é $\sqrt{2}/2$ e sua densidade de centro é $1/16 \simeq 0,06250$. Agora, seja V um A_2 -sub-reticulado em E_8 . Assim,

$$E_6 = \{x \in E_8 : xv = 0, \forall v \in V\} \quad (7.21)$$

é o reticulado 6-dimensional que tem a melhor densidade entre os reticulados de $\mathbb{R}^6$. Seu raio de empacotamento é $\sqrt{2}/2$ e sua densidade de centro é $1/(8\sqrt{3}) \simeq 0,0722$.

Por sua vez, para algum v minimal em E_8 , o conjunto

$$E_7 = \{x \in E_8 : xv = 0\} \quad (7.22)$$

é o reticulado 7-dimensional que tem a melhor densidade nessa dimensão. Seu raio de empacotamento é $\sqrt{2}/2$ e sua densidade de centro é $1/16$. Para conhecer a matriz geradora desses reticulados e outras informações sobre eles, consulte a seção 8 do capítulo 4 de [5].

Outros reticulados, como os usualmente denotados por K_{12} (dimensão 12), Λ_{16} (dimensão 16) e Λ_{24} (reticulado de Leech, dimensão 24) podem ser conhecidos no capítulo 4 de [5]. Cada um deles também fornece empacotamento reticulado com densidade máxima.

A tabela a seguir apresenta as maiores densidades de centro de reticulados conhecidas nas dimensões de 1 a 8, 12, 16 e 24, sintetizando o que foi comentado acima. Os dados foram extraídos da tabela 1.1 do prefácio da terceira edição de [5], na qual também são apresentadas as maiores densidades de centro conhecidas para dimensões até 128.

n	δ	Reticulado
1	$1/2$	$A_1 = \mathbb{Z}$
2	$1/(2\sqrt{3})$	A_2
3	$1/(4\sqrt{2})$	A_3 ou D_3
4	$1/8$	D_4
5	$1/(8\sqrt{2})$	D_5
6	$1/(8\sqrt{3})$	E_6
7	$1/16$	E_7
8	$1/16$	E_8
12	$1/27$	K_{12}
16	$1/16$	Λ_{16}
24	1	Λ_{24} .

(7.23)

7.3 Reticulados algébricos

Nesta seção, veremos que é possível construir reticulados a partir de ideais do anel dos inteiros de um corpo de números. Posteriormente, veremos uma expressão para a densidade de centro de um reticulado obtido dessa forma e daremos alguns exemplos de reticulados que atingem a densidade máxima em algumas dimensões.

Seja $\mathbb{K}$ um corpo de números de grau n . Sabe-se que existem exatamente n distintos monomorfismos $\sigma_i : \mathbb{K} \rightarrow \mathbb{C}$. Seja $\alpha : \mathbb{C} \rightarrow \mathbb{C}$ a conjugação complexa, isto é, $\alpha(i) = -i$. Então, para qualquer

$1 \leq j \leq n$, tem-se que $\alpha \circ \sigma_j = \sigma_k$, $1 \leq k \leq n$. Além disso, $\sigma_j = \sigma_k$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Se $\sigma_j(\mathbb{K}) \subset \mathbb{R}$ então σ_i é chamado de **monomorfismo real de $\mathbb{K}$** .

Considere r_1 o número de índices j tais que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Sendo assim, $n - r_1$ é um número par. Portanto, existe um número natural r_2 tal que $r_1 + 2r_2 = n$. Dessa forma, vamos renumerar os monomorfismo σ como σ_j , $1 \leq j \leq r_1$, se $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, e $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Por essa construção, os primeiros $r_1 + r_2$ monomorfismos determinam os últimos r_2 . Para qualquer $x \in \mathbb{K}$, definimos

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}. \quad (7.24)$$

Definição 7.3.1. A aplicação σ definida na expressão 7.24 é um homomorfismo de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ e é chamado de **homomorfismo de Minkowski** ou **homomorfismo canônico** de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$.

Geralmente, sendo $im(\cdot)$ a parte imaginária de um número complexo e $re(\cdot)$ sua parte real, o homomorfismo de Minkowski é $\sigma : \mathbb{K} \rightarrow \mathbb{R}^n$ definido por

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), re(\sigma_{r_1+1}(x)), im(\sigma_{r_1+1}(x)), \dots, re(\sigma_{r_1+r_2}(x)), im(\sigma_{r_1+r_2}(x))) \quad (7.25)$$

Exemplo 7.3.1. Seja $\mathbb{K} = \mathbb{Q}(i)$ o corpo gaussiano, em que i é a unidade imaginária. Se $\sigma_1 = id$ e σ_2 é a conjugação complexa em $\mathbb{K}$, então tais σ_j são os $\mathbb{Q}$ -monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Neste caso, $r_1 = 0$ e $r_2 = 1$ (pois $\overline{\sigma_1} = \sigma_2$). Assim, para qualquer $x = a + bi \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, o homomorfismo de Minkowski associado a $\mathbb{K}$ é $\sigma(x) = (re(x), im(x)) = (a, b)$.

Exemplo 7.3.2. Considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_5)$, em que $\zeta_5 = e^{2\pi i/5}$. Seja $Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ em que $\sigma_j(\zeta_5) = \zeta_5^{2^{j-1}}$, para $1 \leq j \leq 4$. Assim, $\overline{\sigma_1(x)} = \sigma_3(x)$ e $\overline{\sigma_2(x)} = \sigma_4(x)$. Portanto, $r_1 = 0$ e $r_2 = 2$. Além disso, o homomorfismo de Minkowski associado a $\mathbb{K}$ é $\sigma(x) = (re(\sigma_1(x)), im(\sigma_1(x)), re(\sigma_2(x)), im(\sigma_2(x)))$.

Exemplo 7.3.3. Se $\mathbb{K} = \mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$ (de grau 2) então $r_1 = 2$ e $r_2 = 0$, em que os $\mathbb{Q}$ -monomorfismos de $\mathbb{K}$ são $\sigma_1 = id$ e $\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$ ($a, b \in \mathbb{Q}$). Dessa forma, para qualquer $x = a + b\sqrt{3} \in \mathbb{K}$ ($a, b \in \mathbb{Q}$), o homomorfismo de Minkowski é dado por $\sigma(x) = (a + b\sqrt{3}, a - b\sqrt{3})$.

Definição 7.3.2. Seja $\mathbb{K}$ um corpo de números e r_1 e r_2 dados como acima.

(a) Se $r_2 = 0$ então $\mathbb{K}$ é chamado de corpo de números **totalmente real**, pois, nesse caso, todos os monomorfismos de $\mathbb{K}$ são reais.

(b) Se $r_1 = 0$ então $\mathbb{K}$ é chamado de corpo de números **totalmente imaginário** ou **totalmente complexo**, pois, nesse caso, todos os monomorfismos de $\mathbb{K}$ são não reais.

