Universidade de São Paulo
Instituto de Matemática e Estatística
Bacharelado em Matemática

Teoria Algébrica dos Números e Introdução à Teoria dos Corpos de Classes

Lorenzo Andreaus

Trabalho de Conclusão de Curso
MAT0148 – Introdução ao Trabalho Científico

Comissão Julgadora: Vitor de Oliveira Ferreira – IME-USP (Orientador)
Lucia Satie Ikemoto Murakami – IME-USP
Leila Maria Vasconcellos Figueiredo – IME-USP

São Paulo
2021

Agradecimentos

Gostaria de agradecer aos meus professores e orientadores, Lucia Satie Ikemoto Murakami e Vitor de Oliveira Ferreira, que não só me orientaram nesse trabalho como também ao longo de todo o meu curso, e que foram fundamentais para o meu crescimento matemático ao longo de todos esses quatro anos.

Gostaria de agradecer ainda a todos os meus amigos e professores, em especial aos meus amigos Gabriel Bassan, Lucas Seidy, Ricardo Canesin e Thiago Landim, que participaram das minhas apresentações semanais deste trabalho, e sempre me ajudaram a resolver os problemas que surgiram ao longo da confecção destas páginas. Nesse sentido, gostaria de agradecer ainda ao Gabriel Ribeiro, que me ajudou muito com as questões que surgiram especialmente no final dessa monografia.

Agradeço também à Tia Aninha e ao Tio Victor, que me acolheram com muito amor durante a minha estadia em São Paulo.

Finalmente, gostaria de agradecer à minha família, especialmente aos meus pais Lara e Jürgen e à minha irmã Lia, que sempre me apoiaram durante toda a minha vida e fizeram que este trabalho fosse possível.

Resumo

ANDREAUS, L. **Teoria Algébrica dos Números e Introdução à Teoria dos Corpos de Classes**. 2021. 222 p. Monografia – Bacharelado em Matemática – Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, Brasil.

Nesse trabalho, nós estudamos as bases da Teoria Algébrica dos Números, a área da matemática que estuda os anéis de inteiros algébricos. Nós estudamos a demonstração de resultados como o Teorema da Finitude do Número de Classes, a Identidade Fundamental, o Teorema das Unidades de Dirichlet e o Teorema de Kronecker-Weber, e abordamos assuntos como domínios de Dedekind, valorações e números p-ádicos. Além disso, mostramos como aplicar a teoria em alguns exemplos concretos, e damos uma breve introdução à Teoria dos Corpos de Classes.

Palavras-chave: Teoria dos Números, Teoria Algébrica dos Números, Teoria Algébrica dos Números e Introdução à Teoria dos Corpos de Classes

Abstract

ANDREAUS, L. **Algebraic Number Theory and a Introduction to Class Field Theory**. 2021. 222 p. Monografia – Bacharelado em Matemática – Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, Brazil.

In this work, we study the basis of Algebraic Number Theory, the area of mathematics that studies the rings of algebraic integers. We studied the demonstration of results such as the Theorem of the Finiteness of the Class Number, the Fundamental Identity, Dirichlet's Unit Theorem and Kronecker-Weber Theorem, and we adress subjects such as Dedekind domains, valuations and p-adic numbers. Furthermore, we show how to apply the theory in concrete examples, and we give a brief introduction to Class Field Theory.

Keywords: Number Theory, Algebraic Number Theory, Algebraic Number Theory and a Introduction to Class Field Theory

Sumário

Notações

$\lvert X\rvert$	Cardinalidade do conjunto X
$X \sqcup Y$	União disjunta dos conjuntos X e Y
$\mathbb{N}$	Conjunto dos números naturais: $\{0, 1, 2, \ldots\}$
$\mathbb{N}^*$	Conjunto dos números naturais sem o 0: $\{1, 2, \ldots\}$
$\mathbb{Z}$	Anel dos números inteiros: $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Q}$	Corpo dos números racionais
$\mathbb{R}$	Corpo dos números reais
$\mathbb{C}$	Corpo dos números complexos
$\overline{\mathbb{Q}}$	Corpo dos números algébricos
$\mathcal{O}_{\mathbb{C}}$	Anel dos inteiros algébricos
$\mathcal{O}_K$	Anel de inteiros algébricos do corpo K
$\mathbb{F}_q$	Corpo finito de q elementos
$\mathbb{Z}_p$	Anel dos inteiros p-ádicos
$\mathbb{Z}_{(p)}$	Localização de $\mathbb{Z}$ pelo ideal primo $p\,\mathbb{Z}$
$\mathbb{Q}_p$	Corpo dos números p-ádicos
$\mathcal{D}$	Conjunto dos inteiros livres de quadrados e diferentes de 0 e 1
$A[x_1, \ldots, x_n]$	Anel de polinômios do anel A em n variáveis
$A[\gamma_1, \ldots, \gamma_n]$	Menor anel que contém A e todos os elementos $\gamma_1, \ldots, \gamma_n$
$K(x_1, \ldots, x_n)$	Corpo de funções racionais do corpo K em n variáveis
$K(\gamma_1, \ldots, \gamma_n)$	Menor corpo que contém K e todos os elementos $\gamma_1, \ldots, \gamma_n$
$A[\![x]\!]$	Anel das séries formais sobre o anel A
$K(\!(x)\!)$	Corpo das séries de Laurent sobre o corpo K
$Q(A)$	Corpo de frações do domínio A
$A^\times$	Grupo de unidades do anel A
$S^{-1}A$	Localização do anel A pelo conjunto multiplicativo $S \subseteq A$

$A_{\mathfrak{p}}$	Localização do anel A por $S = A \setminus \mathfrak{p}$, onde $\mathfrak{p}$ é ideal primo de A
$\overline{A}^B$	Fecho integral de A no anel B
$X \oplus Y$	Soma direta das estruturas X e Y
$X + Y$	Soma de X e Y dentro de uma estrutura maior
X/Y	Quociente da estrutura X por Y ou indicação de extensão de anéis
$X \times Y$	Produto direto externo das estruturas X e Y
$G \odot H$	Produto direto interno dos subgrupos G e H
$X \otimes_Z Y$	Produto tensorial das Z-estruturas X e Y
δ_{ij}	Função delta de Kronecker
(a_{ij})	Matriz com entradas a_{ij}
Id	Matriz identidade
$\det B$	Determinante da(o) matriz/operador B
$\operatorname{Tr} B$	Traço da(o) matriz/operador B
$\operatorname{Adj} B$	Matriz adjunta da matriz B
$\binom{n}{k}$	n escolhe k
$\left(\frac{m}{n}\right)$	Símbolo de Legendre/Jacobi de m e n
$\lfloor x \rfloor$	Piso (parte inteira) de x
$\lceil x \rceil$	Teto de x
$\mathfrak{a} \lhd A$	$\mathfrak{a}$ é ideal do anel A
xA	Ideal de A gerado por x
xM	Submódulo de M gerado por x
$\langle x_1, \ldots, x_n \rangle$	Subgrupo/ideal gerado por $x_1, \ldots, x_n$
$N \lhd G$	N é subgrupo normal do grupo G
$m \mid n$	m divide n (em determinado anel)
$\operatorname{Hom}_A(M, N)$	Conjunto dos homomorfismos de A-módulos/álgebras $\varphi\colon M \to N$
$\operatorname{End}_A(M)$	Conjunto dos endomorfismos de A-módulos/álgebras $\varphi\colon M \to M$
id	Operador de identidade
f'	Derivada da função f
$\int f(x)\,dx$	Integral da função f
∂f	Grau do polinômio f

$\dim_K V$	Dimensão de V como K-espaço vetorial
$[X : Y]$	Dimensão de uma extensão de corpos ou índice de subgrupo
$\mathrm{Gal}(L/K)$	Grupo de Galois da extensão L/K
$P_{\alpha,K}$	Polinômio minimal de α sobre o corpo K
$F_{b,B/A}$	Polinômio característico de b em relação à extensão B/A
$\mathrm{Tr}_{B/A}$	Traço da extensão B/A
$N_{B/A}$	Norma da extensão B/A
$\Delta(f)$	Discriminante do polinômio f
$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n)$	Discriminante da n-upla $(\alpha_1, \ldots, \alpha_n)$ em relação à extensão L/K
$\mathfrak{A} \mid \mathfrak{a}$	O ideal $\mathfrak{A}$ está sobre $\mathfrak{a}$
$\mathfrak{d}_{R/A}$	Ideal discriminante de R/A
d_K	Discriminante do corpo K
$W(A)$	Grupo de torção do anel A
$W_n(A)$	Grupo das raízes n-ésimas da unidade do anel A
$\mathscr{P}_n(A)$	Grupo das raízes primitivas n-ésimas da unidade do anel A
$\varphi(n)$	Função de Euler aplicada em n
ζ_n	Raiz primitiva n-ésima da unidade
Φ_n	n-ésimo polinômio ciclotômico
$Z(G)$	Centro do grupo G
$\mathscr{M}(A)$	Conjunto dos A-submódulos não-nulos de $Q(A)$
$I(A)$	Conjunto dos ideais fracionários de A
$\mathscr{J}(A)$	Conjunto dos ideais não-nulos de A
$\mathscr{P}(A)$	Conjunto dos ideais primos não-nulos de A
$P(A)$	Conjunto dos ideais fracionários principais de A
$J(A)$	Conjunto dos ideais fracionários inversíveis de A ou ideal de Jacobson de A
$\mathrm{Pic}(A)$	Grupo de Picard de A
$\mathscr{C}\ell(A)$	Grupo de classes de ideais de A
h_A	Número de classes do ideal A
h_K	Número de classes de $\mathcal{O}_K$
$(A : M)$	Quociente do A-submódulo M
$M \mid N$	O ideal fracionário M divide o ideal fracionário N

