**UNIVERSIDADE FEDERAL DE SERGIPE**

Centro de Ciências Exatas e Tecnologia

Departamento de Matemática

# O número de classes de um corpo de números.

Monografia apresentada ao Departamento de Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do título de Bacharelado em Matemática.

por

**Rafael Fagundes Bitencourt Silva**

Bacharelado em Matemática – São Cristóvão - SE

Orientador: Prof. Dr. Cayo Rodrigo Felizardo Dória

**Janeiro de 2026**

AGRADECIMENTOS

**AGRADECIMENTOS**

Primeiramente, agradeço a Deus por sustentar a minha vida até este ponto. Já é bem mais do que mereço.

Agradeço imensamente ao meu pai e minha mãe, Dorielma Bitencourt dos Santos Silva e José Edilson Silva, que, mesmo receosos com a minha escolha, acreditaram no meu esforço e não só me permitiram seguir na matemática, como me apoiaram até hoje. À toda minha família, sou extremamente grato.

Ao meu orientador, Cayo Dória, que não somente me orientou durante a elaboração deste, mas trilhou comigo uma jornada de dois anos de projetos de pesquisa. Pela sua paciência comigo, sou extremamente grato.

Por fim, agradeço a todos aqueles que estiveram comigo nesta jornada, seja estudando as mesmas matérias juntos, ou participando das mesmas atividades. Menciono em especial Mirelly Ferreira, minha namorada, em cujo abraço repousei inúmeras vezes em momentos difíceis.

Rafael Fagundes Bitencourt Silva.

## RESUMO

Esta monografia visa a tratar da estrutura dos corpos de números e de seus anéis de inteiros, com foco no grupo de classes; mais especificamente, com o objetivo de estudar a sua cardinalidade, procedendo da fundamentação algébrica às construções analíticas. Como aplicações, mostramos fórmulas para o número de classes em tipos de corpos de números essenciais para a Teoria Algébrica dos Números: os corpos ciclotômicos, e os corpos quadráticos.

**Palavras-chave:** Corpos de números, grupo de classes, anel de inteiros, teoria dos números.

**ABSTRACT**

This monograph aims to address the structure of number fields and their ring of integers, focusing on the class group. More specifically, it aims to study its order, proceeding from the algebraic basis to analytical constructions. As applications of the theory, we study the class group of two types of fields, which are essential to Algebraic Number Theory: the cyclotomic fields and quadratic fields.

**Keywords:** Number Fields, class group, ring of integers, number theory.

# Sumário

# Introdução

Uma das motivações centrais da Teoria Algébrica dos Números é o estudo de como propriedades aritméticas clássicas, observadas inicialmente no domínio dos inteiros $\mathbb{Z}$, se comportam quando o contexto é ampliado. Ao passar dos inteiros para estruturas mais gerais, no nosso caso, anéis de inteiros de corpos de números, muitas dessas propriedades deixam de ser universais, revelando novas sutilezas e levantando questões fundamentais sobre a natureza da aritmética nesses ambientes. Esse processo de generalização exige o desenvolvimento de ferramentas capazes de descrever e organizar os fenômenos que emergem nesse quadro mais geral.

Um dos exemplos mais marcantes dessa mudança de comportamento ocorre com a fatoração única em elementos primos, propriedade central dos números inteiros que nem sempre se preserva em anéis de inteiros arbitrários. Este fato é crucial para o aperfeiçoamento de técnicas de solução para problemas diofantinos usando conceitos de divisibilidade (começamos o primeiro capítulo com o exemplo da equação $p = x^2 + y^2$, com $p$ primo), pois frequentemente o estudo de um determinado anel de inteiros é uma ferramenta poderosa na solução de tais problemas. Esta propriedade, porém, não se perde por si só, mas como consequência de outra tão fundamental quanto, mas não tão notada: todo ideal de $\mathbb{Z}$ é principal, ou, na denominação padrão, $\mathbb{Z}$ é um domínio de ideais principais. Visando não apenas a determinar quando um certo anel de inteiros é um domínio de ideais principais ou não, mas também medir o qual distante ele está de sê-lo, surge o grupo de classes, o nosso principal objeto de estudo, cuja cardinalidade queremos, num certo sentido, determinar.

Nosso caminho é dividido em duas etapas, sugeridas pelos títulos dos capítulos: a algébrica e a analítica. Não que uma se separe da outra de forma completamente independente. O Capítulo 1 fornece as ferramentas e resultados essenciais separadamente, o Capítulo 2 as junta numa única fórmula. No que tange aos capítulos, o Capítulo 1 tem como protagonista o anel de inteiros, a ideia que generaliza o anel dos inteiros racionais para corpos de números. Discutimos neles sobre a noção de divisibilidade, sobre as propriedades do seus ideais e, a partir disso, definimos o nosso objeto de estudo, o grupo de classes. Ao final do capítulo, damos uma aplicação da teoria em corpos ciclotômicos. Para este, adotamos a ordem e as notações da referência [6][Chapter 1]. Já no Capítulo 2, o protagonista torna-se uma generalização de uma das funções mais conhecidas da matemática: a função zeta de Riemann, que, no nosso caso, generaliza-se para a função Zeta de Dedekind. Discutimos as propriedades analíticas desta função nas primeiras duas seções e, na terceira, obtemos o nosso principal resultado: uma fórmula que nos permite, quando não calcular, ao menos estimar a ordem do grupo de classes. Como adendo, deixamos duas seções, que aplicam esta fórmula para os já mencionados corpos ciclotômicos, e para os corpos quadráticos. Para este, temos [2][Chapter 5] como principal referência.

Assim sendo, este trabalho não é só um estudo de um objeto da teoria dos números, mas também uma amostra do que os pensares algébrico e analítico podem fazer juntos, e não apenas separados.

# Capítulo 1

# Parte algébrica.

## 1.1 Inteiros gaussianos.

Dado um número primo $p$ diferente de $2$, como saber se podemos escrevê-lo como soma de dois quadrados? Um indício de que talvez o possamos é se tivermos $p \equiv 1 \mod 4$. De fato, como todos os quadrados módulo $4$ serão congruentes a $0$, ou a $1$, e não podemos ter a primeira opção, para $p$ ímpar, é claro que $p \equiv 1 \mod 4$ é uma condição necessária. O que não é tão claro é o surpreendente fato de ela também ser suficiente.

**Teorema 1.1.1.** *Seja $p$ um número primo diferente de $2$, tem-se*

$$p = a^2 + b^2 \text{ com } a, b \in \mathbb{Z} \Leftrightarrow p \equiv 1 \mod 4.$$

A prova deste Teorema depende do fato de que, no anel

$$\mathbb{Z}[i] = \{a + bi |\ a, b \in \mathbb{Z}\},$$

a equação $p = x^2 + y^2$ reescreve-se como $p = (x + iy)(x - iy)$.

**Proposição 1.1.1.** *O anel $\mathbb{Z}[i]$ é um domínio euclidiano com a função $\mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ dada por $\alpha \mapsto |\alpha|^2$. Em particular, $\mathbb{Z}[i]$ é um domínio de fatoração única.*

**Demonstração.** Sejam $\alpha$ e $\beta \in \mathbb{Z}[i]$, queremos mostrar a existência de $\gamma, \rho \in \mathbb{Z}[i]$, $\beta \neq 0$, tais que

$$\alpha = \gamma\beta + \rho, \text{ com } |\rho|^2 < |\beta|^2.$$

É mais que suficiente encontrar $\gamma$ tal que

$$\left| \frac{\alpha}{\beta} - \gamma \right| < 1.$$

E definir $\rho$ como $\alpha - \gamma\beta$. Como $\mathbb{Z}[i]$ é um reticulado em $\mathbb{Q}(i)$ (gerado pelos vetores $1$ e $i$) e $\dfrac{\alpha}{\beta}$ pertence a alguma malha do reticulado, tomemos $\gamma$ como sendo o ponto do reticulado mais próximo de $\dfrac{\alpha}{\beta}$. Ora, $\gamma$ dista de $\dfrac{\alpha}{\beta}$ menos da metade da diagonal da malha, isto é, menos de $\dfrac{\sqrt{2}}{2}$, que é menor do que $1$. □

Voltando à prova do Teorema 1.1.1, restringimos o problema a provar que um primo $p \equiv 1$

$\mod 4$ não permanece primo em $\mathbb{Z}[i]$. De fato, suponhamos que temos isto provado. Seja

$$p = \alpha\beta,$$

com $\alpha, \beta \notin \mathbb{Z}[i]^*$ e $p$ primo. Definimos a *norma* de um elemento $z = x + iy$ como sendo

$$N(x + iy) = (x + iy)(x - iy) = x^2 + y^2 = |z|^2.$$

Pela fórmula, vemos que $N$ é multiplicativa e, portanto

$$p = \alpha\beta \Rightarrow p^2 = N(\alpha)N(\beta).$$

Por outro lado, $\alpha, \beta \notin \mathbb{Z}[i]^*$ implica $N(\alpha), N(\beta) \neq 1$. Pela fatoração única em $\mathbb{Z}$, temos $N(\alpha) = N(\beta) = p$. Ora, se $\alpha = a + bi$ é tal que $N(\alpha) = p$, uma fatoração trivial de $p$ em $\mathbb{Z}[i]$ é

$$\alpha\overline{\alpha} = (a + bi)(a - bi) = N(\alpha) = a^2 + b^2 = p.$$

Portanto, se um primo inteiro não é primo em $\mathbb{Z}[i]$, ele é a norma de algum elemento de $\mathbb{Z}[i]$, donde é soma de dois quadrados.

Seja agora $p = 1 + 4n$, com $n \in \mathbb{N}$. Note que $x = (2n)!$ é solução da congruência

$$-1 \equiv x^2 \mod p.$$

De fato, o Teorema de Wilson nos diz $-1 \equiv (p-1)! \mod p$, portanto,

$$-1 \equiv (1 \cdot 2 \cdot ... \cdot 2n)[(p-1)(p-2)...(p-2n)] \equiv (2n)!(-1)^{2n}(2n)! \equiv [(2n)!]^2 \mod p.$$

Desta última igualdade, temos $p|(x^2 + 1)$ em $\mathbb{Z}$, que implica $p|(x + i)(x - i)$, em $\mathbb{Z}[i]$. Mas os números $\frac{x}{p} \pm \frac{i}{p}$ sequer são inteiros gaussianos, donde $p$ divide um produto, sem dividir nenhum de seus fatores, logo, não é primo.

Este exemplo, que consiste em resolver a equação $p = x^2 + y^2$, mostra como questões aparentemente elementares sobre inteiros podem nos levar a questões sobre divisibilidade em domínios maiores, e serve como um prólogo do que estamos para fazer: estudar uma teoria de divisibilidade para anéis mais gerais (na verdade trataremos principalmente de domínios, mas muitas considerações supõem apenas anéis). Nesse sentido, dois subconjuntos do domínio devem ser encontrados: o conjunto dos seus *primos*, e o conjunto das suas *unidades*. No nosso exemplo concreto, as caracterizações são relativamente simples.

A proposição abaixo descreve o grupo das unidades $\mathbb{Z}[i]$; e é uma consequência direta de estas serem exatamente os elementos de norma $1$. Este fato, por sua vez, dá-se porque a norma de um elemento não-nulo de $\mathbb{Z}[i]$ é um inteiro positivo, e, pela multiplicatividade, temos $N(ab) \geq N(a)$, qualquer que seja $b$ não-nulo. Supondo $a$ uma unidade de $\mathbb{Z}[i]$, temos $1 = N(1) = N(a^{-1}a) \geq N(a)$, e portanto temos $N(a) = 1$. Reciprocamente, se $N(a) = 1$, temos que $\overline{a}$ é o inverso multiplicativo de $a$, e, portanto, $a$ é uma unidade.

**Proposição 1.1.2.** $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

O Teorema abaixo responde quem são todos os primos de $\mathbb{Z}[i]$. Antes de demonstrá-lo, relembremos do seguinte conceito.

**Definição 1.1.1.** *Dois elementos $a$ e $b$ de um anel comutativo com unidade $A$ são ditos associados se $a = \varepsilon b$, com $\varepsilon \in A^*$.*

**Teorema 1.1.2.** *Os primos de $\mathbb{Z}[i]$ são, a menos de associados:*

*1)* $\pi = 1 + i$

*2)* $\pi = a + bi$ *com* $a^2 + b^2 = p$, *sendo* $p$ *primo e* $p \equiv 1 \mod 4$.

*3)* $\pi = p$, *onde* $p$ *é primo inteiro e* $p \equiv 3 \mod 4$.

**Demonstração.** Se $\pi$ é satisfaz $1)$ ou $2)$, então $\pi = \alpha\beta$ implica $p = N(\pi) = N(\alpha)N(\beta)$, com $p$ primo. Mas, se $\alpha, \beta \in \mathbb{Z}[i]$, então $N(\alpha), N(\beta) \in \mathbb{Z}$; donde um destes dois últimos é igual a $1$ e, portanto, $\alpha$ ou $\beta$ é unidade de $\mathbb{Z}[i]$.

Se $\pi = p \equiv 3 \mod 4$, então $p = \alpha\beta \Rightarrow p^2 = N(\alpha)N(\beta)$; se nem $\alpha$ nem $\beta$ é unidade de $\mathbb{Z}[i]$, então $N(\alpha) = N(\beta) = p$, o que implicaria $p \equiv 1 \mod 4$.

Seja $\pi$ um elemento primo de $\mathbb{Z}[i]$. Dado que $N(\pi) = \pi\overline{\pi} = p_1 p_2 \dots p_n$, com $p_i$ primo. Daí, como $\pi$ é primo, e $\pi$ divide o produto $p_1 p_2 \dots p_n$, tem-se $\pi | p$, para $p = p_i$. Mas então $N(\pi) | p^2 \Rightarrow N(\pi) = p$ ou $N(\pi) = p^2$.

Se $N(\pi) = p$, então $\pi = a + bi \Rightarrow a^2 + b^2 = p$. Portanto, se $p = 2$, $\pi$ é associado de $1 + i$, ou satisfaz as condições de $2)$, caso contrário.

Se $N(\pi) = p^2$, então $\pi$ é associado a $p$, nesse caso, $p = 2$ ou $p \equiv 1 \mod 4$ implicaria $p = (a + bi)(a - bi)$ com $a$, $b \in \mathbb{Z}$, e ao menos um desses fatores dividiria $\pi$, sem ser, no entanto, uma unidade. □

Note que a proposição também responde à questão de como um certo primo inteiro $p$ fatora-se em $\mathbb{Z}[i]$. Temos $2 = (1 + i)(1 - i)$, $p = (a + bi)(a - bi)$, com $a^2 + b^2 = p$, se $p \equiv 1 \mod 4$ e $p$ primo de $\mathbb{Z}[i]$, caso $p \equiv 3 \mod 4$. Generalizar esta questão também será um tópico importante deste trabalho.

Note também que os inteiros gaussianos desempenham no corpo

$$\mathbb{Q}(i) = \{a + bi |\ a, b \in \mathbb{Q}\}$$

o mesmo papel que $\mathbb{Z}$ desempenha em $\mathbb{Q}$. Podemos então vê-los como "os inteiros de $\mathbb{Q}[i]$". No entanto, esta noção de integralidade só faz sentido tomando como base os elementos $1$ e $i$ (relembremos que $\mathbb{Q}(i)$ é um espaço vetorial de dimensão $2$ sobre $\mathbb{Q}$, ou, como dizemos, uma extensão quadrática). Podemos, no entanto, fornecer uma caracterização que independe de escolhas de base.

**Proposição 1.1.3.** $\mathbb{Z}[i] = \{\alpha \in \mathbb{Q}(i) |\ \exists\, a, b \in \mathbb{Z}$ *tal que* $\alpha^2 + a\alpha + b = 0\}$

**Demonstração.** Podemos construir um polinômio $x^2 + ax + b$ que tenha um zero no elemento $c + di$ de $\mathbb{Q}(i)$ simplesmente tomando $a = -2c$ e $b = c^2 + d^2$. Logo, se $c$ e $d$ são inteiros, também o são $a$ e $b$. Reciprocamente, como $4b = (2c)^2 + (2d)^2$ e $c = \dfrac{-a}{2}$, com $a \in \mathbb{Z}$, temos $(2c)^2 \equiv (2d)^2 \equiv 0 \mod 4$, donde o denominador de $d$ é, no máximo, $2$. Utilizando, novamente, que os inteiros módulo $4$ são $0$ ou $1$, temos que $c$ e $d$ são inteiros. □

Esta proposição leva-nos à seguinte generalização.

**Definição 1.1.2.** *Seja $K|\mathbb{Q}$ ( ou $K \supseteq \mathbb{Q}$) uma extensão finita de corpos. Dizemos que $K$ é um corpo de números algébricos, ou apenas corpo de números. Um elemento $a$ de $K$ é dito ser um inteiro algébrico, ou apenas um inteiro de $K$, se $f(a) = 0$, para algum $f(x) \in \mathbb{Z}[x]$ mônico. O conjunto dos inteiros de $K$ é chamado o anel de inteiros de $K$.*

No nosso exemplo, obtivemos uma completa descrição das unidades e dos primos do anel de inteiros de $\mathbb{Q}(i)$. No entanto, os métodos utilizados para $\mathbb{Q}(i)$ não funcionam em geral. Por exemplo, $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} |\ a, b \in \mathbb{Q}\}$ também é um corpo de números. Porém, a função correspondente à norma neste corpo, dada por $N(a+b\sqrt{5}) = a^2 - 5b^2$, não o torna um domínio euclidiano. Para lidar com anéis de inteiros de corpos de números mais gerais, precisaremos de mais ferramentas.

## 1.2 Integralidade

Ressaltamos que, neste trabalho, a palavra anel sempre significa anel comutativo com unidade.

**Definição 1.2.1.** *Seja $A \subseteq B$ uma extensão de anéis. Um elemento $b \in B$ é dito ser inteiro sobre $A$ se $f(b) = 0$, para algum $f(x) \in A[x]$ mônico. Dizemos que o anel $B$ é inteiro sobre $A$ se todos os seus elementos são inteiros sobre $A$.*

Gostaríamos de que o conjunto dos elementos de $B$ que são inteiros sobre $A$ fosse fechado para as operações de $B$, ou seja, fechado para a soma e o produto. Isto é, felizmente, verdade. Contudo, não é nada imediato, e depende de uma reinterpretação da noção de integralidade, que, inclusive, depende também do resultado abaixo, que vem da Álgebra Linear.

**Lema 1.2.1.** *Sejam $\mathcal{A}$ uma matriz $(r \times r)$ com entradas num anel e $\mathcal{A}^* = ((-1)^{i+j} \det \mathcal{A}_{ij})$ a sua matriz adjunta. Tem-se*

$$\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A} = \det \mathcal{A} \cdot I_{r\times r}.$$

*Além disso, para $x = (x_1, \ldots, x_r)$ um vetor arbitrário com entradas neste mesmo anel, tem-se*

$$\mathcal{A}x = 0 \Rightarrow \det \mathcal{A} \cdot x = 0.$$

**Proposição 1.2.1.** *Finitos elementos $b_1, \ldots, b_n \in B$ são inteiros sobre $A$ se, e somente se, $A[b_1, \ldots, b_n]$ é um $A-$módulo finitamente gerado.*

**Demonstração.** Seja $b \in B$ inteiro sobre $A$ e $f(x) \in A[x]$ um polinômio mônico de grau $n \geq 1$, tal que $f(b) = 0$. Pelo algoritmo da divisão de polinômios, podemos escrever qualquer $g(x) \in A[x]$ como

$$g(x) = q(x)f(x) + r(x),\ \deg(r(x)) < n.$$

Daí, temos

$$g(b) = r(b) = a_0 + a_1 b + \cdots + a_{n-1}b^{n-1},\ a_i \in A;$$

disso se conclui que $1, b, \ldots, b^{n-1}$ é um sistema de geradores de $A[b]$.

Suponhamos o resultado provado para todo inteiro positivo menor ou igual a $n-1$, onde $n > 1$. Desde que $b_n$ é inteiro sobre $A$, tem-se $b_n$ inteiro sobre $R = A[b_1, \ldots, b_{n-1}]$. Se $\xi_1, \ldots, \xi_r$ formam um sistema de geradores para $R$ (por hipótese de indução, existe um tal sistema, com $r < \infty$), $f(x) \in A[x] \subset R[x]$ é tal que $f(b_n) = 0$ e $\deg(f(x)) = p$, então $\xi_1, \ldots \xi_r, 1, b_n, \ldots, b^{p-1}$ formam um sistema de geradores para $R[b_n] = A[b_1, \ldots, b_n]$. Temos então provada a primeira implicação.

Assumamos agora que $A[b_1, \ldots, b_n]$ é finitamente gerado e que $\omega_1, \ldots \omega_r$ é um sistema de geradores. Seja $b \in A[b_1, \ldots, b_n]$ arbitrário, tem-se

$$b\omega_i = \sum_{j=1}^{r} a_{ij}\omega_j,\ a_{ij} \in A.$$

No conjunto das matrizes $r \times r$ com entradas em $A[b_1, \ldots, b_n]$, consideremos a matriz $bI - (a_{ij})$, a igualdade acima nos diz que

$$(bI - (a_{ij})) \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_r \end{bmatrix} = 0,$$

donde

$$\det(bI - (a_{ij})) \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_r \end{bmatrix} = 0.$$

Portanto, temos $\det(bI - (a_{ij}))\omega_i = 0$, para $i = 1, \ldots, r$. Mas então o polinômio $f(t) = \det(tI - (a_{ij}))$ é mônico, pertence a $A[t]$ e tem $b$ como raiz, donde $b$ é inteiro sobre $A$. □

Desta proposição, obtemos que, se $b_1, \ldots, b_n$ são inteiros sobre $A$, então qualquer elemento $b$ de $A[b_1, \ldots, b_n]$ também o é, pois $A[b_1, \ldots, b_n, b]$ também será um $A$-módulo finitamente gerado. Em particular, obtemos que, se $b_1$ e $b_2$ são inteiros sobre $A$, também o são $b_1 + b_2$ e $b_1 b_2$. Podemos também mostrar a seguinte proposição.

**Proposição 1.2.2.** *Sejam $A \subset B \subset C$ duas extensões de anéis. Se $C$ é inteiro sobre $B$ e $B$ é inteiro sobre $A$, então $C$ é inteiro sobre $A$.*

**Demonstração.** Tomemos $c \in C$ e $c^n + b_1 c^{n-1} + \cdots + b_0$, com $b_i \in B$. Seja $R = A[b_1, \ldots, b_n]$. Teremos $R[c]$ como um $R$-módulo finitamente gerado. Se $B$ é inteiro sobre $A$, então, em particular, cada $b_i$ é inteiro sobre $A$, donde $R[c]$ também é finitamente gerado como um $A$-módulo e, pela proposição anterior, $c$ é inteiro sobre $A$. □

Do que acabamos de provar, temos que o conjunto

$$\overline{A} = \{b \in B |\ b \text{ é inteiro sobre } A\}$$

é um subanel de $B$. Chamamos este subanel o *fecho integral de $A$ em $B$*. Dizemos que $A$ é *integralmente fechado em $B$* se $\overline{A} = A$. Se $A$ for um domínio, com corpo de frações $K$, então o fecho integral $\overline{A}$ de $A$ em $K$ é chamado a *normalização de $A$*. Quando estivermos nos referindo a este fecho integral e tivermos $A = \overline{A}$, diremos apenas que $A$ é integralmente fechado.

Tratemos desta última situação específica, isto é, quando temos $A$ um domínio, $K$ o seu corpo de frações, e $A$ integralmente fechado. Sejam $L|K$ uma extensão finita e $B$ o fecho integral de $A$ em $L$. Se $l_1, \ldots, l_k \in L$ são inteiros sobre $B$, então, para cada $l_i$, obtemos um polinômio mônico com coeficientes em $B$, que tem $l_i$ como um zero. Agrupando todos os coeficientes desses tais polinômios numa sequência finita $\alpha_1, \ldots, \alpha_m$ e denotando $\mathfrak{A} = A[\alpha_1, \ldots, \alpha_m]$, temos, pela Proposição 1.2.1 que $\mathfrak{A}[l_1, \ldots, l_k]$ é um $\mathfrak{A}$-módulo finitamente gerado. Ocorre que $\mathfrak{A}$ é um $A$-módulo finitamente gerado, e, portanto, também o é $\mathfrak{A}[l_1, \ldots, l_k]$. Como temos $\mathfrak{A}[l_1, \ldots, l_k] = A[\alpha_1, \ldots, \alpha_m, l_1, \ldots, l_k]$, então $l_1, \ldots, l_k$ são todos inteiros sobre $A$, e temos $B$ integralmente fechado em $L$.

**Proposição 1.2.3.** *Cada elemento $\beta \in L$ é da forma*

$$\beta = \frac{b}{a},$$

*com $b \in B$ e $a \in A$.*

**Demonstração.** De fato, se

$$a_n\beta^n + \cdots + a_1\beta + a_0 = 0,$$

com $a_j \in A$ e $a_n \neq 0$, então $b = a_n\beta$ é inteiro sobre $A$, pois podemos multiplicar a equação para $\beta$ por $a_n^{n-1}$ e obter

$$(a_n\beta)^n + \ldots a_1'(a_n\beta) + a_0' = 0.$$

□

**Observação 1.2.1.** *É útil observar que, como $A$ é integralmente fechado, um elemento $\beta \in L$ é inteiro sobre $A$ se, e somente se, seu polinômio minimal (sobre $K$) pertence a $A[x]$.*

Duas funções aparecem como ferramentas poderosas no estudo dos inteiros de $L$.

**Definição 1.2.2.** *O traço e a norma de um elemento $x \in L$ são, respectivamente, o traço e o determinante da transformação linear*

$$m_x : L \to L,\ \alpha \mapsto x\alpha,$$

*como um $K-$espaço vetorial. São denotados, respectivamente, por $\mathrm{Tr}_{L|K}$ e $N_{L|K}$.*

Uma outra forma de definir o traço e a norma, é como os coeficientes $a_1$ e $a_n$ no polinômio característico

$$f_x(t) = \det(t\mathrm{Id} - m_x) = t^n - a_1t^{n-1} + \cdots + (-1)^n a_n$$

de $m_x$. Além disso, como $(m_x + m_y) = m_x + m_y$ e $m_{xy} = m_x \circ m_y$, obtemos homomorfismos

$$\mathrm{Tr}_{L|K} : L \to K,\ N_{L|K} : L^* \to K^*,$$

como grupos aditivos e multiplicativos.

No caso de $L|K$ ser uma extensão separável, obtemos uma interpretação do traço e da norma, em termos da teoria de Galois.

**Proposição 1.2.4.** *Se $L|K$ é uma extensão separável e $\sigma : L \to \overline{K}$ percorre todos os $K$-monomorfismos de $L$ em $\overline{K}$, o fecho algébrico de $K$, então:*

*i)* $f_\alpha(t) = \prod_\sigma (t - \sigma(\alpha))$.

*ii)* $\mathrm{Tr}(\alpha) = \sum_\sigma \sigma(\alpha)$.

*iii)* $N(\alpha) = \prod_\sigma \sigma(\alpha)$.

**Demonstração.** Afirmamos que o polinômio característico $f_\alpha$ satisfaz

$$f_\alpha(t) = \varphi_\alpha(t)^d, \text{ com } d = [L : K(\alpha)],$$

onde $\varphi_\alpha(t)$ é o polinômio minimal de $\alpha$ sobre $K$.

De fato, escrevamos

$$\varphi_\alpha(t) = t^m + c_1t^{m-1} + \cdots + c_m.$$

Tem-se que $1, \alpha, \ldots, \alpha^{m-1}$ formam uma base para $K(\alpha)$, visto como $K$-espaço vetorial. Se $x_1, \ldots, x_d$ formam uma base de $L$, visto como $K(\alpha)$ espaço vetorial, então $x_1, x_1\alpha, \ldots, x_1\alpha^{m-1}, x_2, \ldots, x_d\alpha^{m-1}$ formam uma base para $L$, visto como $K$ espaço vetorial. Apliquemos $m_\alpha$ nos elementos desta base,

temos

$$m_\alpha(x_i\alpha^j) = \begin{cases} x_i\alpha^{j+1}, & j < m-1. \\ -c_m x_i - c_{m-1}x_i\alpha - \cdots - c_1 x_i \alpha^{m-1}, & j = m-1. \end{cases}$$

Em coordenadas, temos

$$m_\alpha(0,\ldots,\overset{\overset{m(i-1)+j}{\uparrow}}{1},\ldots,0) = \begin{cases} (0,\ldots,\overset{\overset{m(i-1)+j+1}{\uparrow}}{1},\ldots,0), & j < m-1. \\ (0,\ldots,\overset{\overset{m(i-1)+j}{\uparrow}}{-c_m},\ldots,\overset{\overset{mi+j}{\uparrow}}{-c_1},0,\ldots,0), & j = m-1. \end{cases}$$

Disto se conclui que a matriz de $m_\alpha$ na base supracitada é diagonal por blocos, cada bloco sendo igual a

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1 \end{pmatrix}.$$

Ora, o polinômio característico desta matriz é justamente $\varphi_\alpha(t)$, donde fica claro que $f_\alpha(t) = \varphi_\alpha(t)^d$.

Seja agora $H(L|K)$ o conjunto dos $K$-monomorfismos de $L$ em $\overline{K}$. Como a extensão $L|K$ é separável, a extensão $L|K(\alpha)$ também é separável, donde a relação

$$\sigma \sim \tau \Leftrightarrow \sigma(\alpha) = \tau(\alpha)$$

particiona $H(L|K)$ em $m$ classes de equivalência, cada uma com $d$ elementos, daí, se $\sigma_1,\ldots,\sigma_m$ formam um sistema de representantes de classes, tem-se

$$f_\alpha(t) = \varphi_\alpha(t) = \prod_{i=1}^{n}(t-\sigma_i(\alpha))^d = \prod_{i=1}^{n}\prod_{\tau\sim\sigma_i}(t-\tau(\alpha)) = \prod_{\sigma\in H(L|K)}(t-\sigma(\alpha)).$$

Os outros dois itens seguem diretamente do primeiro. □

**Corolário 1.2.1.** *Numa torre de extensões finitas $M|L|K$, com $M|K$ separável, tem-se*

$$\mathrm{Tr}_{M|K} = \mathrm{Tr}_{L|K}\circ\mathrm{Tr}_{M|L},\ N_{M|K} = N_{L|K}\circ N_{M|L}.$$

**Demonstração.** O conjunto dos $K$-monomorfismos de $M$ num fecho algébrico de $K$, denotado por $\mathrm{Hom}_K(M,\overline{K})$, é particionado pela seguinte relação

$$\sigma \sim \tau \Leftrightarrow \sigma|_L = \tau|_L$$

em $m = [L:K]$ classes de equivalência. Se $\sigma_1,\ldots,\sigma_m$ definem um sistema de representantes dessas classes, então $\mathrm{Hom}_K(L,\overline{K}) = \{\sigma_i|_L | i = 1,\ldots,m\}$ e, portanto

$$\mathrm{Tr}_{M|K}(x) = \sum_{i=1}^{m}\sum_{\sigma\sim\sigma_i}\sigma x = \sum_{i=1}^{m}\mathrm{Tr}_{\sigma_i M|\sigma_i L}(\sigma_i x) = \sum_{i=1}^{m}\sigma_i \mathrm{Tr}_{M|L}(x) = \mathrm{Tr}_{L|K}(\mathrm{Tr}_{M|K}(x)).$$

□

**Definição 1.2.3.** *Dada uma base $\alpha_1,\ldots,\alpha_n$ da extensão separável $L|K$, definimos o seu discriminante*

*como*

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

*em que $\sigma_i$ varia sobre todos os $K$-monomorfismos de $L$ num fecho algébrico $\overline{K}$ de $K$.*

A matriz $(\mathrm{Tr}_{L|K}(\alpha_i \alpha_j))$ é o produto das matrizes $(\sigma_k \alpha_i)^t$ e $(\sigma_k \alpha_j)$, donde podemos escrever

$$d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L|K}(\alpha_i \alpha_j)).$$

Caso tenhamos uma base do tipo $1, \theta, \ldots, \theta^{n-1}$, então a matriz que define o determinante é a matriz de Vandermonde

$$\begin{pmatrix} 1 & \theta_1 & \ldots & \theta^{n-1} \\ 1 & \theta_2 & \ldots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \ldots & \theta_n^{n-1} \end{pmatrix}$$

(em que $\theta_i = \sigma_i \theta$) cujo determinante é

$$\prod_{i<j} (\theta_j - \theta_i)^2,$$

obtido ao multiplicar as $(n-1)$ primeiras colunas por $\theta_1 = \theta$ e subtraí-las cada uma da seguinte.

**Proposição 1.2.5.** *O discriminante de uma base de uma extensão separável é sempre não-nulo. Além disso $(x, y) \mapsto \mathrm{Tr}_{L|K}(xy)$ define uma forma bilinear não-degenerada de $L$, como $K$-espaço vetorial.*

**Demonstração.** A bilinearidade de $\mathrm{Tr}(xy)$ é suficientemente clara, mostremos apenas que é não-degenerada. Sendo $\theta$ um elemento primitivo de $L|K$, isto é, tal que $L = K(\theta)$, tem-se que $1, \theta, \ldots, \theta^{n-1}$ é uma base com respeito a qual a forma é dada pela matriz $M = (\mathrm{Tr}_{L|K}(\theta^{i-1}\theta^{j-1}))_{i,j=1,\ldots,n}$. Ela, é, portanto, não-degenerada, pois

$$\det M = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_j - \theta_i)^2 \neq 0,$$

em vista de $\theta_i = \sigma_i \theta \neq \theta$, se $\sigma_i \neq \mathrm{Id}$.

Como provamos do decorrer do que antecede que o discriminante da base $1, \theta, \ldots, \theta^{n-1}$ é não-nulo, o discriminante de uma base arbitrária será igual a $\det M$ multiplicado pelo quadrado do determinante de uma matriz de mudança de base, que é não-nulo. □

Voltemos agora ao domínio $A$, com corpo de frações $K$, integralmente fechado e com fecho integral em $L$ (com $L|K$ extensão finita e separável) dado por $B$. Como todos os conjugados de um elemento inteiro sobre $A$ são também inteiros sobre $A$, temos

$$\mathrm{Tr}_{L|K}(x), N_{L|K}(x) \in A, \forall x \in B.$$

Além disso, para o grupo de unidades $B^*$, temos

$$x \in B^* \Leftrightarrow N(x) \in A^*.$$

De fato, a primeira implicação é trivial e, se $N(x)a = 1$, com $a \in A$, então $x \left( a \prod_{\sigma \neq Id} \sigma(x) \right) = 1$, donde $x \in B^*$.

O resultado a seguir nos mostra uma boa utilidade do discriminante.

**Lema 1.2.2.** *Seja $\alpha_1, \ldots, \alpha_n$ uma base de $L|K$ contida em $B$, cujo discriminante é $d$. Temos*

$$dB \subseteq A\alpha_1 + \ldots A\alpha_n.$$

**Demonstração.** Basta notar que, se $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \in B$, com $a_j \in K$, então os $a_j$'s são soluções do sistema linear definido por

$$\mathrm{Tr}_{L|K}(\alpha_i\alpha) = \sum_j \mathrm{Tr}_{L|K}(\alpha_i\alpha_j)a_j.$$

Ora, como $\mathrm{Tr}_{L|K}(x) \in A$, para $x$ inteiro sobre $A$, então os $a_j$'s são quocientes de elementos de $A$ pelo determinante $\det(\mathrm{Tr}_{L|K}(\alpha_i\alpha_j))$, que é igual a $d$, donde $d\alpha \in A$, pelo Lema 1.2.1. □

**Definição 1.2.4.** *Um sistema de elementos $\omega_1, \ldots, \omega_n \in B$ tal que todo $b \in B$ pode ser unicamente escrito na forma*

$$b = a_1\omega_1 + \ldots a_n\omega_n,$$

*com $a_i \in A$, é chamado uma base integral de $B$ sobre $A$, ou apenas uma $A$-base de $B$.*

Note que, se tal base existe, então ela é também uma base de $L|K$, pois independência linear sobre $A$ implica a independência linear sobre $K$ e a Proposição 1.2.3 nos garante que ela também gera a extensão. Não podemos, no entanto, mostrar que tal base existe em geral; por outro lado, no caso em que $A$ é um domínio de ideais principais (por vezes escrito ***D.I.P.***), temos um resultado mais geral. Para prová-lo, porém, precisaremos da

**Proposição 1.2.6.** *Se $M$ é um módulo finitamente gerado sobre um domínio de ideais principais, então todo submódulo de $M$ é finitamente gerado.*

Esta proposição é um caso particular da Proposição 6.2 da referência [1], cuja prova omitiremos.

**Proposição 1.2.7.** *Se $L|K$ é finita e separável e $A$ é um **D.I.P.**, então todo $B$-módulo finitamente gerado $M \neq 0$ contido em $L$, também dito $B$-submódulo de $L$, é um $A$-módulo livre de posto $n = [L : K]$, o que denotamos por $\mathrm{rank}(M) = n$. Em particular, $B$ admite uma base integral sobre $A$.*

**Demonstração.** Sendo $\alpha_1, \ldots, \alpha_n$ uma base de $L|K$, multiplicando-os por um elemento de $A$, se necessário, ver Proposição 1.2.3, podemos supor $\alpha_i \in B$. Pelo Lema 1.2.2, temos $dB \subseteq A\alpha_1 + \cdots + A\alpha_n$, em que $d$ é o discriminante da base $\alpha_1, \ldots, \alpha_n$, em particular, $\mathrm{rank}(B) \leq [L : K]$. Por outro lado, um sistema de geradores de $B$ como um $A$-módulo é também um sistema de geradores de $L$ como um $K$-módulo (também pela Proposição 1.2.3); como $L|K$ não pode ser gerada por menos de $[L : K]$ elementos, então temos $\mathrm{rank}(B) = [L : K]$.