Os exemplos 7.3.1 e 7.3.2 apresentam corpos de números totalmente imaginários, enquanto o exemplo 7.3.3 apresenta um corpo de números totalmente real. Com relação a esse assunto, vale a seguinte proposição:

Proposição 7.3.1. *Se $\mathbb{Q} \subset \mathbb{K}$ é uma extensão galoisiana finita então $\mathbb{K}$ é totalmente real ou totalmente complexo.*

Demonstração. Como $\mathbb{Q} \subset \mathbb{K}$ é uma extensão normal, pois é galoisiana, então todo monomorfismo σ de $\mathbb{K}$ satisfaz $\sigma(\mathbb{K}) = \mathbb{K}$. Como $\mathbb{K} \subset \mathbb{R}$ ou $\mathbb{K} \cap (\mathbb{C} - \mathbb{R}) \neq \emptyset$ então $\mathbb{K}$ é totalmente real ou $\mathbb{K}$ é totalmente imaginário, respectivamente. $\square$

A proposição a seguir garante que a imagem de um $\mathbb{Z}$ -submódulo livre de $\mathbb{K}$ de posto n (por exemplo, seu anel de inteiros ou algum ideal de $\mathcal{O}_{\mathbb{K}}$) é um reticulado de $\mathbb{R}^n$, em que n é o grau de $\mathbb{K}$.

Proposição 7.3.2. *Sejam M um $\mathbb{Z}$ -submódulo livre de $\mathbb{K}$ de posto n e σ o homomorfismo de Minkowski associado a $\mathbb{K}$. Se $\{x_1, x_2, \dots, x_n\}$ é uma $\mathbb{Z}$ -base para M então $\sigma(M)$ é um reticulado em $\mathbb{R}^n$ e seu volume é*

$$\text{vol}(\sigma(M)) = 2^{-r_2} \left| \det_{1 \leq i, j \leq n} (\sigma_i(x_j)) \right|. \quad (7.26)$$

Demonstração. Seja D o determinante da matriz $n \times n$ cuja i -ésima coluna é formada pelas n coordenadas do vetor $\sigma(x_i) \in \mathbb{R}^n$. Sabemos que, para qualquer número complexo z , $\text{re}(z) = (z + \bar{z})/2$ e $\text{im}(z) = (z - \bar{z})/(2i)$, em que $\bar{z}$ denota o conjugado complexo de z . Utilizando propriedades de determinantes, cada escalar $1/2$ das r_2 linhas que são formadas por $\text{re}(\sigma_i(x_j))$ ($r_1 + 1 \leq i \leq r_1 + r_2$) e cada escalar $1/(2i)$ das r_2 linhas que são formadas por $\text{im}(\sigma_i(x_j))$ podem ser postos em evidência fora do determinante. Logo, $D = 2^{-r_2} (2i)^{-r_2} D_1$ em que D_1 é o determinante de uma matriz com as primeiras r_1 linhas iguais formadas por $\sigma_i(x_j)$ e com as últimas $2r_2$ linhas intercaladas por $\sigma_{r_1+i}(x_j) + \overline{\sigma_{r_1+i}(x_j)}$ e $\sigma_{r_1+i}(x_j) - \overline{\sigma_{r_1+i}(x_j)}$. A cada par consecutivo dessas últimas $2r_2$ últimas linhas, faz-se a soma das linhas do par. A soma é substituída no lugar da primeira linha do par. Depois, extrai-se mais um escalar 2 de cada uma dessas novas r_2 linhas. Por fim, em cada par consecutivo das últimas $2r_2$ linhas, faz-se a subtração e substitui-se tal valor no lugar da segunda linha do par. Assim, como $\overline{\sigma_{r_1+i}(x_j)} = \sigma_{r_1+r_2+i}(x_j)$, vê-se que $D = 2^{-r_2} (2i)^{-r_2} 2^{r_2} D_2$, em que $D_2 = \det_{1 \leq i, j \leq n} (\sigma_i(x_j))$. Simplificando os cálculos, tem-se que $D = (2i)^{-r_2} \det_{1 \leq i, j \leq n} (\sigma_i(x_j))$.¹ O fato de $\{x_i\}_{1 \leq i \leq n}$ formar uma $\mathbb{Q}$ -base para $\mathbb{K}$ acarreta $\det_{1 \leq i, j \leq n} (\sigma_i(x_j)) \neq 0$ (proposições 2.3.3 e 2.3.5). Portanto, $D \neq 0$. Logo, os vetores $\sigma(x_i)$ são linearmente independentes em $\mathbb{R}^n$. Por esse motivo, o $\mathbb{Z}$ -módulo $\sigma(M)$ que eles

¹ Para ver os cálculos detalhados de D , conforme a descrição feita, consulte o teorema 5.1.1 de [3].

geram é um reticulado em $\mathbb{R}^n$. Ademais, $\text{vol}(\sigma(M)) = |D| = 2^{-r_2} |\det_{1 \leq i, j \leq n}(\sigma_i(x_j))|$, o que conclui a prova. $\square$

Corolário 7.3.1. *Seja $\mathbb{K}$ um corpo de números de grau n cujo discriminante é indicado por $D(\mathbb{K})$. Se I é um ideal (integral) não zero do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ então $\sigma(\mathcal{O}_{\mathbb{K}})$ e $\sigma(I)$ são reticulados em $\mathbb{R}^n$. Além disso,*

$$\text{vol}(\sigma(\mathcal{O}_{\mathbb{K}})) = \frac{\sqrt{|D(\mathbb{K})|}}{2^{r_2}} \quad e \quad \text{vol}(\sigma(I)) = \frac{N(I)\sqrt{|D(\mathbb{K})|}}{2^{r_2}} \quad (7.27)$$

em que $N(I)$ indica a norma do ideal I (definição 2.5.6).

Demonstração. Devido à proposição 2.5.2 e ao corolário 2.5.1, tanto $\mathcal{O}_{\mathbb{K}}$ como I são $\mathbb{Z}$ -módulos livres de posto n . Pela proposição 7.3.2, $\sigma(\mathcal{O}_{\mathbb{K}})$ e $\sigma(I)$ são reticulados em $\mathbb{R}^n$. Agora, seja $\{x_1, x_2, \dots, x_n\}$ uma $\mathbb{Z}$ -base para $\mathcal{O}_{\mathbb{K}}$. Pela proposição 2.3.3, $D(\mathbb{K}) = [\det(\sigma_i(x_j))]^2$. Da equação 7.26, segue então que $\text{vol}(\sigma(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2} \sqrt{|D(\mathbb{K})|}$. Por fim, como $\sigma(I)$ é um subgrupo de $\sigma(\mathcal{O}_{\mathbb{K}})$ de índice $N(I)$, pois $\mathcal{O}_{\mathbb{K}}/I \simeq \sigma(\mathcal{O}_{\mathbb{K}})/\sigma(I)$, então $\text{vol}(\sigma(I)) = N(I)2^{-r_2} \sqrt{|D(\mathbb{K})|}$. $\square$

Se I é um ideal do anel de inteiros $\mathcal{O}_{\mathbb{K}}$, segue do corolário anterior e da equação 7.11 que a densidade de centro do reticulado $\sigma(I)$ é dada pela fórmula

$$\delta(\sigma(I)) = \frac{2^{r_2} \rho^n}{N(I) \sqrt{|D(\mathbb{K})|}}. \quad (7.28)$$

Observe ainda que $N(I) = 1$ se $I = \mathcal{O}_{\mathbb{K}}$.