$\mathcal{O}_v$	Anel de valoração da valoração v
$U^{(n)}$	n-ésimo grupo de unidades
$\mathfrak{N}(\mathfrak{a})$	Norma do ideal $\mathfrak{a}$
μ_K	Cota de Minkowski do corpo K
$e(\mathfrak{P} \mid \mathfrak{p}) = e_{\mathfrak{P}}$	Índice de ramificação de $\mathfrak{P}$
$f(\mathfrak{P} \mid \mathfrak{p}) = f_{\mathfrak{P}}$	Grau de inércia de $\mathfrak{P}$
$g(\mathfrak{P} \mid \mathfrak{p}) = g_{\mathfrak{p}}$	Número de decomposição de $\mathfrak{p}$
$\mathrm{RQ}(n)$	Conjunto dos resíduos quadráticos módulo n
χ_K	Caráter quadrático do corpo quadrático K
$G_{\mathfrak{P}}$ ou $G_{\mathfrak{P}}(L/K)$	Grupo de decomposição do ideal primo $\mathfrak{P}$
$Z_{\mathfrak{P}}$ ou $Z_{\mathfrak{P}}(L/K)$	Corpo de decomposição do ideal primo $\mathfrak{P}$
$I_{\mathfrak{P}}$ ou $I_{\mathfrak{P}}(L/K)$	Grupo de inércia do ideal primo $\mathfrak{P}$
$T_{\mathfrak{P}}$ ou $T_{\mathfrak{P}}(L/K)$	Corpo de inércia do ideal primo $\mathfrak{P}$
$R^i_{\mathfrak{P}}$ ou $R^i_{\mathfrak{P}}(L/K)$	i-ésimo grupo de ramificação do ideal primo $\mathfrak{P}$
$V^i_{\mathfrak{P}}$ ou $V^i_{\mathfrak{P}}(L/K)$	i-ésimo corpo de ramificação do ideal primo $\mathfrak{P}$
$\langle x, y \rangle$	Produto interno dos vetores x e y
$\|x\|$	Norma do vetor x
$B_r(x)$	Bola de centro x e raio r
B_r	Bola de centro 0 e raio r
$\mathrm{vol}(S)$	Volume do conjunto/reticulado S
$K_{\mathbb{R}}$	Espaço de Minkowski do corpo K
$\tilde{A}$	Normalização de A
$\mathrm{Div}(A)$	Grupo dos divisores de A
$\ell_A(M)$	Comprimento do A-módulo M
$\mathcal{P}(A)$	Grupo dos divisores principais
$CH^1(A)$	Grupo de Chow de A
$\hat{K}$	Completamento de um corpo com valor absoluto K
$v_{\mathfrak{p}}$	Valoração $\mathfrak{p}$-ádica
$\|\cdot\|_{\mathfrak{p}}$	Valor absoluto $\mathfrak{p}$-ádico
$\varprojlim_n A/\mathfrak{p}^n$	Limite projetivo dos $A/\mathfrak{p}^n$

$\lvert\cdot\rvert_\infty$	Valor absoluto usual de $\mathbb{Q}$
$e(L \mid K)$ ou $e(w \mid v)$	Índice de ramificação da extensão de corpos com valoração $(L,w)/(K,v)$
K_v	Completamento de (K,v)
$f(L \mid K)$ ou $f(w \mid v)$	Grau de inércia da extensão de corpos com valoração $(L,w)/(K,v)$
$K_\mathfrak{p}$	Completamento de $(K,v_\mathfrak{p})$
G_w ou $G_w(L/K)$	Grupo de decomposição de $w \mid v$
Z_w ou $Z_w(L/K)$	Corpo de decomposição de $w \mid v$
I_w ou $I_w(L/K)$	Grupo de inércia de $w \mid v$
T_w ou $T_w(L/K)$	Corpo de inércia de $w \mid v$
R_w ou $R_w(L/K)$	Grupo de ramificação de $w \mid v$
V_w ou $V_w(L/K)$	Corpo de ramificação de $w \mid v$
G_w ou $G_w(L/K)$	Grupo de decomposição de $w \mid v$
K^v	Henselianização de (K,v)
K^{nr}	Extensão não-ramificada maximal do corpo K
$\overline{K}_s$	Fecho separável do corpo K
$\mathrm{ord}_\alpha(f)$	Ordem de f no ponto $\alpha \in \mathbb{C}$
$\mathbb{A}_K$	Anel de adèles de K
$\mathbb{I}_K$	Grupo de Idèles de K
C_K	Grupo de classes de idèles de K
$\mathfrak{A}_K^1$	Subgrupo dos elementos de I_K com norma 1
C_1^K	$\mathfrak{A}_K^1 \,/K^\times$
$\sigma_\mathfrak{P}$ ou $\left(\frac{L/K}{\mathfrak{P}}\right)$	Elemento de Frobenius de $\mathfrak{P}$
$\mathrm{Frob}_\mathfrak{p}$	Classe de Frobenius de $\mathfrak{p}$
$\sigma_\mathfrak{p}$ ou $\left(\frac{L/K}{\mathfrak{p}}\right)$	Elemento de Frobenius de $\mathfrak{p}$
$\left(\frac{L/K}{\cdot}\right)$	Mapa de Artin

Introdução

A Teoria dos Números é o ramo da matemática que estuda os números inteiros e suas propriedades. Um dos principais interesses de estudo dessa área são as **equações diofantinas**. Uma equação diofantina é simplesmente uma equação polinomial em que só interessam as soluções inteiras. Enquanto não há grande dificuldade em resolver um sistema linear de equações diofantinas, problemas começam a surgir quando aparecem equações de graus maiores. Consideremos os seguintes exemplos:

Fixado n inteiro positivo, a equação diofantina $x^2 - y^2 = n$ não oferece grandes dificuldades, pois podemos fatorar o lado esquerdo para obter $(x-y)(x+y) = n$. Utilizando o Teorema Fundamental da Aritmética, conseguimos encontrar todas as formas de escrever n como produto de dois inteiros. Assim, podemos achar todas as soluções $(x, y) \in \mathbb{Z}^2$ dessa equação diofantina, resolvendo um número finito de sistemas lineares de duas equações. Esse exemplo nos mostra que fatorar pode ajudar muito na resolução de equações diofantinas.

Alterando apenas um pouco essa equação, já aparecem dificuldades: a equação diofantina $x^2 + y^2 = n$ é bem mais difícil de lidar, pois não conseguimos fatorar o lado esquerdo em $\mathbb{Z}$. No entanto, o lado esquerdo se fatora em $\mathbb{Z}[i]$: $x^2 + y^2 = (x+iy)(x-iy)$. Assim, nada mais natural do que estudar esse anel maior, e torcer para que ele seja "bem-comportado" que nem o anel $\mathbb{Z}$. De fato, como veremos, esse anel é um domínio euclidiano. O anel $\mathbb{Z}[i]$ é chamado de **anel dos inteiros de Gauss**, ou ainda de **anel dos inteiros gaussianos**, e ocupa dentro do corpo $\mathbb{Q}(i)$ um papel parecido com o de $\mathbb{Z}$ dentro de $\mathbb{Q}$.

O exemplo acima nos mostra que, para o estudo de equações diofantinas, convém estudar anéis maiores que $\mathbb{Z}$, os chamados **anéis de inteiros algébricos**. O estudo da estrutura desses anéis, isto é, de seus ideais, grupos de unidades, etc., é o principal tema de interesse da **Teoria Algébrica dos Números**.

Infelizmente, nem tudo são flores: há anéis de inteiros algébricos como $\mathbb{Z}[\sqrt{-5}]$ que não são nem sequer um domínio de fatoração única. Podemos tentar corrigir isso olhando para os ideais desses anéis, ao invés de seus elementos. De fato, há um teorema de unicidade da fatoração de ideais em um tipo especial de domínio chamado **domínio de Dedekind**, o que é o caso de $\mathbb{Z}[\sqrt{-5}]$ e, na verdade, de qualquer anel de inteiros algébricos!

O objetivo deste trabalho é dar ao leitor uma introdução às bases da Teoria Algébrica dos Números, começando desde a definição de extensão integral, no Capítulo 1, até a demonstração do importante Teorema de Kronecker-Weber, no Capítulo 11. Esse teorema e as estratégias utilizadas em sua demonstração motivam o estudo de "coisas locais" para provar "coisas globais", o **Princípio Local-Global**. Esse é o princípio básico que rege a chamada **Teoria dos Corpos de Classes**, à qual damos uma breve introdução no Capítulo 12.

Para uma boa compreensão deste trabalho, é indicado ao leitor um conhecimento básico de álgebra linear, álgebra comutativa, teoria dos grupos e teoria de Galois, ao longo de todo o texto. Além disso, em alguns capítulos são utilizados resultados básicos de análise, topologia, espaços métricos e teoria de integração.