Seja agora $\mu_1, \ldots, \mu_r$ um sistema de geradores do $B$-módulo $M \neq 0$. Mais uma vez, utilizando a Proposição 1.2.3, podemos obter $a \in A$ tal que $a\mu_i \in B$, qualquer que seja $i$, de modo que $aM \subseteq B$. Portanto,

$$adM \subseteq dB \subseteq A\alpha_1 + \ldots A\alpha_n.$$

Pela Proposição 1.2.6, temos que $adM$ é finitamente gerado, e livre, visto que $A\alpha_1 + \ldots A\alpha_n$ é livre, donde $M$ também satisfaz essas condições. Finalmente,

$$[L : K] = \mathrm{rank}(M) \leq \mathrm{rank}(M) = \mathrm{rank}(adM) \leq \mathrm{rank}(A\alpha_1 + \ldots A\alpha_n) = [L : K].$$

□

A partir de agora, ao invés de falarmos "uma base integral de $B$ sobre $A$", falaremos apenas "uma base integral de $L|K$". Como tais bases podem ser difíceis de produzir, o resultado abaixo é útil.

**Proposição 1.2.8.** *Sejam $L$ e $L'$ duas extensões de Galois do corpo $K$, $\{\omega_1, \ldots, \omega_n\}$ e $\{\omega'_1, \ldots, \omega'_m\}$ bases de $L|K$ e $L'|K$, respectivamente, de discriminantes $d$ e $d'$. Suponha $L \cap L' = K$. Então $\mathfrak{D} = \{\omega_i\omega'_j; i = 1, \ldots, n; j = 1, \ldots, m\}$ é uma base para $LL'$ (o corpo gerado pela união $L \cup L'$) e $d(\mathfrak{D}) = d^m d'^n$.*

**Demonstração.**

Como os elementos de $LL'$ são somas finitas de produtos $xy$, com $x \in L$ e $y \in L'$, então $\mathfrak{D}$ é de fato um conjunto gerador do espaço vetorial $LL'|K$. Visto que $L|K$ e $L'|K$ são extensões de Galois e $L \cap L' = K$, tem-se que $\mathfrak{S} : Gal(LL'|K) \to Gal(L|K) \times Gal(L'|K)$, dado por $\sigma \mapsto (\sigma|_L, \sigma|_{L'})$, é um homomorfismo de grupos. Caso $\mathfrak{S}(\sigma) = (Id, Id)$, sendo $\mathfrak{l}$ um elemento de $LL'$, podemos escrever $\mathfrak{l} = \sum c_{ij}\omega_i\omega'_j$, com $c_{ij} \in K$. Daí, temos

$$\sigma(\mathfrak{l}) = \sum \sigma(c_{ij})\sigma(\omega_i)\sigma(\omega'_j) = \sum c_{ij}\omega_i\omega'_j = \mathfrak{l},$$

donde $\sigma = Id$ e $\mathfrak{S}$ é injetivo. Além disso, se $(\sigma, \tau) \in Gal(L|K) \times Gal(L'|K)$, então $\sigma$ e $\tau$ podem ser estendidos a automorfismos de um fecho algébrico fixado $\overline{K}$ de $K$, digamos $\tilde{\sigma}$ e $\tilde{\tau}$. Temos as seguintes relações

$$\tilde{\sigma}|_K = \tilde{\sigma}|_{L\cap L'} = \tilde{\tau}|_{L\cap L'} = \tilde{\tau}|_K = Id,$$

$$\tilde{\sigma}(L) = L \text{ e } \tilde{\tau}(L') = L', \text{ pois } L|K \text{ e } L'|K \text{ são normais.}$$

Com isso, podemos definir o $K$-automorfismo $\gamma$ de $LL'$ dado pela ação combinada de $\tilde{\sigma}$ e $\tilde{\tau}$, que satisfaz $\mathfrak{S}(\gamma) = (\sigma, \tau)$. Portanto, $\mathfrak{S}$ é sobrejetivo. Como a imagem de $\mathfrak{S}$ tem $nm$ elementos, então $[LL' : K] = |Gal(LL'|K)| = nm$, donde $\mathfrak{D}$ é uma base de $LL'|K$.

Quanto ao discriminante da base $\mathfrak{D}$, pelo que foi dito acima, ele é o quadrado do determinante da matriz $nm \times nm$ dada por $M = (\sigma_k\omega_i\tau_l\omega'_j)$, com $Gal(LL'|L') = \{\sigma_1, \ldots, \sigma_n\}$ e $Gal(LL'|L) = \{\tau_1, \ldots, \tau_m\}$, donde se tem $Gal(LL'|K) = \{\sigma_1\tau_j\}$. Ora, a matriz $M$ pode ser vista como uma matriz $m \times m$, com entradas $(l, j)$ iguais ao produto $Q\tau_l\omega'_j$, sendo $Q$ a matriz $(\sigma_k\omega_i)$. Isto é, podemos escrever

$$\det M^2 = \det \begin{pmatrix} Q & 0 & \ldots & 0 \\ 0 & Q & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & \ldots & Q \end{pmatrix}^2 \det \begin{pmatrix} I_{n\times n}\tau_1\omega'_1 & \ldots & I_{n\times n}\tau_1\omega'_m \\ \vdots & \ddots & \vdots \\ I_{n\times n}\tau_m\omega'_1 & \ldots & \tau_m\omega'_m \end{pmatrix}^2.$$

Escrevamos $\tau_i\omega'_j = a_{ij}$ e $A = (a_{ij})$, note que a primeira linha de $A$ é igual a

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 & a_{12} & \ldots & a_{1m} & 0 & \ldots & 0 \end{pmatrix},$$

havendo sempre $n - 1$ zeros entre $a_{1l}$ e $a_{1(l+1)}$. Note que, se trocarmos a segunda coluna de $A$ pela $n + 1$-ésima, a terceira pela $2n + 1$-ésima, e assim por diante até a $m$-ésima, obtemos a linha

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} & 0 & \ldots & 0 \end{pmatrix}.$$

Note que, fazendo isso, criamos um bloco $n \times m$, composto pelos $m$ primeiros termos da linha acima, e mais $n - 1$ linhas nulas, além disso, todos os termos da primeira linha após $a_{1m}$ são $0$. Olhemos agora

para a $n+1$-ésima linha da nova matriz, ela é igual a

$$\begin{pmatrix} a_{21} & a_{22} & \dots & a_{2m} & 0 & \dots & 0 \end{pmatrix}.$$

Trocando a segunda linha com a segunda coluna, temos um novo bloco $n \times m$, composto pelas duas primeiras linhas da matriz $A$ e $n-2$ linhas nulas, além disso, todos os termos na segunda linha após $a_{2m}$ são $0$. Continuando este processo até trocarmos a $m$-ésima linha pela $(m-1)n+1-$ésima linha, obtemos um bloco que coincide com a matriz $A$, seguido à direita de um bloco $m \times n$ nulo, e abaixo por um bloco nulo de tamanho $m(n-1) \times m$. Executando o mesmo processo com a matriz do bloco restante repetidas vezes, chegamos a uma matriz diagonal por blocos, cujos blocos são todos iguais a $A$, cada um dos quais precisou de $2(n-1)$ trocas para ser construído, disso se conclui que o determinante da matriz

$$\begin{pmatrix} I_{n\times n}\tau_1\omega_1' & \dots & I_{n\times n}\tau_1\omega_m' \\ \vdots & \ddots & \vdots \\ I_{n\times n}\tau_m\omega_1' & \dots & \tau_m\omega_m' \end{pmatrix}$$

é $(\det A)^n$. Portanto, temos

$$d(\mathfrak{D}) = d^m d'^n.$$

□

A nossa aplicação de maior interesse destes resultados sobre integralidade consiste no fecho integral $\mathfrak{O}_K \subseteq K$ de $\mathbb{Z}$, em que $K$ é um corpo de números. Pela Proposição 1.2.7, todo $\mathfrak{O}_K$-módulo contido $K$ admite uma $\mathbb{Z}$-base $\alpha_1, \dots, \alpha_n$. Como matrizes de mudança base de $\mathbb{Z}$-módulos têm determinante $\pm 1$, então, dado um $\mathbb{Z}$-módulo $\mathfrak{a} \subset K$, dado por uma base $\alpha_1, \dots, \alpha_n$, podemos definir

$$d(\mathfrak{a}) = d(\alpha_1, \dots, \alpha_n)$$

como o discriminante do módulo $\mathfrak{a}$. Em especial,

**Definição 1.2.5.** *O discriminante de uma base integral da extensão $K|\mathbb{Q}$ é chamado discriminante de $K$, e pode ser denotado por $d_K$, $D_K$ ou $D(K)$.*

Em geral, vale o resultado abaixo.

**Proposição 1.2.9.** *Se $\mathfrak{a} \subseteq \mathfrak{a}'$ são dois $\mathfrak{O}_K$-módulos contidos em $K$, então $\mathfrak{a}$ é um subgrupo de índice finito de $\mathfrak{a}'$, e vale*

$$d(\mathfrak{a}) = |\mathfrak{a}'/\mathfrak{a}|^2 d(\mathfrak{a}).$$

Esta proposição é um corolário direto do lema abaixo.

**Lema 1.2.3.** *Sejam $M_0$ um grupo abeliano livre, de posto $n$ e $M$ um subgrupo que também é de posto $n$. Tem-se que $|M_0/M|$ é finito e igual ao módulo do determinante de qualquer matriz de mudança de base de $M_0$ para $M$.*

De fato, pois um $\mathbb{Z}$-módulo finitamente gerado pode ser visto como um grupo abeliano finitamente gerado. Este último lema, por sua vez, é uma consequência do Teorema abaixo.

**Teorema 1.2.1.** *Seja $M$ um grupo abeliano livre de posto $r$. Então todo subgrupo $N$ de $M$ é livre e de posto $s \leq r$. Além disso, existe uma base $\{\mu_1, \dots, \mu_r\}$ de $M$ e inteiros positivos $\alpha_1, \dots, \alpha_s$ tais que $\{\alpha_1\mu_1, \dots, \alpha_s\mu_s\}$ é uma base de $N$.*

Com efeito, o módulo do dito determinante não varia com mudanças de base. A prova deste último Teorema encontra-se em [8][theorem 1.16].

## 1.3 Ideais

Assim como ocorre em $\mathbb{Z}$, qualquer elemento não-nulo do anel de inteiros $\mathfrak{O}_K$ que não seja uma unidade admite uma fatoração em irredutíveis (que, neste contexto, podem também ser chamados primos). De fato, se $\alpha \neq 0$ não é ele próprio irredutível, então $\alpha = \beta\gamma$, com $\beta$ e $\gamma$ não-unidades, donde temos

$$1 < |N_{K|\mathbb{Q}}|(\beta)| < |N_{K|\mathbb{Q}}(\alpha)|,\ 1 < |N_{K|\mathbb{Q}}(\gamma)| < |N_{K|\mathbb{Q}}(\alpha)|;$$

portanto, podemos provar a decomposição em fatores primos argumentando por indução na norma (que é um inteiro, para um elemento do anel de inteiros). No entanto, tal fatoração nem sempre é única. Por exemplo, no anel de inteiros $\mathbb{Z}[\sqrt{5}]$ de $\mathbb{Q}(\sqrt{-5})$, temos

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

A ideia agora é contornar este problema com uma nova teoria de divisibilidade, na qual substituiremos os elementos de $\mathfrak{O}_K$ pelos seus ideais.

De começo, façamos algumas considerações sobre a estrutura de $\mathfrak{O}_K$

**Definição 1.3.1.** *Um anel é dito noetheriano se todos os seus ideais são finitamente gerados.*

**Teorema 1.3.1.** *O anel $\mathfrak{O}_K$ é noetheriano, integralmente fechado e todo ideal primo $\mathfrak{p} \neq 0$ é maximal.*

**Demonstração.** O fato de $\mathfrak{O}_K$ ser noetheriano decorre da Proposição 1.2.6. Desde que $\mathfrak{O}_K$ é o fecho integral de $\mathbb{Z}$ em $K$, tem-se que $\mathfrak{O}_K$ é integralmente fechado.

Seja $\mathfrak{p}$ um ideal primo não-nulo de $\mathfrak{O}_K$. Tem-se que $\mathfrak{p} \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$, isto é, da forma $p\mathbb{Z}$, com $p$ um primo inteiro. Seja agora $y \in \mathfrak{p}$, tem-se

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0, \text{ com } a_i \in \mathbb{Z}.$$

Ora, reduzindo esta última equação módulo $\mathfrak{p}$, concluímos que $a_n \equiv 0 \mod p$. Seja agora $x$ um elemento arbitrário de $\mathfrak{O}_K$. Novamente, $x$ satisfaz uma equação

$$x^m + b_1 x^{m-1} + \ldots b_m = 0,\ b_i \in \mathbb{Z}.$$

substituindo $x$ por $l + h$ onde $h \in \mathfrak{p}$, e $b_i$ por $r_i + pk_i$, com $k_i \in \mathbb{Z}$, tem-se

$$0 = (l+h)^m + (r_1 + pk_1)(l+h)^{m-1} + \cdots + r_n + pk_n \equiv l^m + r_1 l^{m-1} + \ldots r_m \mod \mathfrak{p},$$

donde os elementos do domínio $\overline{\mathfrak{O}} = \mathfrak{O}_K/\mathfrak{p}$ são todos algébricos sobre $k = \mathbb{Z}/p\mathbb{Z}$. Portanto, $\overline{\mathfrak{O}}$ resulta de adjuntar a $k$ uma quantidade finita de elementos algébricos. Como $k$ é um corpo, então $\overline{\mathfrak{O}}$ também é corpo, e isto finaliza a prova. □

O lema abaixo é por vezes útil, em vista de $\mathfrak{O}_K$ ser noetheriano.

**Lema 1.3.1.** *Um anel é noetheriano se, e somente se, toda cadeia ascendente de ideais é estacionária.*

**Demonstração.** Seja $R$ um anel e $I$ um ideal de $R$, que não é finitamente gerado. Tomemos um elemento $a \in I$, se $(a) \neq I$, então tomamos $a_2 \in I = (a_2)$ e consideramos $I_1 = (a_1, a_2)$, que é também um ideal de $R$, contido em $I$. Continuando indutivamente este processo, construímos uma cadeia ascendente

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq I_n \subsetneq \ldots,$$

violando o fato de toda cadeia ascendente de ideais de $R$ ser estacionária.

Reciprocamente, se todo ideal de $R$ é finitamente gerado, tomemos $I_1 \subseteq I_2 \subseteq \dots$ uma cadeia ascendente de ideais. Seja $\mathfrak{I} = \bigcup_{n=1}^{\infty} I_n$. Tem-se que $\mathfrak{I}$ é um ideal e, por hipótese, é finitamente gerado. Seja $a_1, \dots, a_m$ um sistema de geradores, com $a_i \in I_{N_i}$. Tomando $N = \max\{I_{N_j}\}$, temos $a_i \in I_N$, qualquer que seja $i$. Mas, então, vale $\mathfrak{I} \subseteq I_N$, donde $\mathfrak{I} = I_N$. Logo, para $n > N$, tem-se $I_n = \mathfrak{I}$, donde $R$ é noetheriano. □

As propriedades estabelecidas pelo Teorema 1.3.1 são o alicerce da teoria de divisibilidade que estamos para expor. Esta foi desenvolvida primeiramente por Dedekind, o que motiva a

**Definição 1.3.2.** *Um domínio de Dedekind é um domínio noetheriano, integralmente fechado, no qual qual todo ideal primo não-nulo é maximal.*

Primeiramente, trabalharemos com um domínio de Dedekind arbitrário $\mathcal{O}$, ao invés de $\mathfrak{O}_K$. Utilizaremos, via de regra, $\mathfrak{O}_K$, ou apenas $\mathfrak{O}$, para o anel de inteiros de um corpo de números.

**Definição 1.3.3.** *Sendo $\mathfrak{a}$ e $\mathfrak{b}$ dois ideais de $\mathcal{O}$, dizemos que $\mathfrak{a}|\mathfrak{b}$ (lê-se $\mathfrak{a}$ divide $\mathfrak{b}$) se $\mathfrak{b} \subseteq \mathfrak{a}$. Definimos a soma dos ideais $\mathfrak{a}$ e $\mathfrak{b}$ como*

$$\{a + b : a \in \mathfrak{a},\, b \in \mathfrak{b}\}.$$

*Por fim, definimos o seu produto como*

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{r<\infty} a_i b_i : a_i \in \mathfrak{a},\, b_i \in \mathfrak{b} \right\}.$$

É imediato que $\mathfrak{a} + \mathfrak{b}$ é também o menor ideal contendo $\mathfrak{a}$ e $\mathfrak{b}$, isto é, o seu máximo divisor comum. Da mesma forma, temos $\mathfrak{a} \cap \mathfrak{b}$ como o seu mínimo múltiplo comum. Nosso objetivo é mostrar que, com a soma e o produto de ideais, temos o que os elementos de $\mathcal{O}$ podem não ter: a fatoração única.

**Lema 1.3.2.** *Para todo ideal $\mathfrak{a} \neq 0$ de $\mathcal{O}$ existem ideais primos não-nulos $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ tais que*

$$\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq \mathfrak{a}.$$

**Demonstração.** Seja $\mathfrak{M}$ o conjunto dos ideais de $\mathcal{O}$ que não satisfazem a dita propriedade. Suponhamos que $\mathfrak{M} \neq \emptyset$. Do fato de toda cadeia ascendente de ideais de $\mathcal{O}$ ser estacionária, deduz-se que, com a relação de ordem induzida pela inclusão, todo subconjunto totalmente ordenado de $\mathfrak{M}$ tem uma cota superior. Pelo Lema de Zorn, $\mathfrak{M}$ possui um elemento maximal $\mathfrak{a}$. Ora, $\mathfrak{a}$ não pode ser um ideal primo. Por definição, existem elementos $b_1, b_2 \in \mathcal{O}$ tais que $b_1 b_2 \in \mathfrak{a}$, mas $b_1, b_2 \notin \mathfrak{a}$. Definamos $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$ e $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$. Teremos $\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$, mas $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$. Pela maximalidade de $\mathfrak{a}$, $\mathfrak{a}_1$ e $\mathfrak{a}_2$ precisam conter ao menos um produto de ideais primos; isto, porém, implicaria que $\mathfrak{a}$ contém o produto desses produtos, o que é uma contradição. □

Este lema foi o primeiro passo na direção do nosso objetivo, o segundo é o lema abaixo.

**Lema 1.3.3.** *Seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}$, defina*

$$\mathfrak{p}^{-1} = \{x \in K |\ x\mathfrak{p} \subset \mathfrak{O}\}.$$

*Tem-se $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$, para todo ideal $\mathfrak{a} \neq 0$.*

**Demonstração.** Sejam $a \in \mathfrak{p} - \{0\}$ e $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$, com $r$ o menor natural possível. Se $\mathfrak{p}_i \not\subset \mathfrak{p}$,

para todo $i$, então existem $a_i$'s em cada $\mathfrak{p}_i - \mathfrak{p}$, tais que $a_1 \dots a_r \in \mathfrak{p}$, o que é uma contradição, visto que $\mathfrak{p}$ é primo. Dito isso, ao menos um dos $\mathfrak{p}_i$ está contido em $\mathfrak{p}$, digamos $\mathfrak{p}_1$. Visto que $\mathfrak{p}_1$ é um ideal primo, tem-se $\mathfrak{p}_1 = \mathfrak{p}$. Visto que $\mathfrak{p}_2, \dots, \mathfrak{p}_r \not\subseteq (a)$, existe $b \in \mathfrak{p}_2, \dots, \mathfrak{p}_r$ tal que $b \notin a\mathcal{O}$, donde $a^{-1}b \notin \mathcal{O}$. Por outro lado, $b\mathfrak{p} = b\mathfrak{p}_1 \subseteq (a)$, donde $a^{-1}b\mathfrak{p} \subseteq \mathcal{O} \Rightarrow a^{-1}b \in \mathfrak{p}^{-1}$. Concluímos, portanto, que $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Seja agora $\mathfrak{a}$ um ideal e $\alpha_1, \dots, \alpha_n$ um sistema de geradores. Assumamos $a\mathfrak{p}^{-1} = a$. Teremos

$$x \in \mathfrak{p}^{-1} \Rightarrow x\alpha_i = \sum_j a_{ij}\alpha_j, \text{ com } a_{ij} \in \mathfrak{O}.$$

Sendo $A$ a matriz $(x\delta_{ij} - a_{ij})$, tem-se

$$A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0 \Rightarrow (\det A)\alpha_i = 0, \forall i,$$

pelo Lema 1.2.1. Mas $\mathcal{O}$ é um domínio, logo, isso só pode acontecer se $\det A = 0$. Portanto, $x$ é uma raiz do polinômio $f(t) = \det(t\delta_{ij} - a_{ij}) \in \mathfrak{O}[t]$. Como, por definição, tem-se $\mathfrak{O} \subseteq \mathfrak{p}^{-1}$, disso se conclui $\mathfrak{p}^{-1} = \mathfrak{O}$. □

Agora podemos, finalmente, provar o resultado a que visávamos.

**Teorema 1.3.2.** *Todo ideal de $\mathcal{O}$, diferente de $(0)$ e $(1)$, admite uma fatoração única, a menos de reordenação, na forma*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n,$$

*em que $\mathfrak{p}_i$ é um ideal primo não-nulo de $\mathcal{O}$.*

**Demonstração.** *Existência.* Seja $\mathfrak{M}$ o conjunto dos ideais diferentes de $(0)$ e $(1)$ que não admitem uma fatoração em ideais primos. Suponhamos $\mathfrak{M} \neq \emptyset$. Por um argumento análogo ao da prova do Lema 1.3.2, concluímos que existe um elemento maximal $\mathfrak{a} \in \mathfrak{M}$. Como $\mathcal{O}$ é noetheriano, $\mathfrak{a}$ está contido em algum ideal maximal $\mathfrak{p}$. Daí, temos

$$\mathcal{O} \subseteq \mathfrak{p}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}.$$

Por outro lado, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ e $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subset \mathcal{O}$, pelo Lema 1.3.3. Como $\mathfrak{p}$ é um ideal maximal, deve valer $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Ora, $\mathfrak{a}$ é maximal em $\mathfrak{M}$ e $a \neq \mathfrak{p}$, donde $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$; de fato, se $\mathfrak{a}\mathfrak{p}^{-1} = \mathcal{O}$, então $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}\mathfrak{p} = \mathfrak{p}$, violando as hipóteses sobre $\mathfrak{a}$. Portanto, o ideal $\mathfrak{a}\mathfrak{p}^{-1}$ admite uma fatoração em ideais primos, donde também $\mathfrak{a}$ admite, pois se tem $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p}$.

*Unicidade.* Para um ideal primo $\mathfrak{p}$, vale

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ ou } \mathfrak{b} \subseteq \mathfrak{p},$$

ou, noutras palavras,

$$\mathfrak{p}|\mathfrak{a} \text{ ou } \mathfrak{p}|\mathfrak{b}.$$

Sejam

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$$

duas fatorações de $\mathfrak{a}$ em ideais primos. Então $\mathfrak{p}_1|\mathfrak{q}_i$, para algum $i$, digamos $\mathfrak{q}_i = \mathfrak{q}_1$. Dado que $\mathfrak{q}$ é primo

e, portanto, maximal, tem-se $\mathfrak{q}_1 = \mathfrak{p}_1$. Multiplicando por $\mathfrak{p}^{-1}$, obtemos

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

Prosseguindo indutivamente, obtemos $r = s$ e, portanto, após uma possível renumeração, tem-se $\mathfrak{p}_i = \mathfrak{q}_i$, para todo $i$. □

Agrupando juntos os ideais que se repetem na fatoração (note que o produto entre ideais é comutativo), obtemos uma representação de um ideal $\mathfrak{a} \neq 0$ como

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\nu_i}, \text{ com } \nu_i > 0.$$

Se o ideal $\mathfrak{a}$ em questão for principal e $a$ for um de seus geradores, escrevemos $\mathfrak{a} = (a)$. Ao escrevemos que dois ideais $\mathfrak{a}$ e $\mathfrak{b}$ são coprimos, isto é, o seu máximo divisor comum é $(1) = \mathfrak{O}$, escreveremos $(\mathfrak{a}, \mathfrak{b}) = 1$, ao invés de $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$.

Se $\mathfrak{a}_1$ e $\mathfrak{a}_2$ são ideais coprimos, então

$$\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2.$$

Com efeito, $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2$ é imediato. Seja $a \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, como $\mathfrak{a}_1 + \mathfrak{a}_2 = \mathcal{O}$, temos $(\mathfrak{a}_1 + \mathfrak{a}_2)(a) = \mathcal{O}(a) = (a)$; como $(\mathfrak{a}_1 + \mathfrak{a}_2)(a) = \mathfrak{a}_1(a) + \mathfrak{a}_2(a)$, e ambas as parcelas são ideais contidos em $\mathfrak{a}_1\mathfrak{a}_2$, temos a inclusão reversa. O resultado para uma quantidade $n$ arbitrária de ideais coprimos segue facilmente por indução.

Portanto, se $\mathcal{O}$ for um domínio de Dedekind que também é um domínio de fatoração única, sendo $\mathfrak{p}$ um ideal primo de $\mathfrak{O}$, tome um elemento $\pi \in \mathfrak{p}$. Se $\pi$ não é irredutível, então $(\pi) \subseteq (\pi_1)$, em que $\pi_1 | \pi$. Argumentando igualmente com $\pi_1$ e prosseguindo indutivamente, obtemos, por $\mathcal{O}$ ser noetheriano, que $\mathfrak{p}$ contém um elemento irredutível $\pi_n$. Como, num domínio de fatoração única, todo elemento irredutível é primo, então o ideal gerado por $\pi_n$ também é primo, e portanto maximal, donde $\pi_n$ gera $\mathfrak{p}$, e todo ideal primo de $\mathcal{O}$ é principal, logo, todo ideal de $\mathcal{O}$ é principal. Que todo domínio de ideais principais é um domínio de fatoração única é um resultado clássico. Portanto, um domínio de Dedekind é um domínio de fatoração única se, e somente se, for um domínio de ideais principais. Isto será de muita importância daqui para a frente.

O resultado abaixo é mais geral, e vale para qualquer anel (comutativo com unidade).

**Lema 1.3.4** (Teorema chinês dos restos)**.** *Sejam $\mathcal{O}$ um anel, $\mathcal{A}_1, \dots, \mathcal{A}_n \subset \mathcal{O}$ ideais tais que $\mathcal{A}_i + \mathcal{A}_j = \mathcal{O}$, sempre que $i \neq j$, e $\mathcal{I} = \bigcap_{i=1}^{n} \mathcal{A}_i$. Então*

$$\mathcal{O}/\mathcal{I} \cong \bigoplus_{i=1}^{n} \mathcal{O}/\mathcal{A}_i.$$

**Demonstração.** Consideremos o homomorfismo definido por

$$\Psi : \mathcal{O} \to \bigoplus_{i=1}^{n} \mathcal{O}/\mathcal{A}_i,\ \Psi(a) = \bigoplus_{i=1}^{n} (a \mod \mathcal{A}_i).$$

Tem-se $\ker \Psi = \mathcal{B}$. Resta mostrar que $\Psi$ é sobrejetivo. Suponhamos primeiro $n = 2$. Visto que existem $a_1$ e $a_2$, tais que

$$a_1 \in \mathcal{A}_1,\ a_2 \in \mathcal{A}_2 \text{ e } a_1 + a_2 = 1,$$

tem-se que, se $X = x_1 \oplus x_2 \in \mathcal{A}_1 \oplus \mathcal{A}_2$, então $\Psi(x_1a_2 + x_2a_1) = X$.

Para o caso geral, afirmamos

$$\mathcal{A}_i + \bigcap_{j \neq i} \mathcal{A}_j = \mathcal{O}.$$

De fato, para cada $j \neq i$, existe $u_j \oplus v_j \in \mathcal{A}_i \oplus \mathcal{A}_j$, tal que $u_j + v_j = 1$. Ao expandir os termos do produto

$$\prod_j (u_j + v_j),$$

cada termo será da forma $(\text{alguma coleção de } u_j\text{'s})(\text{alguma coleção de } v_j\text{'s})$. Se algum $u_j$ aparece no termo, então ele pertence a $\mathcal{A}_i$, se nenhum aparece, pertence a $\bigcap_{j \neq i} \mathcal{A}_j$. Portanto, tem-se

$$1 = \prod_j (u_j + v_j) \in \mathcal{A}_i + \bigcap_{j \neq i} \mathcal{A}_j,$$

donde a afirmação fica provada.

Da afirmação, portanto, temos que, para cada $i$, podemos tomar $y_i$ tal que

$$y_i \equiv 1 \mod \mathcal{A}_i,\ y_i \equiv 0 \mod \mathcal{A}_j, \text{ com } j \neq i.$$

Disso se conclui que, se $X = x_1 \oplus x_2 \oplus \cdots \oplus x_n \in \bigoplus_{i=1}^n \mathcal{O}/\mathcal{A}_i$, então $\Psi(x_1 y_1 + \cdots + x_n y_n) = X$. □

Queremos agora introduzir uma noção de inverso multiplicativo para os ideais de um domínio de Dedekind $\mathcal{O}$.

**Definição 1.3.4.** *Um ideal fracionário do corpo de frações $K$ de um domínio de Dedekind $\mathcal{O}$ é um $\mathcal{O}$-submódulo de $K$ finitamente gerado. A multiplicação entre ideais fracionários é definida do mesmo modo com que definimos a multiplicação de ideais de $\mathcal{O}$*

A caracterização abaixo é útil para a prova que queremos fazer.

**Proposição 1.3.1.** *Um $\mathcal{O}$-submódulo $\mathfrak{a}$ de $K$ é um ideal fracionário se, e somente se, existe $c \in \mathcal{O} - \{0\}$ tal que $c\mathfrak{a} \subseteq \mathcal{O}$.*

**Demonstração.** Seja $\mathfrak{a}$ um $\mathcal{O}$-submódulo de $K$ finitamente gerado, isto é $\mathfrak{a} = \bigoplus_{i=1}^r x_i \mathcal{O}$, $x_i \in K$. Visto que $K$ é o corpo de frações de $\mathcal{O}$, então podemos escrever $x_i = \dfrac{a_i}{b_i}$, com $a_i, b_i \in \mathcal{O}$ e $b_i \neq 0$. Definindo $c = b_1 \ldots b_r$, temos

$$c\mathfrak{a} = \mathfrak{a} = \bigoplus_{i=1}^r (a_i \prod_{j \neq i} b_j)\mathcal{O} \subseteq \mathcal{O}$$

.

Reciprocamente, suponhamos $c\mathfrak{a} \subseteq \mathcal{O}$, com $c \in \mathcal{O} - \{0\}$, e $\mathfrak{a}$ um $\mathcal{O}$-submódulo de $K$. Seja $\mathfrak{o} \in \mathcal{O}$, tem-se $\mathfrak{o}c\mathfrak{a} = c(\mathfrak{o}\mathfrak{a}) \subseteq c\mathfrak{a}$, donde $c\mathfrak{a}$ é um ideal de $\mathcal{O}$. Como $\mathcal{O}$ é noetheriano, o Lema 1.3.1 implica que $c\mathfrak{a}$ é finitamente gerado como um ideal de $\mathcal{O}$, o que equivale a ser finitamente gerado como um $\mathcal{O}$-submódulo de $K$. □

**Proposição 1.3.2.** *O conjunto dos ideais fracionários de $K$ formam um grupo, o grupo ideal $J_K$ de $K$. A identidade deste grupo é o elemento $(1) = \mathcal{O}$, e o inverso de $\mathfrak{a} \in J_K$ é*

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subseteq \mathcal{O}\}.$$

**Demonstração.** A associatividade e a comutatividade são claras da definição de produtos de ideais. Além disso $\mathfrak{a}(1) = \mathfrak{a}$. Seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}$. O Lema 1.3.3 nos diz que $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$, donde $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$,

visto que $\mathfrak{p}$ é maximal. Portanto, se $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ é um ideal inteiro, então $b = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$ é um inverso de $\mathfrak{a}$. Reciprocamente, se $\mathfrak{ba} = \mathcal{O}$, então $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$ e $x\mathfrak{a} \subseteq \mathcal{O}$ implica $x\mathfrak{ab} \subseteq \mathfrak{b}$; esta última implica $x \in \mathfrak{b}$, posto que $\mathfrak{ab} = \mathcal{O}$. Temos então provado que $\mathfrak{b} = \mathfrak{a}^{-1}$.

Sejam agora $\mathfrak{a}$ um ideal fracionário qualquer e $c \in \mathcal{O} - \{0\}$ tal que $c\mathfrak{a} \subseteq \mathcal{O}$. Visto que $c^{-1}\mathfrak{a}^{-1}$ é o inverso de $c\mathfrak{a}$, temos $\mathfrak{a}\mathfrak{a}^{-1} = (c\mathfrak{a})(c\mathfrak{a})^{-1} = \mathcal{O}$. □

**Corolário 1.3.1.** *Todo ideal fracionário $\mathfrak{a}$ tem uma única fatoração na forma*

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

*em que $v(\mathfrak{p}) \in \mathbb{Z}$ e $v(\mathfrak{p}) = 0$, a menos de uma quantidade finita de ideais $\mathfrak{p}$.*

**Demonstração.** Todo ideal fracionário $\mathfrak{a}$ pode ser escrito como um quociente $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ de dois ideais $\mathfrak{b}$ e $\mathfrak{c}$ de $\mathcal{O}$. O Teorema 1.3.2 nos diz que $\mathfrak{b}$ e $\mathfrak{c}$ possuem fatorações em ideais primos, donde derivamos a fatoração de $\mathfrak{a}$, como afirmada no corolário. Desde que a fatoração é única para $\mathfrak{b}$ e $\mathfrak{c}$, ela também é única para $\mathfrak{a}$ □

Dizemos que um ideal fracionário $\mathfrak{a}$ é *principal* se $\mathfrak{a} = a\mathcal{O}$, com $a \in K$. Os ideais fracionários principais formam um subgrupo do grupo ideal, denotado por $P_k$. É a partir destes dois grupos que se define o nosso objeto de maior interesse.

**Definição 1.3.5.** *O grupo de classes do corpo $K$, denotado por $Cl_K$, é o quociente $J_K/P_K$.*

O grupo de classes, junto do grupo das unidades $\mathcal{O}^*$, completa a sequência exata

$$1 \to \mathcal{O}^* \to K^* \underset{a \mapsto a\mathcal{O}}{\to} J_K \to Cl_K \to 1.$$

O grupo de classes mede o quanto o mapa $a \mapsto a\mathcal{O}$ tende a expandir os elementos. Explicamo-lo: se, por exemplo, $|Cl_k| = 2$, então um ideal fracionário arbitrário tem $50\%$ de chance de ser principal; se, no entanto, $|Cl_K| = 100$, terá apenas $1\%$. Por outro lado, o grupo das unidades $\mathcal{O}^*$ mede o quanto este mapa tende a contrair os elementos, visto que $a\mathcal{O} = \varepsilon a\mathcal{O}$, qualquer que seja $\varepsilon \in \mathcal{O}^*$. Infelizmente, em se tratando de domínios de Dedekind arbitrários e seus corpos de frações, não temos absolutamente nenhum controle sobre a estrutura destes grupos. Porém, para corpos de números e seus anéis de inteiros, algumas finitudes importantes podem ser estabelecidas. Para tanto, precisaremos reinterpretar, novamente, os elementos de um corpo de números. Desta vez, como pontos num reticulado num $\mathbb{R}$-espaço vetorial.

## 1.4 Reticulados

**Definição 1.4.1.** *Seja $V$ um $\mathbb{R}$-espaço vetorial de dimensão $n$ e $E = \{e_1, \dots, e_m\}$ $(m \leq n)$ um subconjunto linearmente independente de $V$. O conjunto $\mathfrak{M}$ das combinações lineares inteiras dos vetores de $E$ é dito um reticulado de dimensão $m$ em $V$; o conjunto $E$ é dito uma base de $\mathfrak{M}$. Caso $m = n$, isto é, caso $E$ também seja uma base de $V$, dizemos que $\mathfrak{M}$ é completo, sendo incompleto, caso contrário.*

Exatamente como acontecia com $\mathbb{Z}$-módulos (pois reticulados também o são), dois conjuntos linearmente independentes $\{e_1, \dots, e_m\}$, $\{f_1, \dots, f_m\}$ geram o mesmo reticulado se, e somente se, são

conectados por uma matriz unimodular, isto é

$$\begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix} = C \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix},$$

com $C$ uma matriz inteira, de determinante $\pm 1$.

Não nos é conveniente que a nossa única definição de reticulado dependa de uma escolha de base. Precisamos, portanto, de uma caracterização que independa de tal escolha. Facilmente se nota que os reticulados estão contidos na classe dos subgrupos de $\mathbb{R}^n$, queremos mostrar agora que eles estão contidos numa classe mais específica: a dos subgrupos *discretos*. Lembremos que, na estrutura métrica padrão de $\mathbb{R}^n$, isto é, com a distância entre dois vetores $x, y$ definida por $d(x, y) = ||x - y||$, em que $||x|| = \sqrt{\langle x, x \rangle}$ e $\langle \cdot, \cdot \rangle$ denota o produto interno canônico, um conjunto é dito discreto quando sua interseção com qualquer *bola* $\mathcal{B}(r) = \{y \in \mathbb{R}^n : ||x|| < r\}$ centrada na origem é finito.