Definição 7.3.3. *Se $\mathbb{K}$ é um corpo de números e I é um ideal não zero de $\mathcal{O}_{\mathbb{K}}$, o reticulado $\sigma(I)$ obtido a partir do homomorfismo de Minkowski σ associado a $\mathbb{K}$ é chamado de **reticulado algébrico** ou **realização geométrica de I** .*

Podemos esclarecer ainda mais a expressão da densidade de centro do reticulado $\sigma(I)$ devido à seguinte proposição:

Proposição 7.3.3. *Sejam $\mathbb{K}$ um corpo de números, $x \in \mathbb{K}$ e σ o homomorfismo de Minkowski associado a $\mathbb{K}$. Então $|\sigma(x)|^2 = c \cdot \text{Tr}_{\mathbb{K}:\mathbb{Q}}(x\bar{x})$, em que*

$$c = \begin{cases} 1, & \text{se } \mathbb{K} \text{ for totalmente real } (r_2 = 0) \\ 1/2, & \text{se } \mathbb{K} \text{ for totalmente imaginário } (r_1 = 0) \end{cases} \quad (7.29)$$

Demonstração. Considere $\sigma_1, \sigma_2, \dots, \sigma_n$ os $n = [\mathbb{K} : \mathbb{Q}]$ monomorfismos de $\mathbb{K}$, sendo $n = r_1 + 2r_2$. Dessa forma, o homomorfismo de Minkowski é dado por

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), re(\sigma_{r_1+1}(x)), im(\sigma_{r_1+1}(x)), \dots, re(\sigma_{r_1+r_2}(x)), im(\sigma_{r_1+r_2}(x))). \quad (7.30)$$

Calculando a norma, tem-se que

$$|\sigma(x)|^2 = \sigma_1(x)^2 + \dots + \sigma_{r_1}^2(x) + re(\sigma_{r_1+1}(x))^2 + im(\sigma_{r_1+1}(x))^2 + \dots + re(\sigma_{r_1+r_2}(x))^2 + im(\sigma_{r_1+r_2}(x))^2 \quad (7.31)$$

Porém, $re(\sigma_i)^2 + im(\sigma_i)^2 = \sigma_i(x)\overline{\sigma_i(x)} = \sigma(x\bar{x})$, $r_1 + 1 \leq i \leq r_1 + r_2$. Sendo assim,

$$|\sigma(x)|^2 = \sigma_1(x)^2 + \dots + \sigma_{r_1}^2(x) + \sigma_{r_1}(x\bar{x})^2 + \dots + \sigma_{r_1+r_2}(x\bar{x})^2 \quad (7.32)$$

Por um lado, se $r_1 = 0$, como $\sigma_{r_2+j}(x\bar{x}) = \overline{\sigma_j(x\bar{x})} = \sigma_j(x\bar{x})$, $1 \leq j \leq r_2$, então $|\sigma(x)|^2 = \sum_{j=1}^{r_2} \sigma_j(x\bar{x}) = \sum_{j=1}^{r_2} \sigma_{r_2+j}(x\bar{x})$ e, daí,

$$2|\sigma(x)|^2 = \sum_{i=1}^n \sigma_i(x\bar{x}). \quad (7.33)$$

Como os $\sigma_i(x\bar{x})$ são os conjugados de $x\bar{x}$, isto implica que $|\sigma(x)|^2 = Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x})/2$.

Por outro lado, se $r_2 = 0$, então $|\sigma(x)|^2 = \sum_{j=1}^{r_2} (\sigma_j(x))^2$. Como $\sigma_i(x\bar{x}) = \sigma_i(x)\sigma_i(\bar{x}) = \sigma_i(x)\sigma_i(x) = (\sigma_i(x))^2$, pois os monomorfismos têm imagem real, então

$$|\sigma(x)|^2 = \sum_{i=1}^n \sigma_i(x\bar{x}) = Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) \quad (7.34)$$

o que conclui a prova. $\square$

Sejam $\mathbb{K}$ um corpo de números e I um ideal não zero de $\mathcal{O}_{\mathbb{K}}$. Se σ é o reticulado de Minkowski associado a $\mathbb{K}$, então o raio de empacotamento do reticulado $\sigma(I)$ é dado por

$$\rho = (1/2) \min\{|\sigma(x)| : x \in I, x \neq 0\} = (1/2) \min\{\sqrt{c Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x})} : x \in I, x \neq 0\}. \quad (7.35)$$

Denotando

$$t_I \triangleq \min\{Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) : x \in I, x \neq 0\} \quad (7.36)$$

podemos concluir a seguinte proposição:

Proposição 7.3.4. *Com as notações anteriores, se $\mathbb{K}$ é um corpo de números totalmente real ou totalmente imaginário de grau n então a densidade de centro de um ideal não zero I em $\mathcal{O}_{\mathbb{K}}$ é*

$$\delta = \frac{t_I^{n/2}}{2^n \sqrt{|D(\mathbb{K})|} N(I)}. \quad (7.37)$$

Observação 7.3.1. Em particular, devido à proposição 7.3.1, a fórmula 7.37 é válida quando $\mathbb{K}$ é uma extensão racional galoisiana.

Demonstração. Se $\mathbb{K}$ é totalmente real, usa-se $c = 1$ na equação 7.35, enquanto que, se $\mathbb{K}$ é totalmente imaginário, usa-se $c = 1/2$ (proposição 7.3.3). No primeiro caso, pelas fórmulas 7.28 e 7.35, tem-se

$$\delta = \frac{(\sqrt{t_I}/2)^n}{N(I)\sqrt{|D(\mathbb{K})|}} = \frac{t_I^{n/2}}{2^n \sqrt{|D(\mathbb{K})|} N(I)}. \quad (7.38)$$

No segundo caso, se $\mathbb{K}$ é totalmente imaginário, então

$$\delta = \frac{2^{n/2} \left(2^{-1} \sqrt{t_I}/2\right)^n}{N(I)\sqrt{|D(\mathbb{K})|}} = \frac{t_I^{n/2}}{2^n \sqrt{|D(\mathbb{K})|} N(I)} \quad (7.39)$$

finalizando a prova. $\square$

Em suma, via Teoria Algébrica dos Números é possível construir reticulados em uma dimensão n utilizando corpos de números de grau n a partir de ideais não zeros do anel de inteiros desses corpos. Além disso, pela proposição 7.3.4, sendo esse corpo $\mathbb{K}$ totalmente real ou totalmente imaginário (por exemplo, quando $\mathbb{K}$ é uma extensão galoisiana de $\mathbb{Q}$), consegue-se construir um reticulado algébrico e obter sua densidade de centro, desde que se conheçam:

1. A estrutura do anel de inteiros de $\mathbb{K}$;
2. O valor $N(I)$ de algum ideal I de $\mathcal{O}_{\mathbb{K}}$;
3. O discriminante $D(\mathbb{K})$;
4. O valor t_I .

Com relação ao item (2), alguns ideais favorecem o cálculo de $N(I)$. Por exemplo, se $I = \mathcal{O}_{\mathbb{K}}$ então $N(I) = 1$. Outro caso é quando $I = \langle a \rangle$ é um ideal principal, $a \in \mathcal{O}_{\mathbb{K}}$. Neste caso $N(I) = N(a)$. Outro caso que pode interessar é quando I é um ideal totalmente ramificado em $\mathbb{K}$. Com isso tudo, há uma grande variedade de ideais de $\mathcal{O}_{\mathbb{K}}$ que podem ser usados para produzir reticulados algébricos de modo que se conheçam suas normas e que, conseqüentemente, permitam o cálculo de suas densidades de centro.