A próxima página traz um resumo dos assuntos abordados em cada um dos 12 capítulos que compõem esse texto:

- O Capítulo 1 trata de extensões de anéis, e é mais técnico, apresentando diversos resultados que serão úteis em todo o texto.
- No Capítulo 2, são definidos os nossos principais objetos de estudo, os **anéis de inteiros algébricos**, e são demonstradas suas propriedades básicas. Além disso, são estudados com mais detalhes os anéis de inteiros algébricos de **corpos quadráticos** e **ciclotômicos**.
- O Capítulo 3, novamente mais técnico, trata dos **domínios de Dedekind** e dos **domínios de valoração discreta**, dois tipos importantes de domínios com propriedades muito boas: a **fatoração única de ideais** no caso dos domínios de Dedekind, e a existência de uma **valoração discreta**, no caso dos domínios de valoração discreta.
- O Capítulo 4 estuda como se comportam as extensões de domínios de Dedekind. Mais especificamente, estuda como um ideal primo se decompõe nessa extensão. Como veremos, essa decomposição está sujeita a uma regra rígida, a **identidade fundamental**, e pode ser determinada explicitamente em **extensões monogêneas**. Nesse capítulo, mostraremos ainda a **finitude do número de classes**, que em certo sentido diz que um anel de inteiros algébricos está "perto" de ser um domínio de ideais principais.
- O Capítulo 5 traz exemplos práticos dos resultados obtidos no Capítulo 4 para corpos quadráticos e ciclotômicos. Como caminho para estudar corpos quadráticos, ele também aborda a famosa **Lei da Reciprocidade Quadrática**.
- O Capítulo 6 estuda as extensões galoisianas de domínios de Dedekind. Nele, mostra-se que toda extensão desse tipo pode ser quebrada em extensões mais simples de serem estudadas.
- No Capítulo 7, mostra-se a importância do **método geométrico**, que se utiliza de técnicas de integração para obter resultados de Teoria Algébrica dos Números. Nele, demonstra-se o **Teorema das Unidades de Dirichlet**. Além disso, obtêm-se a **cota de Minkowski**, que facilita o cálculo do número de classes.
- O Capítulo 8 trata das **ordens**, um tipo de anel que não se comporta tão bem quanto os anéis de inteiros algébricos mas também é importante na prática.
- No Capítulo 9, são definidos os conceitos de **valor absoluto**, **valoração** e **completamento**, e demonstradas suas propriedades básicas. Além disso, são estudados os **números p-ádicos**. Esse capítulo em certo sentido demarca o começo da "Parte 2" do trabalho.
- O Capítulo 10 estuda como valores absolutos e valorações podem ser estendidos em extensões algébricas. Nele, mostra-se a unicidade dessas extensões para **corpos completos** e **corpos henselianos**, além do **Teorema da Extensão** que diz o que ocorre em extensões finitas. Nesse capítulo também são estudadas as **ramificações** em extensões de corpos henselianos, que são em certo sentido uma medida de quão bem uma extensão se comporta.
- O Capítulo 11 é focado na demonstração do importante **Teorema de Kronecker-Weber**, que diz que toda extensão abeliana de $\mathbb{Q}$ está contida em uma extensão ciclotômica. Tão importante quanto esse teorema é a técnica utilizada em demonstração: provar algo difícil e "global" separando em coisas mais fáceis e "locais".
- No Capítulo 12, é feita uma breve introdução à **Teoria dos Corpos de Classes**, que estuda os **corpos globais** e os **corpos locais**, e possui diversas consequências em Teoria dos Números.

Este trabalho utilizou como principais referências os livros [1] e [2]. Além disso, [3] foi bastante utilizado, especialmente a partir do Capítulo 9. O Capítulo 11 teve como base [3], [7], [8] e [9], e o Capítulo 12 teve como base [11]. Além disso, [4], [5], [6], [10], [12], [13], [14], [15], [16], [17] e [18] foram usados como referências auxiliares.

Capítulo 1

Extensões de Anéis

Nesse capítulo, iremos apresentar os conceitos básicos e enunciar e provar os resultados básicos de extensões de anéis, construindo o maquinário que será aplicado aos anéis de inteiros algébricos no próximo capítulo. Ao longo de todo o trabalho, a palavra **anel** sempre se referirá a um anel comutativo com unidade, a menos que especificado o contrário. Além disso, dados A um anel, M um A-módulo, $p(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ e $\varphi \in \mathrm{End}_A(M)$, definimos $p(\varphi) \in \mathrm{End}_A(M)$ por $p(\varphi)(m) := a_0m + a_1\varphi(m) + \cdots + a_n\varphi^n(m)$, onde φ^i denota a composição de φ consigo mesmo i vezes.

1.1. Alguns Resultados sobre Módulos

Começamos provando um importante resultado que generaliza o Teorema de Cayley-Hamilton para módulos finitamente gerados:

Teorema 1.1 (Teorema de Cayley-Hamilton Generalizado)**.** *Sejam A um anel, M um A-módulo finitamente gerado, $\mathfrak{a} \lhd A$ e $\varphi : M \to M$ um homomorfismo de A-módulos tal que $\varphi(M) \subseteq \mathfrak{a}M$.*

Então existe um polinômio mônico

$$\chi(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x] \text{ com } a_0, a_1, \ldots, a_{n-1} \in \mathfrak{a},$$

tal que

$$\chi(\varphi) = \varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_1\varphi + a_0\,\mathrm{id} \in \mathrm{End}_A(M)$$

é o homomorfismo nulo.

A ideia da prova deste teorema é que podemos enxergar M como um $A[x]$ módulo a partir do endomorfismo φ:

Lema 1.2. *Sejam A um anel, M um A-módulo e $\varphi \in \mathrm{End}_A(M)$. Então M é um $A[x]$-módulo com ação dada por $p(x) \cdot m = p(\varphi)(m)$, para todos $p(x) \in A[x]$, $m \in M$.*

A demonstração desse lema é um exercício simples.

Demonstração (do Teorema de Cayley-Hamilton Generalizado): Seja $\{m_1, \ldots, m_n\}$ um conjunto de geradores de M. Então é fácil ver que esses elementos também geram $\mathfrak{a}M$, utilizando apenas coeficientes em $\mathfrak{a}$. Assim, para $1 \leq i \leq n$, podemos escrever

$$\varphi(m_i) = a_{i1}m_1 + \cdots + a_{in}m_n, \text{ para } a_{i1}, \ldots, a_{in} \in \mathfrak{a}.$$

Agora, pelo Lema 1.2, podemos ver M como um $A[x]$-módulo com ação $p(x)\cdot m = p(\varphi)(m)$. Desse modo, $\varphi(m_i) = x\cdot m_i$, e a equação acima equivale a $x\cdot m_i = a_{i1}m_1 + \cdots + a_{in}m_n$, ou ainda

$$\sum_{j=1}^{n}(x\cdot\delta_{ij} - a_{ij})m_j = 0,$$

onde δ_{ij} é o Delta de Kronecker. Mas isso significa que

$$\begin{bmatrix} x-a_{11} & -a_{12} & -a_{13} & \dots & -a_{1n} \\ -a_{21} & x-a_{22} & -a_{23} & \dots & -a_{2n} \\ -a_{31} & -a_{32} & x-a_{33} & \dots & -a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & -a_{n3} & \dots & x-a_{nn} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Chamemos de $B = (x\cdot\delta_{ij} - a_{ij}) \in M_n(A[x])$ a matriz $n\times n$ acima. Multiplicando a equação acima à esquerda pela matriz adjunta de B, temos:

$$(\operatorname{Adj} B)\cdot B\cdot \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad\Rightarrow\quad (\det B)\cdot \operatorname{Id}\cdot \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\Rightarrow \quad \begin{bmatrix} (\det B)\cdot m_1 \\ (\det B)\cdot m_2 \\ \vdots \\ (\det B)\cdot m_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Assim, para $1\le i\le n$, $(\det B)(\varphi)(m_i) = (\det B)\cdot m_i = 0$, de modo que $(\det B)(\varphi)$ se anula em todos os geradores m_i de M. Logo $(\det B)(\varphi)$ é o homomorfismo nulo. Além disso, $\det B$ é um polinômio mônico. Portanto, basta tomarmos $\chi = \det B$, e temos o resultado desejado. □

Corolário 1.3. *Sejam A um anel, M um A-módulo finitamente gerado e $\mathfrak{a}\lhd A$ com $\mathfrak{a}M = M$. Então existe $a\in\mathfrak{a}$ tal que $am = m$ para todo $m\in M$.*

Demonstração. Nessas condições, podemos aplicar o Teorema 1.1 para $\varphi = \mathrm{id}$. Desse modo, garantimos a existência de $a_0, a_1, \dots, a_{n-1}\in\mathfrak{a}$ tais que $a_0\,\mathrm{id} + a_1\,\mathrm{id} + \cdots + a_{n-1}\,\mathrm{id}^{n-1} + \mathrm{id}^n = 0$. Ou seja, $(a_0 + a_1 + \cdots + a_{n-1} + 1)m = 0$ para todo $m\in M$. Tomando $a = -a_0 - a_1 - \cdots - a_{n-1}\in\mathfrak{a}$, vemos que $am = m$ para todo $m\in M$, como queríamos. □

Lembremos que a interseção de todos os ideais maximais de um anel A é um ideal $J(A)$, chamado de **ideal de Jacobson** de A. Além disso, lembremos que dado $x\in A$ nós temos a equivalência $x\in J(A) \iff 1-ax\in A^\times$ para todo $a\in A$.

Como corolário do corolário acima, nós obtemos o Lema de Nakayama para anéis comutativos:

Lema 1.4 (Lema de Nakayama)**.** *Sejam A um anel e $\mathfrak{a}\lhd A$. Então são equivalentes:*

(i) $\mathfrak{a}\subseteq J(R)$.

(ii) Para todo A-módulo finitamente gerado M, $\mathfrak{a}M = M \Rightarrow M = 0$.

(iii) Para todos A-módulos $N\subseteq M$ tais que M/N é finitamente gerado,

$$M = \mathfrak{a}M + N \Rightarrow N = M.$$

Demonstração. $(i) \Rightarrow (ii)$: Pelo Corolário 1.3, se $\mathfrak{a}M = M$ existe $a \in \mathfrak{a}$ tal que $am = m$ para todo $m \in M$. Mas então $(1-a)m = 0$. Como $a \in \mathfrak{a} \subseteq J(A)$, $1-a \in A^\times$ e portanto $m = 0$ para todo $m \in M$, ou seja, $M = 0$.