**Lema 1.4.1.** *Como um subconjunto de $\mathbb{R}^n$, um reticulado $\mathfrak{M}$ é discreto.*

**Demonstração.** Se $\mathfrak{M}$ for um reticulado incompleto, podemos completar a sua base a uma base de $\mathbb{R}^n$, teremos $\mathfrak{M}$ como um subgrupo do reticulado determinado por essa base. Dito isso, podemos restringir nossa demonstração a reticulados completos. Seja $\{e_1, \ldots, e_n\}$ uma base de $\mathfrak{M}$, tomemos $x$ um vetor não-nulo no complemento ortogonal do subespaço gerado por $\{e_2, \ldots, e_n\}$. Não podemos ter $\langle x, e_1 \rangle = 0$, donde podemos definir o vetor $f_1 = \langle x, e_1 \rangle^{-1} x$, que também pertence ao complemento ortogonal supracitado e satisfaz $\langle f_1, e_1 \rangle = 1$. Procedendo desta forma para cada $i$ de $1$ a $n$, formamos um conjunto de vetores $\{f_1, \ldots, f_n\}$ tal que

$$\langle f_i, e_j \rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Seja $z = a_1 e_1 + \ldots, a_n e_n \in \mathfrak{M} \cap \mathcal{B}(r)$. Temos $||z|| < r$ e $a_k = \langle z, f_k \rangle$, para $k = 1, \ldots, n$. A desigualdade de Cauchy-Schwartz nos dá

$$|a_k| = |\langle z, f_k \rangle| \leq ||z|| \cdot ||f_k|| < r||f_k||.$$

Como a última expressão à direita não depende de $z$, há finitas possibilidades para $a_k$, e o lema está provado. □

Abaixo, seguem algumas definições e resultados importantes sobre reticulados.

**Definição 1.4.2.** *Sejam $X \subset \mathbb{R}^n$, com $X \neq \emptyset$ e $z \in \mathbb{R}^n$. O translado de $X$ por $z$ é o conjunto dos pontos na forma $x + z$, com $x \in X$, e é denotado por $X + z$*

**Definição 1.4.3.** *Seja $\{e_1, \ldots, e_m\}$ uma base de um reticulado $\mathfrak{M}$. O conjunto dos pontos na forma*

$$\alpha_1 e_1 + \cdots + \alpha_m e_m, \text{ com } \alpha_i \in [0, 1)$$

*é dito um paralelepípedo fundamental do reticulado $\mathfrak{M}$.*

**Lema 1.4.2.** *Seja $T$ um paralelepípedo fundamental de um reticulado completo $\mathfrak{M}$. O mapa*

$$z \mapsto T_z = T + z, \, z \in \mathfrak{M},$$

*satisfaz:*

$$T_z = T_{z'} \Leftrightarrow z = z',$$

$$z \neq z' \Rightarrow T_z \cap T_{z'} = \emptyset,$$

$$\bigcup_{z \in \mathfrak{M}} T_z = \mathbb{R}^n.$$

**Demonstração.** Digamos que a base usada para construir $T$ seja $\{e_1, \dots e_n\}$.
Seja $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$ um elemento arbitrário de $\mathbb{R}^n$. Definamos $k_i$ maior inteiro menor que $\alpha_i$, para cada $i$. Temos $\alpha_i = k_i + \beta_i$, em que $0 \leq \beta_i < 1$. Daí, temos

$$x = (\beta_1 e_1 + \cdots + \beta_n e_n) + (k_1 e_1 + \cdots + k_n e_n).$$

O ponto $(k_1 e_1 + \cdots + k_n e_n)$ pertence a $\mathfrak{M}$. Como a escrita $\alpha_i = k_i + \beta_i$ é única, cada ponto $x \in \mathfrak{L}^{s,t}$ pertence a um único $T_z$, o que finaliza a prova. □

**Lema 1.4.3.** *Para todo $r > 0$, tem-se que o conjunto $\{z |\ T_z \cap \mathcal{B}(r) \neq \emptyset\}$ é finito.*

**Demonstração.** Utilizemos a mesma notação da demonstração anterior.
Tomemos $d = ||e_1|| + \cdots + ||e_n||$. Se $u = \alpha_1 e_1 + \cdots + \alpha_n e_n \in T$, então

$$||u|| \leq \alpha_1 ||e_1|| + \cdots + \alpha_n ||e_n|| < d.$$

Se $x$ é um ponto na interseção de $T_z$ com $\mathcal{B}(r)$, então $x = u + z$, com $u \in T$ e $z \in \mathfrak{M}$. Logo,

$$||z|| \leq ||x|| + ||-u|| < r + d \in z \in \mathcal{B}(r).$$

Pelo Lema 1.4.1, há finitos $z$ possíveis, portanto, pelo Lema 1.4.2, há finitos $T_z$ possíveis. □

Enfim, temos a caracterização que desejávamos.

**Lema 1.4.4.** *Todo subgrupo discreto de $\mathbb{R}^n$ é um reticulado.*

**Demonstração.** Denotemos por $\mathfrak{G}$ o subespaço de gerado por $\mathfrak{M}$. Digamos $m = \dim \mathfrak{G}$. Sejam $\{e_1, \dots, e_m\}$ uma base de $\mathfrak{G}$ e $\mathfrak{M}_0$ o reticulado determinado por esta base. Como todos os $e_i$'s são combinações lineares inteiras de elementos de $\mathfrak{M}$, temos que $\mathfrak{M}_0$ é um subgrupo de $\mathfrak{M}$. Como cada elemento de $\mathfrak{M}$ pode ser escrito como $x = u_x + z_x$, em que $z_x \in \mathfrak{M}_0$ e $u_x \in T$, o paralelepípedo fundamental de $\mathfrak{M}_0$ construído através da base acima, temos $u_x \in \mathfrak{M}$, para todo $x$ em $\mathfrak{M}$. Visto que $T$ é limitado e $\mathfrak{M}$ é discreto, existe em $\mathfrak{M}$ um conjunto finito de representantes de classe módulo $\mathfrak{M}_0$ dois a dois não congruentes; ou seja, $|\mathfrak{M}/\mathfrak{M}_0| = k < \infty$. Pelo Teorema de Lagrange, aplicado ao grupo $\mathfrak{M}/\mathfrak{M}_0$, temos $kx \in \mathfrak{M}_0$, qualquer que seja $x \in \mathfrak{M}$. Mas então $\mathfrak{M}$ é um subgrupo do reticulado gerado pelos vetores $k^{-1}e_1 \dots k^{-1}e_m$. Pelo Teorema 1.2.1, $\mathfrak{M}$ tem uma base $\{f_1, \dots, f_l\}$, com $l \leq m$. Visto que os vetores $e_1, \dots, e_m$ são linearmente independentes sobre $\mathbb{R}$ e $\mathfrak{M}_0 \subset \mathfrak{M}$, os vetores $f_1, \dots, f_l$ são linearmente independentes sobre $\mathbb{R}$. Portanto, $\mathfrak{M}$ é um reticulado. □

A seguir, damos critério para decidir se um reticulado é, ou não, completo.

**Teorema 1.4.1.** *Um reticulado $\mathfrak{M}$ de $\mathbb{R}^n$ é completo se, e somente se, existe um conjunto limitado $U \subset \mathbb{R}^n$ tal que $\mathbb{R}^n = \bigcup_{z \in \mathfrak{M}} U + z$.*

**Demonstração.** O Lema 1.4.2 nos diz que podemos tomar $U$ como um paralelepípedo fundamental de $\mathfrak{M}$, caso este seja completo. Demonstremos a volta por contraposição. Sejam $\mathfrak{M}$ um reticulado incompleto e $U \subset \mathbb{R}^n$ um conjunto limitado arbitrário. Visto que $U$ é limitado, existe algum número real positivo $r$, tal que $||u|| < r$, para todo $u \in U$. Visto que $\mathfrak{M}$ é incompleto, o subespaço $M$, gerado por $\mathfrak{M}$ é um subespaço próprio. Daí temos que o complemento ortogonal $M'$ possui um vetor não-nulo, donde

possui vetores de comprimento arbitrariamente grandes. Seja $y' \in M'$ tal que $||y'|| \geq r$. Se tivéssemos $y' = u + z$, em que $u \in U$ e $z \in \mathfrak{M}$, a desigualdade de Cauchy-Schwartz nos daria

$$||y'||^2 = \langle y', y' \rangle = \langle y', u \rangle \leq ||y|| \cdot ||u|| < r||y|| \Rightarrow ||y|| < r,$$

uma contradição. □

Seja agora $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ qualquer forma bilinear simétrica positivamente definida de um espaço euclidiano $V$ de dimensão $n$ (podendo, inclusive, ser $V = \mathbb{R}^n$ e $\langle \cdot, \cdot \rangle$ o produto interno canônico). Podemos estabelecer em $V$ uma noção de volume. Não entraremos em muitos detalhes quanto a isso, deixamos porém, a referência [3][chapter 1]. O volume do cubo unitário

$$\Phi_0 = \{x_1 e_1 + \dots x_n e_n |\ x_i \in [0, 1)\}$$

gerado por uma base ortonormal $e_1, \dots, e_n$ por $\mathrm{vol}(\Phi_0) = 1$, Se $v_1, \dots, v_n$ são vetores linearmente independentes em $V$, então o cubo unitário gerado por eles é definido por

$$\Phi = \{x_1 v_1 + \dots x_n v_n | x_i \in [0, 1)\}$$

e seu volume é

$$\mathrm{vol}(\Phi) = |\det A|$$

em que $A = (a_{ij})$ é a matriz de mudança de base de $e_1, \dots, e_n$ para $v_1, \dots, v_n$. Como temos

$$(\langle v_i, v_j \rangle)_{ij} = \left( \sum_{k,l} a_{ik} a_{jl} \langle e_k, e_l \rangle \right)_{ij} = \left( \sum_k a_{ik} a_{jk} \right) = AA^t.$$

Podemos, portanto, escrever

$$\mathrm{vol}(\Phi) = |\det(\langle v_i, v_j \rangle)|^{\frac{1}{2}}.$$

Seja $\Gamma$ o reticulado gerado por $v_1, \dots, v_n$. Temos $\Phi$ como um de seus paralelepípedos fundamentais, e definimos

$$\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi).$$

Como as matrizes de mudança de base de um reticulado têm determinante $\pm 1$, esta definição não depende da escolha de base.

O volume de um conjunto "arbitrário"$X$ é definido como a integral

$$\int_X |\det(\langle v_i, v_j \rangle)|^{\frac{1}{2}}.$$

Também não entraremos em detalhes sobre a finitude ou infinitude desta integral. Em nossas aplicações, o conjunto $X$ será sempre "suficientemente amigável", quase sempre caracterizado por desigualdades simples, de modo que esta integral pode ser tomada como a integral de Riemman. Além disso, em vista do Lema 1.4.2, podemos cobrir qualquer conjunto limitado por uma união finita de translados de um paralelepípedo fundamental de um reticulado completo $\mathfrak{M}$, o que inclui os retângulos da definição da integral de Riemmann. Utilizando esta ideia, sendo $r > 0$ um número real, $\Delta = \mathrm{vol}(\mathfrak{M})$ e $N(a)$ a função que conta quantos pontos de $a\mathfrak{M}$ estão contidos em $X$, como $\mathrm{vol}\left(\frac{1}{r}\mathfrak{M}\right) = \left(\frac{1}{r}\right)^n \mathrm{vol}(\mathfrak{M})$, temos

$$\mathrm{vol}(X) = \lim_{r \to \infty} N(r) \frac{\Delta}{r^n}.$$

Passamos agora ao Teorema mais importante desta seção. Porém, antes de enunciá-lo, definimos alguns conceitos.

**Definição 1.4.4.** *Um subconjunto $X$ de $V$ é dito simétrico se, para todo $x \in X$, tem-se $-x \in X$. E é chamado convexo se, dados $x, y \in X$, o segmento de reta $\{ty + (1-t)x | t \in [0,1]\}$ está contido em $X$.*

**Teorema 1.4.2** (do espaço convexo de Minkowski.)**.** *Sejam $\mathfrak{M}$ um reticulado completo no espaço $V$, $\Delta = \mathrm{vol}(\mathfrak{M})$ e $X$ um conjunto limitado, simétrico e convexo de volume $\mathrm{vol}(X) > 2^n\Delta$. Existe um elemento não-nulo de $\mathfrak{M}$ em $X$.*

**Demonstração.** Afirmamos inicialmente que, se $Y \subset V$ é um conjunto limitado cujos translados $Y_z = Y + z$ por vetores do reticulado $\mathfrak{M}$ são dois a dois disjuntos, então $\mathrm{vol}(Y) \leq \Delta$.

De fato, consideremos $T$ um paralelepípedo fundamental de $\mathfrak{M}$. Pelo Lema 1.4.2, temos $Y = \bigcup_{-z \in \mathfrak{M}} T_{-z}$, daí

$$\mathrm{vol}(Y) = \sum \mathrm{vol}(Y \cap T_{-z}) = \mathrm{vol}\left(T \cap \left(\bigcup Y_z\right)\right) \leq \mathrm{vol}(T).$$

Se $y = u - z$, com $y \in Y$ e $u \in T$, então $y + z \in T$, e vice-versa; logo, temos $Y \cap T_{-z} = Y_z \cap T$. Portanto

$$\mathrm{vol}(Y) = \sum_{z \in \mathfrak{M}} \mathrm{vol}(Y_z \cap T).$$

Dado que os translados $Y_z$ são disjuntos dois a dois, as interseções $Y_z \cap T$ também o são, donde o lado direito dessa igualdade é a soma de volumes de subconjuntos de $T$, que não pode ser maior que $\mathrm{vol}(T)$, pelo que a afirmação fica provada.

Voltemo-nos agora à prova do Teorema. Dado que $\mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2}^n \mathrm{vol}(X) > \Delta$, não podemos ter todos os translados $\frac{1}{2}X + z$ dois a dois disjuntos. Disto se tem que existem $x_1, x_2 \in X$, $z_1, z_2 \in \mathfrak{M}$, tais que

$$z_1 \neq z_2 \text{ e } \frac{1}{2}x_1 + z_1 = \frac{1}{2}x_2 + z_2,$$

donde

$$z_1 - z_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1.$$

Do fato de $X$ ser simétrico e convexo, tem-se

$$\frac{1}{2}x_2 - \frac{1}{2}x_1 = \frac{1}{2}x_2 + \frac{1}{2}(-x_1).$$

Donde $0 \neq z_1 - z_2 \in \mathfrak{M} \cap X$. □

Para simplificar as notações de resultados posteriores, trocaremos a tradicional notação $\mathrm{vol}(X)$, que mantivemos nesta seçao, para apenas $v(X)$.

## 1.5 Teoria de Minkowski

Para esta seção, consideremos $K$ um corpo de números de grau $n$, isto é $[K : \mathbb{Q}] = n < \infty$. A notação $Gal(M|P)$ é usada para significar o *grupo de Galois* da extensão $M|P$.

Seja $K_{\mathbb{C}} = \prod_\tau \mathbb{C}$, em que $\prod_\tau \mathbb{C}$ é o $\mathbb{C}$-espaço vetorial das uplas de elementos de $\mathbb{C}$ indexados pelos monomorfismos $\tau : K \to \mathbb{C}$. Definamos

$$\mathcal{J} : K \to K_{\mathbb{C}},\ \mathcal{J}a = (\tau a)_\tau.$$

Podemos equipar $K_{\mathbb{C}}$ com um *produto escalar hermitiano*, dado por

$$\langle x, y\rangle = \sum_{\tau} x_{\tau}\overline{y_{\tau}}.$$

O termo *hermitiano* se deve às seguintes propriedades, satisfeitas por $H(x,y) = \langle x, y\rangle$: $H(ax+by, z) = aH(x,z) + bH(y,z)$, $H(x,y) = \overline{H(y,x)}$, $H(x,x) > 0$, se $x \neq 0$; todas facilmente verificadas.

Tem-se $Gal(\mathbb{C}|\mathbb{R}) = \{Id, \mathfrak{C}\}$, em que $\mathfrak{C}$ é a conjugação complexa. A ação de $\mathfrak{C}$ sobre os elementos de $\mathfrak{C}$ é definida por $z_{\tau} \mapsto \overline{z}_{\overline{\tau}}$. Definimos $K_{\mathbb{R}} = \prod_{\tau} \mathbb{C}^{+}$ como sendo o subconjunto de $K_{\mathbb{C}}$ fixo por $Gal(\mathbb{C}|\mathbb{R})$, isto é, fixo por $\mathfrak{C}$. Tem-se, portanto, $(z_{\tau})_{\tau} \in K_{\mathbb{R}} \Leftrightarrow z_{\tau} = \overline{z}_{\overline{\tau}} = \overline{z_{\tau}} = z_{\overline{\tau}}$.

Afirmamos que $K_{\mathbb{R}}$ é um $\mathbb{R}$-espaço vetorial de dimensão finita. De fato, sendo $a, b \in \mathbb{R}$ e $(z_{\tau})_{\tau}, (z'_{\tau})\tau \in K_{\mathbb{C}}$, tem-se $\overline{az_{\tau} + bz'_{\tau}} = a\overline{z_{\tau}} + b\overline{z'_{\tau}} = az_{\overline{\tau}} + bz_{\overline{\tau}}$. Além disso, uma base de $K_{\mathbb{R}}$ é claramente dada pelo o conjunto dos elementos de $K_{\mathbb{R}}$ tais que $z_{\rho} = 1$ e $z_{\tau} = 0$, para $\tau \neq \rho$, com $\rho$ percorrendo todos os $\tau$'s reais, unido com o conjunto dos elementos nas formas $z_{\sigma} = z_{\overline{\sigma}} = 1$, ou $z_{\sigma} = i, z_{\overline{\sigma}} = -i$, e $z_{\tau} = 0$, para $\tau \neq \sigma$, onde $\sigma$ percorre todos os $\tau$'s complexos.

Visto que $\tau a = \overline{\tau} a$, qualquer que seja $a \in K$, temos $\mathcal{J}a \in K_{\mathbb{R}}$, para todo $a \in K$. Além disso, podemos definir a função $\mathrm{Tr} : K_{\mathbb{R}} \to \mathbb{R}$ dada por $\sum_{\tau} z_{\tau}$ (visto que $z_{\tau} + z_{\overline{\tau}} \in \mathbb{R}$); denotando por $\mathrm{Tr}_{K|\mathbb{Q}}$ a função traço do corpo $K$, temos $\mathrm{Tr} \circ \mathcal{J} = \mathrm{Tr}_{K|\mathbb{Q}}$. Temos então o mapa comutativo

$$\begin{array}{ccc} K & \xrightarrow{\mathcal{J}} & K_{\mathbb{R}} \\ \downarrow{\scriptstyle \mathrm{Tr}_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q} & \xrightarrow{\mathrm{Id}} & \mathbb{R} \end{array}$$

A restrição de $\langle \cdot, \cdot \rangle$ a $K_{\mathbb{R}} \times K_{\mathbb{R}}$ define um produto escalar em $K_{\mathbb{R}}$, isto é: $\langle x, y\rangle = \overline{\langle y, x\rangle} = \overline{\sum_{\tau} y_{\tau}\overline{x_{\tau}}} = \sum_{\tau} y_{\overline{\tau}} x_{\overline{\tau}} = \sum_{\tau} y_{\tau} x_{\tau}$ e $\langle y, x\rangle = \overline{\langle x, y\rangle} = \overline{\sum_{\tau} y_{\tau} x_{\tau}} = \sum_{\overline{\tau}} y_{\overline{\tau}} x_{\overline{\tau}} = \langle x, y\rangle$; a relação $\langle x, x\rangle \neq 0$, para $x \neq 0$, é herdada diretamente de $K_{\mathbb{C}}$. A métrica associada a esse produto escalar é chamada *métrica canônica de* $K_{\mathbb{R}}$.

**Definição 1.5.1.** *Chamamos o espaço $K_{\mathbb{R}}$ o espaço de Minkowski associado ao corpo $K$.*

A proposição abaixo nos fornece uma escrita mais conveniente para o espaço de Minkowski. Para facilitar a notação, sejam $\rho_1, \ldots, \rho_s$ os monomorfismos reais de $K$ (cuja imagem está contida em $\mathbb{R}$) e $\sigma_1, \overline{\sigma_1} \ldots \sigma_t, \overline{\sigma_t}$ os seus monomorfismos complexos, de modo que $s + 2t = n$

**Proposição 1.5.1.** *A transformação*

$$f : K_{\mathbb{R}} \to \prod_{\tau} \mathbb{R} = \mathbb{R}^{s+2t}$$

*dada por*

$$f(x) = (x_{\rho_1}, \ldots, x_{\rho_s}, \mathrm{Re}x_{\sigma_1}, \mathrm{Im}x_{\sigma_1}, \ldots, \mathrm{Re}x_{\sigma_t}, \mathrm{Im}x_{\sigma_t})$$

*é um isomorfismo. Este isomorfismo transforma o produto escalar $\langle x, y\rangle$ em $(x, y) = \sum_{\tau} \alpha_{\tau}(fx)_{\tau}(fy)_{\tau}$, onde $\alpha_{\tau} = 1$, se $\tau$ é real, e $\alpha_{\tau} = 2$, se $\tau$ é complexo,*

**Demonstração.** Visto que as funções $\mathrm{Re}$ e $\mathrm{Im}$ são $\mathbb{R}$-lineares, segue-se imediatamente que $f$ é uma transformação linear. Claramente se tem $\ker f = \{0\}$, donde $f$ é um isomorfismo. O restante se conclui

de

$$\langle x,y\rangle = \sum_\tau x_\tau \overline{y_\tau} = \sum_\rho x_\rho \overline{y_\rho} + \sum_\sigma (x_\sigma \overline{y_\sigma} + x_{\overline{\sigma}}\overline{y_{\overline{\sigma}}}) = \sum_\rho x_\rho y_\rho + 2\sum_\sigma \mathrm{Re} x_\sigma y_\sigma =$$
$$\sum_\rho x_\rho y_\rho + 2\sum_\sigma \mathrm{Re} x_\sigma \mathrm{Im} y_\sigma + 2\sum_\sigma \mathrm{Im} x_\sigma y_\sigma$$
$$= \sum_\tau \alpha_\tau (fx)_\tau (fy)_\tau.$$

□

O produto escalar $(x,y)$ transfere a métrica canônica de $K_\mathbb{R}$ para $\mathbb{R}^{s+2t}$. O volume definido a partir de $(x,y)$ (denotado por $v'$) difere do obtido a partir do produto interno canônico de $\mathbb{R}^{s+2t}$ (aqui chamado volume de Lebesgue) por um fator $2^t$; isto é, se $X \in K_\mathbb{R}$, $f(X)$ é sua imagem por $f$ em $\mathbb{R}^{s+2t}$, $v(X)$ é o volume de $X$ na métrica canônica e $v_L(f(X))$ é o volume de Lebesgue de $f(X)$ então

$$v(X) = v'(f(X)) = 2^t v_L(f(X)).$$

Neste trabalho, usaremos sistematicamente a métrica canônica.

A proposição abaixo relaciona os ideais de $\mathfrak{O}_K$ aos reticulados do espaço de Minkowski.

**Proposição 1.5.2.** *Seja $\mathfrak{a}$ um ideal não-nulo de $\mathfrak{O}_K$. Então $\Gamma = \mathcal{J}\mathfrak{a}$ é um reticulado completo de $K_\mathbb{R}$. Além disso, tem-se*

$$v(\Gamma) = \sqrt{|d_K|}|\mathfrak{O}_K/\mathfrak{a}|$$

**Demonstração.** Do fato de $\mathfrak{a}$ ser um ideal de $\mathfrak{O}_K$ e, mais particularmente, um subgrupo de $\mathfrak{O}_K$, deduz-se que $\mathfrak{a}$ é um $\mathbb{Z}$-módulo livre de posto menor ou igual a $n = [K:\mathbb{Q}]$. Para todo $x$ não nulo pertencente a $\mathfrak{a}$, tem-se que $x\mathfrak{O}$ é submódulo de $\mathfrak{a}$, de posto $n$, donde $\mathfrak{a}$ também tem posto $n$. Seja $\alpha_1,\ldots,\alpha_n$ uma $\mathbb{Z}$-base de $\mathfrak{a}$. Tem-se $\mathcal{J}\mathfrak{a} = \mathbb{Z}\mathcal{J}\alpha_1 + \cdots + \mathbb{Z}\mathcal{J}\alpha_n$.

Seja $\tau_1,\ldots,\tau_n$ alguma enumeração dos monomorfismos de $K$ para $\mathbb{C}$. Pela Proposição 1.2.9, sabemos que a matriz $A = (\tau_l\alpha_k)_{kl}$ satisfaz

$$d(\mathfrak{a}) = \det A^2 = |\mathfrak{O}_K/\mathfrak{a}|^2 d_K.$$

Por outro lado, ela também satisfaz

$$A\overline{A}^t = \left(\sum_{i=1}^n \tau_i\alpha_l\overline{\tau_i}\alpha_k\right)_{lk} = (\langle \mathcal{J}\alpha_l, \mathcal{J}\alpha_k\rangle).$$

Portanto, temos

$$|\det A| = |\det(\langle \mathcal{J}\alpha_l, \mathcal{J}\alpha_k\rangle)|^{\frac{1}{2}}.$$

Visto que $v(\Gamma) = |\det A|$, temos o resultado provado. □

Esta proposição nos permite provar o Teorema abaixo, que será uma ferramenta bastante útil mais adiante.

**Teorema 1.5.1.** *Sejam $\mathfrak{a}$ um ideal não-nulo de $\mathfrak{O}_K$ e $\{c_\tau;\tau$ monomorfismo de $K$ para $\mathbb{C}\}$ um conjunto de números reais positivos tais que $c_\tau = c_{\overline{\tau}}$ e*

$$\prod_\tau c_\tau > \left(\frac{\pi}{2}\right)^{-t}\sqrt{|d_K|}|\mathfrak{O}_K/\mathfrak{a}|.$$

*Então, existe* $a \in \mathfrak{a} - \{0\}$*, tal que* $|\tau a| < c_\tau$*, qualquer que seja* $\tau$*.*

**Demonstração.** O conjunto $X = \{(z_\tau)_\tau; |z_\tau| < c_\tau\}$ é convexo e simétrico. Podemos computar o seu volume através do isomorfismo $f$. Tem-se $v(X) = 2^t v(f(X))$, onde $f(X)$ é dado por

$$\left\{(x_\tau) \in \prod_\tau \mathbb{R} || x_\rho| < c_\rho, x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2\right\}.$$

Este volume, por sua vez, é dado por

$$\int_{-c_{\rho_1}}^{c_1} dx_{\rho_1} \cdots \int_{-c_{\rho_s}}^{c_{\rho_s}} dx_{\rho_s} \iint\limits_{x_{\sigma_1}^2 + x_{\overline{\sigma_1}}^2 < c_{\sigma_1}^2} dx_{\sigma_1} dx_{\overline{\sigma_1}} \cdots \iint\limits_{x_{\sigma_t}^2 + x_{\overline{\sigma}}^2 < c_{\sigma_t}^2} dx_{\sigma_t} dx_{\overline{\sigma}_t} = 2^s \pi^t \prod_\tau c_\tau.$$

Obtemos, então

$$v(X) = 2^{s+t}\pi^t \prod_\tau c_\tau > 2^{s+t}\pi^t \frac{\pi}{2}^{-t} \sqrt{|d_K|} |\mathfrak{O}_K/\mathfrak{a}| = 2^n v(\Gamma).$$

Aplicando o Teorema 1.4.2, temos que existe um ponto $\mathcal{J}a \in X \cap \mathcal{J}\mathfrak{a}$, com $a \neq 0$, e isto finaliza a prova. □

Convém também expormos uma versão multiplicativa da teoria de Minkowski. Se restringirmos $\mathcal{J}$ a $K^*$, obtemos um homomorfismo de grupos de $K^*$ para $K_\mathbb{C}^* = \prod_\tau \mathbb{C}^*$. A conjugação complexa $\mathfrak{C}$ age em $K_\mathbb{C}^*$ do modo que já definimos. Definindo a função $N : K_\mathbb{C}^* \to \mathbb{C}^*$ dada por $(z_\tau)_\tau \mapsto \prod_\tau z_\tau$, temos outro homomorfismo de grupos. Verifica-se que $N \circ \mathcal{J} : K \to \mathbb{C}^*$ coincide com a norma $N_{K|\mathbb{Q}}$.

Definimos $l : \mathbb{C}^* \to \mathbb{R}$ por $z \mapsto \ln|z|$. Temos que $l$ é um homomorfismo de grupos sobrejetivo. Além disso, $l$ induz um homomomorfismo sobrejetivo $\mathcal{L} : K_\mathbb{C}^* \to \prod_\tau \mathbb{R}$. Podemos ainda restringir a função $\mathrm{Tr}$ a $\prod_\tau \mathbb{R}$, e obteremos o diagrama comutativo

$$\begin{array}{ccccc} K^* & \xrightarrow{\mathcal{J}} & K_\mathbb{C}^* & \xrightarrow{\mathcal{L}} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^* & \xrightarrow{Id} & \mathbb{C}^* & \xrightarrow{l} & \mathbb{R} \end{array}.$$

A ação de $\mathfrak{C}$ em $\prod_\tau \mathbb{R}$ reduz-se a $z_\tau \mapsto z_{\overline{\tau}}$. Temos

$$(\mathcal{L}(z_\tau)_\tau)_{\overline{\tau}} = ((\ln|z_\tau|)_\tau)_{\overline{\tau}} = (\ln|z_{\overline{\tau}}|)_\tau = \mathcal{L}(z_{\overline{\tau}})_\tau,$$

donde a ação de $\mathfrak{C}$ comuta com $\mathcal{L}$ e $x \in \prod_\tau \mathbb{R}$ é fixo por $\mathfrak{C}$ se, e somente se, a sua pré-imagem por $\mathcal{L}$ também é. Ora, o subconjunto de $K_\mathbb{C}^*$ fixo por $\mathfrak{C}$ é justamente $K_\mathbb{R}^*$. Também temos

$$N((z_\tau)_\tau) = \prod_\tau z_\tau = \prod_\tau z_{\overline{\tau}} \Rightarrow N((\overline{z_\tau})_\tau) = \prod_\tau \overline{z_\tau} = \overline{N((z_\tau)_\tau)},$$

donde a ação de $\mathfrak{C}$ também comuta com $N$. Além disso, se $(z_\tau)_\tau \in K_\mathbb{R}$, então $N((z_\tau)_\tau) \in \mathbb{R}^*$. Visto que imagem de $\mathcal{J}$ está sempre contida em $K_\mathbb{R}$, tem-se $\mathcal{J}K^* \subset K_\mathbb{R}$, e podemos reescrever o diagrama

acima como

$$\begin{array}{ccccc} K^* & \xrightarrow{\mathcal{J}} & K_{\mathbb{R}}^* & \xrightarrow{\mathcal{L}} & \prod_\tau \mathbb{R}^+ \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^* & \xrightarrow{Id} & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R} \end{array},$$

em que $\prod_\tau \mathbb{R}^+$ é o subgrupo

$$\left\{(z_\tau)_\tau \in \prod_\tau \mathbb{R} | z_\tau = z_{\overline{\tau}}\right\}.$$

Sejam $\rho_1, \ldots, \rho_s$ todos os $\tau$'s reais e $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_t, \overline{\sigma_t}$ todos os pares de $\tau$'s complexos. Com esta enumeração, podemos escrever

$$\prod_\tau \mathbb{R} = \prod_\rho \mathbb{R} \times \prod_\sigma \mathbb{R}^2,$$

donde obtemos $\prod_\tau \mathbb{R}^+$ como o subgrupo

$$\prod_\rho \mathbb{R} \times \{((x,x)_\sigma)_\sigma | x \in \mathbb{R}\}.$$

Identificando cada tupla $(x,x)$ com o número real $2x$, obtemos um isomorfismo $g : \prod_\tau \mathbb{R}^+ \to \mathbb{R}^{s+t}$. Identificando $\mathcal{L}$ com $g \circ \mathcal{L}$, e $\mathrm{Tr}$ com $\mathrm{Tr} \circ g$, obtemos o diagrama

$$\begin{array}{ccccc} K^* & \xrightarrow{\mathcal{J}} & K_{\mathbb{R}}^* & \xrightarrow{\mathcal{L}} & \mathbb{R}^{s+t} \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^* & \xrightarrow{Id} & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R} \end{array},$$

no qual $\mathcal{L}$ e $\mathrm{Tr}$ se escrevem como

$$\mathcal{L}(z_\tau)_\tau = (\ln|z_{\rho_1}|, \ldots, \ln|z_{\rho_s}|, \ln|z_{\sigma_1}|^2, \ldots, \ln|z_{\sigma_t}|^2)$$

e

$$\mathrm{Tr}(x) = \sum_{i=1}^{s+t} x_i.$$

Note que, se $x = \mathcal{L}y$, então

$$\mathrm{Tr}(x) = \sum_\rho \ln|y_\rho| + \sum_\sigma \ln|y_\sigma|^2 = \ln(|y_{\rho_1}| \ldots |y_{\rho_s}||y_{\sigma_1}|^2 \ldots |y_{\sigma_t}|^2) = \ln|N(y)|.$$

## 1.6 O número de classes

Queremos aplicar a teoria de Minkowski para mostrar que $|Cl_K| < \infty$, sempre que $K$ é um corpo de números. Para tanto, seja $\mathfrak{a} \neq 0$ um ideal de $\mathfrak{O}_K$, consideramos a sua *norma absoluta*

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

Pela Proposição 1.2.9, este índice é finito e, caso $\mathfrak{a}$ seja um ideal principal $(a)$, então

$$\mathfrak{N}(\mathfrak{a}) = |N_{K|\mathbb{Q}}(a)|.$$

De fato, se $\omega_1, \ldots, \omega_n$ é uma $\mathbb{Z}-$base de $\mathfrak{O}_K$, então $a\omega_1, \ldots, a\omega_n$ é uma $\mathbb{Z}-$base de $\mathfrak{a}$. Se $A = (a_{ij})$ é a matriz de mudança de base tal que $a\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$. Pelo Lema 1.2.3, temos $|\det A| = |\mathfrak{O}_K/\mathfrak{a}|$ e, por definição, $\det A = N_{K|\mathbb{Q}}(a)$.

**Proposição 1.6.1.** *Se* $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{v_i}$ *é a fatoração em ideais primos do ideal* $\mathfrak{a} \subseteq \mathfrak{O}_K$*, então*

$$\mathfrak{N}(\mathfrak{a}) = \prod_{i=1}^{r} \mathfrak{N}(\mathfrak{p}_i)^{v_i}.$$

**Demonstração.** Sendo $\mathfrak{p}_i$ e $\mathfrak{p}_j$ são ideais primos distintos de $\mathfrak{O}_K$, temos $\mathfrak{p}_i + \mathfrak{p}_j = \mathfrak{O}_K$, donde $1 \in \mathfrak{p}_i + \mathfrak{p}_j$. Sendo $m, n > 1$ números naturais, elevando esta última equação a $N > m, n$ e usando binômio de Newton, temos $1 \in \mathfrak{p}_i^n + \mathfrak{p}_j^m$. Desse modo, o Lema 1.3.4 nos permite concluir

$$\mathfrak{O}_K/\mathfrak{a} = \bigoplus_{i=1}^{r} \mathfrak{O}_K/\mathfrak{p}_i{}^{v_i}.$$

Podemos, portanto, reduzir a prova ao caso $\mathfrak{a} = \mathfrak{p}^v$, com $\mathfrak{p}$ um ideal primo.

Afirmamos que, na sequência

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^v,$$

cada ideal é distinto do seguinte e cada quociente $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ é um $\mathfrak{O}_K/\mathfrak{p}$-espaço vetorial de dimensão $1$. A primeira parte se deduz da fatoração única. Seja $a \in \mathfrak{p}^i - \mathfrak{p}^{i+1}$ e $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$. Tem-se $\mathfrak{p}^i \supseteq \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}$. Por outro lado, $\mathfrak{b} \neq \mathfrak{p}^i$ implicaria que $\mathfrak{p}^{-i}\mathfrak{b}$ é um divisor próprio de $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$, que é um ideal primo. Portanto, tem-se $\mathfrak{b} = \mathfrak{p}^i$. Ou seja, qualquer elemento de $\mathfrak{p}_i$ pode ser escrito como a soma de um elemento de $(a)$ com um elemento de $\mathfrak{p}^{i+1}$, donde todo elemento do grupo quociente $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ é da forma $\overline{ka}$, com $k \in \mathfrak{O}_K$. Se $k \in \mathfrak{p}$, então $ka \in \mathfrak{p}^{i+1}$ e $\overline{ka} = 0$. Definindo, portanto, $k\overline{a} = \overline{ka}$, em que $k \in \mathfrak{O}_K/\mathfrak{p}$ (aqui estamos usando a mesma notação para uma classe em $\mathfrak{O}_K/\mathfrak{p}$ e um dos seus representantes), temos $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ como um $\mathfrak{O}_K/\mathfrak{p}$-espaço vetorial e $\{\overline{a}\}$ como um conjunto gerador, logo, uma base.

Provada a afirmação, temos $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathfrak{O}_K/\mathfrak{p}$. Podemos, portanto, concluir

$$|\mathfrak{O}/\mathfrak{p}^v| = |\mathfrak{O}/\mathfrak{p}||\mathfrak{p}/\mathfrak{p}^2| \ldots |\mathfrak{p}^{v-1}/\mathfrak{p}^v| = (\mathfrak{O}_K : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2) \ldots (\mathfrak{p}^{v-1} : \mathfrak{p}) = \mathfrak{N}(\mathfrak{p})^v.$$

□

Esta proposição implica diretamente na multiplicatividade da norma absoluta, isto é

$$\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}).$$

Podemos, portanto, estender $\mathfrak{N}$ a um homomorfismo

$$\mathfrak{N} : J_K \to \mathbb{R}$$

definido em todos os ideais fracionários $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}},\ v_{\mathfrak{p}} \in \mathbb{Z}$. O próximo lema é uma ferramenta importantíssima na prova da finitude do grupo de classes.