Com relação ao item (3), a proposição 3.1.3 e o teorema 3.2.1 permitem o cálculo de $D(\mathbb{K})$ quando $\mathbb{K}$ é um corpo quadrático ou um corpo ciclotômico, respectivamente. Os teoremas 3.3.2 e 3.3.3 expressam o discriminante dos corpos $\mathbb{Q}(\eta)$, em que $\eta = \zeta_m - \zeta_m^{-1}$, para $m = 2^n$ e $m = 4p^n$ ($p > 3$ primo). De modo geral, o Teorema do Condutor-Discriminante (teorema 5.4.1) permite o

cálculo do discriminante de qualquer corpo de números, desde de que se conheçam os caracteres de Dirichlet associados a $\mathbb{K}$. Utilizando esse resultado, Trajano P. Nóbrega, José C. Interlando e J.O. Dantas Lopes expressaram o discriminante de subcorpos de $\mathbb{Q}(\zeta_{p^r})$ (p primo) e de corpos de números abelianos. Esses resultados estão acessíveis no capítulo 4 de [26] e os trabalhos originais contendo-os estão indicados na bibliografia da referida dissertação. Abaixo, enunciamos um desses teoremas, que explicita o discriminante de um corpo de números abeliano:

Teorema 7.3.1. *Seja $\mathbb{K}$ um corpo de números abeliano de condutor m . Se a fatoração de m em produto de primos é dada por $m = \prod_{i=1}^r p_i^{e_i}$, em que p_i são primos e $e_i \geq 1$, então o módulo do discriminante de $\mathbb{K}$ é dado por*

$$|D(\mathbb{K})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^r p_i^{\beta_i}} \quad (7.40)$$

em que $\beta_i = \sum_{k=1}^{e_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^k}) : \mathbb{Q}]$.

Como podemos ver, há uma grande variedade de corpos de números que favorecem o cálculo de $|D(\mathbb{K})|$, permitindo que o parâmetro do item (3) seja encontrado sem dificuldade.

O que ainda não é tão fácil de encontrar é o mínimo dos traços de $x\bar{x}$, com $x \in I$, $x \neq 0$, o que permite encontrar o valor do parâmetro t_I do item (4). A tarefa de minimizar $Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x})$ é, na verdade, a de minimizar uma forma quadrática. O capítulo 5 de [9] desenvolve alguns resultados sobre esse tópico para corpos ciclotômicos.

Com relação ao item (1) vale a nossa principal observação. O objetivo central desta dissertação foi oferecer um amplo leque de estruturas de anéis de inteiros de corpos de números. A partir desses anéis, é possível construir novos reticulados algébricos com vistas a maximizar a expressão de sua densidade de centro.

Deve-se notar, por exemplo, que o uso de corpos de números abelianos para obter reticulados algébricos é aconselhado, tendo em vista que uma combinação do Teorema de Kronecker-Weber (teorema 3.3.1), do Teorema de Leopoldt-Letl (teorema 6.3.1) e do teorema 7.3.1 citado acima facilita o encontro de parâmetros na fórmula da densidade de centro (fórmula 7.37). Na próxima seção, reuniremos exemplos de reticulados com densidade ótima em algumas dimensões que puderam ser construídos via homomorfismo de Minkowski.

É possível ainda construir reticulados algébricos por meio do *homomorfismo de Minkowski perturbado* por um elemento α em um corpo de números tal que $\sigma(\alpha)$ é real para todo monomorfismo σ de $\mathbb{K}$ em $\mathbb{C}$. Essa teoria e exemplos podem ser encontrados na seção 5 de [3].

7.4 Construção de reticulados algébricos

Nesta seção, apresentaremos construções de reticulados algébricos com densidade de centro ótima nas dimensões 2, 4, 6 e 8. Ao final, discutiremos sobre algoritmos e métodos que têm sido usados para tentar encontrar reticulados algébricos com densidade ótima em outras dimensões, tais como dimensões ímpares. Nesse ponto, já estaremos explanando sobre perspectivas futuras consequentes a este trabalho.

Dimensão 2: A seguir, apresentamos alguns exemplos de reticulados algébricos com densidade de centro máxima construídos na dimensão 2, isto é, via corpos de números quadráticos. Lembremos, da tabela 7.23 que a densidade de centro máxima na dimensão 2 é igual a $1/(2\sqrt{3}) \simeq 0,2887$.

Exemplo 7.4.1. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_3)$. Note que $\mathbb{K}$ é um corpo ciclotômico de grau $\varphi(3) = 2$. Portanto, $\mathbb{K}$ é um corpo quadrático e é uma extensão racional galoisiana. Pela proposição 3.2.4, o discriminante de $\mathbb{K}$ é*

$$D(\mathbb{Q}(\zeta_3)) = (-1)^{\frac{3-1}{2}} 3^{3-2} = -3. \quad (7.41)$$

Seja $\mathfrak{P} = (1 - \zeta_3)\mathcal{O}_{\mathbb{K}}$ o ideal primo que se ramifica totalmente no anel de inteiros de $\mathbb{K}$ (proposição 3.2.2). Pelo que vimos na seção 3.2, $N(\mathfrak{P}) = 3$. Dentre os parâmetros para se calcular a densidade de centro do reticulado gerado pelo homomorfismo de Minkowski através de $\mathfrak{P}$, falta calcular o valor $t_{\mathfrak{P}}$. Se $x \in \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$, então $x = a_0 + a_1\zeta_3$. Então, como $\zeta_3^2 = -1 - \zeta_3$,

$$x\bar{x} = (a_0 + a_1\zeta_3)(a_0 + a_1\zeta_3^2) = a_0^2 + a_1^2 - a_0a_1 \quad (7.42)$$

donde segue que

$$\text{Tr}_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) = 2(a_0^2 + a_1^2 - a_0a_1) = a_0^2 + a_1^2 + (a_1 - a_0)^2. \quad (7.43)$$

Agora, por um lado, se $x = a + b\zeta \in \mathfrak{P}$ então $x = (1 - \zeta_3)(c + d\zeta_3) = c + d + \zeta_3(2d - c)$, donde segue que $a + b \equiv 0 \pmod{3}$. Por outro lado, se $a + b \equiv 0 \pmod{3}$, então $a + b = 3k$, com $k \in \mathbb{Z}$. Assim, $x = a + b\zeta = k\zeta(1 - \zeta) \in \mathfrak{P}$. Portanto, $x \in \mathfrak{P}$ se, e somente se, $a + b \equiv 0 \pmod{3}$. Daí, para qualquer $x = a + b\zeta_3 \in \mathfrak{P}$, como $a + b = 3k$ ($k \in \mathbb{Z}$), então

$$\text{Tr}_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) = a^2 + b^2 + (b - a)^2 = 6(a^2 + 3k^2 - 3ka). \quad (7.44)$$

Logo, $\text{Tr}_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) \geq 6$, para qualquer $x \in \mathfrak{P}$. Além disso, tomando $a = 1$ e $b = -1$, isto é, $x = 1 - \zeta_3 \in \mathfrak{P}$ e $k = 0$, então $\text{Tr}_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) = 6$. Portanto,

$$t_{\mathfrak{P}} = \min\{\text{Tr}(x\bar{x}) : x \in \mathfrak{P}, x \neq 0\} = 6. \quad (7.45)$$

Aplicando a fórmula da densidade de centro da proposição 7.3.4, tem-se que

$$\delta = \frac{t_{\mathfrak{P}}^{n/2}}{2^n \sqrt{|D(\mathbb{K})|} N(\mathfrak{P})} = \frac{6^{2/2}}{2^2 \cdot 3 \cdot \sqrt{3}} = \frac{1}{2\sqrt{3}}. \quad (7.46)$$

Portanto, o ideal $\mathfrak{P}$ produz, através do homomorfismo de Minkowski, um reticulado de densidade máxima na dimensão 2.