$(ii) \Rightarrow (iii)$: Nós temos $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N = M/N$, por hipótese. Aplicando (ii), concluímos que $M/N = 0$, ou seja, $N = M$.

$(iii) \Rightarrow (i)$: Se $\mathfrak{a} \not\subseteq J(A)$, então existe um ideal maximal $\mathfrak{m} \lhd A$ tal que $\mathfrak{a} \not\subseteq \mathfrak{m}$. Sendo $\mathfrak{m}$ maximal, temos $\mathfrak{a} + \mathfrak{m} = A$, o que é o mesmo que dizer que $\mathfrak{a}A + \mathfrak{m} = A$. Como $\mathfrak{m} \subsetneq A$, mostramos que nesse caso não vale (iii). □

1.2. Extensões de Anéis

Nessa seção, começamos estudando propriamente as extensões de anéis. Como veremos, o tipo mais importante de extensão de anéis para nós serão as extensões integrais.

Definição (Extensão de Anéis/Extensão Finita)**.** Dizemos que o anel B é uma **extensão** do anel A se A for um subanel de B. Indicaremos essa extensão por B/A. Dizemos que B é uma **extensão finita** de A se B for finitamente gerado como A-módulo.

Começamos listando dois resultados técnicos que nos serão úteis. Suas demonstrações são diretas, e portanto são omitidas aqui.

Proposição 1.5. *Sejam A um domínio, $K = Q(A)$ e L/K uma extensão algébrica de corpos. Se $B \subseteq L$ e B/A é uma extensão de anéis, então temos $(A \setminus \{0\})^{-1}B = Q(B)$.*

Proposição 1.6. *Sejam A um domínio, $K = Q(A)$ e M um A-módulo. Então $\{m_1, \ldots, m_r\} \subseteq M$ é LI sobre A se e só se $\{m_1/1, \ldots, m_r/1\} \subseteq M_K$ for LI sobre K, onde[1] $M_K \coloneqq (A \setminus \{0\})^{-1}M$.*

Em particular, se L for uma extensão de K, os elementos $\alpha_1, \ldots, \alpha_r \in L$ serão LI sobre A se e só se eles forem LI sobre K.

A finitude de uma extensão de anéis é uma propriedade transitiva, como mostra o lema abaixo:

Lema 1.7. *Se C/B e B/A forem extensões finitas de anéis, então C/A também será finita.*

Demonstração. (i) Pelas hipóteses, temos:

$$\begin{aligned} C &= B\gamma_1 + \cdots + B\gamma_m, \text{ para alguns } \gamma_1, \ldots, \gamma_m \in C, \text{ e} \\ B &= A\beta_1 + \cdots + A\beta_n, \text{ para alguns } \beta_1, \ldots, \beta_n \in B. \end{aligned}$$

Afirmamos que $C = \sum_{i=1}^m \sum_{j=1}^n A\gamma_i\beta_j$. De fato, a inclusão $(\supseteq)$ é clara. Por outro lado, dado $c \in C$, temos $c = \sum_{i=1}^m b_i\gamma_i$, para alguns $b_1, \ldots, b_m \in B$. Agora, cada b_i pode ser escrito como $b_i = \sum_{j=1}^n a_{ij}\beta_j$, para alguns $a_{i1}, \ldots, a_{in} \in A$. Então:

$$c = \sum_{i=1}^m b_i\gamma_i = \sum_{i=1}^m \sum_{j=1}^n a_{ij}\gamma_i\beta_j,$$

o que mostra a outra inclusão. Assim, C é finitamente gerado como A-módulo, e portanto a extensão C/A é finita. □

[1] A notação M_K normalmente é usada para denotar o K-espaço $M \otimes_A K$, obtido de M por extensão por escalares. Mas $M \otimes_A K \cong (A \setminus \{0\})^{-1}M$, o que justifica a notação utilizada.

Definamos agora o que é uma extensão integral, que é uma espécie de generalização de uma extensão algébrica para o caso de anéis comutativos:

Definição (Elemento Integral/Extensão Integral)**.** Sejam B/A uma extensão de anéis e $\beta \in B$. Dizemos que β é **integral** sobre A se β satisfizer um polinômio mônico com coeficientes em A.

A extensão de anéis B/A será chamada de uma **extensão integral** se todo elemento de B for integral sobre A. Nesse caso, dizemos também que B é **integral** sobre A.

Sejam B/A uma extensão de anéis e $\beta \in B$ integral sobre A. Então β é raiz de um polinômio mônico $f(x) \in A[x]$. Assim, existem $a_0, a_1, \ldots, a_{n-1} \in A$ tais que

$$a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1} + \beta^n = 0 \Rightarrow \beta^n = -a_0 - a_1\beta - \cdots - a_{n-1}\beta^{n-1}.$$

A partir dessa relação, é fácil ver por indução que $A[\beta] = A + A\beta + \cdots + A\beta^{n-1}$, e portanto que a extensão $A[\beta]/A$ é finita. Assim:

Lema 1.8. *Sejam B/A uma extensão de anéis e $\beta \in B$ integral sobre A. Então $A[\beta]/A$ é uma extensão finita.*

Com isso, conseguimos caracterizar as extensões finitas de A como sendo exatamente as extensões integrais finitamente geradas como A-álgebras:

Teorema 1.9. *Seja B/A uma extensão de anéis. Então B/A será uma extensão finita se e só se tivermos $B = A[\beta_1, \ldots, \beta_n]$, para $\beta_1, \ldots, \beta_n \in B$ integrais sobre A. Nesse caso, B será uma extensão integral de A.*

Demonstração. ($\Rightarrow$) Suponhamos que B/A seja uma extensão finita. Então

$$B = A\beta_1 + \cdots + A\beta_n, \text{ para alguns } \beta_1, \ldots \beta_n \in B.$$

Como B é um anel, é claro que $B = A[\beta_1, \ldots, \beta_n]$. Seja $\beta \in B$ qualquer. Consideremos a função $\varphi\colon B \to B$ dada por $\varphi(x) = \beta x$. Então φ é um homomorfismo de A-módulos, e aplicando o Teorema de Cayley-Hamilton generalizado para $M = B$, $\mathfrak{a} = A$ e φ como acima nós garantimos a existência de um polinômio $\chi(x) \in A[x]$ mônico tal que $\chi(\varphi) = 0$. Escrevendo

$$\chi(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + x^m, \text{ com } a_0, a_1, \ldots, a_{m-1} \in A,$$

temos que para todo $b \in B$ vale $\chi(\varphi)(b) = 0$. Em particular, $\chi(\varphi)(1) = 0$, ou seja:

$$\begin{aligned} & a_0 + a_1\varphi(1) + \cdots + a_{m-1}\varphi^{m-1}(1) + \varphi^m(1) = 0 \\ \Rightarrow \quad & a_0 + a_1\beta + \cdots + a_{m-1}\beta^{m-1} + \beta^m = 0. \end{aligned}$$

Assim, $\chi(\beta) = 0$, logo β é integral sobre A. Isso mostra que todo elemento de B é integral sobre A. Em particular, $\beta_1, \ldots, \beta_n$ são integrais sobre A, e como $B = A[\beta_1, \ldots, \beta_n]$ obtemos o resultado desejado.

($\Leftarrow$) Suponhamos $B = A[\beta_1, \ldots, \beta_n]$, onde $\beta_1, \ldots, \beta_n \in B$ são integrais sobre A. Provaremos por indução em n que B é extensão finita de A. Para $n = 1$ o resultado vale pelo Lema 1.8. Suponhamos então o resultado válido para $k - 1 \geq 1$, e provemos que ele também vale para k.

Notemos que $A[\beta_1, \ldots, \beta_k] = A[\beta_1, \ldots, \beta_{k-1}][\beta_k]$ é extensão finita de $A[\beta_1, \ldots, \beta_{k-1}]$ pelo Lema 1.8, já que β_k é integral sobre A e portanto também é integral sobre $A[\beta_1, \ldots, \beta_{k-1}] \supseteq A$. Pela hipótese de indução, $A[\beta_1, \ldots, \beta_{k-1}]/A$ também é uma extensão finita. Assim, pelo Lema 1.7, a extensão $A[\beta_1, \ldots, \beta_k]/A$ é finita, provando o que queríamos. □

Como corolário desse teorema, concluímos que a integrabilidade de extensões também é uma propriedade transitiva:

Lema 1.10. *Se $A \subseteq B \subseteq C$, então C/A é uma extensão integral de anéis se e só se C/B e B/A forem extensões integrais de anéis.*

Demonstração. ($\Rightarrow$) É clara.

($\Leftarrow$) Suponhamos que C/B e B/A sejam integrais. Seja $\alpha \in C$. Então α satisfaz um polinômio mônico com coeficientes em B, ou seja:

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} + \alpha^n = 0, \text{ para alguns } b_0, b_1, \ldots, b_{n-1} \in B.$$

Assim, α é integral sobre $A[b_0, \ldots, b_{n-1}]$, logo pelo Teorema 1.9 o anel $A[b_0, \ldots, b_{n-1}, \alpha]$ é integral sobre $A[b_0, \ldots, b_{n-1}]$, e portanto a extensão $A[b_0, \ldots, b_{n-1}, \alpha]/A[b_0, \ldots, b_{n-1}]$ é finita. Mas também por esse teorema, $A[b_0, \ldots, b_{n-1}]$ é extensão finita de A, já que por hipótese todo elemento de B é integral sobre A.

Concluímos do Lema 1.7 que a extensão $A[b_0, \ldots, b_{n-1}, \alpha]/A$ é finita, e novamente do Teorema 1.9 concluímos que α é integral sobre A. Sendo $\alpha \in C$ qualquer, provamos que C/A é integral. □

Uma propriedade importante da integrabilidade de extensões, especialmente em Teoria de Galois, é que ela se mantém sobre um homomorfismo de anéis. Sua demonstração é direta, sendo portanto omitida aqui.