**Lema 1.6.1.** *Para todo ideal $\mathfrak{a} \neq 0$ de $\mathfrak{O}_K$, existe $a \in \mathfrak{a} - \{0\}$, tal que*

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{\pi}{2}\right)^{-t} \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a})$$

**Demonstração.** Dado um $\varepsilon > 0$, escolhamos números reais $c_\tau \in \mathbb{R}_{>0}$, com $c_\tau = c_{\overline{\tau}}$, tais que

$$\prod_\tau c_\tau = \left(\frac{\pi}{2}\right)^{-t} \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon,$$

O Teorema 1.5.1 nos diz que existe $a \in \mathfrak{a} - \{0\}$, satisfazendo $|\tau a| < c_\tau$. Ora, o conjunto

$$X = \{x \in K_{\mathbb{R}} |\ |x_\tau| < c_\tau\}$$

é limitado; como $\mathcal{J}\mathfrak{a}$ é discreto, sua interseção com $X$ é um conjunto finito. Como, para cada $\varepsilon > 0$, obtemos um $a \in \mathfrak{a} - \{0\}$, tal que $\mathcal{J}a \in X$, deve existir $a \in \mathfrak{a} - \{0\}$ tal que

$$|N_{K|\mathfrak{Q}}(a)| = \prod_\tau |\tau a| \leq \left(\frac{\pi}{2}\right)^{-t} \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

□

**Teorema 1.6.1.** *O grupo de classes $Cl_K = J_K/P_K$ é finito. Sua ordem $h = (J_K : P_K)$ é chamada número de classes de $K$.*

**Demonstração.** Afirmamos que, para cada primo $p \in \mathbb{Z}$, o conjunto de ideais primos $\mathfrak{p}$ de $\mathfrak{O}_K$, tais que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ é finito. Mais do que isso, se é não-vazio, então estes ideais são justamente os ideais primos que dividem o ideal $(p) = p\mathfrak{O}_K$.

De fato, se $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, então $p \in \mathfrak{p}$, logo, tem-se $\mathfrak{p}|(p)$. Reciprocamente, se $\mathfrak{p}|(p)$, então $p\mathbb{Z} = (p) \cap \mathbb{Z} \subseteq \mathfrak{p} \cap \mathbb{Z} = q\mathbb{Z}$, com $q$ primo, donde $p = q$. Visto que a fatoração em ideais primos tem sempre um número finito de fatores, existem apenas finitos ideais primos satisfazendo $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

Se $\mathfrak{p}$ é um ideal primo de $\mathfrak{O}_K$, então $\mathfrak{O}_K/\mathfrak{p}$ é uma extensão finita de $\mathbb{Z}/p\mathbb{Z}$ ($\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$) e, portanto,

$$\mathfrak{N}(\mathfrak{p}) = |\mathfrak{O}_K/\mathfrak{p}| = p^f.$$

Visto que a quantidade de pares $(p, f)$, com $p$ e $f$ inteiros positivos, satisfazendo $p^f < C$, com $C$ uma constante positiva, é finita, tem-se que existe uma quantidade finita de ideais primos de $\mathfrak{O}_K$, com norma limitada.

Como todo ideal de $\mathfrak{O}_K$ admite uma única fatoração como produto de ideais primos e a norma é multiplicativa, também são finitos os ideais de $\mathfrak{O}_K$ que possuem norma limitada.

Seja $[\mathfrak{a}]$ uma classe em $Cl_K$, queremos mostrar que existe $\mathfrak{a}_1 \in [\mathfrak{a}]$, tal que

$$\mathfrak{N}(\mathfrak{a}_1) \leq M = \left(\frac{\pi}{2}\right)^{-t} \sqrt{|d_K|}.$$

A Proposição 1.3.1 e o Teorema 1.5.1 nos fornecem elementos $\gamma \in \mathfrak{O}_K - \{0\}$ e $\alpha \neq 0$, tais que $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$, $\alpha \in \mathfrak{b}$ e

$$|N_{K|\mathbb{Q}}(\alpha)|\mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}(\alpha\mathfrak{b}^{-1}) \leq M,$$

pelo Lema 1.6.1. Podemos tomar $\mathfrak{a}_1 = \alpha\gamma^{-1}\mathfrak{a}$ e finalizar a prova. □

## 1.7 O Teorema das unidades de Dirichlet.

O nosso objetivo nesta seção é estudar a estrutura do grupo das unidades de $\mathfrak{O}_K$. Consideremos o homomorfismo $\mathcal{L}$ no diagrama (construído na Seção 1.5),

$$\begin{array}{ccccc} K^* & \xrightarrow{\mathcal{J}} & K_{\mathbb{R}}^* & \xrightarrow{\mathcal{L}} & \prod_\tau \mathbb{R}^+ \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^* & \xrightarrow{Id} & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R} \end{array}.$$

Chamamos a imagem $\mathcal{L}K_{\mathbb{R}}^*$ o *espaço logarítmico* de $K$. Se $\varepsilon \in K^*$, escrevemos $l(\varepsilon) = (\mathcal{L} \circ \mathcal{J})x$. Chamamos $l(\varepsilon)$ a *representação logarítmica* de $\varepsilon$.

Notemos que, sendo e $\varepsilon \in \mathfrak{O}_K^*$ o mapa $\varepsilon \mapsto l(\varepsilon)$ não é injetivo. De fato, se $\varepsilon$ é uma raiz da unidade, então o módulo de qualquer $\sigma(\varepsilon)$ é $1$, se $\sigma : K \to \mathbb{C}$ é um monomorfismo, de modo que $l(\varepsilon) = 0$. Daí, o primeiro passo para utilizarmos o mapa $\varepsilon \mapsto l(\varepsilon)$ no estudo da estrutura do grupo de unidades de $\mathfrak{O}_K^*$ é discutirmos a estrutura do seu núcleo.

Consideremos $\alpha \in \mathfrak{O}_K^*$ um elemento do núcleo de $\alpha \mapsto l(\alpha)$, que denotaremos por $W$. Como a imagem $\mathcal{J}\mathfrak{O}_K$ é um reticulado em $K_{\mathbb{R}}$ e a condição $l(\alpha) = 0$ equivale a

$$|\sigma_i(\alpha)| = 1,\ i = 1 \ldots, s+t,$$

em que $\sigma_i$ percorre todos os monomorfismos reais de $K$ para $\mathbb{C}$, e um de cada par de monomorfismos complexos conjugados. O Lema 1.4.1 nos diz que $W$ é finito.

Para todo $\alpha \in W$, temos $\alpha^k \in W$, para todo inteiro positivo $k$. Como $W$ é finito, temos $\alpha^k = \alpha^l$, com $k$ e $l$ inteiros positivos e $l > k$, donde $\alpha^{l-k} = 1$, e $\alpha$ é uma raiz da unidade. Além disso, como $\{1, -1\} \subset W$, temos que a ordem de $W$ é par. Tem-se, além disso, que $W$ é cíclico ( [7][chapter 1, section 1.2, theorem 2]). Portanto, temos o seguinte:

**Teorema 1.7.1.** *O grupo das unidades de $\mathfrak{O}_K$ que satisfazem $l(\varepsilon) = 0$ é cíclico e de ordem par. Como um conjunto, esse grupo consiste nas raízes da unidade de $K$ contidas em $\mathfrak{O}_K$.*

Tendo concluído este passo, denotaremos por $\mathfrak{G}$ o conjunto $l(\mathfrak{O}_k^*)$. Visto que $N(\varepsilon) = \pm 1$, para $\varepsilon \in \mathfrak{O}_K^*$, temos $\ln|N(\varepsilon)| = 0$. Portanto, vale

$$\sum_{i=1}^{s+t} l_i(\varepsilon) = 0.$$

Se $\mathfrak{S}$ é o subespaço de $\mathbb{R}^{s+t}$ dos vetores que possuem a soma das coordenadas nulas, temos que $\mathfrak{G} \subset \mathfrak{S}$, a dimensão de $\mathfrak{S}$ é portanto $s + t - 1$.

**Proposição 1.7.1.** *$\mathfrak{G}$ é um reticulado.*

**Demonstração.** O Lema 1.4.4 nos dispensa de mostrar mais do que a discrição de $\mathfrak{G}$. Seja $r > 0$ e suponhamos $l(\varepsilon) \in \mathcal{B}(r)$. Se $\rho_1, \ldots, \rho_s$ são os monomorfismos reais de $K$ para $\mathbb{C}$, e $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_t, \overline{\sigma_t}$, de modo que $[K : \mathbb{Q}] = n = s + 2t$, temos

$$l_i(\varepsilon) \leq |l_i(\varepsilon)| \leq ||l(\varepsilon)|| \Rightarrow l_k(\varepsilon) < r.$$

Esta última desigualdade nos dá

$$|\rho_k(\varepsilon)| < e^r,\ k = 1, \ldots, s,$$

$$|\sigma_j(\varepsilon)| < e^{\frac{r}{2}}\ j = 1, \ldots, t.$$

Logo, temos que $\mathcal{J}\mathfrak{O}_K^*$ é um subconjunto limitado do Espaço de Minkowski. Visto que $\mathcal{J}\mathfrak{O}_K^*$ está contido no reticulado $\mathcal{J}\mathfrak{O}_K$, existem finitos vetores $l(\varepsilon)$. □

Dado que $\mathfrak{G}$ é um reticulado no subespaço $\mathfrak{S}$, temos o seguinte:

**Proposição 1.7.2.** *$\mathfrak{G}$ é um reticulado de dimensão menor ou igual a $s + t - 1$.*

Queremos mostrar que $\mathfrak{G}$ é um reticulado completo em $\mathfrak{S}$, isto é, que sua dimensão é $s+t-1$. Visto que isto implicaria que grupo das unidades de $\mathfrak{O}_K$ é o produto direto do grupo cíclico $\mu(K)$, das raízes da unidades de $K$, e um grupo abeliano de posto $s + t - 1$, cujo sistema de geradores será chamado *sistema de unidades fundamentais de $K$*. Porém, para prová-lo, precisaremos do lema abaixo

**Lema 1.7.1.** *A menos de associados, há apenas finitos elementos de $\mathfrak{O}_K$ com uma dada norma $N_{K|\mathbb{Q}}(\alpha) = a$.*

**Demonstração.** Para $a \in \mathbb{Z}$, $a > 1$, existe em cada classe do grupo quociente $\mathfrak{O}_K/(a)$, a menos de associados, apenas finitos $\alpha$'s tais que $|N(\alpha)| = |N_{K|\mathbb{Q}}(\alpha)| = a$. De fato, se $\beta = \alpha + a\gamma$, $\gamma \in \mathfrak{O}_K$, é tal que $|N(\alpha)| = |N(\beta)|$, então

$$\frac{\alpha}{\beta} = \pm 1 + \frac{N(\beta)}{\beta}\gamma \in \mathfrak{O}_K$$

pois, substituindo $\beta$ na expressão para o seu polinômio minimal

$$\phi_\beta(t) = t^n - \mathrm{Tr}(\beta)t^{n-1} + \cdots + (-1)^n N(\beta),$$

obtemos que $\dfrac{N(\beta)}{\beta} \in \mathfrak{O}_K$. Por um argumento análogo, obtemos $\dfrac{\beta}{\alpha} = 1 \pm \dfrac{N(\alpha)}{\alpha}\gamma \in \mathfrak{O}_K$. Portanto, $\beta$ é associado de $\alpha$. Assim, a menos de associados, há no máximo $|\mathfrak{O}_K/(a)|$ elementos de norma $\pm a$. □

**Teorema 1.7.2** (das unidades de Dirichlet)**.** *Toda unidade $\varepsilon$ de $\mathfrak{O}_K$ é unicamente escrita na forma*

$$\varepsilon = \zeta \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r},$$

*em que $r = s + t - 1$, $a_i \in \mathbb{Z}$, $\varepsilon_i \in \mathfrak{O}_K^*$ e $\zeta$ é uma raiz da unidade de $\mathfrak{O}_K$.*

**Demonstração.** Como já dissemos, queremos provar que $l(\mathfrak{O}_K^*)$ é completo em $\mathfrak{S}$. Utilizando o Teorema 1.4.1, queremos encontrar um conjunto limitado $U$, tal que os seus translados por representações logarítmicas de $\mathfrak{O}_K^*$ cubram totalmente $\mathfrak{S}$. Notemos que um ponto $\alpha$ de $K_\mathbb{R}^*$ é tal que $l(\alpha) \in \mathfrak{S}$ se, e somente se $|N(\alpha)| = 1$.

Denotemos $S$ o conjunto de todos os pontos $x \in K_\mathbb{R}$ que satisfazem $|N(x)| = 1$. Se um ponto $x = (x_\tau)_\tau \in K_\mathbb{R}$ satisfaz $N(x) = \pm 1$, com $|x_{\rho_i}| < C$, $i = 1, \ldots, s$ e $|x_{\sigma_j}| < \sqrt{C}$, $j = 1, \ldots, t$, para algum

$C > 1$, então $l_k(x) < \ln C$, em que $l_k$ é a $k$-ésima coordenada da representação logarítmica; e temos

$$l_k(x) = -\sum_{i \neq k} l_i(x) > -(s+t-1)\ln C,$$

donde, se $X_0$ é um conjunto limitado em $S$, então $l(X_0)$ também o é em $\mathfrak{S}$. Queremos mostrar que os produtos $(\mathcal{J}\varepsilon)X_0$ cobrem $S$, para algum subconjunto limitado $X_0$.

Seja $y \in S$ arbitrário, e seja $\mathfrak{M} = \mathcal{J}\mathfrak{O}_K^*$. O determinante da transformação $x \mapsto yx$ é $N(y)$; e como $y \in S$, então é $\pm 1$. Como os volumes de $\mathfrak{M}$ e $y\mathfrak{M}$ são iguais, isto é, iguais a $\Delta$.

Escolhamos $c_\tau$'s tais que

$$Q = \prod_\tau c_\tau > \frac{\pi}{2}^{-t} |d_K| \mathfrak{N}(\mathfrak{O}_K) = \frac{\pi}{2}^{-t} |d_K|.$$

Denotemos $X$ o conjunto dos pontos tais que $|x_\tau| < c_\tau$. O Teorema 1.5.1 nos diz que existe um ponto não-nulo $z = y(\mathcal{J}\alpha) \in X$, $\alpha \in \mathfrak{O}_K$. Como $N(z) = N(y)N(\alpha) = \pm N(\alpha)$ e $|N(z)| < \prod_\tau c_\tau = Q$, $|N(\alpha)| < Q$.

O Lema 1.7.1 nos diz que somente finitos elementos não dois a dois associados de $\mathfrak{O}_K$ podem ter norma com valor absoluto menor do que $Q$. Fixemos $\alpha_1, \ldots, \alpha_N \in \mathfrak{O}_K$ tais que qualquer outro $\beta \in \mathfrak{O}_K$ de norma menor que $Q$ é associado de algum deles. Daí, temos $\alpha = \alpha_i \varepsilon$, em que $\varepsilon \in \mathfrak{O}_K^*$. Podemos escrever $y$ como

$$y = (\mathcal{J}\alpha^{-1})z = (\mathcal{J}\alpha_i^{-1})(\mathcal{J}\varepsilon)z \in X.$$

Definamos

$$X_0 = S \cap \left( \bigcup_{i=1}^{N} X\mathcal{J}\alpha_i^{-1} \right).$$

De $y$ e $x \in S$, temos $X\mathcal{J}\alpha_i^{-1} \in S$, logo $X\mathcal{J}\alpha_i^{-1} \in X_0$. Da equação obtida para $y$ resulta $y \in X_0\mathcal{J}\varepsilon^{-1}$. Como $y$ foi escolhido arbitrariamente, segue-se que $S$ é completamente coberto pelos produtos $X_0\mathcal{J}\varepsilon$ e, por tanto, como $l(S) = \mathfrak{S}$, temos que $\mathfrak{S}$ é completamente coberto pelos translados $l(X_0) + l(\varepsilon)$. □

Usaremos o resto desta seção para definir um importante número associado a um corpo de números $K$. Identificando $\prod_\tau \mathbb{R}^+ = \mathbb{R}^{s+t}$ (ver Seção 1.5), o subespaço $\mathfrak{S}$ torna-se ele próprio um $\mathbb{R}$-espaço de dimensão finita. Podemos, portanto, falar do volume $v(l(\mathfrak{O}_K^*))$. Sejam $\varepsilon_1, \ldots, \varepsilon_r$, $r = s + t - 1$, um sistema de unidades fundamentais e $\Phi$ o paralelepípedo fundamental de $l(\mathfrak{O}_K^*)$, gerado por $l(\varepsilon_1), \ldots, l(\varepsilon_r)$. O vetor

$$l_0 = \frac{1}{\sqrt{s+t}}(1, \ldots, 1) \in \mathbb{R}^{s+t}$$

é ortogonal a todos eles e tem comprimento $1$. O volume de $\Phi$ é igual ao volume do paralelepípedo fundamental gerado por $l_0, l(\varepsilon_1), \ldots, l(\varepsilon_r)$. Este último volume, porém, é igual a

$$\pm \det \begin{pmatrix} l_{01} & l(\varepsilon_1)_1 & \ldots & l(\varepsilon_r)_1 \\ \vdots & \vdots & \ddots & \vdots \\ l_{0(s+t)} & l(\varepsilon_1)_{s+t} & \ldots & l(\varepsilon_r)_{s+t} \end{pmatrix}.$$

Somando todas as linhas a uma fixada, por exemplo, à primeira, esta terá todas as entradas nulas, exceto pela primeira, que igualará $\sqrt{s+t}$, obtemos, portanto a

**Proposição 1.7.3.** *O volume de um paralelepípedo fundamental de $l(\mathfrak{O}_K^*)$ é dado por*

$$\sqrt{s+t}R,$$

*em que $R$ é um dos menores de posto $r = s + t - 1$ da matriz*

$$\begin{pmatrix} l(\varepsilon_1)_1 & \dots & l(\varepsilon_r)_1 \\ \vdots & \ddots & \vdots \\ l(\varepsilon_1)_{s+t} & \dots & l(\varepsilon_r)_{s+t} \end{pmatrix}.$$

*Este número é chamado o **regulador** do corpo $K$*

## 1.8 Extensões de domínios de Dedekind

Sendo $K$ um corpo de números, todo ideal primo $\mathfrak{p}$ de $\mathfrak{O}_K$ contém um número primo. Mais do que isso, tem-se $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, com $p$ um número primo. Nesta seção, estudaremos como o ideal gerado pelo primo $p$ se fatora em primos de $\mathfrak{O}_K$ (às vezes, por abuso, dizemos apenas primos de $K$). Iniciaremos, porém, com um domínio de Dedekind $o$ genérico, ao invés de $\mathbb{Z}$, e, ao invés de $\mathfrak{O}_K$, tomaremos $\mathcal{O}$, o fecho integral de $o$ em seu corpo de frações.

**Proposição 1.8.1.** *Sejam $o$ um domínio de Dedekind com corpo de frações $K$, $L|K$ uma extensão finita e separável, $\mathcal{O}$ o fecho integral de $o$ em $L$. Tem-se que $\mathcal{O}$ é um domínio de Dedekind.*

**Demonstração.** Visto que $\mathcal{O}$ é o fecho integral de $o$ em $L$, então $\mathcal{O}$ é integralmente fechado em $L$. Se $\mathfrak{B}$ é um ideal primo não-nulo de $\mathcal{O}$, então $\mathfrak{p} = \mathfrak{B} \cap o$ é um ideal primo de $o$. Substituindo $\mathbb{Z}$ por $o$ e raciocinando como na prova do Teorema 1.3.1, obtemos que o domínio $\mathcal{O}/\mathfrak{B}$ é uma extensão algébrica de $o/\mathfrak{p}$. Ora, se $\mathcal{O}$ não fosse um corpo, então teria um ideal primo não-nulo que, intersectado com $o/\mathfrak{p}$, resultaria num ideal primo não-nulo de $o/\mathfrak{p}$, um absurdo. Logo, $\mathfrak{B}$ é ideal maximal de $\mathcal{O}$.

Seja $\{\alpha_1, \dots, \alpha_n\}$ uma base de $L|K$ contida em $\mathcal{O}$, de discriminante $d$. Sabemos que $d \neq 0$ e $d\mathcal{O} \subseteq \sum \alpha_i o$, donde $d^{-1}\alpha_1, \dots, d^{-1}\alpha_n$ gera $\mathcal{O}$ como um $o$-módulo. Se $M$ é um ideal de $\mathcal{O}$, então $M$ também é um $o$-módulo finitamente gerado. Ora, se $x_1, \dots, x_r$ é um sistema de geradores de $M$ como $o$-módulo, então $\{d^{-1}\alpha_i x_j | i = 1, \dots n; j = 1, \dots, r\}$ define um sistema de geradores de $M$ como um $\mathcal{O}$-módulo. Daí, tem-se que todo ideal de $\mathcal{O}$ é um $\mathcal{O}$-módulo finitamente gerado e o Lema 1.3.1 finaliza a prova. □

Sejam $o$, $\mathcal{O}$, $K$ e $L$ como no resultado anterior e $\mathfrak{p}$ um ideal primo de $o$. Tomemos $\pi \in \mathfrak{p} - \mathfrak{p}^2$ ($\mathfrak{p} \neq 0$). Teremos $\pi o = \mathfrak{p}\mathfrak{a}$, em que $\mathfrak{a} \not\subset \mathfrak{p}$. Como $\mathfrak{p}$ também é maximal, temos $\mathfrak{p} + \mathfrak{a} = o$. Escrevendo $1 = b + s$, com $b \in \mathfrak{p}$ e $s \in \mathfrak{a}$, obtemos $s \notin \mathfrak{p}$ e $s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi o$. Não podemos, portanto, ter $\mathfrak{p}\mathcal{O} = \mathcal{O}$; pois isto implicaria $s\mathcal{O} \subseteq s\mathfrak{p}\mathcal{O} \subseteq \mathfrak{p}\mathfrak{a}\mathcal{O} \subseteq \pi\mathcal{O}$, donde $s = \pi x$, com $x \in \mathcal{O} \cap K = o$, que implica $s \in \pi o \subseteq \mathfrak{p}$. Tem-se, portanto, $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$, para todo ideal primo de $o$.

Assim como quando tínhamos $o = \mathbb{Z}$, temos que todo ideal primo $\mathfrak{p}$ de $o$ decompõe-se em $\mathcal{O}$ de uma única forma como

$$\mathfrak{p}\mathcal{O} = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r},$$

com $\mathfrak{B}_i$ um ideal primo de $\mathcal{O}$; além disso, os ideais $\mathfrak{B}_i$ são exatamente os ideais primos de $\mathcal{O}$ que satisfazem

$$\mathfrak{B} \cap o = \mathfrak{p}.$$

**Definição 1.8.1.** *Se $\mathfrak{p}$ é um ideal primo de $o$ e $\mathfrak{P}$ é um ideal primo de $\mathcal{O}$ tal que*

$$\mathfrak{P} \cap o = \mathfrak{p},$$

*dizemos que $\mathfrak{P}$ está acima de $\mathfrak{p}$. Além disso, cada expoente $e_i$ da fatoração*

$$\mathfrak{p}\mathcal{O} = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r}$$

*são chamados índices de ramificação de $\mathfrak{B}_i$ e*

$$[\mathcal{O}/\mathfrak{B}_i : o/\mathfrak{p}]$$

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

Os $f_i$'s e os $e_i$'s assim definidos estão relacionados por uma lei surpreendente.

**Proposição 1.8.2.** *Seja $L|K$ uma extensão separável. A seguinte identidade vale*

$$\sum_{i=1}^{r} e_i f_i = n = [L : K].$$

**Demonstração.** Pelo Teorema chinês dos restos, a igualdade

$$\mathcal{O}/\mathfrak{p}\mathcal{O} = \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{B}^{e_i}$$

nos diz que o $o/\mathfrak{p}$-espaço vetorial $\mathcal{O}/\mathfrak{p}\mathcal{O}$ é soma direta dos $o/\mathfrak{p}$-espaços vetoriais $\mathcal{O}/\mathfrak{B}^{e_i}$. Denotemos $o/\mathfrak{p} = k$. É suficiente mostrar

$$\dim_k \mathcal{O}/\mathfrak{p}\mathcal{O} = n \text{ e } \dim_k \mathcal{O}/\mathfrak{B}^{e_i} = f_i e_i.$$

Para provar a primeira, sejam $\omega_1, \dots, \omega_m$ representantes de classes $\overline{\omega_1}, \dots, \overline{\omega_m}$ que formam uma base de $\mathcal{O}/\mathfrak{p}\mathcal{O}$. Queremos mostrar que $\omega_1, \dots, \omega_m$ formam uma base de $L|K$.

Suponhamos que se tenha

$$a_1\omega_1 + \dots a_m\omega_m = 0,$$

com $a_i \in o$ e $a_i \neq 0$, para algum $i$. Seja $\mathfrak{a}$ o ideal $(a_1, \dots, a_m)$ de $o$. O Lema 1.3.3 nos diz que podemos tomar $a \in \mathfrak{a}^{-1}$ tal que $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, o que implica $a\mathfrak{a} \not\subseteq \mathfrak{p}$. Temos, portanto, que nem todos os elementos $aa_i \in o$ pertencem a $\mathfrak{p}$. No entanto a congruência

$$aa_1\omega_1 + \dots + aa_m\omega_m \equiv 0 \mod \mathfrak{p}$$

não pode ser satisfeita, se nem todos os $a_i \neq 0$, para algum $i$, uma contradição. Daí fica provado que $\{\omega_1, \dots, \omega_m\}$ é um conjunto linearmente independente sobre $K$.

Sejam agora $M$ e $N$ os $o$-módulos $o\omega_1 + \dots + o\omega_m$ e $\mathcal{O}/M$, respectivamente. O supradito nos mostra que $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, donde $\mathfrak{p}N = N$. Como $L|K$ é separável, tem-se que $\mathcal{O}$ e $N$ são $o$-módulos finitamente gerados. Seja $\alpha_1, \dots, \alpha_s$ um sistema de geradores de $N$, visto que $\mathfrak{p}N = \mathfrak{p}\alpha_1 + \dots \mathfrak{p}\alpha_s$, temos

$$\alpha_i = \sum_{j=1}^{s} a_{ij}\alpha_j,$$

com $a_{ij} \in \mathfrak{p}$. Definamos $A = (a_{ij})_{ij} - I$, em que $I$ é a matriz identidade $s \times s$, e seja $B$ a matriz adjunta

de $A$. Temos

$$A\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_s\end{bmatrix} = 0 \text{ e } BA = (\det A)I.$$

Segue-se daí

$$0 = BA\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_s\end{bmatrix} = \det A\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_s\end{bmatrix},$$

donde $dN = 0$, que implica $d\mathcal{O} \subseteq M$. Por outro lado, cada entrada de $A$ é $0$ ou $-1 \mod \mathfrak{p}$, sendo $-1$ apenas aquelas que estiverem na diagonal principal, donde $\det A \equiv (-1)^s \mod \mathfrak{p}$, que implica $\det A \neq 0$. Posto que cada elemento de $L$ é da forma $\dfrac{l}{k}$, com $l \in \mathcal{O}$ e $k \in K$, e $L = dL$, temos que todo elemento de $L$ é da forma

$$\frac{b_1}{dk_1}\omega_1 + \cdots + \frac{b_m}{dk_m}\omega_m,$$

com $b_i, k_i \in K$. Fica, portanto, provado que $\{\omega_1, \ldots, \omega_m\}$ é um conjunto gerador de $L|K$; como este conjunto é linearmente independente sobre $K$, ele é uma base de $L|K$.

Provemos agora a segunda afirmação. Temos a seguinte cadeia descendente

$$\mathcal{O}/\mathfrak{B}_i^{e_i} \supseteq \mathfrak{B}/\mathfrak{B}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{B}_i^{e_i-1}/\mathfrak{B}_i^{e_i} \supseteq 0.$$

Cada quociente $\mathfrak{B}_i^p/\mathfrak{B}_i^{e_i}$, bem como o quociente $\mathcal{O}/\mathfrak{B}_i^{e_i}$ é um $K$-espaço vetorial. Consideremos o homomorfismo

$$\xi : \mathcal{O} \to \mathfrak{B}_i{}^p/\mathfrak{B}_i^{p+1},\ \xi(a) = a\alpha,$$

em que $p = 1, 2 \ldots, e_i - 1$ e $\alpha \in \mathfrak{B}^p - \mathfrak{B}^{p-1}$. Temos que $\ker \xi = \mathfrak{B}_i$. Além disso, temos que $\mathfrak{B}_i^p$ é o máximo divisor comum entre $\alpha\mathcal{O}$ e $\mathfrak{B}_i^{p+1}$, donde $\mathfrak{B}_i^p = \alpha\mathcal{O} + \mathfrak{B}_i^{p+1}$. Daí, obtemos $\mathfrak{B}_i^p/\mathfrak{B}_i^{p+1} = \alpha\mathcal{O}$, donde se conclui que $\xi$ é sobrejetivo. Concluímos, portanto, que, para qualquer $p$, vale

$$\mathfrak{B}_i^p/\mathfrak{B}_i^{p+1} \cong \mathcal{O}/\mathfrak{B}_i,$$

e, portanto, $\dim_K \mathfrak{B}^p/\mathfrak{B}^{p+1} = \dim_K \mathcal{O}/\mathfrak{B}_i = f_i$.

Na cadeia descendente acima, podemos quocientar cada termo na forma $\mathfrak{B}_i^p/\mathfrak{B}_i^{e_i}$ pelo seu posterior, obtemos um quociente na forma $\mathfrak{B}_i^p/\mathfrak{B}_i^{p+1}$, com $p = 1, 2 \ldots, e_i - 1$. Consideremos o mapa canônico $\mathcal{O}/\mathcal{B}_i^{e_i} \to (\mathcal{O}/\mathfrak{B}_i^{e_i})/(\mathfrak{B}/\mathfrak{B}_i^{e_i}) \cong \mathcal{O}/\mathfrak{B}_i$, o Teorema do núcleo e da imagem nos fornece

$$\dim_K \mathcal{O}/\mathfrak{B}_i^{e_i} = \dim_K \mathcal{O}/\mathfrak{B}_i + \dim_K \mathfrak{B}_i/\mathfrak{B}_i^{e_i} = f_i + \dim_K \mathfrak{B}_i/\mathfrak{B}_i^{e_i}.$$

Considerando agora o mapa canônico $\mathfrak{B}_i/\mathfrak{B}_i^{e_i} \to (\mathfrak{B}_i/\mathfrak{B}_i^{e_i})/(\mathfrak{B}_i^2/\mathfrak{B}_i{}^{e_i}) \cong \mathfrak{B}_i/\mathfrak{B}_i^2 \cong \mathcal{O}/\mathfrak{B}_i$, obtemos

$$\dim_K \mathfrak{B}_i/\mathfrak{B}_i^{e_i} = f_i + \dim_K \mathfrak{B}_i^2/\mathfrak{B}_i^{e_i} \Rightarrow \dim_K \mathcal{O}/\mathfrak{B}_i^{e_i} = 2f_i + \dim_K \mathfrak{B}_i^2/\mathfrak{B}_i^{e_i}.$$

Continuando este processo, obtemos

$$\dim \mathcal{O}/\mathfrak{B}_i^{e_i} = \sum_{j=o}^{e_i-1} f_i = e_i f_i.$$

□

Suponha agora que temos uma extensão separável $L|K$ dada por um elemento primitivo $\theta \in \mathcal{O}$, com polinômio minimal

$$p(x) \in o[x].$$

Podemos demonstrar um resultado parcial sobre a natureza da fatoração de $\mathfrak{p}\mathcal{O}$. Parcial, porque exclui um número finito de ideais, aqueles que não são coprimos com o *condutor* de $o[\theta]$

$$\mathfrak{F} = \{\alpha \in \mathcal{O} |\ \alpha\mathcal{O} \subseteq o[\theta]\}.$$

**Observação 1.8.1.** *Visto que $L = K(\theta)$ e $\mathcal{O}$ é um $o-$módulo finitamente gerado, não podemos ter $\mathfrak{F} = 0$.*

**Proposição 1.8.3.** *Seja $\mathfrak{p}$ um ideal primo de $o$ coprimo com o condutor $\mathfrak{F}$ de $o[\theta]$. Seja também*

$$\overline{p}(x) = \prod_{i=1}^{r} \overline{p_i}(x)^{e_i}$$

*a fatoração em fatores irredutíveis do polinômio $\overline{p}(x) \in o/\mathfrak{p}[x]$, obtido a partir do polinômio minimal $p(x) \in o[x]$ de $\theta$ via redução módulo $\mathfrak{p}$, com cada $p_i(x) \in o[x]$ mônico. Tem-se que os ideais primos de $\mathcal{O}$ sobre $\mathfrak{p}$ são*

$$\mathfrak{B}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O},\ i = 1, \ldots, r.$$

*Além disso, $f_i = \deg \overline{p_i}(x)$ e*

$$\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{B}_i^{e_i}.$$

**Demonstração.** Escrevamos $\mathcal{O}' = o[\theta]$ e $\overline{o} = o/\mathfrak{p}$. Visto que $\mathfrak{F}$ e $\mathfrak{p}\mathcal{O}$ são coprimos, temos $\mathfrak{F} + \mathfrak{p}\mathcal{O} = \mathcal{O}$. Se $\mathfrak{f}\mathcal{O} \subseteq o[\theta]$, com $\mathfrak{f} \in \mathfrak{F}$, então $\mathfrak{f} \cdot 1 \in o[\theta]$, donde $\mathfrak{F} \subseteq \mathcal{O}'$ e, portanto, $\mathfrak{p}\mathcal{O} + \mathcal{O}' = \mathcal{O}$. Daí, temos que a restrição do homomorfismo canônico $\mathcal{O} \to \mathcal{O}/\mathfrak{p}\mathcal{O}$ a $\mathcal{O}'$ é um homomorfismo sobrejetivo, cujo núcleo é $\mathfrak{p}\mathcal{O} \cap \mathcal{O}'$. Se $x$ pertence a este núcleo, então, por um lado, $x = g(\theta)$, com $\deg g_i(x) \leq n = [L : K] = \deg p(x)$ e $g_i(x) \in \mathfrak{p}[x]$, e, por outro lado, $x = f_i(\theta)$, com $f \in o[x]$. Como a escrita de qualquer elemento de $L$ na forma $h(\theta)$, com $\deg h(x) < n$ e $h(x) \in K[x]$ é única, temos $f = g$, que implica $\mathfrak{p}\mathcal{O} \cap \mathcal{O}' = \mathfrak{p}\mathcal{O}'$. Daí, pelo primeiro Teorema do isomorfismo, temos

$$\mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \mathcal{O}/\mathfrak{p}\mathcal{O}.$$

O homomorfismo representado pelo mapa

$$o[x] \overset{f(x)\mapsto \overline{f}(x)}{\longrightarrow} o/\mathfrak{p}[x] \overset{\overline{g}(x)\mapsto \overline{g}(x)+(\overline{p}_i(x))}{\longrightarrow} \overline{o}[x]/(\overline{p}(x))$$

é um homomorfismo sobrejetivo. Como podemos representar $\overline{f}(x)$ como $f(x) + \mathfrak{p}[x]$, o núcleo deste homomorfismo é o conjunto

$$\{f(x) \in o[x] |\ f(x) + \mathfrak{p}[x] \in (p(x) + \mathfrak{p}[x])\} = \mathfrak{p}[x] + (p(x)).$$

Visto que $\mathcal{O}' = o(\theta) \cong o[x]/(p(x)) = \{f(x) + (p(x)) |\ f(x) \in o[x]\}$, temos que o homomorfismo $f(x) + (p(x)) \mapsto f(x) + ((p(x)) + \mathfrak{p}[x])$ é sobrejetivo, e tem núcleo exatamente igual a $\mathfrak{p}[x]$. Donde $\mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \overline{o}[x]/(\overline{p}(x))$. Temos, portanto, a cadeia de isomorfismos

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \overline{o}[x]/(\overline{p}(x)).$$

Em vista da fatoração de $\overline{p}(x)$, o Teorema chinês dos restos nos dá

$$R = \overline{o}[x]/(\overline{p}(x)) \cong \bigoplus_{i=1}^{r} \overline{o}[x]/(\overline{p}_i(x))^{e_i}.$$

Visto que $(\overline{p_i}(x))|(\overline{p}_i(x))^{e_i}$, o Teorema da correspondência nos diz que $\overline{p}_i(x)[\overline{o}[x]/(\overline{p}_i(x))^{e_i}]$ é um ideal primo de $\overline{o}[x]/(\overline{p}_i(x))^{e_i}$, donde $\overline{p}_i(x)R$ também é um ideal primo de $R$. Por outro lado, os ideais primos de $R = \overline{o}[x]/(\overline{p}(x))$ são justamente os ideais primos de $\overline{o}[x]$ que dividem $(\overline{p}(x))$, que são exatamente os ideais gerados pelos polinômios irredutíveis que dividem $\overline{p}(x)$. Concluímos, portanto, que os ideais primos de $R$ são os ideais principais $\overline{p}_i(x)R = (\overline{p}_i(x))$.

Tendo em vista que $f(x) \mapsto f(\theta)$ é um isomorfismo de $R$ para $\overline{\mathcal{O}} = \mathcal{O}/\mathfrak{p}\mathcal{O}$, temos, a correspondência entre ideais é preservada, donde os ideais primos $\overline{\mathfrak{B}_i}$ de $\overline{\mathcal{O}}$ são as pré-imagens dos ideais $(\overline{p}_i(x))$ por este isomorfismo, isto é $\overline{\mathfrak{B}_i} = (p_i(\theta) + \mathfrak{p}\mathcal{O})\overline{\mathcal{O}}$. Se $\deg \overline{p}_i(x) = d$, então $\{1, \theta, \ldots, \theta^{d-1}\}$ é uma $\overline{o}$-base de $\overline{\mathcal{O}}/\overline{\mathfrak{B}_i}$, como $\overline{o}$-espaço vetorial, em particular, tem-se $[\overline{\mathcal{O}} : \overline{\mathfrak{B}_i}] = \deg \overline{p}_i(x)$.

Por outro lado, ao ideal $\overline{\mathfrak{B}_i}$ de $\overline{\mathcal{O}}$ corresponde o ideal $\mathfrak{B}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$ de $\mathcal{O}$, pelo mapa canônico $\mathcal{O} \to \mathcal{O}/\mathfrak{p}\mathcal{O}$. Como estes ideais contém $\mathfrak{p}\mathcal{O}$ e correspondem aos ideais primos de $\overline{\mathcal{O}}$, novamente, o Teorema da correspondência nos diz que cada $\mathfrak{B}_i$ é um ideal primo de $\mathcal{O}$, além disso, tem-se $\mathfrak{B}_i \cap o = \mathfrak{p}$.