Através do ideal $(1 - \zeta_p)\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ é ainda possível construir reticulados nas dimensões $p - 1$, em que p é um número primo. Generalizando o que fizemos no exemplo anterior, é possível mostrar que para qualquer $x = \sum_{i=0}^{p-2} a_i \zeta_p^i \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$,

$$x \in (1 - \zeta_p)\mathcal{O}_{\mathbb{Q}(\zeta_p)} \iff \sum_{i=0}^{p-2} a_i \equiv 0 \pmod{p}. \quad (7.47)$$

Com isso, mostra-se que t_I , em que $I = (1 - \zeta_p)\mathcal{O}_{\mathbb{Q}(\zeta_p)}$, é igual a $2p$. Dessa forma, similarmente ao que fizemos no exemplo anterior, a densidade de centro do reticulado produzido por esse ideal é

$$\delta = \frac{(p-1)^{\frac{p-1}{2}}}{2^{p-1} p^{\frac{p-2}{2}}}. \quad (7.48)$$

Para ver mais sobre isso e consultar uma tabela com a densidade de centro de alguns reticulados gerados por I , variando p , consulte [2].

Outra maneira de construir um reticulado algébrico de dimensão 2, agora através do próprio anel de inteiros de um corpo de números, é dada a seguir.

Exemplo 7.4.2. Considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_6)$. Como $\varphi(6) = 2$ é o grau de $\mathbb{K}$ então $\mathbb{K}$ é um corpo quadrático. Na verdade, como $\zeta_6 = 1/2 + i(\sqrt{3}/2)$ então $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. Da proposição 3.1.2, vê-se que $|D(\mathbb{K})| = 3$. Além disso, para qualquer $x \in \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_6]$,

$$x\bar{x} = (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2 \quad (7.49)$$

em que a e b são inteiros. Assim, $\text{Tr}_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) = 2(a^2 + 3b^2)$. Portanto, se $I = \mathcal{O}_{\mathbb{K}}$ então $t_I = 2$. Daí, obtém-se que a densidade de centro do reticulado algébrico produzido pelo anel de inteiros de $\mathbb{K}$ é

$$\delta = \frac{t_I^{n/2}}{2^n \sqrt{|D(\mathbb{K})|} N(I)} = \frac{2^{2/2}}{2^2 \sqrt{3}} = \frac{1}{2\sqrt{3}}, \quad (7.50)$$

que é a máxima densidade de centro de um reticulado na dimensão 2.

Dimensão 4: A seguir, buscaremos encontrar um reticulado algébrico na dimensão 4 cuja densidade de centro seja máxima, isto é, igual a $1/8$. Para isso, considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_8)$. Seu

anel de inteiros é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_8]$ e seu discriminante é igual a 256. Uma base para este corpo é $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$. Seu grupo de Galois é $Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_i : \sigma_i(\zeta_8) = \zeta_8^i, i = 1, 3, 5, 7\} \simeq \mathbb{Z}_8^* = \{1, 3, 5, 7\}$. O objetivo é encontrar um ideal principal I de $\mathcal{O}_{\mathbb{K}}$ tal que $1/8 = (t_I^2)/(2^4 N(I) \sqrt{|D(\mathbb{K})|})$, isto é, tal que $t_I^2 = 2^5 N(I)$. Considere $I = (a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3)\mathcal{O}_{\mathbb{K}}$ um ideal principal de $\mathcal{O}_{\mathbb{K}}$, em que $a, b, c, d \in \mathbb{Z}$ e $\alpha = a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3 \in \mathcal{O}_{\mathbb{K}}$. Assim,

$$N_{\mathbb{K}:\mathbb{Q}}(I) = N_{\mathbb{K}:\mathbb{Q}}(a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3) =$$

$$= a^4 + b^4 - 4ab^2c + 2a^2c^2 + c^4 + 4a^bd - 4bc^2d + 2b^2d^2 + 4acd^2 + d^4 \quad (7.51)$$

Agora, para cada $x = \alpha(i + j\zeta_8 + k\zeta_8^2 + l\zeta_8^3) \in I$, com $i, j, k, l \in \mathbb{Z}$, tem-se que

$$\begin{aligned} Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) &= 4a^2i^2 + 4b^2i^2 + 4c^2i^2 + 4d^2i^2 + 8abij + 8bcij - 8adij + 8cdij + 4a^2j^2 + 4b^2j^2 + \\ &+ 4c^2j^2 + 4d^2j^2 + 8abjk + 8bcjk - 8adjk + 8cdjk + 4a^2k^2 + 4b^2k^2 + 4c^2k^2 + 4d^2k^2 - 8abil - 8bcil \\ &+ 8adil - 8cdil + 8abkl + 8bckl - 8adkl + 8cdkl + 4a^2l^2 + 4b^2l^2 + 4c^2l^2 + 4d^2l^2. \end{aligned} \quad (7.52)$$

Tomando $a = b = c = 1$, obtém-se o ideal $I = (1 + \zeta_8 + \zeta_8^2 + \zeta_8^3)\mathcal{O}_{\mathbb{K}}$, cuja norma é $N(I) = 8$. Neste caso, $Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) = 16i^2 + 16ij + 16j^2 + 16jk + 16k^2 - 16il + 16kl + 16l^2$ cujo mínimo é obviamente 16 (basta tomar $i = 1$ e $j = k = l = 0$). Portanto, o ideal principal $I = (1 + \zeta_8 + \zeta_8^2 + \zeta_8^3)\mathcal{O}_{\mathbb{K}}$ produz um reticulado algébrico cuja densidade de centro é máxima, igual a $1/8$.

Os cálculos acima nos permitiram encontrar um ideal principal do anel de inteiros de $\mathbb{K}$ que maximizasse a densidade de centro do reticulado produzido por ele através do homomorfismo de Minkowski. Para fazer os cálculos da norma de α e do traço de $x\bar{x}$ acima foi utilizado o software Sage Math. O método utilizado anteriormente parece ser interessante para produzir reticulados com densidade pré-determinada. No entanto, para dimensões maiores do que 4, as contas ficam muito extensas e, por isso, esse método não se mostra tão eficiente.

Dimensão 6: Para obter reticulados algébricos na sexta dimensão com densidade de centro máxima igual a $1/(8\sqrt{3})$, [9] utilizou a seguinte proposição, que calcula uma expressão para o traço de $x\bar{x}$ quando x é um inteiro algébrico de $\mathbb{K}$.

Proposição 7.4.1 ([9], teorema 5.2.1). *Seja $\mathbb{L} = \mathbb{Q}(\zeta_n)$, em que $n = \prod_{i=1}^s p_i^{e_i}$, com cada p_i primo e $e_i \geq 1$, $n \neq 2^r$ ($r \geq 2$), e $m = \varphi(n)$. Se $x = \sum_{i=0}^{m-1} a_i \zeta_n^i \in \mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_n]$ então*

$$Tr_{\mathbb{L}:\mathbb{Q}}(x\bar{x}) = \frac{n}{P} \left(\varphi(P) \sum_{i=0}^{m-1} a_i^2 + 2 \sum_{j=1}^{\varphi(P)-1} \mu\left(\frac{P}{t_j}\right) \varphi(t_j) A_{\frac{n}{Pj}} \right) \quad (7.53)$$

em que $P = p_1 \dots p_s$, $t_j = \text{mdc}(j, P)$ ($1 \leq j \leq \varphi(P) - 1$), μ é a função de Möbius (veja a equação 1.1) e $A_k = a_0 a_k + a_1 a_{k-1} + \dots + a_{m-1-k} a_{m-1}$, para qualquer $1 \leq k \leq m - 1$.