Proposição 1.11. *Seja B uma extensão integral de A. Se T é um anel qualquer e $\sigma\colon B \to T$ é um homomorfismo de anéis, então $\sigma(B)$ é integral sobre $\sigma(A)$.*

Uma noção muito importante é a de **fecho integral**, que pode ser pensada como um análogo à definição de fecho algébrico para extensões de anéis.

Definição (Fecho Integral)**.** Seja B uma extensão de A. Então o **fecho integral** da extensão B/A, denotado por $\overline{A}^B$, é definido por:

$$\overline{A}^B := \{\beta \in B\colon \beta \text{ é integral sobre } A\}.$$

O fecho integral de uma extensão é sempre um anel, como mostra o corolário abaixo:

Corolário 1.12. *Se B é uma extensão de A, $\overline{A}^B$ é um subanel de B que contém A. Além disso, todo subanel $R \supseteq A$ de B que é um A-módulo finitamente gerado está contido em $\overline{A}^B$.*

Demonstração. É claro que $A \subseteq \overline{A}^B \subseteq B$. Em particular, $0, 1, -1 \in \overline{A}^B$. Assim, para vermos que $\overline{A}^B$ é um anel basta mostrarmos que se $\alpha, \beta \in \overline{A}^B$ então $\alpha + \beta, \alpha\beta \in \overline{A}^B$. Mas $\alpha + \beta, \alpha\beta \in A[\alpha, \beta]$. Como α e β são integrais sobre A, $A[\alpha, \beta]/A$ é integral pelo Teorema 1.9, logo $\alpha + \beta$ e $\alpha\beta$ são integrais sobre A, e portanto estão em $\overline{A}^B$, como gostaríamos.

Se $R \subseteq B$ é um A-módulo finitamente gerado, então R/A é finito, logo pelo Teorema 1.9 a extensão R/A é integral, ou seja, $R \subseteq \overline{A}^B$. □

Esse resultado nos permite concluir, na verdade, que $\overline{A}^B$ é a união de todos os A-submódulos de B finitamente gerados.

Definição (Extensão Integralmente Fechada/Domínio Integralmente Fechado)**.** Seja B/A uma extensão de anéis. Dizemos que A é **integralmente fechado** sobre B se $\overline{A}^B = A$. Nesse caso, ainda dizemos que a extensão B/A é **integralmente fechada**. Se A for um domínio integralmente fechado sobre seu corpo de frações $Q(A)$, dizemos que A é **integralmente fechado**, ou ainda **normal**.

O corolário abaixo mostra que o nome fecho integral "faz sentido": ele de fato se comporta como um fecho.

Corolário 1.13. *Sejam $A \subseteq R \subseteq B$ anéis. Então $\overline{A}^B \subseteq \overline{R}^B$. Além disso, $A \subseteq \overline{A}^B = \overline{\overline{A}^B}^B$. Ou seja, $\overline{A}^B$ é integralmente fechado em B.*

Demonstração. A única afirmação não-trivial é que $\overline{\overline{A}^B}^B = \overline{A}^B$. Como a inclusão ($\supseteq$) é clara, basta mostrarmos que $\overline{\overline{A}^B}^B \subseteq \overline{A}^B$. Se $\beta \in \overline{\overline{A}^B}^B$, então $\overline{A}^B[\beta]/\overline{A}^B$ é extensão integral. Como $\overline{A}^B/A$ também é extensão integral, temos pelo Lema 1.10 que $\overline{A}^B[\beta]/A$ é integral. Logo β é integral sobre A, ou seja, $\beta \in \overline{A}^B$. Assim, $\overline{\overline{A}^B}^B = \overline{A}^B$, como gostaríamos. □

Um resultado simples, porém importante, é que todo domínio de fatoração única é integralmente fechado:

Teorema 1.14. *Seja A um domínio de fatoração única. Então A é integralmente fechado.*

Demonstração. Seja $r/s \in Q(A)$ integral sobre A, com $r, s \in A \setminus \{0\}$. Como A é um DFU, podemos supor r e s primos entre si. Então temos:

$$a_0 + a_1\left(\frac{r}{s}\right) + \cdots + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \left(\frac{r}{s}\right)^n = 0, \text{ para alguns } a_0, a_1, \ldots, a_{n-1} \in A.$$

Multiplicando por s^n, obtemos:

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + r^n = 0.$$

Então $s \mid r^n$. Como r e s são primos entre si, devemos ter $s \in A^\times$, e portanto $r/s \in A$. Assim, todo elemento de $Q(A)$ integral sobre A é um elemento de A. □

O fecho integral "comuta" com localizações:

Proposição 1.15. *Seja B/A uma extensão de anéis, e seja S um subconjunto multiplicativo de A. Então $\overline{S^{-1}A}^{S^{-1}B} = S^{-1}\overline{A}^B$. Em particular, B/A integral implica em $S^{-1}B/S^{-1}A$ integral, e B/A integralmente fechada implica em $S^{-1}B/S^{-1}A$ integralmente fechada.*

Demonstração. Podemos supor que $0 \notin S$. Senão, teríamos $S^{-1}A = S^{-1}B = 0$ e os resultados seriam triviais.

($\subseteq$) Seja $x \in \overline{S^{-1}A}^{S^{-1}B}$. Escrevamos $x = b/s$, onde $b \in B$ e $s \in S$. Como x satisfaz um polinômio mônico em $(S^{-1}A)[x]$,

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{a_1}{s_1}x + \frac{a_0}{s_0} = 0, \text{ para alguns } a_0, \ldots, a_{n-1} \in A, s_0, \ldots, s_{n-1} \in S.$$

Então temos

$$\frac{b^n}{s^n} + \frac{a_{n-1}b^{n-1}}{s_{n-1}s^{n-1}} + \cdots + \frac{a_1 b}{s_1 s} + \frac{a_0}{s_0} = 0.$$

Multiplicando por $s^n s_0 s_1 \cdots s_{n-1}$, obtemos uma equação da forma

$$\frac{c_n b^n + c_{n-1}b^{n-1} + \cdots + c_1 b + c_0}{1} = 0, \text{ onde } c_0, \ldots, c_{n-1}, c_n \in A, c_n = s_0 s_1 \cdots s_{n-1} \in S.$$

Então existe $t \in S$ tal que

$$t c_n b^n + t c_{n-1} b^{n-1} + \cdots + t c_1 b + t c_0 = 0.$$

Para cada $0 \leq i \leq n$, chamemos $d_i = t c_i$. Notemos que $d_n \in S$, e que vale

$$d_n b^n + d_{n-1} b^{n-1} + \cdots + d_1 b + d_0 = 0.$$

Multiplicando agora por d_n^{n-1}:

$$(d_n b)^n + d_{n-1}(d_n b)^{n-1} + d_{n-2}d_n(d_n b)^{n-2} + \cdots + d_1 d_n^{n-2}(d_n b) + d_0 d_n^{n-1} = 0.$$

Denotemos $y \coloneqq d_n b \in B$. Então, pela equação acima:

$$y^n + d_{n-1}y^{n-1} + d_{n-2}d_n y^{n-2} + \cdots + d_1 d_n^{n-2} y + d_0 d_n^{n-1} = 0,$$

portanto $y \in \overline{A}^B$. Assim, $x = b/s = y/(d_n s) \in S^{-1}\overline{A}^B$.

($\supseteq$) Seja $x \in S^{-1}\overline{A}^B$. Então $x = b/s$, onde $b \in \overline{A}^B$, $s \in S$. Sabemos que temos

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0, \text{ para alguns } a_0, \ldots, a_{n-1} \in A.$$

Então, dividindo por s^n:

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_1}{s^{n-1}}\left(\frac{b}{s}\right) + \frac{a_0}{s^n} = 0,$$

ou seja,

$$x^n + \frac{a_{n-1}}{s}x^{n-1} + \cdots + \frac{a_1}{s^{n-1}}x + \frac{a_0}{s^n} = 0,$$

mostrando que $x \in \overline{S^{-1}A}^{S^{-1}B}$.

Assim, temos $\overline{S^{-1}A}^{S^{-1}B} = S^{-1}\overline{A}^B$, como queríamos. As observações finais seguem diretamente desse resultado. □

Se L/K for uma extensão de corpos, é fácil ver que o fecho integral $\overline{K}^L$ coincide com o fecho algébrico de K em L (o subcorpo de L dos elementos que são algébricos sobre K). Consideremos agora um domínio A com corpo de frações $K = Q(A)$, e uma extensão de corpos L/K. Então temos uma relação entre o fecho integral $\overline{A}^L$ e o fecho algébrico $\overline{K}^L$:

Teorema 1.16. *Sejam A um domínio, $K = Q(A)$ e L um corpo que é extensão de K. Então:*

$$Q(\overline{A}^L) = (A \setminus \{0\})^{-1}\overline{A}^L = \overline{K}^L.$$

Em particular, temos $Q(\overline{A}^L) = L$ se e só se L/K for uma extensão algébrica.

A demonstração desse resultado é direta, utilizando argumentos semelhantes aos da proposição anterior.