Por fim, temos

$$\mathcal{O}/\mathfrak{B}_i \cong (\mathcal{O}/\mathfrak{p}\mathcal{O})/(\mathfrak{B}_i/\mathfrak{p}\mathcal{O}) = \overline{\mathcal{O}}/\overline{\mathfrak{B}_i} \cong R/(\overline{p}_i(x)) \cong \overline{\mathcal{O}}[x]/(\overline{p}_i(x)),$$

donde

$$f_i = [\mathcal{O}/\mathfrak{B}_i : \overline{\mathcal{O}}] = [\overline{\mathcal{O}}[x]/(\overline{p}_i(x)) : \overline{\mathcal{O}}] = \deg \overline{p}_i(x).$$

Como a pré-imagem de $(0) = (\overline{p}(x)) = \bigcap_{i=1}^{r}(\overline{p}_i(x))^{e_i}$ pelo isomorfismo $\overline{\mathcal{O}} \to R$ é $\mathfrak{p}\mathcal{O}$, temos

$$\mathfrak{p}\mathcal{O} = \bigcap_{i=1}^{r} \mathfrak{B}_i^{e_i} = \prod_{i=1}^{r} \mathfrak{B}_i^{e_i}.$$

Visto que $\overline{p}(x) = \prod_{i=1}^{r} \overline{p}_i(x)^{e_i}$, temos $\sum_{i=1}^{r} e_i f_i = n = [L : K]$, donde os $\mathfrak{B}_i$'s são exatamente os ideais primos de $\mathcal{O}$ sobre $\mathfrak{p}$, e finalizamos a demonstração. □

**Definição 1.8.2.** *Dizemos que o ideal primo $\mathfrak{p}$ decompõe-se totalmente em $L$ se, na decomposição*

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r},$$

*temos $r = [L : K]$ (isto é, $e_i = f_i = 1$, pela Proposição 1.8.2). Dizemos que $\mathfrak{p}$ não se decompõe se $r = 1$. O ideal $\mathfrak{P}_i$ é dito não-ramificado sobre $o$ se $e_i = 1$ e $\mathcal{O}/\mathfrak{P}_i|o/\mathfrak{p}$ é separável. Caso contrário (isto é, se $e_i \neq 1$ ou $\mathcal{O}/\mathfrak{P}_i|o/\mathfrak{p}$ não é separável), dizemos que $\mathfrak{P}_i$ é ramificado. Caso $f_i = 1$, isto é, caso $\mathcal{O}/\mathfrak{P}_i \cong o/\mathfrak{p}$, $\mathfrak{B}_i$ é dito totalmente ramificado. O ideal primo $\mathfrak{p}$ é dito não-ramificado se todos os $\mathfrak{P}_i$'s são não-ramificados, sendo ramificado, caso contrário. A extensão $L|K$ é dita não-ramificada se todos os ideais primos de $o$ são não-ramificados em $L$.*

Apesar do destaque que o caso em que $\mathfrak{p}$ é ramificado recebe na definição anterior, este é uma exceção. Com efeito, temos a

**Proposição 1.8.4.** *Se $L|K$ é separável, então há somente finitos ideais primos de $K$ que são ramificados em $L$.*

**Demonstração.** Seja $\theta \in L$ um elemento primitivo da extensão $L|K$, com polinômio minimal $p(X) \in o[x]$, de grau $n$. Seja também $\mathfrak{p}$ um ideal primo de $o$, coprimo com o condutor $\mathfrak{F}$. Consideremos o

discriminante

$$d = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2 \in \mathcal{O}$$

de $p(x)$. Pela Proposição 1.8.3, tem-se que os índices de ramificação $e_i$ de quaisquer ideais primos da fatoração de $\mathfrak{p}$ serão iguais a $1$ se, e somente se, todo polinômio irredutível $\overline{p}_i(x) \in (\mathcal{o}/\mathfrak{p})[x]$ da fatoração de $\overline{p}(x)$ aparecer com exponente $1$. Ora, se $\mathfrak{p}$ for coprimo com $(d)$, então $\overline{d} \equiv d \mod \mathfrak{p}$ certamente não é zero em $\mathcal{o}/\mathfrak{p}$, o que implica que $\overline{p}(x)$ não tem raízes múltiplas. Ora, se $\overline{p}$ não tem raízes múltiplas, então nenhum polinômio irredutível pode dividi-lo, quando elevado a qualquer potência maior que $1$. Como na prova da proposição anterior, temos $\mathcal{O}/\mathfrak{B}_i \cong (\mathcal{o}/\mathfrak{p})[x]/(\overline{p}_i(x)) \cong (\mathcal{o}/\mathfrak{p})(\overline{\theta})$, em que $\overline{\theta} \equiv \theta \mod \mathfrak{p}$. □

## 1.9 Teoria de ramificação de Hilbert

A questão da decomposição em primos numa extensão finita $L|K$ torna-se bem mais rica se assumirmos que $L|K$ é uma extensão de Galois (ou seja, que além de finita e separável, ela é também normal). Isto porque os ideais primos de $\mathcal{o}$ estão sujeitos à ação do grupo de Galois $G = Gal(L|K) = G(L|K)$.

Dado $a \in \mathcal{O}$ (o anel de inteiros de $L$), tem-se $\sigma a \in \mathcal{O}$, qualquer que seja $\sigma \in G$ ($\sigma a$ é sempre um conjugado de $a$). Em outras palavras, $G$ age em $\mathcal{O}$. Se $\mathfrak{B}$ é um ideal primo de $\mathcal{O}$ sobre $\mathfrak{p}$, também o é $\sigma\mathfrak{B}$. De fato, $c\sigma(b_1) + d\sigma(b_2) = \sigma(cb_1 + db_2) \in \sigma\mathfrak{B}$, para $b_1, b_2 \in \mathfrak{B}$ e $c, d \in \mathcal{o}$ ($G$ fixa $K$, portanto fixa $\mathcal{o}$), donde $\sigma\mathfrak{B}$ é um ideal de $\mathcal{O}$. Sejam $a, b \in \mathcal{O}$ tais que $ab \in \sigma\mathfrak{B}$. Temos $\sigma^{-1}(a)\sigma^{-1}(b) \in \mathfrak{B}$ e, como $\mathfrak{B}$ é um ideal primo, $\sigma^{-1}(a)$ ou $\sigma^{-1}(b) \in \mathfrak{B}$; aplicando $\sigma$, temos que $\sigma\mathfrak{B}$ é um ideal primo. Por fim, como $\sigma$ fixa $\mathcal{o}$, temos $\sigma\mathfrak{B} \cap \mathcal{o} = \mathfrak{B} \cap \mathcal{o} = \mathfrak{p}$. Dizemos que o ideal $\sigma\mathfrak{B}$ é um conjugado de $\mathfrak{B}$. A próxima proposição estabelece que, se conhecemos $G$ e apenas um ideal primo $\mathfrak{B}$ sobre $\mathfrak{p}$, então conhecemos todos os outros.

**Proposição 1.9.1.** *O grupo de Galois $G(L|K)$ age transitivamente no conjunto dos ideais primos de $\mathcal{O}$ sobre um mesmo ideal primo $\mathfrak{p}$ de $\mathcal{o}$; isto é, fixando um destes ideais $\mathfrak{B}$, todos os outros são a imagem de $\mathfrak{B}$ via algum $\sigma \in G(L|K)$.*

**Demonstração.** Consideremos o ideal $\mathfrak{P} = \prod_{\sigma \in G(L|K)} \sigma\mathfrak{B}$. Seja $\mathfrak{B}'$ um ideal primo de $\mathcal{O}$ sobre $\mathfrak{p}$. Se $\mathfrak{B}' \neq \sigma\mathfrak{B}$, qualquer que seja $\sigma$, então $\mathfrak{P}$ é coprimo com $\mathfrak{B}'$, donde $\mathfrak{B}' + \mathfrak{P} = \mathcal{O}$ e, portanto, existe $x \in \mathcal{O}$ tal que

$$x \equiv 0 \mod \mathfrak{B}' \text{ e } x \equiv 1 \mod \sigma\mathfrak{B},\ \forall\, \sigma.$$

Visto que a norma $N_{L|K}(x) = \prod_{\sigma \in G(L|K)} \sigma x$ é um elemento de $\mathcal{o}$, então $x \in \mathfrak{B}' \cap \mathcal{o} = \mathfrak{p}$ (por hipótese). Por outro lado, aplicando $\sigma^{-1}$ em $x \notin \sigma\mathfrak{B}$, para cada $\sigma$, obtemos que $\sigma x \notin \mathfrak{B}$, qualquer que seja $\sigma$. Como $\mathfrak{B}$ é um ideal primo, esta última conclusão nos diz que $N_{L|K}(x) = \prod_\sigma \sigma x \notin \mathfrak{B} \cap \mathcal{o} = \mathfrak{p}$, que é uma contradição. □

**Proposição 1.9.2.** *Seja $\mathfrak{B}$ um ideal primo de $\mathcal{O}$ sobre $\mathfrak{p}$, um ideal primo de $\mathcal{o}$. Valem:*

*i)* $G_{\mathfrak{B}} = \{\sigma \in G(L|K) | \sigma\mathfrak{B} = \mathfrak{B}\}$ *é subgrupo de* $G(L|K)$.

*ii) Se* $Z_{\mathfrak{B}}$ *é o corpo intermediário de* $L|K$ *fixado por* $G_{\mathfrak{B}}$, *então*

$$\mathfrak{p} \textit{ decompõe-se totalmente} \Leftrightarrow Z_{\mathfrak{B}} = L \Leftrightarrow G_{\mathfrak{B}} = \{Id\},$$

$$\mathfrak{p} \textit{ não se decompõe} \Leftrightarrow Z_{\mathfrak{B}} = K \Leftrightarrow G_{\mathfrak{B}} = G(L|K).$$

*iii) Se $\sigma\mathfrak{B}$ é um ideal primo conjugado de $\mathfrak{B}$, então*

$$G_{\sigma\mathfrak{B}} = \sigma G_{\mathfrak{B}} \sigma^{-1}.$$

**Demonstração.** $i)$ De fato, tomando $\sigma, \beta \in G_{\mathfrak{B}}$, tem-se $\mathfrak{B} = \sigma^{-1}(\sigma\mathfrak{B}) = \sigma^{-1}B$ e $\beta\sigma\mathfrak{B} = \beta(\sigma\mathfrak{B}) = \beta\mathfrak{B} = \mathfrak{B}$.

$ii)$ É suficiente mostrar que o número de ideais primos distintos que dividem $\mathfrak{p}\mathcal{O}$ é igual a $|G/G_{\mathfrak{B}}|$, com $G = G(L|K)$. Ora, a Proposição 1.9.1 nos diz que um ideal primo $\mathfrak{I}$ sobre $\mathfrak{p}$ é diferente de $\mathfrak{B}$ se, e somente se, $\mathfrak{I} = \sigma\mathfrak{B}$, com $\sigma \in G - G_{\mathfrak{B}}$. Daí, tomando um sistema de representantes das classes de $G/G_{\mathfrak{B}}$ e fazendo $\sigma$ percorrer todos estes representantes, obtemos todos os ideais primos distintos sobre $\mathfrak{p}$.

$iii)$ Com efeito, se $\tau \in G$, então

$$\tau \in G_{\sigma\mathfrak{B}} \Leftrightarrow \tau\sigma\mathfrak{B} = \sigma\mathfrak{B} \Leftrightarrow \sigma^{-1}\tau\sigma \in G_{\mathfrak{B}} \Leftrightarrow \tau \in \sigma G_{\mathfrak{B}} \sigma^{-1}.$$

□

**Definição 1.9.1.** *O subgrupo $G_{\mathfrak{B}}$ da proposição anterior é chamado o grupo de decomposição de $\mathfrak{B}$ sobre $K$. O corpo $Z_{\mathfrak{B}}$ é chamado o corpo de decomposição de $\mathfrak{B}$ sobre $K$.*

Um outro ganho do caso galoisiano é a

**Proposição 1.9.3.** *Sejam $L|K$ uma extensão de Galois, $\mathcal{o}$ o anel de inteiros de $K$ e $\mathcal{O}$ o anel de inteiros de $L$. Seja também $\mathfrak{p}$ um ideal primo de $\mathcal{o}$. Os índices de ramificação $e_i$ da fatoração em ideais primos*

$$\mathfrak{p}\mathcal{O} = \mathfrak{B}_1^{e_i} \dots \mathfrak{B}_r^{e_r},$$

*bem como os graus de inércia*

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

*não dependem de $i$. Em outras palavras, $e_i = e$ e $f_i = f$, para $i = 1, \dots, r$.*

**Demonstração.** Escrevamos $\mathfrak{B}_1 = \mathfrak{B}$, de modo que qualquer $\mathfrak{B}_i$ possa ser escrito como $\sigma_i\mathfrak{B}$, para algum $\sigma_i \in G = G(L|K)$. Note que

$$\Phi : \mathcal{O}/\mathfrak{B} \longrightarrow \mathcal{O}/\sigma_i\mathfrak{B},\ \Phi(x + \mathfrak{B}) = \sigma_i x + \sigma_i\mathfrak{B},$$

é um isomorfismo de corpos. Com efeito, a aditividade, a multiplicatividade e a sobrejetividade são triviais, se $x \in \ker\Phi$, então

$$\sigma_i x \in \sigma_i\mathfrak{B} \Leftrightarrow x \in \mathfrak{B},$$

donde temos a injetividade.

Temos, portanto,

$$f_i = [\mathcal{O}/\mathfrak{B}_i : \mathcal{O}/\mathfrak{p}] = [\mathcal{O}/\sigma_i\mathfrak{B} : \mathcal{O}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{B} : o/\mathfrak{p}] = f.$$

Verifica-se facilmente que

$$\mathfrak{B}^p | \mathfrak{p}\mathcal{O} \Leftrightarrow \sigma_i(\mathfrak{B}^p) | \sigma_i(\mathfrak{p}\mathcal{O}).$$

Por outro lado, visto que $\sigma_i$ fixa $\mathcal{O}$, tem-se

$$\sigma_i(\mathfrak{B}^p)|\sigma_i(\mathfrak{p}\mathcal{O}) \Leftrightarrow \sigma_i(\mathfrak{B})^p|\mathfrak{p}\mathcal{O},$$

donde o expoente de $\mathfrak{B}_i$ é igual ao expoente de $\mathfrak{B} = \mathfrak{B}_1$, para todo $i$. □

A igualdade dos índices de ramificação no caso galoisiano é bastante útil, pois nos permite escrever a decomposição de qualquer ideal primo $\mathfrak{p}$ em $\mathcal{O}$ na forma

$$\mathfrak{p}\mathcal{O} = \left( \prod_{\sigma \in G/G_{\mathfrak{B}}} \sigma\mathfrak{B} \right)^e.$$

A proposição abaixo nos mostra a relação entre $e$, $f$, $Z_{\mathfrak{B}}$ e $G_{\mathfrak{B}}$.

**Proposição 1.9.4.** *Seja $\mathfrak{B}_Z = \mathfrak{B} \cap Z_{\mathfrak{B}}$ o ideal primo de $Z_{\mathfrak{B}}$ sob $\mathfrak{B}$. Tem-se*

*i) $\mathfrak{B}$ é o único ideal primo de $L$ sobre $\mathfrak{B}_Z$.*

*ii) $\mathfrak{B}$ tem índice de ramificação $e$ e grau de inércia $f$ sobre $Z_{\mathfrak{B}}$.*

*iii) Os índices de ramificação e graus de inércia de $\mathfrak{B}_Z$ sobre $K$ são todos iguais a $1$.*

**Demonstração.** $i)$ Visto que $G(L|Z_{\mathfrak{B}}) = G_{\mathfrak{B}}$, a Proposição 1.9.1 nos diz ideais primos sobre $\mathfrak{B}_Z$ são os $\sigma\mathfrak{B}$, para $\sigma \in G_{\mathfrak{B}}$, mas estes são todos iguais a $\mathfrak{B}$.

Temos, pela Proposição 1.8.2, que $n = [L : K] = efr$, onde $r$ é a quantidade de ideais primos distintos da forma $\sigma_i\mathfrak{B}$, com $\sigma \in G = G(L|K)$, que é igual a $|G/G_{\mathfrak{B}}|$. Por outro lado, $L|K$ extensão de Galois nos fornece $|G| = n$, donde

$$n = ef\frac{n}{|G_{\mathfrak{B}}|} \Rightarrow [L : Z_{\mathfrak{B}}] = |G_{\mathfrak{B}}| = ef.$$

Sejam $e'$ e $e''$ os índices de ramificação de $\mathfrak{B}$ sobre $Z_{\mathfrak{B}}$ e de $\mathfrak{B}_Z$ sobre $K$, respectivamente. Se $\mathcal{O}_{\mathfrak{B}}$ é o anel de inteiros de $Z_{\mathfrak{B}}$, então

$$\mathfrak{p}\mathcal{O}_{\mathfrak{B}} = \mathfrak{B}_Z^{e''}(\text{ alguns outros ideais }).$$

Em vista de $\mathfrak{B}_Z\mathcal{O} = \mathfrak{B}^{e'}$, obtemos

$$\mathfrak{p}\mathcal{O} = \mathfrak{B}^{e'e''}(\text{ alguns outros ideais }).$$

Ora, a Proposição 1.9.3 implica $e = e'e''$. A identidade análoga para os graus de inércia vem de

$$f = [\mathcal{O}/\mathfrak{B} : \mathcal{O}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{B} : \mathcal{O}_{\mathfrak{B}}/\mathfrak{B}_Z][\mathcal{O}_{\mathfrak{B}}/\mathfrak{B}_Z : \mathcal{O}/\mathfrak{p}] = f'f''.$$

A Proposição 1.8.2 aplicada a $\mathfrak{B}_Z$ nos diz que $[L : Z_{\mathfrak{B}}] = e'f'$. Esta última, em conjunto com as identidades obtidas acima, implicam $e' = e$, $f' = f$, $e'' = f'' = 1$, donde $ii)$ e $iii)$ ficam provadas. □

Podemos ainda dar uma interpretação do índice de ramificação $e$ e do grau de inércia $f$ com um maior viés à teoria de grupos. Visto que $\sigma\mathcal{O} = \mathcal{O}$ e $\sigma\mathfrak{B} = \mathfrak{B}$, para $\sigma \in G_{\mathfrak{B}}$, todo $\sigma \in G_{\mathfrak{B}}$ induz um automorfismo

$$\overline{\sigma} : \mathcal{O}/\mathfrak{B} \to \mathcal{O}/\mathfrak{B},\ a \mod \mathfrak{B} \mapsto \sigma a \mod \mathfrak{B}$$

do corpo residual $\mathcal{O}/\mathfrak{B}$.

**Proposição 1.9.5.** *A extensão $\mathcal{O}/\mathfrak{B}|o/\mathfrak{p}$ é normal e admite um homomorfismo sobrejetivo*

$$G_{\mathfrak{B}} \longrightarrow G(\mathcal{O}/\mathfrak{B}|o/\mathfrak{p}).$$

**Demonstração.** Visto que o grau de inércia de $\mathfrak{B}_Z$ sobre $K$ é $1$, temos $\mathcal{O}_Z/\mathfrak{B}_Z \cong o/\mathfrak{p}$, e podemos considerar $Z_{\mathfrak{B}} = K$, que equivale a $G_{\mathfrak{B}} = G(L|K) = G$. Sejam $\theta \in \mathcal{O}$ tal que $\theta \equiv \overline{\theta} \mod \mathfrak{B}$, $f(x)$, respectivamente, $\overline{g}(x)$, o polinômio minimal de $\theta$ sobre $K$, respectivamente, de $\overline{\theta}$ sobre $o/\mathfrak{p}$. Temos que $\overline{\theta}$ é uma raiz de $\overline{F}(x) = f(x) \mod \mathfrak{p}$. Logo, $\overline{g}(x)$ divide $\overline{f}(x)$ em $(o/\mathfrak{p})[x]$. Visto que $L|K$ é normal, $f(x)$ decompõe-se em fatores lineares sobre $\mathcal{O}$. Portanto, $\overline{f}(x)$ decompõe-se em fatores lineares sobre $o/\mathfrak{p}$, donde $\overline{g}(x)$ também admite tal fatoração; isto prova que $\mathcal{O}/\mathfrak{B}|o/\mathfrak{p}$ é uma extensão normal.

Seja agora $\overline{\theta}$ um elemento primitivo da maior extensão intermediária separável de $\mathcal{O}/\mathfrak{B}|o/\mathfrak{p}$ e

$$\overline{\sigma} \in G(\mathcal{O}/\mathfrak{B}|o/\mathfrak{p}) = G(o/\mathfrak{p}(\overline{\theta})|o/\mathfrak{p}).$$

Como $\overline{\sigma}\overline{\theta}$ é uma raiz de $\overline{g}(x)$, logo de $\overline{f}(x)$, existe $\theta' \in \mathcal{O}$ tal que $f(\theta') = 0$ e $\theta' \equiv \overline{\sigma}\overline{\theta} \mod \mathfrak{B}$. Por outro lado, existe $\sigma \in G$ tal que $\theta' = \sigma\theta$. Por fim, $\sigma\theta \equiv \overline{\sigma}\overline{\theta} \mod \mathfrak{B}$ implica que o homomorfismo em questão leva $\sigma$ em $\overline{\sigma}$; isto conclui a sobrejetividade. □

**Definição 1.9.2.** *O núcleo $I_{\mathfrak{B}}$ do homomorfismo*

$$G_{\mathfrak{B}} \longrightarrow G(\mathcal{O}/\mathfrak{B}|o/\mathfrak{p})$$

*é chamado o grupo de inércia de $\mathfrak{B}$ sobre $K$. O corpo*

$$T_{\mathfrak{B}} = \{x \in L | \sigma x = x \ \forall \sigma \in I_{\mathfrak{B}}\}$$

*é chamado o corpo de inércia de $\mathfrak{B}$ sobre $K$.*

As propriedades de $I_{\mathfrak{B}}$ e $T_{\mathfrak{B}}$ estão expressas na

**Proposição 1.9.6.** *A extensão $T_{\mathfrak{B}}|Z_{\mathfrak{B}}$ é normal e*

$$G(T_{\mathfrak{B}}|Z_{\mathfrak{B}}) \cong G(\mathcal{O}/\mathfrak{B}|o/\mathfrak{p},\ G(L|T_{\mathfrak{B}}) = I_{\mathfrak{B}}.$$

*Além disso, se $\mathcal{O}/\mathfrak{B}|o/\mathfrak{p}$ é separável, tem-se*

$$|I_{\mathfrak{B}}| = [L : T_{\mathfrak{B}}] = e,\ |G_{\mathfrak{B}}/I_{\mathfrak{B}}| = [T_{\mathfrak{B}} : Z_{\mathfrak{B}}] = f.$$

*Ainda neste caso, se $\mathfrak{B}_T$ é ideal primo de de $T_{\mathfrak{B}}$ abaixo de $\mathfrak{B}$:*

*i) O índice de ramificação de $\mathfrak{B}$ sobre $\mathfrak{B}_T$ é $e$ e o seu grau de inércia é $1$.*

*ii) O índice de ramificação de $\mathfrak{B}_T$ sobre $\mathfrak{B}_Z$ é $1$, e o seu grau de inércia é $f$.*

**Demonstração.** A normalidade e os isomorfismos não carecem de prova e as duas outras afirmações seguem de $|G_{\mathfrak{B}}| = ef$. Note que $G(L|T_{\mathfrak{B}}) = I_{\mathfrak{B}}$ implica que $I_{\mathfrak{B}}$ também é o grupo de inércia de $\mathfrak{B}$ sobre $T_{\mathfrak{B}}$, donde a Proposição 1.9.4 aplicada à extensão $L|T_{\mathfrak{B}}$ nos diz que $G(\mathcal{O}/\mathfrak{B}|\mathcal{O}_T/\mathcal{B}_T) = \{Id\}$, donde $\mathcal{O}/\mathfrak{B} = \mathcal{O}_T/\mathcal{B}_T$. Aplicando a Proposição 1.8.2, os dois últimos itens seguem-se. □

## 1.10 Corpos ciclotômicos

Balanceemos a abstração dos resultados e conceitos até então desenvolvidos com uma aplicação um pouco mais concreta. Dentre todos os corpos de números, os corpos da forma $\mathbb{Q}(\zeta)$, com $\zeta$ uma raiz $n$-ésima primitiva da unidade, chamados corpos ciclotômicos, ocupam um papel de destaque. Nesta seção, utilizaremos as ideias da teoria geral para estudá-los.

Comecemos por determinar o anel de inteiros de $\mathbb{Q}(\zeta)$. Para tanto, precisaremos do

**Lema 1.10.1.** *Sejam $n = l^\nu$ uma potência de primo, $\zeta$ uma $n$-ésima raiz primitiva da unidade e $\lambda = 1-\zeta$. Então o ideal principal $(\lambda) = \lambda\mathfrak{O}$, em que $\mathfrak{O}$ é o anel de inteiros de $\mathbb{Q}(\zeta)$, é um ideal primo sobre $l\mathbb{Z}$ tal que $[\mathfrak{O}/(\lambda) : \mathbb{Z}/l\mathbb{Z}] = 1$, isto é, o grau de inércia de $\lambda$ sobre $\mathbb{Q}$ é $1$. Além disso, temos*

$$l\mathfrak{O} = (\lambda)^d,\ d = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(l^\nu) = l^{\nu-1}(l-1),$$

*com $\varphi$ a função* phi de Euler*. Isto, por sua vez, implica que a base $1, \zeta, \ldots, \zeta^{d-1}$ de $\mathbb{Q}(\zeta)|\mathbb{Q}$ tem discriminante*

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s,\ s = l^{\nu-1}(\nu l - \nu - 1).$$

**Demonstração.** O polinômio minimal de $\zeta$ sobre $\mathbb{Q}$ é o $n$-ésimo polinômio ciclotômico

$$\phi_n(x) = \frac{x^{l^\nu} - 1}{x^{l^{\nu-1}} - 1} = x^{l^{\nu-1}(l-1)} + x^{l^{\nu-1}(l-2)} + \cdots + x^{l^{\nu-1}} + 1.$$

Além disso, como este também será o polinômio minimal de qualquer outra raiz $n$-ésima primitiva da unidade, e estas são da forma $\zeta^g$, com $mdc(g, n) = 1$, podemos substituir $x = 1$ em $\phi_n(x)$ e obter

$$l = \prod_{g \in [\mathbb{Z}/n\mathbb{Z}]^*} (1 - \zeta^g). \tag{1.1}$$

Por outro lado, temos $1 - \zeta^g = \varepsilon_g(1-\zeta)$, com $\varepsilon_g = \dfrac{1-\zeta^g}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{g-1} \in \mathfrak{O}$. Tomando $g' \in \mathbb{Z}$ tal que $gg' \equiv 1 \mod n$, temos

$$\varepsilon_g^{-1} = \frac{1-\zeta}{1-\zeta^g} = \frac{1-(\zeta^g)^{g'}}{1-\zeta^g} = 1 + \zeta^g + \cdots + \zeta^{g(g'-1)} \in \mathfrak{O}.$$

Ou seja, $\varepsilon_g \in \mathcal{O}^*$. Substituindo na igualdade para $l$, obtemos

$$l = \left( \prod_{g \in [\mathbb{Z}/n\mathbb{Z}]^*} \varepsilon_g \right) \lambda^{\phi(l^\nu)} \Rightarrow l\mathfrak{O} = (\lambda^{\phi(l^\nu)}) = (\lambda)^d.$$

Como $d = [\mathbb{Q}(\zeta) : \mathbb{Q}]$, devemos ter necessariamente $(\lambda)$ primo, pois, havendo ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ tais que $(\lambda) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$, a Proposição 1.8.2 nos daria $\sum_{i=1}^r e_i f_i = 1$, em que $f_i$ são os graus de inércia de $\mathfrak{p}_i$ sobre $l\mathbb{Z}$, donde $e_i = f_i = 1$, para algum $i$ e $e_i = 0$, para os demais $i$'s, donde $(\lambda) = \mathfrak{p}_1$, e portanto é um ideal primo, cujo grau de inércia é $1$.

Sejam agora $\zeta_1 = \zeta, \ldots, \zeta_d$ os conjugados de $\zeta$. Denotando por $\phi_n'(x)$ a derivada do polinômio $\phi_n(x) = (x - \zeta_1) \cdots (x - \zeta_d)$, obtemos

$$\phi_n'(x) = \prod_{j \neq i} (x - \zeta)_j + (x - \zeta_i)q(x) \Rightarrow \phi_n(\zeta_i) = \prod_{j \neq i} (x - \zeta)_j$$

e, portanto,

$$d(1,\zeta,\ldots,\zeta^{d-1}) = \prod_{i\neq j}(\zeta_i-\zeta_j)^2 = \prod_{i=1}^{d}\phi_n'(\zeta_i) = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\phi_n'(\zeta)).$$

Diferenciando a equação

$$(x^{l^{\nu-1}}-1)\phi_n(x) = x^{l^\nu}-1$$

e substituindo $x=\zeta$, obtemos

$$(\xi-1)\phi_n'(\zeta) = l^\nu\zeta^{-1},$$

em que $\xi=\zeta^{l^{\nu-1}}$, que é uma $l$-ésima raiz primitiva da unidade. Por outro lado, em vista de o produto em (1.1) ser o produto de uma renumeração dos $\zeta_i$'s, temos $N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1)=\pm l$, donde, pelo Corolário 1.2.1

$$N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\xi-1) = N_{\mathbb{Q}(\xi)|\mathbb{Q}}(N_{\mathbb{Q}(\zeta)|\mathbb{Q}(\xi)}(\xi-1)) = N_{\mathbb{Q}(\xi)|\mathbb{Q}}\left(\prod_{\sigma\in Gal(\mathbb{Q}(\zeta)|\mathbb{Q}(\xi))}\sigma(\xi-1)\right) =$$
$$N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1)^{[\mathbb{Q}(\xi):\mathbb{Q}(\zeta)]} = N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1)^{l^{\nu-1}} = \pm l^{l^{\nu-1}};$$

Visto que $\zeta^{-1}$ tem norma $\pm1$, obtemos

$$d(1,\zeta,\ldots,\zeta^{d-1}) = \pm N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\phi_n'(\zeta)) = \pm l^{\nu l^{\nu-1}(l-1)-l^{\nu-1}} = l^s.$$

□

O anel de inteiros de $\mathbb{Q}(\zeta)$ para $n$ arbitrário é determinado na proposição abaixo.

**Proposição 1.10.1.** *Uma $\mathbb{Z}$-base do anel de inteiros de $\mathbb{Q}(\zeta)$ é dada por $1,\zeta,\ldots,\zeta^{d-1}$, com $d=\varphi(n)$. Em particular*

$$\mathfrak{O} = \mathbb{Z}+\mathbb{Z}\zeta+\cdots+\mathbb{Z}\zeta^{d-1} = \mathbb{Z}[\zeta]$$

**Demonstração.** Provamos primeiro no caso em que $n$ é uma potência de primo $l^\nu$. Neste caso, o Lema 1.10.1 nos fornece $d(1,\zeta,\ldots,\zeta^{d-1})=l^s$, daí, pelo Lema 1.2.2

$$l^s\mathfrak{O}\subseteq\mathbb{Z}[\zeta]\subseteq\mathfrak{O}.$$

O mesmo Lema 1.10.1 diz que $\mathfrak{O}/\lambda\mathfrak{O}\cong\mathbb{Z}/l\mathbb{Z}$, donde concluímos $\mathfrak{O}=\mathbb{Z}+\lambda\mathfrak{O}$. Com maior razão, então, temos

$$\mathbb{Z}[\zeta]+\lambda\mathfrak{O}=\mathfrak{O}.$$

Multiplicando por $\lambda$ e substituindo $\lambda\mathfrak{O}=\lambda^2\mathfrak{O}+\lambda\mathbb{Z}[\zeta]$ em $\mathfrak{O}=\mathbb{Z}+\lambda\mathfrak{O}$, obtemos $\lambda^2\mathfrak{O}+\mathbb{Z}[\zeta]=\mathfrak{O}$.

Continuando indutivamente este processo, obtemos $\lambda^t\mathfrak{O}+\mathbb{Z}[\zeta]=\mathfrak{O}$, para $t\geq1$. Fazendo $t=s\varphi(l^\nu)$, obtemos, novamente, pelo Lema 1.10.1,

$$\mathfrak{O}=\lambda^t\mathfrak{O}+\mathbb{Z}[\zeta]=l^s\mathfrak{O}+\mathbb{Z}[\zeta]=\mathbb{Z}[\zeta].$$

Seja agora $n=l_1^{\nu_1},\ldots,l_r^{\nu_r}$. O elemento $\zeta_i=\zeta^{\frac{n}{l_i^{\nu_i}}}$ é uma $l_i^{\nu_i}$-ésima raiz primitiva da unidade e

$$\mathbb{Q}(\zeta)=\mathbb{Q}(\zeta_1)\ldots\mathbb{Q}(\zeta_r).$$

Com efeito, a inclusão da direita para a esquerda é trivial, pois cada $\zeta_i$ é uma potência de $\zeta$. Tendo em

vista que $\frac{n}{l_i^{\nu_i}}$ é coprimo com $\frac{n}{l_j^{\nu_j}}$, para qualquer $i \neq j$, existem inteiros $a_1, \ldots, a_r$, tais que

$$a_1 \frac{n}{l_1^{\nu_1}} + \ldots a_r \frac{n}{l_r^{\nu_r}} = 1 \Rightarrow \zeta = \prod_{i=1}^{r} \zeta_i^{a_i},$$

o que prova a outra inclusão.

Para cada $i = 1, \ldots, r$, os elementos $1, \zeta_i, \ldots, \zeta_i^{d_i - 1}$, em que $d_i = \varphi(l_i^{\nu_i})$ formam uma base de $\mathbb{Q}(\zeta_i)|\mathbb{Q}$, cujo discriminante é $\pm l_i^{s_i}$. Estes discriminantes são todos dois a dois coprimos, donde o Proposição 1.2.8 nos diz que os produtos $\zeta_1^{j_1}, \ldots, \zeta_r^{j_r}$, com $j_i = 0, \ldots, d_i - 1$ formam uma base integral de $\mathbb{Q}(\zeta)|\mathbb{Q}$ (como a função $\varphi$ é multiplicativa em inteiros coprimos, esta base tem $\varphi(n)$ elementos). Como cada um destes elementos é uma potência de $\zeta$, qualquer $\alpha \in \mathfrak{O}$ pode ser escrito como $f(\zeta)$, com $f \in \mathbb{Z}[x]$. Tendo em vista que o polinômio minimal $m_\zeta$ de $\zeta$ sobre $\mathbb{Q}$ tem grau $\varphi(n)$, $f$ pode ser reduzido (módulo $m_\zeta$) a um polinômio de grau menor ou igual a $\varphi(n) - 1$. Obtemos, portanto, uma representação

$$\alpha = a_0 + a_1\zeta + \cdots + a_{d-1}\zeta^{d-1},$$

em que $d = \varphi(n) - 1$. □

Sabendo que $\mathbb{Z}[\zeta]$ é o anel de inteiros de $\mathbb{Q}(\zeta)$, podemos agora explicitar uma lei de decomposição para os números primos $p$ em ideais primos de $\mathbb{Z}[\zeta]$, cuja simplicidade é de se impressionar.