Exemplo 7.4.3. *Considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_9)$ de grau $\varphi(9) = 6$. O discriminante desse corpo é $D(\mathbb{K}) = \pm 3^9$, seu anel de inteiros é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_9]$ e $\{1, \zeta_9, \zeta_9^2, \dots, \zeta_9^5\}$ é uma $\mathbb{Q}$ -base de $\mathbb{K}$. Considere $I = (1 + \zeta_9 + \zeta_9^2 + \zeta_9^3 + \zeta_9^4 + \zeta_9^5)\mathcal{O}_{\mathbb{L}}$. Por ser um ideal principal, $N(I) = N(1 + \zeta_9 + \zeta_9^2 + \zeta_9^3 + \zeta_9^4 + \zeta_9^5) = 9$. Para qualquer $x \in I$ tem-se que*

$$x = (1 + \zeta_9 + \zeta_9^2 + \zeta_9^3 + \zeta_9^4 + \zeta_9^5)(a_0 + a_1 \zeta_9 + a_2 \zeta_9^2 + a_3 \zeta_9^3 + a_4 \zeta_9^4 + a_5 \zeta_9^5) \quad (7.54)$$

com cada $a_i \in \mathbb{Z}$. Pela proposição 7.4.1,

$$Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) = 18 \left(S + \sum_{i=0}^5 a_i^2 \right) \quad (7.55)$$

em que $S = a_0 a_1 + a_1 a_2 - a_0 a_3 + a_2 a_3 - a_0 a_4 - a_1 a_4 + a_3 a_4 - a_0 a_5 - a_1 a_5 - a_2 a_5 + a_4 a_5$. Logo, $t_I = 18$ (basta tomar $a_0 = 1$ e $a_i = 0$ para $i \neq 0$). Portanto, a densidade de centro do reticulado algébrico gerado por I é

$$\delta = \frac{18^3}{2^6 \cdot 9 \cdot \sqrt{3^9}} = \frac{1}{8\sqrt{3}} \quad (7.56)$$

que é a densidade máxima encontrada na dimensão 6.

Dimensão 8: Utilizando o mesmo raciocínio do caso anterior, mostremos um exemplo de reticulado algébrico na oitava dimensão.

Exemplo 7.4.4. *Considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_{20})$ de grau $\varphi(20) = 8$ e $I = (-1 - \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4)\mathcal{O}_{\mathbb{K}}$ um ideal de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$. O corpo $\mathbb{K}$ tem discriminante $D(\mathbb{K}) = \pm 2^8 \cdot 5^6$. Além disso, $N(I) = N(-1 - \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4) = 80$. Para qualquer $x \in I$, tem-se que*

$$x = (-1 - \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4) \left(\sum_{i=0}^7 a_i \zeta_{20}^i \right) \quad (7.57)$$

em que cada $a_i \in \mathbb{Z}$. Assim, pela proposição 7.4.1,

$$Tr_{\mathbb{K}:\mathbb{Q}}(x\bar{x}) = 40 \left(S + \sum_{i=0}^7 a_i^2 \right) \quad (7.58)$$

em que $S = a_0a_1 + a_1a_2 - a_0a_3 + a_2a_3 - a_0a_4 - a_1a_4 + a_3a_4 - a_1a_5 - a_2a_5 + a_4a_5 + a_0a_6 - a_2a_6 - a_3a_6 + a_5a_6 + a_0a_7 + a_1a_7 - a_3a_7 - a_4a_7 + a_6a_7$. Logo, tomando $a_0 = 1$ e $a_i = 0$ para $i \neq 0$, tem-se que $t_I = 40$. Neste caso, a densidade de centro do reticulado algébrico obtido a partir de I é

$$\delta = \frac{40^4}{2^8 \cdot 80 \cdot \sqrt{2^8 \cdot 5^6}} = \frac{1}{16} \quad (7.59)$$

que é a densidade de centro máxima na oitava dimensão.

Enfim, mostramos que é possível construir reticulados algébricos através do homomorfismo de Minkowski para dimensões 2, 4, 6 e 8. Em sua maioria, os resultados apresentados nesta seção devem-se aos estudos de Agnaldo, [9]. Também Cintya, [3], construiu reticulados algébricos para as dimensões 2, 4, 6, 8 e 12 através de uma “perturbação” no homomorfismo de Minkowski. Por sua vez, Carina, [2], apresentou uma série de construções de reticulados algébricos através de corpos ciclotômicos. Em sua tese, Grasielle, [17], também apresenta construção de reticulados D_n rotacionados para dimensões $n = 2^{r-2}$ ($r \geq 5$) e $n = (p-1)/2$ (p primo).

No entanto, até o momento não foi encontrado reticulado algébrico em dimensões ímpares cuja densidade de centro coincida com a densidade ótima. Em particular, não foi obtido ainda nenhum reticulado algébrico nas dimensões 3, 5 e 7. A busca por reticulados algébricos nessas dimensões constitui parte de nossos objetivos futuros.

Conclusão

Enfim, concluímos esta dissertação apresentando uma área de estudos onde a teoria desenvolvida ao longo de todo este texto pode ser aplicada. Na primeira seção, demos noções gerais e básicas sobre reticulados, matriz geradora, matriz de Gram e determinante de um reticulado. Na segunda seção, tratamos do problema do Empacotamento Esférico, atualmente muito útil à teoria dos Códigos Corretores de Erros. Na terceira seção, fizemos uma conexão entre reticulados e a Teoria Algébrica dos Números ao definir reticulados algébricos via o homomorfismo de Minkowski. Aí fizemos um comentário sobre os parâmetros envolvidos na fórmula da densidade de centro de reticulados algébricos produzidos por ideais de anéis de inteiros de corpos de números. Por fim, na quarta seção demos exemplos de reticulados algébricos construídos nas dimensões 2, 4, 6 e 8.

Conclusão

Enfim, apresentamos neste trabalho uma grande variedade de corpos de números e seus respectivos anéis de inteiros. Inicialmente, estudamos os anéis de inteiros monogênicos, ou seja, aqueles que têm base integral potente. A primeira classe de corpos que estudamos foram os quadráticos, $\mathbb{Q}(\sqrt{d})$, cujo anel de inteiros provamos ser $\mathbb{Z}[\theta]$, em que $\theta = \sqrt{d}$ ou $\theta = (1/2)(1 + \sqrt{d})$. Depois, nos dedicamos a mostrar que o anel de inteiros de um corpo ciclotômico $\mathbb{Q}(\zeta)$ é $\mathbb{Z}[\zeta]$ e que o anel de inteiros do subcorpo ciclotômico maximal real $\mathbb{Q}(\zeta + \zeta^{-1})$ é $\mathbb{Z}[\zeta + \zeta^{-1}]$.

Curiosos pela observação de que todos os anéis de inteiros citados anteriormente eram monogênicos, nos dedicamos à compreensão do artigo [32], que estudou a monogênese do anel de inteiros em alguns corpos de números abelianos imaginários, a saber $\mathbb{Q}(\zeta_n - \zeta_n^{-1})$, com $n = 2^m$ e $n = 4p^m$ ($p > 2$ primo). Porém, como vimos no capítulo 4, utilizando os conceitos de discriminante e de diferente, o referido autor mostrou que o corpo $\mathbb{Q}(\zeta_n - \zeta_n^{-1})$ não possui anel de inteiros monogênico quando $n = 3p^n$, em que $p > 3$ é primo.