Sendo A um anel, $K = Q(A)$ e L/K extensão de corpos, parece razoável que, dado um elemento $\alpha \in \overline{A}^L$, o polinômio minimal $P_{\alpha,K}(x) \in K[x]$ esteja em $A[x]$. Porém, isso nem sempre é verdade:

Exemplo 1.17. *Seja A um domínio que não é integralmente fechado, e consideremos a extensão $Q(A)/A$. Então existe $\alpha \in Q(A) \setminus A$ que é integral sobre A. Assim, $f(\alpha) = 0$ para algum $f(x) \in A[x]$ mônico. É claro que f tem grau maior ou igual a 2, caso contrário teríamos $\alpha \in A$. Por outro lado, o polinômio minimal de α em $Q(A)$ é $x - \alpha \notin A[x]$.*

O exemplo acima mostra que uma condição necessária para garantirmos que a implicação $\alpha \in \overline{A}^L \Rightarrow P_{\alpha,K}(x) \in A[x]$ seja verdadeira é que A seja integralmente fechado. De fato, essa condição é também suficiente:

Teorema 1.18. *Seja B/A uma extensão de domínios.*

(a) Se $f, g \in B[x]$ forem dois polinômios mônicos tais que $fg \in \overline{A}^B[x]$, então $f, g \in \overline{A}^B[x]$.

(b) Sejam A um anel, $K = Q(A)$ e L/K uma extensão de corpos. Então, para todo $\gamma \in \overline{A}^L$, temos $P_{\gamma,K} \in \overline{A}^K[x]$. Em particular, se A for integralmente fechado, temos $P_{\gamma,K} \in A[x]$.

Demonstração. (a) Seja Ω um fecho algébrico de $Q(B)$. Então f e g se fatoram linearmente em $\Omega[x]$, digamos $f(x) = (x-\alpha_1)\cdots(x-\alpha_m)$ e $g(x) = (x-\beta_1)\cdots(x-\beta_n)$, onde temos $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in \Omega$. Desse modo:

$$fg(x) = (x-\alpha_1)\cdots(x-\alpha_m)(x-\beta_1)\cdots(x-\beta_n) \in \overline{A}^B[x].$$

Como $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ são raízes do polinômio mônico $fg \in \overline{A}^B[x]$, vemos que esses elementos são integrais sobre $\overline{A}^B$, e portanto são também integrais sobre A, já que a extensão $\overline{A}^B/A$ é integral. Assim, esses números pertencem a $\overline{A}^\Omega$, e portanto

$$\begin{aligned} f(x) &= (x-\alpha_1)\cdots(x-\alpha_m) \in (\overline{A}^\Omega \cap B)[x] = \overline{A}^B[x], \text{ e} \\ g(x) &= (x-\beta_1)\cdots(x-\beta_n) \in (\overline{A}^\Omega \cap B)[x] = \overline{A}^B[x]. \end{aligned}$$

(b) Como $\gamma \in \overline{A}^L$, temos $f(\gamma) = 0$ para algum $f \in A[x]$ mônico. Sabemos que $P_{\gamma,K} \mid f$ em $K[x]$, logo existe $g \in K[x]$ tal que $f = gP_{\gamma,K}$. Como f e $P_{\gamma,K}$ são mônicos, g também deve ser mônico, e como $f \in A[x] \subseteq \overline{A}^K[x]$ segue do item (a) que $P_{\gamma,K} \in \overline{A}^K[x]$.

□

1.3. Álgebras Étale, Traço e Norma

Nesta seção, estudaremos as álgebras étale. A noção de álgebra étale generaliza a de uma extensão finita e separável de corpos, e tem a vantagem de ser "fechada por mudança de base". Dada uma extensão de corpos K'/K e um K-espaço vetorial V, podemos considerar o K'-espaço $V \otimes_K K'$, dado por extensão de escalares. Mesmo se V for um corpo, é possível que $V \otimes_K K'$ não seja um corpo. Mas como veremos, se V for uma K-álgebra étale, $V \otimes_K K'$ será uma K'-álgebra étale de mesma dimensão.

Também definiremos noções importantes de extensões de corpos, as noções de polinômio característico, traço e norma, e provaremos suas propriedades básicas.

Definição (Álgebra Étale)**.** Seja K um corpo. Uma **álgebra étale** sobre K é uma K-álgebra L que é isomorfa a um produto direto finito de extensões finitas e separáveis de corpos com base em K. Isto é, existem extensões finitas e separáveis $L_1, \ldots, L_m$ de K tais que $L \cong L_1 \times \cdots \times L_m$ como uma K-álgebra. A **dimensão** $\dim_K L$ de uma K-álgebra étale L é igual à sua dimensão como um K-espaço.

Note que se $L \cong L_1 \times \cdots \times L_m$ então $\dim_K L = \dim_K L_1 + \cdots + \dim_K L_m$, de modo que a dimensão de uma álgebra étale é sempre finita.

Exemplo 1.19. *Se K for um corpo separavelmente fechado, toda álgebra étale sobre K é isomorfa a K^n para algum n inteiro positivo.*

Veremos agora que as álgebras étale de fato são "fechadas por mudança de base", e mais do que isso, que a mudança de base preserva dimensões:

Proposição 1.20. *Seja L uma K-álgebra étale, e seja K'/K uma extensão de corpos qualquer. Então $L \otimes_K K'$ é uma K'-álgebra étale e nós temos $\dim_{K'}(L \otimes_K K') = \dim_L K$.*

Demonstração. Suponhamos $L \cong \prod_{i=1}^m L_i$. Cada L_i/K é uma extensão finita e separável, e portanto $L_i = K(\alpha_i)$ para algum $\alpha_i \in L_i$. Chamando de $f_i(x) \in K[x]$ o polinômio minimal de α_i sobre K, temos $f_i(x)$ irredutível e separável. Suponhamos que a fatoração de f_i em irredutíveis de $K'[x]$ seja $f_i = f_{i1} \cdots f_{ir_i}$. Esses irredutíveis são distintos dois a dois, pela separabilidade de f_i. Assim, pelo Teorema Chinês dos Restos, temos um isomorfismo de K'-álgebras:

$$L_i \otimes_K K' \cong \frac{K[x]}{\langle f_i(x)\rangle} \otimes_K K' \cong \frac{K'[x]}{\langle f_i(x)\rangle} \cong \prod_{j=1}^{r_i} \frac{K'[x]}{\langle f_{ij}(x)\rangle}.$$

Desse modo, nós temos:

$$L \otimes_K K' \cong \left(\prod_{i=1}^m L_i\right) \otimes_K K' \cong \prod_{i=1}^m (L_i \otimes_K K') \cong \prod_{i=1}^m \prod_{j=1}^{r_i} \frac{K'[x]}{\langle f_{ij}(x)\rangle},$$

o que mostra que $L \otimes_K K'$ é uma álgebra étale, de dimensão

$$\sum_{i=1}^m \sum_{j=1}^{r_i} \partial\, f_{ij} = \sum_{i=1}^m \partial\, f_i = \sum_{i=1}^m \dim_K L_i = \dim_K L,$$

como queríamos. □

Como corolário da demonstração da proposição acima nós temos, no caso de L/K ser uma extensão separável de corpos:

Corolário 1.21. *Seja $L \cong K[x]/\langle f(x)\rangle$ uma extensão finita e separável de um corpo K, definida por um polinômio separável irredutível $f(x) \in K[x]$. Seja K'/K uma extensão de corpos qualquer, e seja $f(x) = f_1(x) \cdots f_r(x)$ a fatoração de f em polinômios irredutíveis de $K'[x]$. Então nós temos um isomorfismo canônico de K'-álgebras étale*

$$L \otimes_K K' \cong \prod_{j=1}^r \frac{K'[x]}{\langle f_j(x)\rangle}.$$

No caso em que o corpo para o qual estendemos escalares é separavelmente fechado, temos uma fórmula para calcular essa extensão:

Proposição 1.22. *Sejam K um corpo, L uma K-álgebra étale e Ω uma extensão de K separavelmente fechada. Então temos um isomorfismo de Ω-álgebras étale:*

$$L \otimes_K \Omega \cong \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \Omega,$$

dado por $\beta \otimes 1 \mapsto (\sigma(\beta))$, para todo $\beta \in L$, onde aqui $\mathrm{Hom}_K(L,\Omega)$ denota os homomorfismos de K-álgebras entre L e Ω.

Demonstração. Sendo $L \cong \prod_{i=1}^m L_i$, nós temos $\mathrm{Hom}_K(L,\Omega) \cong \prod_{i=1}^m \mathrm{Hom}_K(L_i,\Omega)$. Como temos que $L \otimes_K \Omega \cong \prod_{i=1}^m (L_i \otimes_K \Omega)$, podemos supor sem perda de generalidade que L é um corpo, e portanto uma extensão finita e separável de K. Então temos $L \cong K[x]/\langle f(x)\rangle$, para algum polinômio irredutível e separável $f(x) \in K[x]$.

Como Ω é separavelmente fechado, f se decompõe em fatores lineares de $\Omega[x]$, digamos $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, com $\alpha_1, \ldots, \alpha_n \in \Omega$ distintos dois a dois. Dado $\sigma \in \mathrm{Hom}_K(K[x]/\langle f(x)\rangle, \Omega)$, temos $f(\sigma(\overline{x})) = \sigma(f(\overline{x})) = 0$. Assim, $\sigma(\overline{x}) = \alpha_j$ para algum $1 \leq j \leq n$. Note que isso determina completamente σ. Reciprocamente, para cada $1 \leq j \leq n$ a avaliação $K[x] \to \Omega$ dada por $x \mapsto \alpha_j$ se anula em $\langle f(x)\rangle$, e portanto induz um homomorfismo $\sigma_j \colon K[x]/\langle f(x)\rangle \to \Omega$, dado por $\overline{x} \mapsto \alpha_j$. Logo $\mathrm{Hom}_K(K[x]/\langle f(x)\rangle, \Omega) = \{\sigma_1, \ldots, \sigma_n\}$.