**Proposição 1.10.2.** *Seja $n = \prod_{p \text{ primo}} p^{v_p(n)}$, com $v_p(n)$ o expoente da maior potência de $p$ que divide $n$. Para cada $p$, seja $f_p$ o menor natural tal que*

$$p^{f_p} \equiv 1 \mod \frac{n}{p^{v_p(n)}}.$$

*Se $\zeta$ é uma $n$-ésima raiz primitiva da unidade, e $\mathbb{Z}[\zeta]$ é o anel de inteiros de $\mathbb{Q}(\zeta)$, temos*

$$p\mathbb{Z}[\zeta] = (\mathfrak{p}_1 \ldots \mathfrak{p}_r)^{\varphi(p^{v_p(n)})},$$

*em que $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ são ideais primos distintos e $[\mathbb{Z}[\zeta]/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = f_p$.*

**Demonstração.** Denotemos $\mathcal{O} = \mathbb{Z}[\zeta]$, o condutor de $\mathcal{O}$ é todo o anel de inteiros, logo, podemos aplicar a Proposição 1.8.3, e obter que, para cada $p$, $f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = \deg \overline{p_i}(x)$, com $\overline{f}(x) = f(x) \mod p$ e $\overline{p_i}(x)$ um fator irredutível de $\overline{\phi_n}(x)$. Escrevamos $n = p^{v_p(n)}m$. Se $\xi_i$ percorre todas as $m$-ésimas raízes primitivas da unidade e $\eta_j$ percorre todas as $p^{v_p(n)}$-ésimas, temos que o produto $\xi_i\eta_j$ percorre todas as $n$-ésimas raízes primitivas da unidade, donde podemos escrever

$$\phi_n(x) = \prod_{i,j}(x - \xi_i\eta_j).$$

Por outro lado, em $\mathcal{O}/\mathfrak{p}$ ($\mathfrak{p} = \mathfrak{p}_i$, para algum $i$) tem-se $x^{p^{v_p(n)}} - 1 = (x-1)^{p^{v_p(n)}}$, substituindo $x = \eta_j$, temos $\eta_j \equiv 1 \mod \mathfrak{p}$. Como $\phi_{p^{v_p(n)}}(x)$ tem grau $\varphi(p^{v_p(n)})$, tem-se

$$\phi_n(x) = \prod_i (x - \xi_i)^{\varphi(p^{v_p(n)})} \equiv \phi_m(x)^{\varphi(p^{v_p(n)})} \mod \mathfrak{p}.$$

Em particular, temos a congruência

$$\phi_n(x) \equiv \phi_m(x)^{\varphi(p^{v_p(n)})} \mod p.$$

Note que, se $[\mathcal{O}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = f$, então todo $x \in \mathcal{O}/\mathfrak{p}$ satisfaz $x^{p^f-1} = 1$, pois $p^f - 1$ é a cardinalidade do grupo multiplicativo de $\mathcal{O}/\mathfrak{p}$. Logo, se $v_p(n) = 0$ (o que é verdade para todo $p$, a menos de uma quantidade finita), como $x^n - 1$ e $nx^{n-1}$ não têm nenhuma raiz em comum, temos que $x^n - 1 \mod \mathfrak{p}$ não tem raízes múltiplas. Temos, portanto, que o mapa canônico $\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}$ determina uma bijeção entre as $n$-ésimas raízes primitivas da unidade de $\mathcal{O}$ e as de $\mathcal{O}/\mathfrak{p}$; de fato, se $\zeta$ é uma $n-$ésima raiz primitiva da unidade, também sua imagem $\zeta \mod \mathfrak{p}$ deverá sê-lo, pois o contrário implicaria $\zeta \mod \mathfrak{p}$ ser uma raiz de $x^r - 1$, com $r$ um divisor próprio de $n$, contradizendo o fato de $x^n - 1$ ter $n$ raízes distintas em $\mathcal{O}/\mathfrak{p}$. Além disso, sendo $\mathbb{F}_q$ o corpo finito de $q$ elementos, temos que $\mathbb{F}_q$ tem uma raiz $m$-ésima primitiva da unidade se, e somente se, $m|q-1$, pois $\mathbb{F}_q^*$ é cíclico, de ordem $q-1$. Como $n = m$ no caso que estamos considerando, temos $f_p = \min\{f \in \mathbb{N} |\ p^f \equiv 1 \mod n\}$, que é precisamente o grau da menor extensão de $\mathbb{Z}/p\mathbb{Z}$ que contém a raiz $n$-ésima primitiva da unidade $\zeta \mod p$. Concluímos, então, que o corpo finito de $p^{f_p}$ elementos é o corpo de fatoração de $\overline{\phi}_n(x)$. Como este polinômio divide $x^n - 1 \mod \mathfrak{p}$, que não têm raízes múltiplas, temos que, se

$$\overline{\phi}_n(x) = \overline{p_1}(x) \dots \overline{p_r}(x)$$

é a fatoração de $\overline{\phi}_n(x)$ em irredutíveis sobre $\mathbb{Z}/p\mathbb{Z}$, então cada $\overline{p_i}(x)$ será o polinômio minimal de alguma $n$-ésima raiz primitiva da unidade de $\mathbb{F}_{p^{f_p}}$, cujo grau será $f_p$.

Se, por fim, tivermos $v_p(n) \geq 1$, então, como $p$ não divide $m$, o mesmo argumento mostrará que $\overline{\phi}_n(x)$ se fatora como um produto de polinômios irredutíveis sobre $\mathbb{Z}/p\mathbb{Z}$, todos de grau igual a $\min\{f \in \mathbb{N} | p^f \equiv 1 \mod m\} = f_p$; e isto finda a demonstração. □

O corolário abaixo enfatiza dois casos especiais da lei de decomposição.

**Corolário 1.10.1.** *Seja $\zeta$ uma raiz $n-$ésima primitiva da unidade. Um número primo $p$ é ramificado em $\mathbb{Q}(\zeta)$ se, e somente se,*

$$n \equiv 0 \mod p,$$

*com a exceção do caso $p = 2 = mdc(4, n)$. Um número primo $p \neq 2$ decompõe-se totalmente em $\mathbb{Q}(\zeta)$ se, e somente se,*

$$p \equiv 1 \mod n.$$

**Demonstração.** Escrevendo $n = p^{v_p(n)}m$, a Proposição 1.10.2 nos diz que, se $p$ se ramifica em ideais $\mathfrak{p}_1 \dots \mathfrak{p}_r$. Como $\varphi(n) = \varphi(p^{v_p(n)})\varphi(m)$, a Proposição 1.8.2 nos dá

$$rf_p = \varphi(m).$$

Ora, para que $p$ se ramifique, como cada ideal primo $\mathfrak{p}_i$ tem índice de ramificação igual a $\varphi(p^{v_p(n)})$, é necessário e suficiente $\varphi(p^{v_p(n)}) > 1$, o que ocorre sempre que $p \neq 2$ e $v_p(n) \geq 1$, ou $p = 2$ e $v_p(n) > 1$. Se $p$ se decompõe totalmente, temos $\varphi(n)$ ideais primos sobre $p$, isto é, $r = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, a equação anterior nos obriga a admitir $f_p = 1$ e $n = m$. □

# Capítulo 2

# Parte analítica

## 2.1 Domínios fundamentais e a função Zeta de Dedekind

O objetivo deste capítulo é demonstrar e aplicar uma fórmula que, quando não nos permite calcular com exatidão, permite-nos ao menos estimar o número de classes $h$ de um corpo de números $K$ de grau $s+2t$, sendo $s$ o número de monomorfismos reais de $K$ para $\mathbb{C}$ e $t$ o número de pares de monomorfismos complexos conjugados. Para tanto, usaremos extensivamente as representações $\mathcal{J}$ e $l$ em $K_{\mathbb{R}} \cong \mathbb{R}^{s+2t}$ e $\mathbb{R}^{s+t}$ definidas na Seção 1.5, que chamamos, respectivamente, *representação geométrica* e *representação logarítmica*. Mantemos a notação $l(a)$ para a representação logarítmica; entretanto, usamos $x(a)$, ao invés de $\mathcal{J}a$. Por abuso de notação, denotaremos por apenas $N(\mathfrak{a})$ e $N(a)$ a norma absoluta do ideal $\mathfrak{a}$, definida na Seção 1.6 por $\mathfrak{N}(\mathfrak{a})$, e a norma do elemento $a \in K$, definida na Seção 1.2 por $N_{K|\mathbb{Q}}(a)$. Dito isso, introduzamos um dos conceitos que nomeiam esta seção.

**Definição 2.1.1.** *A função Zeta de Dedekind do corpo $K$ aplicada ao número real $s > 1$ é a série*

$$\zeta_K(s) = \sum_{\mathfrak{a} \text{ ideal de } \mathfrak{O}_K} \frac{1}{N(\mathfrak{a})^s}.$$

*No caso $K = \mathbb{Q}$, e $\mathfrak{O}_K = \mathbb{Z}$, chamamos $\zeta_{\mathbb{Q}}$ a função Zeta de Riemman, e escrevemos apenas $\zeta(s)$, em lugar de $\zeta_{\mathbb{Q}}(s)$.*

Claro que, para justificar o nome "função", precisamos mostrar que tal série define uma função em $\mathbb{R}_{>1}$, isto é, precisamos mostrar que $\zeta_K(s)$ converge, para $s > 1$. Mostraremos ainda mais do que isso, porém, precisamos de mais alguns conceitos e resultados.

**Definição 2.1.2.** *Seja $m$ o número de raízes da unidade contidas em $K$. Um subconjunto $X$ de $K_{\mathbb{R}}$ é dito um domínio fundamental de $K$ se ele consiste dos pontos $x$, tais que*

*1)* $N(x) \neq 0$.

*2) Na representação*

$$l(x) = \xi l^* + \xi_1 l(\varepsilon_1) + \ldots \xi_r l(\varepsilon_r),$$

*com $l^* = (1, \ldots, 1, 2, \ldots, 2)$, totalizando $s$ componentes $1$ e $t$ componentes $2$, $\varepsilon_1, \ldots, \varepsilon_r$ um sistema de unidades fundamentais de $K$, temos $0 \leq \xi_i < 1$*

*3)* $0 \leq \arg x_1 < \dfrac{2\pi}{m}$*, em que $x_1 = x_{\sigma_1}$, caso $s = 0$, e $x_{\rho_1} = x_1 > 0$, caso $s \geq 1$ (ver o final da Seção 1.5).*

Seja $\xi$ um real positivo e $x \in K_{\mathbb{R}}^*$, temos

$$l(\xi x) = \ln \xi l^* + l(x),$$

donde os vetores $l(\xi x)$ e $l(x)$ têm os mesmos coeficientes para $l(\varepsilon_1), \ldots, l(\varepsilon_i)$. Como $N(\xi x) = \xi^n N(x)$, $N(x) \neq 0$, $\arg \xi x_1 = \arg x_1$, então $x \in X \Rightarrow \xi x \in X$. Em outras palavras, $X$ é um cone em $\mathbb{R}^n$ (note que $X$ contém ao menos o raio gerado por $x(1)$).

**Lema 2.1.1.** *Seja $y \in \mathbb{K}_{\mathbb{R}}^*$. Existe uma única representação de $y$ na forma $xx(\varepsilon)$, com $\varepsilon \in \mathfrak{O}_K^*$ e $x$ pertencente ao domínio fundamental $X$.*

**Demonstração.** Sejam $\varepsilon_1, \ldots, \varepsilon_r$ um sistema de unidades fundamentais de $K$ e $m$ o número de raízes da unidade de $\mathfrak{O}_K$. Sabemos que, na representação logarítmica, podemos escrever

$$l(y) = \lambda l^* + \lambda_1 l(\varepsilon_1) + \cdots + \lambda_r l(\varepsilon_r).$$

Escrevamos $\lambda_i = k_i + \xi_i$, com $k_i \in \mathbb{Z}$ e $\xi_i \in [0, 1)$. Tomemos a unidade $\eta = \varepsilon_1^{k_1} \ldots \varepsilon_r^{k_r}$ e $z = yx(\eta^{-1})$, temos

$$l(z) = l(y) + l(\eta^{-1}) = \lambda l^* + \lambda_1 l(\varepsilon_1) + \cdots + \lambda_r l(\varepsilon_r) - k_1 l(\varepsilon_1) - \cdots - k_r l(\varepsilon_r) = \lambda l * + \xi_1 l(\varepsilon_1) + \cdots + \xi_r l(\varepsilon_r).$$

Se $\varphi = \arg z_1$, existe um inteiro $k$ tal que $0 \leq \varphi - \dfrac{2k\pi}{m} < \dfrac{2\pi}{m}$. Visto que os monomorfismos $\sigma_i : K \to \mathbb{C}$ levam $m$-ésimas raízes da unidade em $m$-ésimas raízes da unidade, tomemos $\zeta$ a raiz da unidade tal que $\sigma_1(\zeta) = \cos \dfrac{2k\pi}{m} + i \sin \dfrac{2k\pi}{m}$. Definindo $x = zx(\zeta^{-k})$, obtemos $\arg x_1 = \arg z_1 - \dfrac{2k\pi}{m}$, donde $\arg x_1 \in \left[0, \dfrac{2k\pi}{m}\right)$. Como o produto é definido coordenada a coordenada, é claro que $N(x) \neq 0$, além disso, $l(x) = l(z) = l(y)$, donde $x \in X$. Por fim, temos

$$y = zx(\eta) = xx(\zeta^k)x(\eta) = xx(\varepsilon),$$

com $\varepsilon = \eta\zeta^k$.

Suponhamos $xx(\varepsilon) = x'x(\varepsilon')$, teremos $l(x) - l(x') = l(\varepsilon') - l(\varepsilon)$. Os coeficientes de $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ no lado direito são são inteiros, enquanto que os do lado esquerdo são não negativos e menores do que $1$. Concluímos, portanto, que estes coeficientes precisam ser zero, donde $\varepsilon$ e $\varepsilon'$ diferem por uma $m$-ésima raiz da unidade $\zeta$. Daí, concluímos que $x = x'x(\zeta)$, e como $\arg x_1, \arg x_1' \in \left[0, \dfrac{2\pi}{m}\right)$, temos $\arg \sigma_1(\zeta) < \dfrac{2\pi}{m}$, mas $\sigma_1(\zeta)$ é uma $m$-ésima raiz da unidade, logo, seu argumento é da forma $\dfrac{2k\pi}{m}$, com $k = 0, 1, 2, \ldots, m-1$. Portanto, temos $\arg \sigma_1(\zeta) = 0$ e $\zeta = 1$. □

**Teorema 2.1.1.** *Cada $y \in K^*$ possui um único associado cuja representação geométrica pertence ao domínio fundamental $X$.*

**Demonstração.** Usando o Lema 2.1.1, escrevamos $x(y) = xx(\varepsilon)$. Definindo $\alpha = y\varepsilon^{-1}$, temos $x(\alpha) = x \in X$. Reciprocamente, se $\alpha$ é um associado de $y$ cuja representação geométrica pertence a $X$, podemos escrever $x(y) = x(\alpha)x(\varepsilon)$, com $\varepsilon$ uma unidade. Temos, portanto, que $\alpha$ é unicamente determinado pela escrita do Lema 2.1.1, que é única. □

O próximo resultado, apesar de aparentemente desconectado do nosso objetivo, resulta num dos termos que há de aparecer na fórmula que buscamos.

**Lema 2.1.2.** *O volume do conjunto $T$, dos pontos $x$ do domínio fundamental $X$ que satisfazem $|N(x)| \leq$*

$1$ *é finito, e igual a*

$$v = \frac{2^s \pi^t R}{m}.$$

**Demonstração.** Em cada raio contido em $X$, isto é, em cada conjunto da forma $(0, \infty)x$, com $x \in X$, há um e apenas um elemento cuja norma é igual a $1$ (a saber, $N(x)^{-1}x$). Denotemos o conjunto desses tais elementos por $S$. A partir de agora, consideraremos $T$ como o conjunto dos elementos na forma $\xi s$, em que $\xi \in (0, 1]$ e $s \in S$.

Sabemos que todo elemento $x \in \mathbb{R}^n$ com coordenadas não-nulas se escreve na forma

$$\xi l^* + \xi_1 l(\varepsilon_1) + \ldots \xi_r l(\varepsilon_r),\ \xi, \xi_i \in \mathbb{R}.$$

A soma das coordenadas da representação logarítmica de $x$ na base canônica de $\mathbb{R}^{s+t}$ é igual a $\ln |N(x)|$. Por outro lado, utilizando a representação acima, esta soma é

$$(s+2t)\xi + \sum_{i=1}^{s+t}\sum_{j=1}^{r} \xi_j l_i(\varepsilon_j) = n\xi + \sum_{j=1}^{r}\sum_{i=1}^{s+t} \xi_j l_i(\varepsilon_j) = n\xi + \sum_{j=1}^{r} \xi_j \left( \sum_{i=1}^{r} l_i(\varepsilon_j) \right) = n\xi.$$

Concluindo que $\xi = \dfrac{\ln |N(x)|}{n}$. Se $x \in S$, temos que $l(x) = \xi_1 l(\varepsilon_1) + \ldots \xi_r l(\varepsilon_r)$, com $\xi_i \in [0, 1)$. Disto se segue que as coordenadas dos pontos de $S$ em sua representação logarítmica são limitadas, digamos $l_i(x) < \rho$, com $\rho > 0$. Temos, portanto, $|x_k| < e^{\rho}$, para $1 \leq k \leq s$, e $|x_k| < e^{\frac{\rho}{2}}$, para $s+1 \leq k \leq s+t$. Daí, tanto $S$ quanto $T$ são limitados.

Qualquer transformação linear invertível multiplica o volume de um conjunto pelo módulo do seu determinante. Se a transformação em questão é $x \mapsto xx(\varepsilon)$, com $\varepsilon$ uma unidade de $\mathfrak{O}_K$, então o volume é multiplicado por $|N(x(\varepsilon))| = |N(\varepsilon)| = 1$, donde esta transformação preserva volumes.

Consideremos $\zeta$ a $m$-ésima raiz da unidade de $\mathfrak{O}_K$ tal que $\sigma_1(\zeta) = \cos \dfrac{2\pi}{m} + i \sin \dfrac{2\pi}{m}$. Definamos os conjuntos $T_k$, em que $k = 0, 1, \ldots, m-1$, como as imagens de $T$ pela transformação $x \mapsto xx(\zeta^k)$. Se um dos seus volumes existe, então $v(T)$ existe, e temos $v(T_k) = v(T)$, para qualquer $k$. Temos as seguintes propriedades

$$|N(xx(\zeta^k))| = |N(x)|,$$

$$l(xx(\zeta^k)) = l(x),$$

$$\arg(xx(\zeta^k))_1 = \arg x_1 + \frac{2\pi k}{m}.$$

Pela definição de domínio fundamental, estas propriedades nos dizem que $T_k$ é dado por

(1) $N(x) \in (0, 1]$.

(2) Os coeficientes $\xi_i$ pertencem ao intervalo $[0, 1)$

(3) $\arg x_1 \in \left[ \dfrac{2\pi k}{m}, \dfrac{2\pi(k+1)}{m} \right)$.

Concluímos, portanto, que os $T_k$'s são dois a dois disjuntos e sua união $\bigcup_k T_k$ é definida por retirar a terceira das três condições acima.

Seja $T'$ o conjunto dos pontos $x \in \bigcup_k T_k$ tais que $x_i > 0$, para $i = 1, \ldots, s$. Fixemos uma escolha de $s$ números $\delta_1, \ldots, \delta_s$, em que $\delta_i = \pm 1$. Sendo $\mathfrak{d}$ o ponto $(\delta_1, \ldots, \delta_s; 1, \ldots, 1)$, a transformação linear $x \mapsto \mathfrak{d}x$ preserva volume. Visto haver $2^s$ destas tais transformações, aplicamos cada uma a $T'$,

obtendo assim $2^s$ conjuntos dois a dois disjuntos, cuja união é $\bigcup_k T_k$. Se $T'$ tem um volume não-nulo finito $\nu$, seguir-se-á

$$v(T) = \frac{2^s \nu}{m}. \tag{2.1}$$

Novamente, sendo $x \in \mathbb{R}^n$ com coordenadas não-nulas, a representação logarítmica nos dá

$$l_j(x) = \frac{e_j}{n} \ln |N(X)| + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k) \ (j = 1, \ldots, s+t),$$

em que $e_j = 1$, se $1 \leq j \leq s$, e $e_j = 2$, se $s+1 \leq j \leq s+t$. Escrevendo as coordenadas $x_{s+j}$ na forma $y_j + iz_j$, podemos fazer a mudança de variáveis

$$\begin{cases} x_k = \rho_k, & k = 1, \ldots, s \\ y_j = \rho_{s+j} \cos \phi_j, \ z_j = \rho_{s+j} \sin \phi_j, & j = 1, \ldots, t \end{cases}.$$

A matriz jacobiana desta mudança de variáveis é

$$J = \begin{pmatrix} I_s & 0 & \cdots & 0 \\ 0 & B_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_t \end{pmatrix},$$

em que $I_s$ é a identidade $s \times s$ e, para cada $j = 1, \ldots, t$,

$$B_j = \begin{pmatrix} \cos \phi_j & -\rho_{s+j} \sin \phi_j \\ \sin \phi_j & \rho_{s+j} \cos \phi_j \end{pmatrix},$$

portanto, temos $\det J = \prod_{j=1}^{t} \rho_{s+j}$. Como $l_j(x) = \ln \rho_j^{e_j}$ (lembremos que $l_k(x) = \ln |x_k|$ e que $|x_{s+j}| = |\rho_j||\cos \phi_j + i \sin \phi_j| = |\rho_j|$) e $N(x) = \prod \rho_j^{e_j}$, em termos das variáveis $\rho_1, \ldots, \rho_{s+t}$, $\phi_1, \ldots, \phi_t$, obtemos que $T'$ fica definido pelas condições

i) $\rho_1 > 0, \ldots, \rho_{s+t} > 0$, $\prod \rho_j^{e_j} \leq 1$.

ii) Em cada equação

$$\ln \rho_j^{e_j} = \frac{e_j}{n} \ln \left( \prod \rho_j^{e_j} \right) + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k),$$

os coeficientes $\xi_k$ pertencem ao intervalo $[0, 1)$.

Notemos que tais condições não nos dizem nada sobre os $\phi_j$'s. Podemos, então, toma-los no intervalo $[0, 2\pi)$. Definimos uma nova mudança de variáveis, agora das variáveis $\rho_1, \ldots, \rho_{s+t}$ para $\xi, \xi_1, \ldots, \xi_r$, pela fórmula

$$\ln \rho_j^{e_j} = \frac{e_j}{n} \ln \xi + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k). \tag{2.2}$$

Somando todas estas equações e usando

$$\sum_{j=1}^{s+t} e_j = n, \ \sum_{j=1}^{s+t} l_j(\varepsilon_k) = 0, \tag{2.3}$$

obtemos

$$\xi = \prod_{j=1}^{s+t} \rho_j^{e_j}.$$

Em termos das novas variáveis, o conjunto $T'$ é determinado por $\xi \in (0,1]$ e $\xi_k \in [0,1)$. Verifica-se

$$\frac{\partial \rho_j}{\partial \xi} = \frac{\rho_j}{n\xi}, \; \frac{\partial \rho_j}{\partial \xi_k} = \frac{\rho_j}{e_j} l_j(\varepsilon_k),$$

donde a matriz jacobiana de 2.2 é

$$\begin{aligned} J &= \begin{vmatrix} \frac{\rho_1}{n\xi} & \frac{\rho_2 I_1}{e_1}(e_1) & \cdots & \frac{\rho_3 I_1}{e_1}(e_r) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\rho_{s+t}}{n\xi} & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(e_1) & \cdots & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(e_r) \end{vmatrix} \\ &= \frac{\rho_1 \cdots \rho_{s+t}}{n\xi 2^t} \begin{vmatrix} e_1 & l_1(e_1) & \cdots & l_1(e_r) \\ \vdots & \vdots & \ddots & \vdots \\ e_{s+t} & l_{s+t}(e_1) & \cdots & l_{s+t}(e_r) \end{vmatrix}. \end{aligned}$$

Somando todas as linhas desta última matriz à primeira e utilizando as equações de 2.3, obtemos o regulador $R$ do corpo $K$. Daí, temos

$$\det J = \frac{R}{2^t \rho_1, \ldots, \rho_{s+t}}.$$

Concluímos, portanto, que o volume $\nu$ de $T'$ é finito, pois podemos computá-lo como segue

$$\begin{aligned} \nu &= \int_{T'} \cdots \int dx_1 \ldots dx_s dy_1 dz_1 \ldots dy_t dz_t \\ &= \int_{T'} \cdots \int \rho_{s+1} \ldots \rho_{s+t} d\rho_1 \ldots d\rho_{s+t} d\phi_1 \ldots d\phi_t \\ &= 2^t \pi^t \int \cdots \int \det J(\rho_{s+1} \ldots \rho_{s+t}) d\xi d\xi_1 \ldots d\xi_r \\ &= \pi^t R. \end{aligned}$$

Substituindo $\nu$ em 2.1, finalmente obtemos

$$v(T) = \frac{2^s \pi^t R}{m}.$$

□

## 2.2 O princípio de Dirichlet

Os nossos resultados sobre a função Zeta de Dedekind $\zeta_K$ serão consequências do seguinte Teorema de Dirichlet sobre séries mais gerais. A sua prova não é das mais simples, mas isto é compensado pela simplicidade que fornece ao corolário que o sucede.

**Teorema 2.2.1.** *Seja $X$ um cone em $\mathbb{R}^n$ que não contém a origem, e $F : X \to \mathbb{R}$ uma função contínua satisfazendo as seguintes propriedades:*

*i)*

$$F(x) > 0, \ \forall \ x; \tag{2.4}$$

*ii)*

$$\xi > 0, \ x \in X \ \Rightarrow F(\xi x) = \xi^n F(x); \tag{2.5}$$

*iii)*

$$v\left(T \coloneqq \{x \in X | F(x) \leq 1\}\right) = v < \infty; \tag{2.6}$$

*sejam também $\mathfrak{M}$ um reticulado em $\mathbb{R}^n$, $\Delta$ o volume de um dos seus paralelepípedos fundamentais e $\zeta_F(s)$ a série*

$$\zeta_F(s) = \sum_{x \in \mathfrak{M} \cap X} \frac{1}{F(x)^s}. \tag{2.7}$$

*Temos que $\zeta_F$ converge para $s > 1$ e*

$$\lim_{s \to 1^+} (s-1)\zeta_F(s) = \frac{v}{\Delta} \tag{2.8}$$

Antes da demonstração, notemos que o conjunto dos pontos de $X$ tais que $F(x) = 1$ intersecta cada raio de $X$ em exatamente um ponto e divide o cone em dois conjuntos, sendo um deles um conjunto limitado com volume não-nulo, do qual ele próprio é a fronteira. Além disso, se tivermos de antemão um conjunto limitado, com volume não-nulo, podemos facilmente definir a função $F$, simplesmente definindo $F \equiv 1$ neste conjunto e impondo 2.5.

**Demonstração.** Para $r > 0$, denotemos $\mathfrak{M}_r = r^{-1}\mathfrak{M}$. Temos $v(\mathfrak{M}_r) = \dfrac{\Delta}{r^n}$. Visto que $\mathfrak{M}_r$ é também um reticulado e $T$ é limitado, podemos definir $N(r) =$ o número de pontos de $\mathfrak{M}_r$ pertencentes a $T$. Pelas considerações que seguem a definição de volume, temos

$$v = v(T) = \lim_{r \to \infty} N(r)\frac{\Delta}{r^n} = \Delta \lim_{r \to \infty} \frac{N(r)}{r^n}.$$

Consideremos agora o conjunto $rT$. O número de pontos de $\mathfrak{M}$ pertencentes a $rT$ é também igual a $N(r)$ e , como $T = \{x \in X | F(x) \leq 1\}$ e vale 2.5, temos $N(r) = |\mathfrak{M} \cap rT| = |\{x \in X | F(x) \leq r^n\}|$. Visto que $\mathfrak{M} \cong \mathbb{Z}^m$, com $m \leq n$ então $\mathfrak{M}$ é enumerável, e podemos construir uma sequência $(x_k)$, com $x_k \in \mathfrak{M} \cap X$, tal que

$$0 < F(x_1) < F(x_2) < \cdots < F(x_k) < \ldots$$

Definamos $r_k \coloneqq F(x_k)^{\frac{1}{n}}$. Temos que todos os pontos $x_1, \ldots, x_k$ pertencem a $r_k T$, donde $N(r_k) > k$. Por outro lado, para $\varepsilon > 0$, o ponto $x_k$ não pertence a $(r_k - \varepsilon)T$, donde $N(r_k - \varepsilon) < k$. Temos, portanto, a seguinte desigualdade

$$N(r_k - \varepsilon) < k \leq N(r_k).$$

Multiplicando o último termo à esquerda por $\dfrac{(r_k - \varepsilon)^n}{(r_k - \varepsilon)^n r_k^n}$, e os demais por $\dfrac{1}{r_k^n}$, obtemos

$$\frac{N(r_k - \varepsilon)}{(r_k - \varepsilon)^n}\left(\frac{r_k - \varepsilon}{r_k}\right)^n < \frac{k}{r_k^n} \leq \frac{N(r_k)}{r_k^n},$$

Tomando o limite quando $k \to \infty$, isto é, quando $r_k \to \infty$, obtemos

$$\lim_{k\to\infty} \frac{k}{F(x_k)} = \frac{v}{\Delta}.$$

Como $\lim_{k\to\infty} \frac{k^s}{F(x_k)^s} = \left(\frac{v}{\Delta}\right)^s \neq 0$, então, para $k$ suficientemente grande, podemos tomar $\frac{1}{F(x_k)^s} < \left(\left(\frac{v}{\Delta}\right)^s + \delta\right)\frac{1}{k^s}$, para algum $\delta > 0$. O teste da comparação com a série que define $\zeta(s)$ nos dá a convergência de $\zeta_F$, quando $s > 1$.

Novamente, para $k$ suficientemente grande ($k \geq k_0$), temos

$$\left(\left(\frac{v}{\Delta}\right) - \varepsilon\right)\frac{1}{k} < \frac{1}{F(x_k)} < \left(\left(\frac{v}{\Delta}\right) + \varepsilon\right)\frac{1}{k}.$$

Elevando a $s > 1$ e somando todos os termos, com $k \geq k_0$, e usando que $\zeta(s) - \sum_{k=1}^{k_0-1} \frac{1}{k^s} = \sum_{k=k_0}^{\infty} \frac{1}{k^s}$ converge, obtemos

$$\left(\frac{v}{\Delta} - \varepsilon\right)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s} \leq \sum_{k=k_0}^{\infty} \frac{1}{F(x_k)^s} \leq \left(\frac{v}{\Delta} + \varepsilon\right)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s}.$$

Sabemos que $\lim_{s\to 1^+}(s-1)\sum_{k=1}^{k_0-1} \frac{1}{k^s} = 0$, bem como $\lim_{s\to 1^+}(s-1)\sum_{k=1}^{k_0-1} \frac{1}{F(x_k)^s} = 0$; o primeiro limite nos diz que $\lim_{s\to 1^+}(s-1)\sum_{k=k_0}^{\infty} \frac{1}{k^s} = 1$, donde, para $s$ em intervalos da forma $(1, 1+\delta)$, com $\delta > 0$ suficientemente pequeno, a série $\sum_{k=k+0}^{\infty} \frac{1}{F(x_k)^s}$ é limitada, com os limitantes inferiores e superiores tendendo, respectivamente a $\left(\frac{v}{\Delta} - \varepsilon\right)$ e $\left(\frac{v}{\Delta} + \varepsilon\right)$, à medida que $\delta \to 0$. Daí, somando $\sum_{k=1}^{k_0} \frac{1}{F(x_k)^s}$ em todos os termos da desigualdade e multiplicando-a por $(s-1)$, obtemos

$$\frac{v}{\Delta} - \varepsilon \leq \lim_{s\to 1^+} \inf (s-1)\zeta_K(s) \leq \lim_{s\to 1^+} \sup (s-1)\zeta_K(s) \leq \frac{v}{\Delta} + \varepsilon.$$

Como $\varepsilon$ é arbitrário, temos $\liminf_{s\to 1^+}(s-1)\zeta_K(s) = \limsup_{s\to 1^+}(s-1)\zeta_K(s) = \frac{v}{\Delta}$, e isto finaliza a demonstração. □

**Corolário 2.2.1.** *Se $\mathfrak{M}$ é o reticulado gerado pelas representações geométricas de um ideal $\mathfrak{a}$ de $\mathfrak{O}_K$, com $K$ um corpo de números de grau $n$ e $X$ é um domínio fundamental, então, para $s > 1$,*

$$\lim_{s\to 1^+}(s-1)\sum_{x\in\mathfrak{M}\cap X} \frac{1}{N(x)^s} = \frac{v}{\Delta},$$

*com $\Delta$ o volume de um paralelepípedo fundamental de $\mathfrak{M}$ e $v$ o volume do conjunto $T = \{x \in X | N(x) \leq 1\}$.*

**Demonstração.** Basta notar que $N(x(\alpha)) = N(\alpha)$ satisfaz 2.4, 2.5 e 2.6 □

## 2.3 A fórmula de Euler e a fórmula para o número de classes

O Teorema abaixo tem um papel central em tudo o que o sucede. Ele nos diz que conhecer a função $\zeta_K$ equivale a conhecer o comportamento de $N(\mathfrak{p})$, quando $\mathfrak{p}$ percorre os ideais primos de $\mathfrak{O}_K$.

**Teorema 2.3.1** (Fórmula de Euler)**.** *Para $s > 1$, vale a equação*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left( \frac{1}{1 - N(\mathfrak{p})^{-s}} \right),$$

*em que $\mathfrak{p}$ percorre todos os ideais primos de $\mathfrak{O}_K$.*

**Demonstração.** Qualquer que seja $\mathfrak{p}$ o ideal primo, o termo $\dfrac{1}{1 - N(\mathfrak{p})^{-s}}$ é a soma dos termos de uma progressão geométrica com razão menor que $1$ em módulo, daí, temos

$$\frac{1}{1 - N(\mathfrak{p})^{-s}} = \sum_{k=0}^{\infty} \frac{1}{N(\mathfrak{p})^{sk}}.$$

Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ todos os ideais primos cujas normas não excedem um certo natural $N$. Multiplicando as somas obtidas para cada $\mathfrak{p}_i$, obtemos uma soma cujos termos são todos os números na forma $\dfrac{1}{N(\mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r})^s}$, isto é, a série obtida de $\zeta_K(s)$, retirando-lhe todos os termos da forma $\dfrac{1}{N(\mathfrak{a})^s}$, com $\mathfrak{a}$ divisível por algum ideal de norma maior que $N$. Ou seja, para um natural $N$ arbitrário, temos

$$\prod_{N(\mathfrak{p}) \leq N} \frac{1}{1 - N(\mathfrak{p})^{-s}} \leq \zeta_K(s).$$

Fazendo $N \to \infty$, temos a primeira desigualdade.

A desigualdade inversa é obtida a partir da soma $\sum_{N(\mathfrak{a}) \leq M} \dfrac{1}{N(\mathfrak{a})^s}$, que está contida na soma dos termos $\dfrac{1}{N(\mathfrak{a}^s)}$, com $\mathfrak{a}$ divisível por algum ideal primo $\mathfrak{p}$, tal que $N(\mathfrak{p}) \leq M$, que é precisamente o produto $\prod_{N(\mathfrak{p}) \leq M} \dfrac{1}{1 - N(\mathfrak{p})^{-s}}$, basta fazer $M \to \infty$. □

Enfim, temos o resultado que almejávamos desde o início do capítulo.

**Teorema 2.3.2.** *Seja $K$ um corpo de números e $\zeta_K(s)$ a função*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

*em que $\mathfrak{a}$ percorre todos os ideais de $\mathfrak{O}_K$. Vale a igualdade*

$$\lim_{s \to 1^+} (s-1)\zeta_K(s) = \left( \frac{2^{s+t} \pi^t R}{m\sqrt{D}} \right) h,$$

*em que $R$ é o regulador de $K$, $D$ é o discriminante de $\mathfrak{O}_K$, $m$ é o número de raízes da unidade de $\mathfrak{O}_K$ e $h = |Cl_K|$.*

**Demonstração.** Primeiro dividimos a série que representa $\zeta_K(s)$ na forma

$$\zeta_K(s) = \sum_{C \in Cl_K} \sum_{\mathfrak{a} \in C} \frac{1}{N(\mathfrak{a})^s}.$$

Na classe $C^{-1}$, escolhamos um ideal $\mathfrak{a}'$ contido em $\mathfrak{O}_K$ (cuja existência é garantida pela Proposição 1.3.1) para cada $\mathfrak{a} \in C$, o produto $\mathfrak{a}\mathfrak{a}'$ é um ideal principal $(\alpha)$, com $\alpha \in K$. A correspondência $\mathfrak{a} \mapsto (\alpha)$ é uma bijeção entre ideais de $\mathfrak{O}_K$ da classe $C$ e ideais principais contidos em $C^{-1}$ contidos

em $\mathfrak{a}'$. Pelas propriedades da norma, temos

$$N(\mathfrak{a})N(\mathfrak{a}') = |N(\alpha)|.$$

Daí, concluímos

$$\sum_{\mathfrak{a}\in C} \frac{1}{N(\mathfrak{a})^s} = N(\mathfrak{a}')^s \sum_{(\alpha),\ \alpha\in\mathfrak{a}'} \frac{1}{|N(\alpha)|^s}.$$

Note que a soma acima não varia com o elemento $\alpha$, mas com o ideal $(\alpha)$, como dois elementos $\alpha_1$ e $\alpha_2$ geram o mesmo ideal principal se, e somente se, $\alpha_1 = \alpha_2\varepsilon$, com $\varepsilon \in \mathfrak{O}_K^*$, isto é, se eles são associados, podemos tomar a soma anterior com $\alpha$ percorrendo um sistema de representantes das classes de associados de $\mathfrak{a}'$.

Pelo Teorema 2.1.1, reescrevemos

$$\sum_{(\alpha),\ \alpha\in\mathfrak{a}'} \frac{1}{|N(\alpha)|^s} = \sum_{x\in\mathfrak{M}\cap X} \frac{1}{|N(x)|^s},$$

em que $\mathfrak{M}$ é o reticulado obtido de $\mathfrak{a}'$ pela representação geométrica, e $X$ é um domínio fundamental em $K_{\mathbb{R}}$.

Pelo corolário Corolário 2.2.1, temos

$$\lim_{s\to 1^+}(s-1)\sum_{\mathfrak{a}\in C}\frac{1}{N(\mathfrak{a})^s} = \lim_{s\to 1^+}(s-1)\sum_{x\in\mathfrak{M}\cap X}\frac{1}{|N(x)|^s} = \frac{v}{\Delta}.$$

Como $v = \dfrac{2^s\pi^t R}{m}$ e $\Delta = 2^{-t}N(\mathfrak{a}')\sqrt{|D|}$, obtemos

$$\lim_{s\to 1^+}(s-1)\sum_{x\in\mathfrak{M}\cap X}\frac{1}{|N(x)|^s} = \frac{2^{s+t}\pi^t R}{m\sqrt{|D|}}.$$

Donde

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \lim_{s\to 1^+}(s-1)\sum_{C\in Cl_K}\frac{2^{s+t}\pi^t R}{m\sqrt{|D|}} = \left(\frac{2^{s+t}\pi^t R}{m\sqrt{|D|}}\right)h$$

□

## 2.4 O número de classes de um corpo ciclotômico

Nesta seção, exploraremos um dos casos em que se pode dar uma fórmula explícita para o número de classes: o caso em que $K = \mathbb{Q}(\zeta)$, com $\zeta$ uma $m$-ésima raiz primitiva da unidade. Para isto, precisaremos da noção de caractere numérico módulo $m$, da qual tratamos propriamente em A.3.

**Definição 2.4.1.** *Sendo $\chi^* : [\mathbb{Z}/m\mathbb{Z}]^* \to \mathbb{C}^*$ um homomorfismo de grupos, um caractere numérico módulo $m$ é a função multiplicativa sobre os inteiros obtida a partir das relações $\chi(a) = \chi^*(\overline{a})$, se $(a,m) = 1$, e $\chi(a) = 0$, se $(a,m) > 1$.*

**Definição 2.4.2.** *A $L$-série do caractere $\chi$ é o produto*

$$L(s,\chi) = \prod_{p\ primo}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Por um argumento análogo ao usado na prova do Teorema 2.3.1, apenas usando a multiplicatividade e comutatividade do caractere $\chi$, podemos justificar o nome série, e escrever

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

Esta última série também é chamada *a série de Dirichlet* do caractere $\chi$. A convergência de $L(s,\chi)$ é justificada pelo resultado abaixo.