Mudando o foco, passamos a analisar quais anéis de inteiros possuíam base normal. Como base normal é uma base formada pelas imagens de um elemento α pelos automorfismos do grupo de Galois de um certo corpo de números, nos restringimos às extensões galoisianas finitas sobre $\mathbb{Q}$. Provamos o Teorema de Hilbert-Speiser, que afirmou que um corpo de números abeliano K de condutor n possui base integral normal se, e somente se, n é ímpar e livre de quadrados.

Generalizando o Teorema de Hilbert-Speiser, nos dedicamos a mostrar o Teorema de Leopoldt-Letl no sexto capítulo, segundo o qual todo corpo de números abeliano K possui anel de inteiros dado por $\mathcal{O}_K = R_K T = \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G] \eta_d$, em que n é o condutor de K , R_K é uma $\mathbb{Z}$ -ordem de $\mathbb{Q}[G]$, T é um elemento de $\mathcal{O}_K$ e os outros parâmetros foram definidos no capítulo 6. Apesar da primeira igualdade ter sido mostrada em 1959 no artigo [19], apresentamos a demonstração do teorema citado conforme desenvolvida por [20] em 1990.

Finalmente, no último capítulo, aplicamos os conhecimentos obtidos sobre Teoria Algébrica dos

Números e, em particular, sobre anéis de inteiros de alguns corpos de números apresentados no texto para construir reticulados algébricos. Mostramos exemplos de reticulados construídos via o homomorfismo de Minkowski que apresentam densidade de centro ótima nas dimensões 2, 4, 6 e 8. No entanto, comentamos que ainda não são conhecidos exemplos de reticulados algébricos com densidade de centro ótima em dimensões ímpares.

Com relação à produção da dissertação em si, fazemos ainda alguns comentários. Inicialmente, foi proposto pelo orientador deste trabalho o estudo dos artigos [32] e [12], tendo em vista as futuras aplicações que isso poderia ter a reticulados algébricos. O primeiro artigo foi estudado logo no início do desenvolvimento desta dissertação e exigiu aprofundamento de alguns tópicos em Teoria Algébrica dos Números, como os apresentados na seção 2.7. Esse estudo deu origem aos teoremas 3.3.2, 3.3.3 e 4.3.1 e aos seus lemas. Comparando o artigo original às demonstrações apresentadas, é possível notar o trabalho minucioso que foi feito para detalhar os resultados citados. Com relação ao segundo artigo proposto inicialmente, houve uma mudança de planos. Ao iniciar sua leitura, tomamos conhecimento do artigo [20], que prova o Teorema de Leopoldt-Letl (antes desconhecido pelo autor e pelo seu orientador). Notando sua possível utilidade aos nossos estudos futuros, decidimos nos dedicar ao minucioso detalhamento da teoria apresentada nesse artigo. Isso exigiu grandes esforços. Primeiramente, tivemos que estudar de maneira profunda os conceitos de caracteres, que deram origem ao quinto capítulo desta dissertação. Depois, tendo em vista alguns resultados não demonstrados ou menos detalhados no referido artigo, tivemos que pesquisar em outros artigos de autoria de Kurt Girstmair e Heinrich-Wolfgang Leopoldt as soluções para os nossos problemas. Em termos de experiência pessoal do autor, uma das maiores dificuldades enfrentadas foi provar de maneira autônoma os resultados do capítulo 6. Com exceção do Teorema de Leopoldt-Letl e dos dois lemas anteriores a ele (que foram rigorosamente provados pelo autor de [20]), quase todos os outros resultados do capítulo 6 foram demonstrados autonomamente pelo autor desta dissertação. Isso exigiu um trabalho minucioso, uma longa pesquisa e até mesmo a leitura de algumas partes do artigo [19], em alemão.

Com relação às perspectivas futuras, nossos principais objetivos consistem em aplicar os resultados desenvolvidos nesta dissertação, em especial no capítulo 6, à teoria de reticulados algébricos. Por exemplo, um dos nossos propósitos é buscar reticulados algébricos com densidade de centro ótima em espaços de dimensão ímpar, o que ainda não foi encontrado. Além disso, também devemos concentrar esforços na busca da minimização da força traço presente na fórmula da densidade de centro de reticulados algébricos em algumas extensões de corpos de números (veja 7.36). A monogênese de

anéis de inteiros é ainda outro tópico (mais teórico) que pretendemos aprofundar no futuro.

Enfim, concluímos este trabalho com o sentimento de missão cumprida e com a expectativa de que esta dissertação dê futuras contribuições a outras teses, dissertações e artigos. Agradecemos aos leitores e esperamos que este trabalho tenha contribuído para seu crescimento intelectual.

Referências

- [1] ALACA, Saban; WILLIAMS, Kenneth. **Introductory Algebraic Number Theory**. Nova Iorque. Cambridge University Press, 2004.
- [2] ALVES, Carina. **Reticulados via Corpos Ciclotômicos**. Dissertação (Mestrado em Matemática). Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, fev. 2005.
- [3] BENEDITO, Cintya Wink de Oliveira. **Famílias de Reticulados Algébricos e Reticulados Ideais**. Dissertação (Mestrado em Matemática). Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, fev. 2010.
- [4] BRINKHUIS, Jan. Normal integral bases and complex conjugation. [s.l.] **Journal für die reine und angewandte Mathematik**. Volume 1987, Issue 375-376, jan. 1987.
- [5] CONWAY, John; SLOANE, Neil. **Sphere Packings, Lattices and Groups**. 3. ed. Nova Iorque. Springer-Verlag, 1998.
- [6] DOMINGUES, Hygino; IEZZI, Gelson. **Álgebra Moderna**. 4. ed. São Paulo. Atual Editora. 2003.
- [7] ENDLER, Otto. **Teoria dos números algébricos**. 2. ed. Rio de Janeiro. Projeto Euclides. Instituto de Matemática Pura e Aplicada, 2006.
- [8] ENDLER, Otto. **Teoria dos Corpos**. Publicações Matemáticas. Instituto de Matemática Pura e Aplicada, 2012.
- [9] FERRARI, Agnaldo José. **Reticulados Algébricos via Corpos Abelianos**. Dissertação (Mestrado em Matemática). Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, fev. 2008.