Temos então uma sequência de isomorfismos canônicos de Ω-álgebras:

$$\frac{K[x]}{\langle f(x)\rangle} \otimes_K \Omega \cong \frac{\Omega[x]}{\langle f(x)\rangle} \cong \prod_{j=1}^{n} \frac{\Omega[x]}{\langle x-\alpha_j\rangle} \cong \prod_{j=1}^{n} \Omega,$$

e é fácil verificar que os isomorfismos acima levam $\overline{x}\otimes 1 \mapsto (\alpha_1,\ldots,\alpha_n) = (\sigma_1(\overline{x}),\ldots,\sigma_n(\overline{x}))$. Sendo este um isomorfismo de álgebras, vemos que para todo $p(x)\in K[x]$ nós temos

$$p(\overline{x})\otimes 1 \mapsto (p(\sigma_1(\overline{x})),\ldots,p(\sigma_n(\overline{x}))) = (\sigma_1(p(\overline{x})),\ldots,\sigma_n(p(\overline{x}))).$$

Via $L\cong K[x]/\langle f(x)\rangle$, obtemos um isomorfismo $L\otimes_K \Omega \to \prod_{j=1}^{n}\Omega = \prod_{\sigma\in \mathrm{Hom}_K(L,\Omega)}\Omega$ entre Ω-álgebras que satisfaz $\beta\otimes 1\mapsto(\sigma(\beta))$ para todo $\beta\in L$, como queríamos. □

Exemplo 1.23. *Consideremos a extensão de corpos $\mathbb{Q}(i)/\mathbb{Q}$. Os únicos homomorfismos de corpos $\mathbb{Q}(i)\to\mathbb{C}$ são a identidade e a conjugação complexa. Assim, pela proposição acima, vemos que $\mathbb{Q}(i)\otimes_{\mathbb{Q}}\mathbb{C}\cong\mathbb{C}\times\mathbb{C}$, com isomorfismo dado por $(a+bi)\otimes 1\mapsto(a+bi,a-bi)$.*

Nosso próximo objetivo é definir os conceitos de polinômio característico, traço e norma para álgebras étale. A definição, de fato, se generaliza para extensões livres de anéis de posto finito:

Definição (Polinômio Característico, Traço e Norma)**.** Sejam A um anel e B uma extensão de A que é uma A-álgebra livre de posto finito. Dado $b\in B$ qualquer, definimos o **polinômio característico** $F_{b,B/A}(x)\in A[x]$, a **norma** $N_{B/A}(b)\in A$ e o **traço** $\mathrm{Tr}_{B/A}(b)\in A$ como sendo respectivamente o polinômio característico, o determinante e o traço do operador $T_b\colon B\to B$ de multiplicação por b. Estando claros B e A, denotaremos apenas $F_b(x)$, $N(b)$ e $\mathrm{Tr}(b)$.

Temos as seguintes propriedades básicas:

Proposição 1.24. *Seja A um anel e seja B/A uma extensão livre de posto finito n.*

(a) $\mathrm{Tr}_{B/A}\colon B\to A$ *é um homomorfismo de A-módulos e* $N_{B/A}\colon B\to A$ *é multiplicativa, e induz um homomorfismo de grupos* $N_{B/A}\colon B^\times\to A^\times$*. Assim, dados $b_1,b_2\in B$ e $a\in A$, temos* $\mathrm{Tr}(ab_1+b_2)=a\,\mathrm{Tr}(b_1)+\mathrm{Tr}(b_2)$ *e* $N(b_1b_2)=N(b_1)N(b_2)$.

(b) Seja $b\in B$ qualquer. Então $\partial F_b = n$, e escrevendo $F_b(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n$, com $a_0,a_1,\ldots,a_{n-1}\in A$, temos $\mathrm{Tr}(b)=-a_{n-1}$ *e* $N(b)=(-1)^n a_0$.

(c) Seja $a\in A$ qualquer. Então $\mathrm{Tr}(a)=na$ *e* $N(a)=a^n$.

(d) Seja C/A outra extensão livre de posto finito. Então $B\times C/A$ também é uma extensão livre de posto finito, e dado $\alpha=(b,c)\in B\times C$ qualquer nós temos:

$$\begin{aligned} F_{\alpha,B\times C/A}(x) &= F_{b,B/A}(x)\cdot F_{c,C/A}(x),\\ N_{B\times C/A}(\alpha) &= N_{B/A}(b)\cdot N_{C/A}(c),\\ \mathrm{Tr}_{B\times C/A}(\alpha) &= \mathrm{Tr}_{B/A}(b)+\mathrm{Tr}_{C/A}(c).\end{aligned}$$

Demonstração. (a) Dados $b_1,b_2\in B$ e $a\in A$, temos $T_{ab_1+b_2}=aT_{b_1}+T_{b_2}$, e tomando traços obtemos $\mathrm{Tr}(ab_1+b_2)=a\,\mathrm{Tr}(b_1)+\mathrm{Tr}(b_2)$, mostrando a linearidade do traço. Temos ainda $T_{b_1b_2}=T_{b_1}T_{b_2}$, e portanto tomando o determinante obtemos $N(b_1b_2)=N(b_1)N(b_2)$. Logo a norma é multiplicativa. Assim, se $u\in B^\times$, $N(u)N(u^{-1})=N(1)=1^n=1$ pelo item (c), de modo que $N(u)\in A^\times$.

(b) Segue diretamente das definições de polinômio característico, traço e norma e de resultados da álgebra linear.

(c) Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de B/A. Como $a \in A$, a matriz de multiplicação por a nessa base é uma matriz diagonal com todas as entradas a. Assim, é claro que seu traço é na e seu determinante é a^n, de onde obtemos o que queríamos.

(d) Sejam $\{\beta_1, \ldots, \beta_m\}$ e $\{\gamma_1, \ldots, \gamma_n\}$ bases de B e C como A-módulos, respectivamente. Então $(\beta_1, 0), \ldots, (\beta_m, 0), (0, \gamma_1), \ldots, (0, \gamma_n)$ formam uma base de $B \times C$ como A-módulo. A matriz de T_α em relação a essa base é uma matriz por blocos diagonal 2×2, sendo um bloco correspondente a $T_b\colon B \to B$ e o outro a $T_c\colon C \to C$. Com isso, é fácil ver que valem as igualdades desejadas.

□

O polinômio característico, a norma e o traço se comportam bem com extensão de escalares:

Proposição 1.25. *Seja B/A uma extensão livre de posto finito n, e seja $\varphi\colon A \to A'$ um homomorfismo de anéis. Então o A'-módulo $B' = B \otimes_A A'$ é livre de posto n, e para todo $b \in B$ nós temos:*

$$\begin{aligned} F_{b\otimes 1, A'/B'}(x) &= \varphi(F_{b,B/A}(x)), \\ N_{B'/A'}(b \otimes 1) &= \varphi(N_{B/A}(b)), \\ \mathrm{Tr}_{B'/A'}(b \otimes 1) &= \varphi(\mathrm{Tr}_{B/A}(b)). \end{aligned}$$

Demonstração. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de B/A. Então $\{\beta_1 \otimes 1, \ldots, \beta_n \otimes 1\}$ é uma base de B'/A'. Seja $b \in B$ qualquer, e seja $M = (m_{ij}) \in \mathrm{M}_{n\times n}(A)$ a matriz de T_b na base $\{\beta_1, \ldots, \beta_n\}$. Assim, para $1 \leq j \leq n$ temos $\beta_j b = \sum_{i=1}^n m_{ij}\beta_i$. Agora:

$$(\beta_j \otimes 1)(b \otimes 1) = \beta_j b \otimes 1 = \left(\sum_{i=1}^n m_{ij}\beta_i\right) \otimes 1 = \sum_{i=1}^n \varphi(m_{ij})(\beta_i \otimes 1).$$

Isso mostra que a matriz de $T_{b\otimes 1}$ na base $\{\beta_1 \otimes 1, \ldots, \beta_n \otimes 1\}$ é $M' = (\varphi(m_{ij})) \in \mathrm{M}_{n\times n}(A')$. Assim:

$$\begin{aligned} F_{b\otimes 1, B'/A'}(x) &= \det(x\,\mathrm{Id} - M') = \det(x\,\mathrm{Id} - \varphi(M)) = \varphi(\det(x\,\mathrm{Id} - M)) = \varphi(F_{b,B/A}(x)), \\ N_{B'/A'}(b \otimes 1) &= \det M' = \det \varphi(M) = \varphi(\det M) = \varphi(N_{B/A}(b)), \\ \mathrm{Tr}_{B'/A'}(b \otimes 1) &= \mathrm{Tr}\, M' = \mathrm{Tr}\, \varphi(M) = \varphi(\mathrm{Tr}\, M) = \varphi(\mathrm{Tr}_{B/A}(b)). \end{aligned}$$

□

Voltando ao caso de álgebras étale, nós temos:

Teorema 1.26. *Seja K um corpo com fecho separável Ω, e seja L uma K-álgebra étale. Então para todo $\alpha \in L$ nós temos:*

$$\begin{aligned} F_{\alpha,L/K}(x) &= \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} (x - \sigma(\alpha)), \\ N_{L/K}(\alpha) &= \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(\alpha), \\ \mathrm{Tr}_{L/K}(\alpha) &= \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(\alpha). \end{aligned}$$