**Lema 2.4.1.** *Se a sequência de números complexos $(a_n)_{n\in\mathbb{N}}$ é tal que $A_n=\sum_{i=1}^{n}a_n$ é limitada, então a série*

$$f(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

*converge para $s>0$. Se $\sigma>0$, então esta convergência é uniforme em $[\sigma,\infty)$ (isto é, $f$ é contínua neste intervalo). Em particular, $L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ é contínua em $(0,\infty)$, para $\chi\neq\chi_0$.*

**Demonstração.** Fixemos $\sigma>0$. Para $\varepsilon>0$ arbitrário, podemos tomar $n_0$ tal que $\dfrac{1}{n^\sigma}<\varepsilon$, qualquer que seja $n>n_0$. Note que isso vale para qualquer $s>\sigma$. Tomemos $M>N>n_0$, temos

$$\begin{aligned}\sum_{k=N}^{M}\frac{a_k}{k^s}&=\sum_{k=N}^{M}\frac{A_k-A_{k-1}}{k^s}=\sum_{k=N}^{M}\frac{A_k}{k^s}-\sum_{k=N-1}^{M-1}\frac{A_k}{(k+1)^s}\\&=\frac{A_M}{M^s}-\frac{A_{N-1}}{N^s}+\sum_{k=N}^{M-1}A_k\left(\frac{1}{k^s}-\frac{1}{(k+1)^s}\right).\end{aligned}$$

Ora, a soma $\sum_{k=N}^{M-1}A_k\left(\frac{1}{k^s}-\frac{1}{(k+1)^s}\right)$ é igual a $\dfrac{A_N}{N^s}-\dfrac{A_M}{M^s}$. Sendo $C>0$ tal que $|A_k|<C$, pela desigualdade triangular, temos

$$\left|\sum_{n=k}^{M}\frac{a_n}{n^s}\right|\leq\frac{C}{M^s}+\frac{C}{N^s}+C\left|\frac{1}{N^s}-\frac{1}{M^s}\right|=\frac{2C}{N^s}<2C\varepsilon,$$

como $\varepsilon$ é arbitrário, o que acabamos de provar as primeira e segunda afirmações do resultado. Para a última, note que, se $G$ é um grupo finito de ordem $m$ e $\chi$ é um caractere não trivial de $G$, então, tomando $h\in G$ tal que $\chi(h)\neq 1$, temos

$$\chi(h)\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(h)\chi(g)=\sum_{g\in G}\chi(g)\Rightarrow\sum_{g\in G}\chi(g)=0.$$

Tomando $G=[\mathbb{Z}/m\mathbb{Z}]^*$ e $\chi$ um caractere numérico módulo $m$, temos $\sum\chi(k)=0$, se $k$ percorre um sistema completo de resíduos módulo $m$. Daí, escrevendo $n=qm+r$, com $0\leq r<m$, donde $|A_n|=\sum_{k=1}^{r}|\chi(k)|<m$, donde $L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ satisfaz todas as propriedades desejadas. □

Podemos agora alcançar o nosso objetivo.

**Teorema 2.4.1.** *Sejam $\zeta=\cos\dfrac{2\pi}{m}+i\sin\dfrac{2\pi}{m}$ uma $m$-ésima raiz primitiva da unidade, $a$ um inteiro e $\chi\neq\chi_0$ um caractere numérico módulo $m$. Defina*

$$\tau_a(\chi)=\sum_{x\mod m}\chi(x)\zeta^{ax}.$$

*Então, para $s > 0$, temos a seguinte fórmula para $L(1, \chi)$*

$$L(1,\chi) = -\frac{1}{m}\sum_{k=1}^{m-1}\tau_k(\chi)\ln(1-\zeta^{-k}).$$

*Portanto, temos a seguinte fórmula para o número de classes do corpo $\mathbb{Q}(\zeta)$*

$$h = \left(\frac{\omega\sqrt{|D|}}{2^{s+t}\pi^t R}\right)\left[\prod_{\mathfrak{p}|(m)}\left(1-\frac{1}{N(\mathfrak{p})^s}\right)\right]^{-1}\cdot\prod_{p|m}\left(1-\frac{1}{p^s}\right)\cdot\prod_{\chi\neq\chi_0}\left[-\frac{1}{m}\sum_{k=1}^{m-1}\tau_k(\chi)\ln(1-\zeta^{-k})\right].$$

*Em que $\omega$ é o número de raízes da unidade de $K = \mathbb{Q}(\zeta)$, $D$ é o seu discriminante, e $R$, o seu regulador.*

**Demonstração.** Aplicando o Teorema 2.3.2 a $\mathbb{Q}$, tendo em vista que todo $\mathbb{Z}-$módulo finitamente gerado de $\mathbb{Q}$ possui um sistema de geradores com um único elemento, isto é, todo ideal fracionário de $\mathbb{Q}$ é principal, $s = m = 1$, $t = 0$ e $R = D = 1$, temos

$$\lim_{s\to 1^+}(s-1)\zeta(s) = 1, \tag{2.9}$$

em que $\zeta(s)$ é a função Zeta de Riemann padrão. Voltando ao caso geral, podemos reescrever a expressão para $\zeta_K(s)$ obtida em Teorema 2.3.1 como

$$\zeta_K(s) = \prod_{p\in\mathbb{Z}\text{ primo }}\prod_{\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}\left(1-\frac{1}{N(\mathfrak{p})^s}\right)^{-1}.$$

Somente um número finito de termos correspondem a ideais primos que dividem $(m)$, denotemos este produto por

$$G(s) = \prod_{\mathfrak{p}|(m)}\left(1-\frac{1}{N(\mathfrak{p})^s}\right)^{-1}.$$

Se $p$ e $m$ são coprimos, então a Proposição 1.10.2 nos diz que $N(\mathfrak{p}) = p^{f_p}$, com $f_p$ a ordem da classe $\overline{p}$ em $[\mathbb{Z}/m\mathbb{Z}]^*$. Além disso, ela também nos diz que o número de ideais primos distintos que dividem $p$ (isto é, tais que $\mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}$) é igual a $\dfrac{\varphi(m)}{f_p}$. Temos, portanto,

$$\zeta_K(s) = G(s)\prod_{(p,m)=1}\left(1-\frac{1}{p^{f_p s}}\right)^{-\frac{\varphi(m)}{f_p}}.$$

Substituindo $x = p^{-s}$ em $1 - x^{f_p} = \prod_{k=1}^{f_p-1}(1-\varepsilon^k x)$, com $\varepsilon = \cos\dfrac{2\pi}{f_p} + i\sin\dfrac{2\pi}{f_p}$, obtemos

$$1-\frac{1}{p^{f_p s}} = \prod_{k=1}^{f_p-1}\left(1-\frac{\varepsilon^k}{p^s}\right).$$

Trazendo de volta a potência $\dfrac{-\varphi(m)}{f_p}$, obtemos que o produto

$$\prod_{k=1}^{f_p-1}\left(1-\frac{\varepsilon^k}{p^s}\right)^{\frac{-\varphi(m)}{f_p}}$$

tem exatamente $\varphi(m)$ termos, para qualquer $p$. Posto existirem $\dfrac{\varphi(m)}{f_p}$ caracteres de $\mathbb{Z}/m\mathbb{Z}^*$ que, quando aplicados a $\overline{p}$, resultam em $\varepsilon^k$ (se necessário, consultar A.3), podemos reescrever ainda

$$\prod_{k=1}^{f_p-1}\left(1-\frac{\varepsilon^k}{p^s}\right)^{\frac{-\varphi(m)}{f_p}} = \prod_{\chi}\left(1-\frac{\chi(\overline{p})}{p^s}\right)^{-1},$$

em que $\chi$ percorre todos os caracteres do grupo $\mathbb{Z}/m\mathbb{Z}^*$. Porém, como $\chi(p)=0$, se $(p,m)>1$, para $\chi$ um caractere numérico módulo $m$, podemos usar caracteres numéricos, ao invés dos próprios caracteres de $[\mathbb{Z}/m\mathbb{Z}]^*$, e teremos

$$\zeta_K(s) = G(s)\prod_{p}\prod_{\chi}\left(1-\frac{\chi(\overline{p})}{p^s}\right)^{-1},$$

revertendo a ordem do produto, obtemos

$$\zeta_K(s) = G(s)\prod_{\chi} L(s,\chi).$$

Note que Teorema 2.3.1 aplicado a $\mathbb{Q}$ nos dá

$$\zeta(s) = \prod_{p}\left(1-\frac{1}{p^s}\right)^{-1};$$

em contrapartida, sendo $\chi_0$ o caractere trivial, temos

$$L(s,\chi_0) = \prod_{(p,m)=1}\left(1-\frac{1}{p^s}\right)^{-1},$$

donde concluímos

$$L(s,\chi_0) = \prod_{p|m}\left(1-\frac{1}{p^s}\right)\zeta(s).$$

Agora defina

$$F(s) \coloneqq \prod_{p|m}\left(1-\frac{1}{p^s}\right)G(s),$$

para ter

$$\zeta_K(s) = F(s)\zeta(s)\prod_{\chi\neq\chi_0} L(s,\chi).$$

Pelo Lema 2.4.1, temos que a série $\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ converge para $s>0$ e

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

Multiplicando por $(s-1)$ em ambos os lados e tirando o limite quando $s\to 1^+$, por 2.4 obtemos

$$h = \left(\frac{\omega\sqrt{|D|}}{2^{s+t}\pi^t R}\right)\lim_{s\to 1^+}(s-1)\zeta(s)F(s)\prod_{\chi\neq\chi_0}L(s,\chi) = \left(\frac{\omega\sqrt{|D|}}{2^{s+t}\pi^t R}\right)F(1)\prod_{(\chi\neq\chi_0)}L(1,\chi).$$

Precisamos agora tratar dos termos $L(s,\chi)$. Omitindo da série de $L(s,\chi)$ os termos que são zero e

usando que $n_1 \equiv n_2 \mod m \Rightarrow \chi(n_1) = \chi(n_2)$, escrevemos

$$L(s,\chi) = \sum_{(x,m)=1} \chi(x) \left( \sum_{n \equiv x \mod m} \left(\frac{1}{n}\right)^s \right).$$

A série no interior do somatório pode ser reescrita como

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s},\ c_n = \begin{cases} 0, & n \not\equiv x \mod m \\ 1 & n \equiv x \mod m \end{cases}.$$

Fixemos $\zeta = \cos\dfrac{2\pi}{m} + i \sin\dfrac{2\pi}{m}$ e consideremos a identidade

$$\sum_{k=0}^{m-1} \zeta^{rk} = \begin{cases} 0, & r \not\equiv 0 \mod m \\ m, & r \equiv 0 \mod m \end{cases},$$

ver Proposição A.1.2, ela nos dá a seguinte fórmula para os $c_n$'s

$$c_n = \frac{1}{m} \sum_{k=0}^{m-1} \zeta^{(x-n)k}.$$

Concluímos, portanto

$$L(s,\chi) = \sum_{(x,m)=1} \chi(x) \sum_{n=1}^{\infty} \left( \frac{1}{m} \sum_{k=0}^{m-1} \zeta^{(x-n)k} \right) \frac{1}{n^s} \tag{2.10}$$

$$= \frac{1}{m} \sum_{k=0}^{m-1} \left( \sum_{(x,m)=1} \chi(x)\zeta^{xk} \right) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s} \tag{2.11}$$

$$= \frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s} \tag{2.12}$$

(nas igualdades acima, $x$ varia num sistema de representantes das classes do grupo $[\mathbb{Z}/m\mathbb{Z}]^*$). Substituindo $s = 1$, obtemos

$$L(1,\chi) = \frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n}.$$

É um fato bem conhecido que a série $\sum_{n=1}^{\infty} \frac{z^n}{n}$ converge para $|z| \leq 1$ e representa o ramo da função $-\ln(1-z)$, cuja parte imaginária está no intervalo $(-\frac{\pi}{2}, \frac{\pi}{2})$. Podemos então substituir então $z = \zeta^{-k}$ e obter

$$\sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n} = -\ln(1-\zeta^{-k}),$$

substituindo este valor na expressão para $L(1,\chi)$, e este último na expressão para $h$, chegamos ao resultado. □

## 2.5 O número de classes em corpos quadráticos

**Definição 2.5.1.** *Um corpo quadrático é um corpo $K$, tal que $[K : \mathbb{Q}] = 2$.*

Verifica-se que todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, com $d$ um inteiro livre de quadrados. Nosso objetivo é expor uma fórmula para o número de classes de um corpo quadrático. Como viemos fazendo até então, precisamos entender os ideais primos de $K$, para podermos utilizar o Teorema 2.3.1. Neste sentido, temos o Teorema abaixo. Porém, antes de prová-lo, lembremos que, sendo $p$ um número primo ímpar e $m$ um inteiro, o *Símbolo de Legendre* $\left(\frac{m}{p}\right)$ é definido por

$$\left(\frac{m}{p}\right) = \begin{cases} 0, & p|m \\ 1, & (p,m)=1 \text{ e existe } x \in \mathbb{Z} \text{ tal que } x^2 \equiv m \mod p \\ -1, & (p,m)=1 \text{ e não existe } x \in \mathbb{Z} \text{ tal que } x^2 \equiv m \mod p \end{cases} \tag{2.13}$$

É possível mostrar que, via uma identificação, o Símbolo de Legendre também é dado pelo elemento

$$\overline{m}^{\frac{p-1}{2}},\ \overline{m} \in \mathbb{Z}/p\mathbb{Z}.$$

A prova desta equivalência se encontra, por exemplo, em [7][Chapter I, section 3.2, theorem 5]. O *Símbolo de Jacobi* é definido como o produto dos símbolos de Legendre da fatoração em primos do denominador, isto é, se $b = p^{e_1} \dots p_k^{e_k}$ é a fatoração em primos do número inteiro positivo ímpar $b$, e $a$ é um inteiro coprimo com $b$, o Símbolo de Jacobi é definido por

$$\left[\frac{a}{b}\right] = \prod_i \left(\frac{a}{p_i}\right)^{e_i}.$$

No entanto, utilizaremos a notação $\left(\frac{a}{b}\right)$, também para o Símbolo de Jacobi. A Lei da reciprocidade quadrática para o Símbolo de Jacobi (logo, para o Símbolo de Legendre, restrito a primos ímpares) nos diz que, sendo $a$ e $b$ ímpares coprimos,

$$\left(\frac{a}{b}\right)\left(\frac{b}{|a|}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}, \tag{2.14}$$

sua prova pode ser encontrada em [5][Chapter 5, Proposition 5.5.2].

Precisaremos ainda do Teorema abaixo.

**Teorema 2.5.1.** *O anel de inteiros de um corpo quadrático $K = \mathbb{Q}(\sqrt{d})$ é da forma $\mathbb{Z}[\omega]$, com $\omega = \frac{1+\sqrt{d}}{2}$, se $d \equiv 1 \mod 4$, e $\omega = \sqrt{d}$, com $d \equiv 2$ ou $3 \mod 4$.*

Cuja prova pode ser encontrada em [2][Chapter 2, section 7, theorem 1] numa linguagem mais geral.

**Teorema 2.5.2.** *Num corpo quadrático de discriminante $D$, o ideal $(p) = p\mathfrak{O}_K$ fatora-se como*

$$(p) = \mathfrak{p}^2,\ N(\mathfrak{p}) = p$$

*se, e somente se, $p|D$. Se $p$ não divide $D$ e $p \neq 2$, então*

$$(p) = \mathfrak{p}\mathfrak{p}',\ N(\mathfrak{p}) = N(\mathfrak{p}') = p, \text{ se } \left(\frac{D}{p}\right) = 1$$

$$(p) = \mathfrak{p},\ N(\mathfrak{p}) = p^2, \text{ se } \left(\frac{D}{p}\right) = -1$$

*Se* $2$ *não divide* $D$*, então*

$$(2) = \mathfrak{p}\mathfrak{p}',\ N(\mathfrak{p}) = N(\mathfrak{p}') = 2,\ \textit{se}\ D \equiv 1 \mod 8$$

$$(2) = \mathfrak{p},\ N(\mathfrak{p}) = 4,\ D \equiv 5 \mod 8.$$

**Demonstração.** Primeiramente, note que, pela Proposição 1.8.2, temos as seguintes possibilidades

a) $(p) = \mathfrak{p}\mathfrak{p}',\ \mathfrak{p} \neq \mathfrak{p}'$;

b) $(p) = \mathfrak{p}$;

c) $(p) = \mathfrak{p}^2$;

nas quais temos, respectivamente: $N(\mathfrak{p}) = N(\mathfrak{p}') = p$, $N(\mathfrak{p}) = p^2$ e $N(\mathfrak{p}) = p$.

Sabemos que todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, com $d$ um inteiro livre de quadrados. Seja $p$ um primo ímpar que não divide $d$. O Teorema anterior nos diz que o anel de inteiros de $K$ ($K = \mathbb{Q}(\sqrt{d})$) é $\mathbb{Z}[\sqrt{d}]$ ou $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, dependendo se $d \equiv 3$ ou $2 \mod$ , ou se $d \equiv 1 \mod 4$. No primeiro caso, temos $\mathfrak{F} = (1) = \mathfrak{O}_K$, em que $\mathfrak{F}$ é o condutor de $\mathfrak{O}_K$, e temos $(p)$ e $\mathfrak{F}$ coprimos. No caso em que $\mathfrak{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, temos $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, como um subgrupo de índice $2$. De fato, se $b$ é par, então $a + b\left[\frac{1+\sqrt{d}}{2}\right] \in \mathbb{Z}[\sqrt{d}]$ e, se $b$ é ímpar, escrevemos $b = 2m + 1$, com $m \in \mathbb{Z}$ e temos $a + b\left[\frac{1+\sqrt{d}}{2}\right] - \frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\sqrt{d}]$, donde

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z}[\sqrt{d}] \bigsqcup \left(\frac{1+\sqrt{d}}{2} + \mathbb{Z}[\sqrt{d}]\right).$$

Portanto, todo ideal de $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ contido em $\mathbb{Z}[\sqrt{d}]$ deve ter índice múltiplo de $2$, e o maior destes tais ideais é justamente $(2)$. Daí, temos $\mathfrak{F} = (2)$, que é claramente coprimo com $(p)$. Daí, podemos usar a Proposição 1.8.3 para dizer que os ideais primos distintos que dividem $(p)$ estão em bijeção com os divisores irredutíveis de $x^2 - d$ módulo $p$; como este polinômio é irredutível, ou tem duas raízes distintas em $\mathbb{Z}/p\mathbb{Z}$, então $(p)$ não pode ter uma fatoração do tipo $c)$. Além disso, $(p)$ terá uma fatoração do tipo $a)$ ou $b)$ a depender de $x^2 - d$ ser ou não irredutível módulo $p$, o que, por sua vez, é equivalente a $d$ ser ou não um quadrado módulo $p$, isto é $(p)$ tem uma fatoração do tipo $a)$ se, e somente se, $\left(\frac{d}{p}\right) = 1$, e do tipo $b$ se, e somente se, $\left(\frac{d}{p}\right) = -1$.

Caso $p|d$, como $d$ é livre de quadrados, temos $(\sqrt{d})^2 = (p)(d_1)$, com $p$ e $d_1$ coprimos, donde também os ideais $(p)$ e $(d_1)$ são coprimos. Pela unicidade da fatoração $(\sqrt{d})^2 = (p)(d_1)$ nos diz que os todos os ideais primos que dividem $(p)$ têm expoente par, o que só é possível numa fatoração do tipo $c)$. Note que este argumento não depende de $p$ ser ou não ímpar, e que, como o discriminante de $\mathbb{Q}(\sqrt{d})$ é $d$ ou $4d$ (a depender de $d$ ser congruente a $1$ módulo $4$, ou não), podemos trocar $d$ por $D$, sem nenhum prejuízo à demonstração.

Agora, se $p = 2$ e $2$ não divide $D \equiv 1 \mod 4$, como $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}\left(\frac{1+\sqrt{D}}{2}\right)$ e o polinômio

mínimo de $\frac{1+\sqrt{d}}{2}$ é

$$x^2 + x + \frac{1-D}{4},$$

que é redutível módulo $2$ se, e somente se, $2$ divide $\frac{1-D}{4}$, o que só acontece se $D \equiv 1 \mod 8$, o caso restante é coberto por $D \equiv 5 \mod 8$ (estas são as únicas opções, tendo em vista que $D \equiv 1 \mod 4$). Portanto, $(2)$ tem uma fatoração do tipo $a)$ se $D \equiv 1 \mod 8$, e do tipo $b)$ se $D \equiv 1 \mod 8$.

□

Seja $p$ um primo ímpar e $d = D \equiv 1 \mod 4$. Pela Lei da reciprocidade quadrática para o Símbolo de Jacobi, temos

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\frac{d-1}{2}}\left(\frac{p}{|d|}\right) = \left(\frac{p}{|D|}\right). \tag{2.15}$$

Seja agora $d \equiv 3 \mod 4$, temos

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\frac{d-1}{2}}\left(\frac{p}{|d|}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{|d|}\right). \tag{2.16}$$

Seja agora $d = 2d'$, $(2, d') = 1$.

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{d'}{p}\right) = (-1)^{\frac{p^2-1}{8}+\frac{(p-1)(d'-1)}{4}}\left(\frac{p}{|d'|}\right) \tag{2.17}$$

A expressão no extremo direito de 2.15 depende apenas do resíduo de $p$ módulo $|d| = |D|$. Já no caso de 2.16, depende do resíduo de $p$ módulo $|d|$ e do número $(-1)^{\frac{p-1}{2}}$. Isto é, depende também do resíduo de $d$ módulo $4$, logo, pelo Teorema Chinês dos restos, depende do resíduo de $p$ módulo $4|d| = |D|$. Por fim, em 2.17, ela depende do resíduo de $p$ módulo $|d|$, do número $(-1)^{\frac{p^2-1}{8}}$, isto é, do resíduo de $p$ módulo $4$, e também de $(-1)^{\frac{p-1}{2}}$, que corresponde ao resíduo de $p$ módulo $4$. Estas, por sua vez, reduzem-se à dependência do número $8|d| = |D|$. Logo, em todos os três casos, o tipo de decomposição de $p$ depende apenas do resíduo de $p$ módulo $|D|$. Com estas considerações em mente, definimos uma função sobre os inteiros $x$ coprimos com o discriminante $|D|$, que é, na verdade, um caractere módulo $|D|$.

**Definição 2.5.2.** *A função*

$$\chi(p) = \begin{cases} \left(\frac{p}{|D|}\right), & \text{se } d \equiv 1 \mod 4 \\ (-1)^{\frac{p-1}{2}}\left(\frac{p}{|d|}\right) & \text{se } d \equiv 3 \mod 4 \\ (-1)^{\frac{p^2-1}{8}+\frac{(p-1)(d'-1)}{4}}\left(\frac{p}{|d'|}\right) & \text{se } d = 2d' \end{cases}.$$

*é chamada o caractere de $K$.*

**Observação 2.5.1.** *Note que nenhum dos argumentos para mostrar que $\left(\frac{D}{p}\right)$ dependia apenas do resíduo de $p$ módulo $|D|$ usou o fato de $p$ ser primo, portanto, os mesmos argumentos mostram que, trocando, $p$ por $x$ na definição acima, com $x$ inteiro coprimo com $D$, $\chi(x)$ depende apenas do resíduo de $x$ módulo $|D|$. Como o símbolo de Jacobi é multiplicativo em inteiros coprimos, verifica-se que, para $(x, D) = 1 = (x', D)$, tem-se $\chi(x)\chi(x') = \chi(xx')$. Impondo $\chi(a) = 0$, para $(a, D) > 1$, obtemos um caractere numérico módulo $|D|$.*

Podemos reescrever o Teorema 2.5.2 em função do caractere $\chi$.

**Teorema 2.5.3.** *Num corpo quadrático de discriminante $D$, o ideal $(p) = p\mathfrak{O}_K$, com $p$ primo, fatora-se como*

$$(p) = \mathfrak{p}^2,\ N(\mathfrak{p}) = p$$

*se, e somente se, $\chi(p) = 0$. Se $p$ não divide $D$, então*

$$(p) = \mathfrak{p}\mathfrak{p}',\ N(\mathfrak{p}) = N(\mathfrak{p}') = p,\ \textit{se}\ \chi(p) = 1$$

$$(p) = \mathfrak{p},\ N(\mathfrak{p}) = p^2,\ \textit{se}\ \chi(p) = -1.$$

Visto que $\chi$ é definido a partir de um Símbolo de Jacobi com "denominador"$d$, e não $D$, poder-se-ia perguntar se $\chi$ não seria induzido por algum caractere módulo $d$. O lema abaixo vem responder esta pergunta não apenas para $d$, mas para qualquer divisor de $D$.

**Lema 2.5.1.** *O caractere de um corpo quadrático é um caractere primitivo módulo $|D|$ (em que $D$ é o seu discriminante).*

**Demonstração.** Queremos usar o Lema A.2.1, para tanto, primeiro consideremos um primo $p \neq 2$, que divide $D$. Dado qualquer resíduo não quadrático $s$ módulo $p$ e tomemos $x$ uma solução do sistema

$$\begin{cases} x \equiv s & \mod p \\ x \equiv 1 & \mod \frac{2|D|}{p} \end{cases}.$$

Afirmamos que $\chi(x) = \left(\frac{x}{p}\right) = \left(\frac{s}{p}\right) = -1$. Isto segue da definição de $\chi$, caso $d = D \equiv 1 \mod 4$. Caso $d \equiv 3 \mod 4$, então

$$\chi(x) = (-1)^{\frac{x-1}{2}}\left(\frac{x}{|d|}\right) = \prod_{q|d}\left(\frac{x}{q}\right) = \left(\frac{x}{p}\right) = \left(\frac{s}{p}\right) = 1.$$

Já para $D = 4d$, com $d \equiv 3 \mod 4$, lembrando que um sistema na forma

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \end{cases}$$

tem solução se, e somente se $a_1 \equiv a_2 \mod (m_1, m_2)$, resolvemos as congruências

$$\begin{cases} x \equiv 3 & \mod 4 \\ x \equiv 1 & \mod 2|d| \end{cases}$$

e obtemos $\chi(x) = (-1)^{\frac{x-1}{2}} = -1$. Caso tenhamos $d = 2d'$, $D = 4d = 8d'$, então, resolvemos as congruências

$$\begin{cases} x \equiv 5 & \mod 8 \\ x \equiv 1 & \mod 4|d'| \end{cases}$$

e obtemos $\chi(x) = (-1)^{\frac{x^2-1}{8}} = -1$. □

É de nosso interesse calcular a $L$-série $L(1, \chi)$. No entanto, isso não depende de $\chi$ ser o caractere de um corpo quadrático $K$, depende apenas de $\chi$ ser par, isto é, se $\chi(-1) = 1$, ou ímpar, $\chi(-1) = -1$. De fato, temos o

**Teorema 2.5.4.** *Seja $\chi$ um caractere primitivo módulo $m > 1$. Se $\chi$ é par, então,*

$$L(1,\chi) = -\frac{\tau(\chi)}{m} \sum_{(k,m)=1, k\leq m} \overline{\chi}(k) \ln|1-\zeta^k|.$$

*Se $\chi$ é ímpar, então*

$$L(1,\chi) = \pi i \tau(\chi) m^{-2} \sum_{(k,m)=1, k<m} \overline{\chi}(k) k$$

**Demonstração.** Primeiro, mostraremos que, se $(a,m) = r > 1$, então

$$\tau_a(\chi) = \sum_{x \mod m} \chi(x)\zeta^{ax} = 0,$$

com $\zeta = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$. De fato, se $m = rd$ então $\zeta^a$ é uma $d$-ésima raiz primitiva da unidade e, portanto, $\zeta^{az} = \zeta^a$, se $z \equiv 1 \mod d$. Daí, se tomarmos $z \equiv 1 \mod d$, com $(z,m) = 1$ e $\chi(z) \neq 1$ (isto é, como no Lema A.2.1), temos que, se $x$ percorre um sistema completo de resíduos módulo $m$, também $zm$ o faz e

$$\tau_a(\chi) = \sum_{x \mod m} \chi(zx)\zeta^{azx} = \chi(z)\tau_a(\chi) \Rightarrow \tau_a(\chi) = 0,$$

pois $\chi(z) \neq 1$.

Se $(a,m) = 1$, então $ax$ percorre um sistema completo de resíduos módulo $m$, sempre que $x$ o faz, e, portanto, multiplicando por $\chi(a)$, obtemos

$$\tau_a(\chi) = \chi^{-1}(a)\tau(\chi)$$

(lembrando que $\tau(\chi) = \tau_1(\chi)$). Repetindo a argumentação usada para calcular $L(1,\chi)$ no Teorema 2.4.1, temos

$$L(1,\chi) = -\frac{1}{m}\sum_{k=1}^{m-1} \tau_k(\chi)\ln(1-\zeta^{-k}).$$

Substituindo nesta fórmula os respectivos $\tau_k(\chi)$'s, obtemos

$$L(1,\chi) = -\frac{\tau(\chi)}{m} \sum_{(k,m)=1} \overline{\chi(k)}\ln(1-\zeta^{-k})$$

(como $\chi(k)$ é uma raiz da unidade, seu inverso multiplicativo coincide com seu conjugado). Analisemos a soma

$$S_\chi = \sum_{(k,m)=1} \overline{\chi(k)}\ln(1-\zeta^{-k}). \tag{2.18}$$

O número $1-\zeta^{-k}$, para $0 < k < m$, pode ser representado na forma

$$1-\zeta^{-k} = 2ie^{-i\frac{\pi k}{m}}\sin\frac{\pi k}{m} = e^{i\frac{\pi}{2}}e^{-i\frac{\pi k}{m}}\sin\frac{\pi k}{m} = e^{i\left(\frac{\pi}{2}-\frac{\pi k}{m}\right)}\sin\frac{\pi k}{m} = \sin\frac{k\pi}{m}\left(\cos\left(\frac{\pi}{2}-\frac{k\pi}{m}\right) + i\sin\left(\frac{\pi}{2}-\frac{k\pi}{m}\right)\right).$$

Daí,

$$\ln(1-\zeta^{-k}) = \ln|1-\zeta^{-k}| + i\pi\left(\frac{1}{2}-\frac{k}{m}\right).$$

Não só isso, desde que $1-\zeta^k$ e $1-\zeta^{-k}$ são conjugados, então

$$\ln(1-\zeta^{-k}) = \ln|1-\zeta^{-k}| - i\pi\left(\frac{1}{2}-\frac{k}{m}\right).$$

Supondo que $\chi$ é par, podemos livremente trocar $-k$ por $k$ e obter

$$S_\chi = \sum_{(k,m)=1} \overline{\chi(k)}\ln(1-\zeta^k).$$

Somando com 2.18, obtemos

$$2S_\chi = \sum_{(k,m)=1} \overline{\chi(k)}[\ln(1-\zeta^{-k}) + \ln(1-\zeta^k)] = 2\sum_{(k,m)=1} \overline{\chi(k)}\ln|1-\zeta^k|,$$

o que prova o resultado, neste caso.

Se $\chi$ é ímpar, então $\chi(-k) = -\chi(k)$ nos fornece

$$S_\chi = -\sum_{(k,m)=1} \overline{\chi(k)}\ln(1-\zeta^k).$$

Subtraindo esta expressão de 2.18, obtemos

$$2S_\chi = \sum_{(k,m)=1} \overline{\chi(k)}[\ln(1-\zeta^{-k}) - \ln(1-\zeta^k)] = 2\sum_{(k,m)=1} \overline{\chi(k)}\pi i\left(\frac{1}{2}-\frac{k}{m}\right),$$

o que finaliza a demonstração. □

**Teorema 2.5.5.** *O caractere de um corpo quadrático real é par, e o caractere de um corpo quadrático imaginário é ímpar.*

**Demonstração.** Sendo $\chi$ o caractere $\mathbb{Q}(\sqrt{d})$. Se $d \equiv 1 \mod 4$, então

$$\chi(-1) = \left(\frac{-1}{|d|}\right) = (-1)^{\frac{|d|-1}{2}} = (-1)^{\frac{d-1}{2}+\frac{|d|-1}{2}}.$$

Se $d \equiv 3 \mod 4$, então

$$\chi(-1) = -\left(\frac{-1}{d}\right) = -(-1)^{\frac{|d|-1}{2}} = (-1)^{\frac{d-1}{2}+\frac{|d|-1}{2}}.$$

Se $d = 2d'$, então

$$\chi(-1) = (-1)^{\frac{d'-1}{2}}\left(\frac{-1}{|d'|}\right) = (-1)^{\frac{d'-1}{2}+\frac{|d'|-1}{2}}.$$

Por outro lado, se $a$ é ímpar, então

$$\frac{a-1}{2}+\frac{|a|-1}{2} = \begin{cases} a-1, & \text{se } a>0 \\ -1 & \text{se } a<0 \end{cases}.$$

Fazendo $a=-1$, isso prova o resultado. □

Assim como ocorreu com corpos ciclotômicos, precisaremos calcular a soma

$$\tau(\chi) = \sum_{x \mod |D|} \chi(x)\zeta^x,$$

com $\zeta = \cos\dfrac{2\pi}{|D|} + i\sin\dfrac{2\pi}{|D|}$, visto que ela aparece na fórmula para $L(1,\chi)$. Novamente, isto não será feito por um método que se aplique especificamente a $\chi$, mas a um caso um pouco mais geral.

**Teorema 2.5.6.** *Seja $\chi$ um caractere primitivo módulo $m$ tal que $\chi^2 = \chi_0$ e $\zeta = \cos\dfrac{2\pi}{m} + i\sin\dfrac{2\pi}{m}$, então*

$$\tau(\chi) = \sum_{\overline{x}\in[\mathbb{Z}/m\mathbb{Z}]^*} \chi(x)\zeta^x = \begin{cases} \sqrt{m}, & \chi(-1) = 1, \\ i\sqrt{m}, & \chi(-1) = -1. \end{cases}$$

**Demonstração.** Provaremos completamente apenas o caso em que $m = p$ é um primo ímpar. O caso geral é deduzido a partir deste. Como o grupo dos caracteres quadráticos módulo $p$ tem ordem $2$, e os caracteres $\chi_0$ e $\left(\frac{\cdot}{p}\right)$ pertencem a este grupo, então podemos tomar $\chi$ como o símbolo de Legendre módulo $p$. Isto é

$$\tau(\chi) = \sum_{\overline{x}\in[\mathbb{Z}/m\mathbb{Z}]^*} \left(\frac{x}{p}\right)\zeta^x.$$

Como $\overline{\zeta} = \zeta^{-1}$, temos

$$\overline{\tau(\chi)} = \sum_{\overline{x}\in[\mathbb{Z}/m\mathbb{Z}]^*} \left(\frac{x}{p}\right)\zeta^{-x} = \sum_{\overline{x}\in[\mathbb{Z}/m\mathbb{Z}]^*} \left(\frac{-x}{p}\right)\zeta^x = \left(\frac{-1}{p}\right)\tau(\chi).$$

Por outro lado, temos $\overline{\tau(\chi)}\tau(\chi) = p$. De fato, temos

$$\overline{\tau(\chi)}\tau(\chi) = \sum_{1\le x\le p-1}\sum_{1\le y\le p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{x-y} = \sum_{1\le z\le p-1}\sum_{1\le y\le p-1}\left(\frac{zy}{p}\right)\left(\frac{y}{p}\right)\zeta^{y(z-1)} = \sum_{1\le z\le p-1}\left(\frac{z}{p}\right)\sum_{1\le y\le p-1}\zeta^{y(z-1)}.$$

Note que a soma $\sum_{1\le y\le p-1}\zeta^{y(z-1)}$ é igual a $p-1$, se $z = 1$. Caso $z \neq 1$, ela é igual a soma de todas as $p$-ésimas raízes da unidade, com exceção de $1$, logo, é igual a $-1$. Portanto

$$\sum_{1\le z\le p-1}\left(\frac{z}{p}\right)\sum_{1\le y\le p-1}\zeta^{y(z-1)} = \left(\frac{1}{p}\right)(p-1) - \sum_{2\le z\le p-1}\left(\frac{z}{p}\right) = p - 1 - (-1) = p,$$

pois $\mathbb{Z}/p\mathbb{Z}$ tem o mesmo número de quadrados não-nulos e não-quadrados não-nulos. Portanto,

$$\tau(\chi) = \begin{cases} \pm\sqrt{p}, & p \equiv 1 \mod 4, \\ \pm i\sqrt{p}, & p \equiv 3 \mod 4. \end{cases} \tag{2.19}$$

A maior dificuldade da demonstração reside em eliminar os sinais negativos.