- [10] GIRSTMAIR, Kurt. Character Coordinates and Annihilators of Cyclotomic Numbers. **Manuscripta Math.** 59, no. 3, 375-389, 1987.
- [11] GIRSTMAIR, Kurt. An Index Formula for the Relative Class Number of an Abelian Number Field. **Journal of Number Theory** 32, p. 100-110, 1989.
- [12] GIRSTMAIR, Kurt. On the trace of the ring of integers of an abelian number field. **Acta Arithmetica** 62, no. 4, p. 383-389, 1992.
- [13] HASSE, Helmut. **Vorlesungen Über Zahlentheorie**. Berlin. Springer-Verlag, 1950.
- [14] HOFFMAN, Kenneth; KUNZE, Ray. **Linear Algebra**. 2. ed. Nova Jersey. Prentice-Hall, 1971.
- [15] HUNGERFORD, Thomas. **Algebra**. Nova Iorque. Springer-Verlag, 1974.
- [16] JOHNSTON, Henri. **Notes on Galois Modules**. Disponível em <https://www.dpmms.cam.ac.uk/~hlj31/GM_CourseNotes101.pdf>. Acesso em 08 dez. 2014.
- [17] JORGE, Grasielle Cristiane. **Reticulados q -ários e algébricos**. Tese (Doutorado em Matemática). Instituto de Matemática, Estatística e Computação Científica, UNICAMP, Campinas, 2012.
- [18] LIMA, Elon Lages. **Elementos de Topologia Geral**. Rio de Janeiro. Textos Universitários. SBM, 2009.
- [19] LEOPOLDT, Von Heinrich-Wolfgang. Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, **J. reine angew. Math.** 201, 119-149, 1959.
- [20] LETTL, Günter. The ring of integers of an abelian number field. **J. reine angew. Math.** 404, p. 162-170, 1990.
- [21] LANG, Serge. **Cyclotomic Fields I and II**. Comb. 2. ed. Springer Science+Business Media New York, 1990.
- [22] LANG, Serge. **Algebra**. Rev. 3. ed. Springer, 2002.
- [23] MARCUS, Daniel. **Number Fields**. Nova Iorque. Springer-Verlag, 1977.
- [24] MILIES, Francisco Cesar Polcino. **Anéis e Módulos**. São Paulo. Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo, 1972.

- [25] MILIES, Francisco Cesar Polcino; SEHGAL, Sudarshan. **An Introduction to Group Rings**. Holanda. Kluwer Academic Publishers, 2002.
- [26] QUILLES, Cátia Regina de Oliveira. **Discriminante de Corpos de Números**. Dissertação (Mestrado em Matemática). Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, fev. 2006.
- [27] REINER, Irving. **Maximal Orders**. Clarendon Press, Oxford, 2003.
- [28] RIBENBOIM, Paulo. **Classical Theory of Algebraic Numbers**. 1 ed. Nova Iorque. Springer-Verlag, 2001.
- [29] ROBINSON, Derek. **A Course in the Theory of Groups**. 2. ed. Nova Iorque. Springer-Verlag, 1995.
- [30] SAMUEL, Pierre. **Algebraic Theory of Numbers**. Paris. Hermann, 1970.
- [31] SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro. Coleção Matemática Universitária. Instituto de Matemática Pura e Aplicada, 2009.
- [32] SHAH, Syed Inayat Ali; NAKAHARA, Toru. Monogenesis of the rings of integers in certain imaginary abelian fields. **Nagoya Math. J.** Vol. 168, p. 85-92, 2002.
- [33] STEWART, Ian; TALL, David. **Algebraic Number Theory and Fermat's Last Theorem**. 3. ed. Natick. A K Peters, 2002.
- [34] WASHINGTON, Lawrence. **Introduction to Cyclotomic Fields**. 2. ed. Nova Iorque. Springer-Verlag, 1995.

Índice

- R -reticulado completo, [38](#)
- $\mathbb{K}$ -
 - automorfismo, [28](#)
 - homomorfismo, [28](#)
 - isomorfismo, [28](#)
 - monomorfismo, [28](#)
- álgebra, [37](#)
 - de grupo, [41](#)
- índice de ramificação, [73](#)
- algoritmo da Divisão Euclidiana, [27](#)
- anel, [28](#)
 - de integridade, [28](#)
 - de inteiros, [66](#)
 - Noetheriano, [58](#)
- anel de grupo, [41](#)
- anel de inteiros
 - monogênico, [118](#)
 - não monogênico, [118](#)
- automorfismo, [28](#)
- base
 - de potências, [109](#)
 - integral, [67](#)
 - de potências (BIP), [118](#)
- normal (BIN), [113](#)
- normal, [110](#)
- potente, [109](#)
- Basiszahl, [171](#)
- caractere, [123](#)
 - conjugado, [123](#)
 - coordenado de Leopoldt, [161](#)
 - de Dirichlet, [136](#)
 - primitivo, [140](#)
 - modular módulo n , [136](#)
 - trivial, [133](#)
- classe
 - de ramo, [154](#)
 - residual, [31](#)
- condutor, [97](#), [137](#)
- congruência, [30](#)
- conjunto
 - das classes residuais módulo m , [31](#)
- corpo, [28](#)
 - ciclotômico, [87](#)
 - de números, [66](#)
 - totalmente imaginário, [194](#)
 - totalmente real, [194](#)

- quadrático, 83
- densidade
 - de centro, 189
 - de empacotamento, 189
- determinante, 49
 - do reticulado, 187
- diferente, 79, 80
- discriminante, 53
 - de elemento, 55
 - do corpo de números, 69
 - relativo, 75
- divisor de zero, 53
- domínio, 28
 - de Dedekind, 58
 - de integridade, 28
 - integralmente fechado, 47
- elemento
 - integral, 44
 - primitivo, 28
- empacotamento
 - esférico, 189
 - reticulado, 189
- endomorfismo, 28
- epimorfismo, 28
- equação de dependência integral, 44
- fecho
 - integral, 46
- função
 - de Euler, 32
 - de Möbius, 27
 - parte potente, 153
- grau
 - de inércia, 73
 - do corpo de números, 66
- grupo, 27
- homomorfismo
 - de Minkowski, 193
 - injetor, 28
 - sobrejetor, 28
- ideal
 - abaixo, 72
 - acima, 72
 - discriminante, 53
 - fracionário, 61
 - integral, 61
 - irredutível, 65
 - primo
 - brandamente ramificado, 116
 - severamente ramificado, 116
 - totalmente decomposto, 74
 - totalmente inerte, 74
 - totalmente ramificado, 74
 - ramificado, 74
- identidade de Bezout, 27
- inteiro algébrico, 66
- isomorfismo, 28
- Lema
 - de Dedekind, 110
 - de Gauss, 91
 - de Zorn, 26
- módulo, 29
 - Noetheriano, 57

- matriz
 - de Gram, 187
 - geradora, 186
- monomorfismo, 28
- norma, 49
 - do ideal, 70
 - relativa, 77
- operador de mudança, 135
- ordem, 38, 39
- período, 108
 - de Gauss, 98, 104
- polinômio
 - característico, 49
 - ciclotômico, 90
- Princípio da Boa Ordem, 25
- produto
 - interno de caracteres, 133
- propriedade de Separação, 129
- raio de empacotamento, 189
- raiz
 - n -ésima da unidade, 87
 - n -ésima primitiva da unidade, 87
- ramificação, 74
- região fundamental, 182
- reticulado, 181
 - A_n , 190
 - D_n , 191
 - E_6 , E_7 e E_8 , 191
 - algébrico, 195
 - completo, 181
 - fcc, 190
 - hexagonal, 190
- soma
 - de Gauss, 146
 - primitiva, 150
- subálgebra, 37
- subcorpo
 - ciclotômico, 96
 - maximal real, 97
- subgrupo
 - discreto, 184
- suporte, 40, 136
- Teorema
 - Chinês do Resto, 32
 - da Base Normal, 112
 - da Igualdade Fundamental, 74
 - de Euler, 27
 - de Hilbert-Speiser, 117
 - de Kronecker-Weber, 96
 - de Leopoldt-Lettl, 177
 - do Condutor-Discriminante, 143
 - do Elemento Primitivo, 28, 109
 - Fundamental da Aritmética, 27
 - Fundamental de Galois, 29
 - Fundamental dos Grupos Abelianos Finitamente Gerados, 30
- Teoria de Galois, 29
- traço, 49
 - relativo, 77
- unidade ciclotômica, 88
- volume do reticulado, 186