Para fazer esta eliminação, precisaremos reescrever $\tau(\chi)$ numa forma mais conveniente. Para começar, seja a matriz

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \zeta & \dots & \zeta^{(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{p-1} & \dots & \zeta^{(p-1)^2} \end{pmatrix}.$$

Uma vez que o mapa $x \mapsto x^2$ para $x \in \mathbb{Z}/p\mathbb{Z}$ atinge $0$ uma vez e cada resíduo quadrático duas vezes e

o polinômio $z^{p-1}-1$ fatora-se como $(z-1)(z^{p-2}+\cdots z+1)$ e $\zeta \neq 1$, obtemos

$$\zeta^{p-2}+\cdots+\zeta=-1 \Rightarrow \tau(\chi)=\sum_{a\in[\mathbb{Z}/p\mathbb{Z}^*]^2}\zeta^a-\sum_{b\notin[\mathbb{Z}/p\mathbb{Z}^*]^2}\zeta^b=1+2\sum_a\zeta^a=\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\zeta^{x^2},$$

ora, esta última expressão é o traço da matriz $A$. Sejam $\lambda_1\ldots,\lambda_p$ as raízes do polinômio característico de $A$, como $A^2v=\lambda_i^2v$, se $v$ é um autovetor de $A$ associado ao autovalor $\lambda_i$, então as raízes do polinômio característico de $A^2$ são $\lambda_1^2\ldots,\lambda_p^2$. Por outro lado, podemos facilmente obter uma expressão para a entrada $a_{ij}$ de $A^2$, pois

$$\sum_{x=0}^{p-1}\zeta^{ix}\sum_{y=0}^{p-1}\zeta^{jy}=\sum_{t=0}^{p-1}\zeta^{t(i+j)}=\begin{cases}p, & i+j\equiv 0 \mod p\\ 0, & i+j\not\equiv 0 \mod p\end{cases}.$$

Obtemos portanto,

$$A^2=p\begin{pmatrix}1&0&\ldots&0\\0&\ldots&0&1\\0&\ldots&1&0\\\vdots&\ddots&\vdots&\vdots\\0&1&\ldots&0\end{pmatrix}.$$

A matriz $\dfrac{A^2}{p}$ é a matriz da permutação induzida por $\pi(i)=-i$, com $i$ percorrendo $0,1,\ldots,p-1 \mod p$. Tal permutação possui um ponto fixo $0$, e $\dfrac{p-1}{2}$ transposições (2-ciclos). Portanto, tomando $e_i=(0,0,\ldots 1,\ldots,0)$, $i$ variando de $0$ a $p-1$ e a coordenada $1$ na $i+1$-ésima entrada, o operador linear $T$ (em $\mathbb{C}^p$) definido por $\dfrac{A^2}{p}$ é determinado por $Te_i=e_{\pi(i)}$. Além disso, podemos escrever

$$\mathbb{C}^p=\langle e_0\rangle\oplus\langle e_1,e_{p-1}\rangle\oplus\cdots\oplus\langle e_{\frac{p-1}{2}},e_{\frac{p+1}{2}}\rangle,$$

em que cada subespaço $\langle e_i,e_{p-i}\rangle$ é $T$-invariante. Como a matriz de $T|_{\langle e_i,e_{p-i}\rangle}$ nesta base é $\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $T|_{\langle e_i,e_{p-i}\rangle}$ possui autovalores $\tilde{e_i}$ e $\tilde{e}_{p-i}$, tais que $T\tilde{e_i}=e_i$ e $T\tilde{e}_{p-i}=-\tilde{e}_{p-i}$. Portanto, temos $\dfrac{p+1}{2}$ autovalores $1$ e $\dfrac{p-1}{2}$ autovalores $-1$, donde os autovalores (as raízes do polinômio característico) de $A^2$ são $p$, com multiplicidade $\dfrac{p+1}{2}$ e $-p$, com multiplicidade $\dfrac{p-1}{2}$. Daí, temos que os autovalores de $A$ são $\pm\sqrt{p}$ e $\pm i\sqrt{p}$. Sendo $a,b,c,d$ suas respectivas multiplicidades, temos

$$\tau(\chi)=[(a-b)+(c-d)i]\sqrt{p}\ ,\ a+b=\frac{p+1}{2}\text{ e }c+d=\frac{p-1}{2}.$$

Comparando com 2.19, obtemos

$$\begin{cases}a-b=\pm1,\ c=d, & p\equiv 1 \mod 4\\ a=b,\ c-d=\pm1, & p\equiv 3 \mod 4\end{cases}. \tag{2.20}$$

Para determinar $a,b,c$ e $d$, precisamos de outra relação entre eles.

Visto que $\det A$ é um determinante de Vandermonde, temos

$$\det A=\prod_{0\leq s<r\leq p-1}(\zeta^r-\zeta^s);$$

definindo $\eta = \cos\frac{\pi}{p} + i\sin\frac{\pi}{p}$, como $\eta^2 = \zeta$, pondo $\eta^{(r+s)}$ em evidência em $\eta^{2r} - \eta^{2s} = \eta^{(r+s)+r-s} - \eta^{(r+s)-(r-s)}$, obtemos

$$\det A = \prod_{r>s} \eta^{(r+s)} \prod_{r>s} 2i \sin\left(\frac{(r-s)\pi}{p}\right). \tag{2.21}$$

Como há $\frac{p(p-1)}{2}$ pares da forma $(r,s)$, com $r > s$, em que $r$ e $s$ percorrem $0, 1, \ldots, p-1$, podemos pôr $(2i)^{\frac{p(p-1)}{2}}$ em evidência no último produtório, além disso, o produtório à esquerda dele é igual a $\eta^{\sum_{r=1}^{p-1}\sum_{s=0}^{r-1}(r+s)}$, e como $\eta^{2p} = 1$, ao notarmos

$$\sum_{r=1}^{p-1}\sum_{s=0}^{r-1}(r+s) = \sum_{r=1}^{p-1}\left(r^2 + \frac{r(r-1)}{2}\right) = 2p\left(\frac{p-1}{2}\right)^2,$$

obtemos

$$\det A = (2i)^{\frac{p(p-1)}{2}} \prod_{r>s} \sin\left(\frac{(r-s)\pi}{p}\right).$$

Por outro lado, como $A^2 = pJ$, em que $J$ resulta de permutar as colunar $i$ e $p-i$ da matriz identidade $p \times p$ (índices das entradas variando de $0$ a $p-1$), obtemos

$$\det A = \pm i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}.$$

Comparando as duas expressões para $\det A$, e usando que $\sin\frac{(r-s)\pi}{p}$ é sempre positivo nas condições satisfeitas por $r$ e $s$, logo $\det A = i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}$.

Por outro lado, temos

$$\det A = p^{\frac{a}{2}}(-1)^b p^{\frac{b}{2}} i^c p^{\frac{c}{2}} (-1)^d i^d p^{\frac{d}{2}} = i^{2b+c-d} p^{\frac{p}{2}}.$$

Se $p \equiv 1 \mod 4$, então

$$2b \equiv p\left(\frac{(p-1)}{2}\right) \equiv \frac{p+1}{2} - \frac{p-1}{2} \equiv 1 \mod 4$$

e como

$$a - b = \frac{p+1}{2} - 2b,$$

temos $a - b = 1$, por 2.20. Por fim, se $p \equiv 3 \mod 4$, então

$$c - d \equiv -\frac{-(p-1)}{2} + 2b \equiv -\frac{p-1}{2} + \frac{p+1}{2} \equiv 1 \mod 4,$$

donde $c - d = 1$. Visto que $\tau(\chi) = [(a-b) + (c-d)i]\sqrt{p}$, temos o resultado provado, para $p$ primo ímpar.

Para generalizar o resultado, consideramos primeiro o caractere módulo $4$ dado por $\chi(x) = (-1)^{\frac{x-1}{2}}$ e os caracteres módulo $8$

$$\chi'(x) = (-1)^{\frac{x^2-1}{8}} \text{ e } \chi''(x) = (-1)^{\frac{(x^2-1)}{8} + \frac{x-1}{2}}.$$

Computa-se as somas $\tau(\chi)$, $\tau(\chi')$ e $\tau(\chi'')$, e se obtém $2i$, $2\sqrt{2}$, $2i\sqrt{2}$. Utilizando a Proposição A.3.2 e aplicando a fórmula do Proposição A.3.1, obtemos, por exemplo, para o caso $m = 8r$,

$$\chi(x) = (-1)^{\frac{(x^2-1)}{8} + \frac{x-1}{2}} \left(\frac{x}{p_1}\right) \ldots \left(\frac{x}{p_s}\right).$$

Seja $\alpha$ o número de primos entre $p_1, \ldots, p_s$ congruentes a $3$ módulo $4$. Então

$$\tau(\chi) = 2i\sqrt{2}i^{\alpha}\sqrt{r}(-1)^{\frac{(r^2-1)}{8}+\frac{r-1}{2}}\left(\frac{2}{r}\right)\prod_{k\neq j}\left(\frac{p_k}{p_j}\right) =$$
$$\sqrt{m}i^{\alpha+1+2\alpha+\alpha(\alpha-1)} =$$
$$i^{(\alpha+1)^2}\sqrt{m} =$$
$$\begin{cases}\sqrt{m}, & \chi(-1) = (-1)^{\alpha-1} = 1\\ i\sqrt{m}, & \chi(-1) = (-1)^{\alpha+1} = -1\end{cases}.$$

As outras possibilidades para $\chi$ são tratadas de maneiras análogas. Damos a demonstração por encerrada aqui. □

**Teorema 2.5.7.** *Sejam $K$ um corpo quadrático e $h = |Cl_K|$. Então,*

$$h = \begin{cases}\frac{\sqrt{|D|}}{2\ln\varepsilon}L(1,\chi), & \textit{se } K \textit{ é real}\\ \frac{m\sqrt{|D|}}{2\pi}L(1,\chi), & \textit{se } K \textit{ é imaginário.}\end{cases}$$

*Nas fórmulas acima, $D$ é o discriminante de $K$, $\varepsilon$ é uma unidade fundamental de $K$, $\chi$ é o caractere de $K$ e $m$ é o número de raízes da unidade contidas em $K$.*

**Demonstração.** Utilizando o Teorema 2.3.2, e lembrando que, para corpos quadráticos reais, tem-se $m = 2$ e $R = \ln\varepsilon$, obtemos

$$h = \begin{cases}\frac{\sqrt{|D}}{2\ln\varepsilon}\lim_{s\to1^+}(s-1)\zeta_K(s), & \text{se } K \text{ é real}\\ \frac{m\sqrt{|D|}}{2\pi}\lim_{s\to1^+}(s-1)\zeta_K(s), & \text{se } K \text{ é imaginário.}\end{cases}$$

Utilizando o Teorema 2.5.2, obtemos que cada fator do produtório que resulta de aplicar Teorema 2.3.1 a $\zeta_K(s)$ é da forma $\left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{1}{p^s}\right)^{-1}$, $\left(1-\frac{1}{p^2s}\right) = \left(1-\frac{1}{p^s}\right)^{-1}\left(1+\frac{1}{p^s}\right)$, ou $\left(1-\frac{1}{p^s}\right)^{-1}$, para cada ideal primo correspondente ao primo inteiro $p$. Em qualquer dos casos, o fator se reescreve como

$$\left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}.$$

Disto, concluímos

$$\zeta_K(s) = \zeta(s)\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1} = \zeta_K(s)L(1,\chi).$$

Multiplicando por $(s-1)$, tomando o limite quando $s\to1^+$ e aplicando Teorema 2.3.2 a $\mathbb{Q}$, como fizemos na primeira parte da prova do Teorema 2.4.1, obtemos

$$\lim_{s\to s^+}(s-1)\zeta_K(s) = L(1,\chi),$$

e o resultado está provado. □

Tendo em vista que os métodos usados nesta seção não foram tão explícitos, como no caso de corpos ciclotômicos, vamos exemplificá-los, aplicando-os ao corpo $\mathbb{Q}(\sqrt{-5})$. Este corpo possui apenas duas raízes da unidade, $\pm1$. E como seu anel de inteiros é $\mathbb{Z}[\sqrt{-5}]$, seu discriminante é $-20$. O caractere de $\mathbb{Q}(\sqrt{-5})$ é

$$\chi(x) = (-1)^{\frac{x-1}{2}}\left(\frac{x}{5}\right).$$

Daí, usando a fórmula do Teorema 2.5.4, juntamente com Teorema 2.5.5 obtemos, sem nenhuma simplificação,

$$L(1,\chi) = \pi i \frac{(i\sqrt{20})}{400} \sum_{(k,20)=1,\ k\leq 20} (-1)^{\frac{k-1}{2}} \left(\frac{k}{5}\right) k.$$

Daí, usando o Teorema 2.5.7, temos

$$h = \frac{2\sqrt{20}}{2\pi} \pi i \frac{(i\sqrt{20})}{400} \sum_{(k,20)=1,\ k\leq 20} (-1)^{\frac{k-1}{2}} \left(\frac{k}{5}\right) k = 2,$$

então $Cl_{\mathbb{Q}(\sqrt{-5})}$ tem exatamente duas classes, sendo o melhor dos piores casos, isto é, o mais próximo possível de ser um domínio de fatoração única, sem de fato o ser.

# Referências Bibliográficas


[1] ATIYAH, M. F., AND MACDONALD, I. G. *Introduction to commutative algebra*. CRC Press, 2018.

[2] BOREVICH, Z. I., AND SHAFAREVICH, I. R. *Number Theory*. Academic Press, 1986.

[3] CASSELS, J. W. S. *An introduction to the geometry of numbers*. Springer Science & Business Media, 1996.

[4] HUNGERFORD, T. W. *Algebra*, vol. 73. Springer Science & Business Media, 2012.

[5] IRELAND, K., AND ROSEN, M. I. *A classical introduction to modern number theory*, vol. 84. Springer Science & Business Media, 1990.

[6] NEUKIRCH, J. *Algebraic Number Theory*, vol. 322. Springer Science & Business Media, 2013.

[7] SERRE, J.-P. *A course in arithmetic*, vol. 7. Springer Science & Business Media, 2012.

[8] STEWART, I., AND TALL, D. *Algebraic number theory and Fermat's last theorem*. AK Peters/CRC Press, 2001.

# Apêndice A

# Apêndice

## A.1 Caracteres de Dirichlet

Seja $G$ um grupo abeliano finito de ordem $m \in \mathbb{N}$, dizemos que $\chi : G \to \mathbb{C}$ é um *caractere* de $G$ se é um homomorfismo multiplicativo. Note que, pelo Teorema de Lagrange, se $g \in G$, então $g^m = 1$ e portanto $1 = \chi(g^m) = \chi(g)^m$, donde poderíamos ter tomado $\chi : G \to \mu_{\mathbb{C}}(m)$, em que $\mu_{\mathbb{C}}(m)$ é o grupo das $m$-ésimas raízes da unidade. Denotemos o conjunto dos caracteres de $G$ por $\mathfrak{X}(G)$. Como $\overline{\zeta} = \zeta^{-1}$, para qualquer $\zeta \in \mu_{\mathbb{C}}(m)$, $\overline{\chi} = \chi^{-1} \in \mathfrak{X}(G)$. Definimos $\chi_0 \in \mathfrak{X}(G)$ por $g \mapsto 1$ (chamado caractere trivial ou unitário) e, se $\chi_1, \chi_2 \in \mathfrak{X}(G)$, definimos $\chi_1\chi_2$ por $g \mapsto \chi_1(g)\chi_2(g)$. Com estas definições $\mathfrak{X}(G)$ torna-se um grupo abeliano. Queremos mostrar que, em geral $G \cong \mathfrak{X}(G)$. Isto, porém, é consequência de um Teorema mais geral, sobre a estrutura de grupos abelianos finitos. A sua prova não será apresentada aqui, mas pode sem encontrada em [4][Chapter II, pp.64-67, Structure Theorem for Finite Abelian groups].

**Teorema A.1.1.** *Todo grupo abeliano finito pode ser escrito como o produto direto de subgrupos cíclicos.*

Assim sendo, se $G = \prod_{i=1}^{r} \langle g_i \rangle$ e $m_i$ denota a ordem de $g_i$ (neste caso, referimo-nos ao menor inteiro positivo $k$ tal que $g_i^k = 1_{G_m}$, porém, no caso do subgrupo $\langle g_i \rangle$, $m_i$ também denota ordem do grupo), então $m_1 \dots m_r = m$. Visto que podemos escrever qualquer $g \in G$ como $\prod_{i=1}^{r} g_i^{e_i(g)}$, temos, portanto, um homomorfismo natural

$$\mathfrak{X} : \mathfrak{X}(G) \to \prod_{i=1}^{r} \mathfrak{X}(\langle g_i \rangle),\ \chi \mapsto (\chi|_{\langle g_1 \rangle}, \dots, \chi|_{\langle g_r \rangle}). \tag{A.1}$$

Afirmamos que $\mathfrak{X}$ é injetivo. De fato, se $\chi$ pertence ao núcleo de $\mathfrak{X}$, então $\chi|_{\langle g_i \rangle}$ também é o caractere trivial de $\mathfrak{X}(\langle g_i \rangle)$. Este último caractere é trivial se, e somente se, $\chi(g_i) = 1$, ou seja, $\chi$ é trivial. Agora, para cada subgrupo cíclico $\langle g_i \rangle$, seja $\chi_i$ um caractere em $\mathfrak{X}(\langle g_i \rangle)$. O caractere de $G$ dado por

$$\chi(g_1^{e_1} \cdots g_r^{e_r}) = \chi_1(g_1^{e_1}) \cdots \chi_r(g_r^{e_r})$$

é tal que $\chi|_{\langle g_i \rangle} = \chi_i$. Logo, $\mathfrak{X}$ é um isomorfismo. Por outro lado, se $\chi$ é o caractere de $\langle g_i \rangle$ definido por $\chi(g_i) = \zeta$, com $\zeta$ uma raiz $m_i$-ésima primitiva da unidade, e $\chi'$ é outro caractere de $\langle g_i \rangle$, então

$\chi'(g_i) = \zeta^q$, para algum inteiro $q$, donde $\chi' = \chi^q$ e $\mathfrak{X}(\langle g_i \rangle) = \langle \chi \rangle$. Logo, temos $\langle g_i \rangle \cong \mathfrak{X}(\langle g_i \rangle)$, donde

$$\mathfrak{X}(G) \cong \prod_{i=1}^{r} \mathfrak{X}(\langle g_i \rangle) \cong \prod_{i=1}^{r} \langle g_i \rangle = G.$$

Podemos tornar o Teorema A.1.1 explícito para o grupo $[\mathbb{Z}/m\mathbb{Z}]^*$.

**Definição A.1.1.** *Um caractere do grupo $\mathfrak{X}([\mathbb{Z}/m\mathbb{Z}]^*)$ é dito um caractere módulo $m$.*

**Proposição A.1.1.** *Seja $m = m_1 \dots m_r$, com $m_1, \dots, m_r$ inteiros positivos coprimos. Então cada caractere módulo $m$ é unicamente escrito na forma*

$$\chi(a) = \prod_{i=1}^{r} \chi_i(a_i),$$

*em que $\chi_i$ é um caractere módulo $m_i$, $a_i$ é determinado pelas congruências $a_i \equiv a \mod m_i$ e $a_i \equiv 1 \mod \dfrac{m}{m_i}$.*

Tendo em mente as ideias aqui expostas, esta proposição é uma consequência do Teorema Chinês dos restos, cuja prova omitiremos.

Seja agora $G$ um grupo abeliano finito de ordem $m$ e $H$ um subgrupo de ordem $n$. A restrição $\chi|_H$ de um caractere $\chi$ de $G$ define um caractere de $H$. A função $\mathcal{T}(\chi) = \chi|_H$ define um homomorfismo entre $\mathfrak{X}(G)$ e $\mathfrak{X}(H)$. Seja $A$ o núcleo deste homomorfismo. Se $\chi \in A$, então $\chi^*(xH) = \chi x$ define um caractere do grupo quociente $G/H$. Reciprocamente, se $\psi$ é um caractere de $G/H$, então, definindo $\chi x = \psi(xH)$, obtemos um caractere de $G$ tal que $\chi^* = \psi$. Se $\chi$ e $\chi'$ são caracteres distintos em $A$, $x \notin H$ e $\chi x \neq \chi' x$, então $\chi^*(xH) \neq \chi'^*(xH)$. Temos, portanto, que o número de caracteres de $A$ é igual ao número de caracteres de $G/H$, que é igual a $\dfrac{m}{n}$. Tendo em vista que $\mathfrak{X}(G)/A \cong \mathcal{T}(H)$, temos que $|\mathcal{T}(H)| = n = |H|$, portanto, todo caractere de $H$ é a restrição de algum caractere de $G$ a $H$. E mais:

**Teorema A.1.2.** *Se $G$ é um grupo abeliano finito e $H$ é um subgrupo de $G$, então qualquer caractere de $H$ pode ser estendido a um caractere de $G$ de $|G/H|$ formas diferentes.*

**Corolário A.1.1.** *Se $x$ é um elemento de $G$ diferente da identidade, então existe um caractere de $G$ tal que $\chi x \neq 1$.*

**Demonstração.** De fato, basta estender um caractere não-unitário do subgrupo $\langle x \rangle$. □

**Corolário A.1.2.** *Se o elemento $x$ do grupo $G$ não está contido no subgrupo $H$, então existe um caractere $\chi$ do grupo $G$ tal que $\chi x \neq 1$ e $\chi(z) = 1$, para $z \in H$.*

**Demonstração.** Com efeito, basta estender o caractere trivial de $H$ para um caractere não-trivial de $\langle x, H \rangle$ e, por fim, estender este último a um caractere de $G$. □

**Proposição A.1.2.** *Valem as fórmulas:*

*i)* $\sum_{x \in G} \chi x = \begin{cases} n, & \chi = \chi_0 \\ 0, & \chi \neq \chi_0. \end{cases}$

*ii)* $\sum_{\chi \in \mathfrak{X}(G)} \chi x = \begin{cases} n, & x = 1 \\ 0, & x \neq 1. \end{cases}$

**Demonstração.** Para o primeiro item, basta notar que, se $\chi \neq \chi_0$ e $\chi(z) \neq 1$, então

$$\sum_{x \in G} \chi x = \sum_{x \in G} \chi z x = \chi z \sum_{x \in G} \chi x \Rightarrow \sum_{x \in G} \chi x = 0.$$

Para o segundo item, basta tomar um caractere $\chi'$, tal que $\chi' x \neq 1$, e obter

$$\sum_{\chi \in \mathfrak{X}(G)} \chi x = \sum_{\chi \in \mathfrak{X}(G)} (\chi' \chi) x = \chi' x \sum_{\chi \in \mathfrak{X}(G)} \chi x \Rightarrow \sum_{\chi \in \mathfrak{X}(G)} \chi x = 0.$$

□

## A.2 Caracteres numéricos

Denotemos agora por $G_m$ o grupo $[\mathbb{Z}/m\mathbb{Z}]^*$. Podemos associar cada caractere de $G_m$ a uma função multiplicativa sobre os inteiros coprimos com $m$, definida por $\tilde{\chi}(a) = \chi\overline{a}$ ($\overline{a}$ denota a classe de $G_m$ que contém $a$). Estendemos esta função a todos os inteiros, simplesmente definindo $\tilde{\chi}(a) = 0$, caso $(a, m) > 1$. Tal extensão é dita um *caractere módulo* $m$. Por abuso de notação, utilizaremos a mesma notação tanto para o caractere de $G_m$, quanto para o caractere numérico dele derivado. Isto não há de causar nenhuma confusão, visto que distintos caracteres de $G_m$ induzem distintos caracteres numéricos módulo $m$.

Seja $m'$ um número natural divisível por $m$. Dizemos que um caractere numérico módulo $m'$ é *induzido* por um caractere numérico $\chi$ módulo $m$ se $\chi'(a) = \chi(a)$, para $(a, m) = 1$, e $\chi'(a) = 0$, se $(a, m) > 1$. Se $\chi$ é um caractere numérico módulo $m$ que não é induzido por um caractere numérico módulo um divisor próprio $d$ de $m$, então $\chi$ é dito *primitivo*.

**Lema A.2.1.** *Para que um caractere $\chi$ módulo $m$ seja primitivo, é necessário e suficiente que, para cada divisor próprio $d$, exista um inteiro $z$, tal que $(z, m) = 1$, $z \equiv 1 \mod d$ e $\chi(z) \neq 1$.*

**Demonstração.** Se $\chi$ não é primitivo, então é induzido por algum caractere $\chi_1$ módulo algum divisor próprio $d$ de $m$. Isto implica $\chi(a) = \chi_1(a)$, para todo $a$ coprimo com $m$. Em particular, para todo $x$ coprimo com $m$ com $x \equiv 1 \mod d$, temos que $\chi(x) = \chi_1(1) = 1$. Reciprocamente, suponhamos existir um divisor próprio $d$ de $m$ tal que todo inteiro $x$ que satisfaz $x \equiv 1 \mod d$ e $(x, m) = 1$ também satisfaz $\chi(x) = 1$. Primeiro, observamos que se $a'$ é tal que $(a', m) = 1$ e $a \equiv a' \mod d$, então $a' \equiv xa \mod m$, para algum $x$ coprimo com $m$. Como $x \equiv 1 \mod d$ e a hipótese nos diz que isso implica $\chi(x) = 1$, temos $\chi(a') = \chi(x)\chi(a) = \chi(a)$. Logo, está bem definido o caractere $\chi_1$ módulo $d$ dado por $\chi_1(a) = 0$, para $(a, m) > 1$ e $\chi_1(a) = \chi(a)$ para $(a, m) = 1$ e, portanto, $\chi$ é induzido por $\chi_1$, ou seja, $\chi$ não é primitivo.

□

## A.3 Somas gaussianas e caracteres especiais

Seja $\chi$ um caractere módulo $m$. Nesta seção, consideramos apenas caracteres numéricos. Seja $\zeta = \cos\dfrac{2\pi}{m} + i \sin\dfrac{2\pi}{m}$, a expressão

$$\tau_a(\chi) = \sum_{x \mod m} \chi(x)\zeta^{ax},$$

é chamada a *soma gaussiana* de $\chi$ com respeito a $a$. Quando tivermos $a = 1$, escrevemos apenas $\tau(\chi)$.

**Proposição A.3.1.** *Seja $\chi_1, \dots \chi_r$ a fatoração de $\chi$ obtida na Proposição A.1.1. A seguinte fórmula é válida*

$$\tau_a(\chi) = \tau_a(\chi_1) \dots \tau_a(\chi_r)\chi_1\left(\frac{m}{m_1}\right) \dots \chi_r\left(\frac{m}{m_r}\right),$$

*em que $\tau_a(\chi_i) = \sum_{x \mod m_i} \zeta_i^{ax}$, com $\zeta_i = \zeta^{\frac{m}{m_i}}$.*

**Demonstração.** Pelo Teorema Chinês dos Restos, podemos fazer corresponder bijetivamente a cada $x \in \mathbb{Z}/m\mathbb{Z}$ uma $r$-upla $(x_1, \dots, x_r)$, com $x_i \in \mathbb{Z}/m_i\mathbb{Z}$. Explicitamente, tomemos inteiros $k_i$ tais que

$$\frac{m}{m_i}k_i \equiv 1 \mod m_i,$$

basta tomar o mapa

$$(x_1, \dots, x_r) \mapsto \sum_{i=1}^{r} \frac{m}{m_i}k_i x_i \mod m.$$

Podemos então escrever

$$\sum_{x \mod m} \chi(x)\zeta^{ax} = \sum_{x_1 \mod m_1} \cdots \sum_{x_r \mod m_r} \prod_{i=1}^{r} \chi_i(x_i)\zeta^{a\sum_{j=1}^{r}\frac{m}{m_j}k_j x_j} = \tag{A.2}$$

$$\prod_{i=1}^{r}\left(\sum_{x_i \mod m_i} \chi_i(x_i)\zeta_i^{ak_i x_i}\right). \tag{A.3}$$

Substituindo $y_i = k_i x_i$ (abusaremos da notação, e escreveremos $k_i^{-1}$ para o inverso módulo $m$), obtemos

$$\sum_{x_i \mod m_i} \chi_i(x_i)\zeta_i^{ak_i x_i} = \sum_{x_i \mod m_i} \chi(k_i^{-1}y_i)\zeta_i^{ay_i} = \chi_i(k_i^{-1}) \sum_{y_i \mod m_i} \chi(y_i)\zeta_i^{ay_i} = \chi_i(k_i^{-1})\tau_a(\chi_i). \tag{A.4}$$

Pela escolha dos $k_i$'s, temos $k_i^{-1} \equiv \frac{m}{m_i} \mod m_i$. Logo, $\chi_i(k_i^{-1}) = \chi_i\left(\frac{m}{m_i}\right)$. Agrupando os termos de volta no produtório, temos o resultado provado. □

Consideremos o caractere módulo $4$ dado por $\chi(x) = (-1)^{\frac{x-1}{2}}$. Como o único divisor próprio de $4$ é $2$, e temos simultaneamente $(3, 2) = 1$ e $3 \equiv 1 \mod 2$, o Lema A.2.1 nos diz que $\chi$ é primitivo. Como só existem duas unidades módulo $4$, este é o único caractere primitivo módulo $4$ que existe. Semelhantes computações mostram que os caracteres

$$\chi'(x) = (-1)^{\frac{x^2-1}{8}} \text{ e } (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}}$$

são os únicos caracteres primitivos módulo $8$, pois $(-1)^{\frac{x-1}{2}}$ também define um caractere módulo $8$, e existem apenas $4$ unidades em $\mathbb{Z}/8\mathbb{Z}$. Estas considerações são úteis, em vista da

**Proposição A.3.2.** *Se existe um caractere quadrático ($\chi^2 = \chi_0$) primitivo módulo $m$, então $m$ é da forma $r$, $4r$ ou $8r$, com $r$ um inteiro livre de quadrados. Além disso, todo caractere quadrático primitivo será da forma*

*a)* $\chi(x) = \left(\frac{x}{r}\right)$, $(x, r) = 1$.

*b)* $\chi(x) = (-1)^{\frac{x-1}{2}}\left(\frac{x}{r}\right)$, $(x, 2r) = 1$.

*c)* $\chi(x) = (-1)^{\frac{x^2-1}{8}}\left(\frac{x}{r}\right)$, $(x, 2r) = 1$.

*d)* $\chi(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}}\left(\frac{x}{r}\right)$, $(x, 2r) = 1$.

**Demonstração.** Primeiramente, escrevamos $m$ na forma $2^a r$, com $r$ ímpar. Usando o Lema A.2.1, temos

$$\chi = \chi_a \chi_r,$$

com $\chi_a$ um caractere módulo $2^a$ e $\chi_r$ um caractere módulo $r$. Argumentando igualmente com $\chi_r$, temos

$$\chi_r = \chi_{p_i^{e_i}} \cdots \chi_{p_r^{e_r}}.$$

Necessitamos que $\chi_a$ e $\chi_r$ sejam também primitivos. De fato, se, por exemplo, tivermos $\chi_r$ induzido por algum caractere $\chi_d$ módulo um divisor próprio de $r$, então $\chi$ será induzido por $\chi_a\chi_d$, que é um caractere módulo $2^a d$. A mesma argumentação para $\chi_r$ nos diz que cada $\chi_{p_i^{e_i}}$ é primitivo também. Além disso, tanto $\chi_a$ quanto os $\chi_{p_i^{e_i}}$'s são quadráticos, em vista de $\chi$ o ser.

Seja $\chi'$ um caractere qualquer módulo uma potência de um primo ímpar $p^e$, com $e > 1$. O grupo das unidades de $\mathbb{Z}/p^e\mathbb{Z}$ tem $\varphi(p^e) = p^{e-1}(p-1)$ elementos. Seja $H$ o subgrupo determinado pelas classes de congruência módulo $p^e$ dos elementos de

$$\{x \in \mathbb{Z} |\ x^{p-1} \equiv 1 \mod p^e\}$$

e $\pi : H \to [\mathbb{Z}/p\mathbb{Z}]^*$ o homomorfismo redução módulo $p$. Se $\pi(x) = 1$, então, como $x \equiv 1 \mod p$, temos $x = 1 + kp$ (aqui estamos abusando da notação, e usando o mesmo símbolo para um inteiro e a sua classe de congruência). O binômio de Newton então nos dá

$$(1+kp)^{p-1} - 1 = \sum_{j=1}^{p-1} \binom{p-1}{n} k^j p^j.$$

Por outro lado, sendo $v_p : \mathbb{Z} - 0 \to \mathbb{N}$ a função que mede a maior potência (de expoente não-negativo) de $p$ que divide o argumento, temos

$$v_p((1+kp)^{p-1} - 1) \geq e,$$

pela definição de $H$. Por outro lado, na soma obtida para $(1+kp)^{p-1} - 1$, o termo que minimiza $v_p$ é aquele com $j = 1$, para o qual temos

$$v_p\left(\binom{p-1}{1} kp\right) = 1 + v_p(k).$$

Por outro lado, verifica-se $v_p(a+b) = \min\{v_p(a), v_p(b)\}$, se $v_p(a) \neq v_p(b)$. Portanto, temos

$$v_p((1+kp)^{p-1} - 1) = 1 + v_p(k).$$

Da nossa primeira desigualdade, obtemos $v_p(k) \geq e - 1$, que implica $x \equiv 1 \mod p^e$. Logo, $\pi$ é injetiva.

Por outro lado, se $x \in \mathbb{Z}$ é tal que $x^{p-1} \equiv 1 \mod p$, então existe $y \in \mathbb{Z}$, tal que $y \equiv x \mod p$ e $y^{p-1} \equiv 1 \mod p^e$. De fato, façamos a prova por indução no expoente, sendo $e = 1$ o caso trivial. Supondo que, para $k \geq 1$, temos $y_k \equiv x \mod p$ e $y_k^{p-1} \equiv 1 \mod p^k$, então, tomemos $y_{k+1} = y_k + tp^k$,

com $t$ inteiro. Expandindo pelo binômio de Newton. temos

$$y_{k+1}^{p-1} = \sum_{j=0}^{p-1} \binom{p-1}{j} y_k^{p-1-j} (tp^k)^j.$$

Quando $j \geq 2$, temos que $p^{2k} \geq p^{k+1}$ divide o termo correspondente na soma. Ou seja

$$y_{k+1}^{p-1} \equiv y_k^{p-1} + y_k^{p-2}(p-1)tp^k \mod p^{k+1}.$$

Para que $y_{k+1}^{p-1} \equiv 1 \mod p^{k+1}$, devemos ter

$$p^{k+1} | [(y_k^{p-1} + (p-1)y_k^{p-2}tp^k) - 1].$$

Por hipótese de indução, $y_k^{p-1} \equiv 1 \mod p^k$, donde $y_k^{p-1} - 1 = p^k M$, com $M$ inteiro. Portanto, a relação que queremos se reescreve como

$$p^{k+1} | [p^k M + (p-1)y_k^{p-2}p^k t].$$

Para isto ser verdade, basta que $(p-1)y_k^{p-2}t \equiv -M \mod p$. Como esta última congruência pode ser resolvida em $t$, temos provada a nossa afirmação.

Portanto, a imagem de $\pi$ coincide com conjunto dos elementos de $[\mathbb{Z}/p\mathbb{Z}]^*$ que satisfazem a equação $x^{p-1} - 1 = 0$, que é o próprio grupo $[\mathbb{Z}/p\mathbb{Z}]^*$, logo, $\pi$ é um isomorfismo. Escrevendo $[\mathbb{Z}/p^e\mathbb{Z}]^* \cong H \times [\mathbb{Z}/p^e\mathbb{Z}]^*/H \cong [\mathbb{Z}/p\mathbb{Z}]^* \times [\mathbb{Z}/p^e\mathbb{Z}]^*/H = [\mathbb{Z}/p\mathbb{Z}]^* \times U$ temos que $\chi$ se escreve como $\tilde{\chi}\chi_U$, em que $\tilde{\chi}$ é um caractere módulo $p$. Como $\chi$ é quadrático, temos que $\chi_U$ precisa ser unitário; pois $|U| = p^{e-1}$ e, portanto, a imagem de um homomorfismo de $\chi_U$ a um grupo de ordem $2$ precisa ser apenas $1$, donde $\chi$ é unicamente determinado pela sua restrição a $H$ e, portanto, $\chi(x)$ é unicamente determinado pela classe de $x$ módulo $p$, e $\chi$ não pode ser primitivo. Como as nossas hipóteses implicam que cada $\chi_{p_i^{e_i}}$ é primitivo, temos $e_i = 1$. Como o único caractere quadrático não-unitário módulo um primo ímpar é o Símbolo de Legendre, temos $\chi_{p_i} = \left(\frac{\cdot}{p_i}\right)$. Concluímos então que o produto dos $\chi_{p_i}$ é, por definição, o Símbolo de Jacobi $\left(\frac{\cdot}{r}\right)$.

Para $\chi_a$, queremos que $a$ não possa ser maior que $3$. Afirmamos que, para qualquer inteiro $u$ tal que $u \equiv 1 \mod 8$ e $d = 2^e$, com $e > 3$, existe um inteiro $v$, tal que $u \equiv v^2 \mod d$. A prova desta afirmação seguirá por indução. Para $e = 4$, isso pode ser feito por computação explícita, visto que os inteiros congruentes a $1$ módulo $8$ são $1$ ou $9$ módulo $16$, que são quadrados. Suponhamos o resultado válido para $k \geq 4$. Por hipótese de indução, podemos escrever

$$u = v_k^2 + C2^k,$$

para $C$ inteiro. Queremos encontrar um inteiro $t$ tal que $v_{k+1} = v_k + t2^{k-1}$ satisfaça $v_{k+1}^2 \equiv u \mod 2^{k+1}$. Temos

$$v_{k+1}^2 = v_k^2 + t2^k v_k + t^2 2^{2k-2}.$$

Como $k \geq 4$, temos $2k - 2 \geq k + 1$ e, portanto, $t^2 2^{2k-2}$ é divisível por $2^{k+1}$. Daí, temos

$$v_{k+1}^2 \equiv v_k^2 + t2^k v_k \mod 2^{k+1}.$$

Daí, a congruência que queremos satisfeita é

$$v_k^2 + t2^k v_k \equiv v_k^2 + C2^k \mod 2^{k+1},$$

para a qual basta $tv_k = C \mod 2$. Como $v_k$ é necessariamente ímpar, podemos tomar $t = C$, e teremos $v_k^2 \equiv u \mod 2^{k+1}$.

Tendo provada esta afirmação, como $\chi_a$ é um caractere quadrático módulo $2^a$, ele não pode ser primitivo, visto que, se $u \equiv 1 \mod 8$, então (mais uma vez, abusando da notação ) $\chi_a(u) = \chi_a(v^2) = 1$. Daí, se $x \equiv y \mod 8$, então $\chi_a(x) = \chi_a(ty) = \chi(y)$, com $t \equiv 1 \mod 8$. Portanto, cada caractere quadrático módulo $2^a$, com $a > 3$, depende apenas da sua redução módulo $8$. □