Demonstração. Seja $n = \dim_K L$, e sejam $\sigma_1, \ldots, \sigma_n$ os elementos de $\mathrm{Hom}_K(L, \Omega)$. Então, pelas Proposições 1.22, 1.24 e 1.25, nós temos:

$$\begin{aligned} F_{\alpha, L/K}(x) &= F_{\alpha\otimes 1, L\otimes_K \Omega/\Omega}(x) = F_{(\sigma_1(\alpha),\ldots,\sigma_n(\alpha)),\Omega^n/\Omega}(x) = \prod_{j=1}^{n}(x - \sigma_j(\alpha)), \\ N_{L/K}(\alpha) &= N_{(L\otimes_K\Omega)/\Omega}(\alpha\otimes 1) = N_{\Omega^n/\Omega}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) = \prod_{j=1}^{n}\sigma_j(\alpha) \\ \mathrm{Tr}_{L/K}(\alpha) &= \mathrm{Tr}_{(L\otimes_K\Omega)/\Omega}(\alpha\otimes 1) = \mathrm{Tr}_{\Omega^n/\Omega}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) = \sum_{j=1}^{n}\sigma_j(\alpha), \end{aligned}$$

uma vez que o polinômio característico, a norma e o traço são preservados por extensão de escalares (1.25), $L \otimes_K \Omega \cong \Omega^n$ por um isomorfismo de Ω-álgebras que leva $\alpha \otimes 1$ em $(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$ (1.22), o polinômio característico, a norma e o traço se comportam bem com produtos (1.24 item (d)) e cada $\sigma_j(\alpha)$ possui polinômio característico, norma e traço em relação à extensão Ω/Ω iguais a $x - \sigma_j(\alpha)$, $\sigma_j(\alpha)$ e $\sigma_j(\alpha)$, respectivamente. □

Consideremos agora o caso em que L/K é uma extensão finita de corpos. Nesse caso, a cada $\alpha \in L$ nós podemos associar, além do seu polinômio característico $F_\alpha(x) \in K[x]$, seu polinômio minimal $P_\alpha(x) \in K[x]$. Esses polinômios são relacionados da seguinte forma:

Proposição 1.27. *Seja L/K uma extensão finita de corpos de grau n, e seja $\alpha \in L$. Sendo $m = [L : K(\alpha)]$, nós temos $F_{\alpha,L/K}(x) = P_{\alpha,K}(x)^m$. Em particular, $F_{\alpha,L/K}(\alpha) = 0$. Além disso, escrevendo*

$$P_{\alpha,K}(x) = a_0 + a_1 x + \cdots + a_{\ell-1}x^{\ell-1} \in K[x],$$

temos $N_{L/K}(\alpha) = (-1)^n a_0^m$ e $\mathrm{Tr}_{M/K}(\alpha) = -m a_{\ell-1}$.

Demonstração. Seja $\ell = [K(\alpha) : K]$. Então $1, \alpha, \ldots, \alpha^{\ell-1}$ formam uma base de $K(\alpha)/K$. Seja $\{\beta_1, \ldots, \beta_m\}$ uma base de $L/K(\alpha)$. Então sabemos que os $m\ell = n$ elementos

$$\beta_1, \beta_1\alpha, \ldots, \beta_1\alpha^{\ell-1}, \beta_2, \beta_2\alpha, \ldots, \beta_2\alpha^{\ell-1}, \ldots, \beta_m, \beta_m\alpha, \ldots, \beta_m\alpha^{\ell-1}$$

formam uma base da extensão L/K. É fácil ver que a matriz de multiplicação por α com relação a essa base pode ser vista como uma matriz diagonal $m \times m$ em blocos de tamanho $\ell \times \ell$, sendo todos os blocos da diagonal iguais à matriz companheira de P_α. Com isso, é fácil ver que $F_\alpha(x) = P_\alpha(x)^m$, como queríamos. Agora, notemos que o coeficiente independente de $F_\alpha(x)$ é a_0^m, de modo que pela Proposição 1.24 nós temos $N(\alpha) = (-1)^n a_0^m$. Além disso, o coeficiente de x^{n-1} é $m a_{\ell-1}$, de modo que pela mesma proposição nós temos $\mathrm{Tr}(\alpha) = -m a_{\ell-1}$. □

Para obter informações sobre extensões de corpos a partir do que fizemos para álgebras étale, notemos que, sendo L/K uma extensão finita de corpos e Ω um fecho separável de K, o conjunto $\mathrm{Hom}_K(L, \Omega)$ dos homomorfismos de K-álgebras de L em Ω nada mais é do que o conjunto das K-imersões de L em Ω. Assim, no caso de L/K ser separável, nós obtemos como consequência direta do Teorema 1.26 o seguinte resultado, que permite calcular o polinômio característico, o traço e a norma de um elemento de L a partir de seus conjugados:

Corolário 1.28. *Seja L/K uma extensão finita e separável de corpos de grau n, e seja Ω um fecho separável de K que contém L. Sejam $\sigma_1, \ldots, \sigma_n \colon L \to \Omega$ todas as K-imersões de L em Ω.*

Então para todo $\alpha \in L$ nós temos:

$$\begin{aligned} F_{\alpha,L/K}(x) &= \prod_{j=1}^{n}(x-\sigma_j(\alpha)); \\ N_{L/K}(\alpha) &= \prod_{j=1}^{n}\sigma_j(\alpha); \\ \mathrm{Tr}_{L/K}(\alpha) &= \sum_{j=1}^{n}\sigma_j(\alpha). \end{aligned}$$

O traço e a norma em extensões de corpos também têm propriedades transitivas:

Proposição 1.29. *Seja $M/L/K$ uma torre de extensões finitas de corpos. Então:*

$$\begin{aligned} N_{M/K} &= N_{L/K}\circ N_{M/L}, \\ \mathrm{Tr}_{M/K} &= \mathrm{Tr}_{L/K}\circ \mathrm{Tr}_{M/L}\,. \end{aligned}$$

Demonstração. Sejam $m = [M : L]$ e $n = [L : K]$. Fixemos bases $\{\alpha_1, \ldots, \alpha_n\}$ de L/K e $\{\beta_1, \ldots, \beta_m\}$ de M/L. Então os elementos

$$\alpha_1\beta_1, \alpha_2\beta_1, \ldots, \alpha_n\beta_1, \ldots, \alpha_1\beta_m, \alpha_2\beta_m, \ldots, \alpha_n\beta_m$$

formam uma base de M/K. Seja $\gamma \in M$. Comecemos considerando o caso em que $\gamma \in L$. Nesse caso, a matriz de multiplicação por γ em M nessa base é uma matriz $m \times m$ por blocos de tamanho $n \times n$, diagonal e cujos blocos na diagonal são todos iguais à matriz A de multiplicação por γ em L com relação à base $\{\alpha_1, \ldots, \alpha_n\}$. Assim:

$$\begin{aligned} N_{M/K}(\gamma) &= (\det A)^m = (N_{L/K}(\gamma))^m = N_{L/K}(\gamma^m) = N_{L/K}(N_{M/L}(\gamma)), \text{ e} \\ \mathrm{Tr}_{M/K}(\gamma) &= m(\mathrm{Tr}\, A) = m\,\mathrm{Tr}_{L/K}(\gamma) = \mathrm{Tr}_{L/K}(m\gamma) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\gamma)), \end{aligned}$$

pelo item (c) da Proposição 1.24. Suponhamos agora que $M = L(\gamma)$. Nesse caso, podemos tomar $\beta_j = \gamma^{j-1}$, para $1 \le j \le m$. Assim, temos uma base de M/K formada pelos elementos

$$\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots, \alpha_1\gamma, \alpha_2\gamma, \ldots, \alpha_n\gamma, \ldots, \alpha_1\gamma^{m-1}, \alpha_2\gamma^{m-1}, \ldots, \alpha_n\gamma^{m-1}.$$

Notemos que a matriz de multiplicação por γ nessa base é igual a uma matriz $m \times m$ por blocos de tamanho $n \times n$ da forma:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -A_0 \\ \mathrm{Id} & 0 & \cdots & 0 & -A_1 \\ 0 & \mathrm{Id} & \cdots & 0 & -A_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \mathrm{Id} & -A_{m-1} \end{pmatrix},$$

cujo determinante é $(-1)^{mn}\det A_0$ e cujo traço é $-\mathrm{Tr}\, A_{m-1}$. Denotemos

$$P_{\gamma,L}(x) = c_0 + c_1x + \cdots + c_{m-1}x^{m-1} + x^m \in L[x].$$

Então $\gamma^m = -c_0 - c_1\gamma - \cdots - c_{m-1}\gamma^{m-1}$, e vemos que cada matriz A_i é igual à matriz do operador $T_{c_i}\colon L \to L$ com relação à base $\{\alpha_1, \ldots, \alpha_n\}$ de L/K. Desse modo, $\det A_0 = N_{L/K}(c_0)$ e $\mathrm{Tr}\, A_{m-1} = \mathrm{Tr}_{L/K}(c_{m-1})$. Além disso, pela Proposição 1.27 nós temos $\mathrm{Tr}_{M/L}(\gamma) = -c_{m-1}$ e $N_{M/L}(\gamma) = (-1)^m c_0$. Portanto:

$$\begin{aligned} N_{M/K}(\gamma) &= (-1)^{mn}\det A_0 = (-1)^{mn}N_{L/K}(c_0) = N_{L/K}((-1)^m c_0) = N_{L/K}(N_{M/L}(\gamma)), \text{ e} \\ \mathrm{Tr}_{M/K}(\gamma) &= -\mathrm{Tr}\, A_{m-1} = -\mathrm{Tr}_{L/K}(c_{m-1}) = \mathrm{Tr}_{L/K}(-c_{m-1}) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\gamma)). \end{aligned}$$

Finalmente, consideremos o caso geral, isto é, $\gamma \in M$ qualquer. Nesse caso, pelos resultados já demonstrados, nós temos:

$$\begin{aligned} N_{M/K}(\gamma) &= N_{L(\gamma)/K}(N_{M/L(\gamma)}(\gamma)) = N_{L(\gamma)/K}(\gamma^{[M:L(\gamma)]}) = N_{L(\gamma)/K}(\gamma)^{[M:L(\gamma)]} \\ &= N_{L/K}(N_{L(\gamma)/L}(\gamma))^{[M:L(\gamma)]} \\ &= N_{L/K}(N_{L(\gamma)/L}(\gamma^{[M:L(\gamma)]})) \\ &= N_{L/K}(N_{M/L}(\gamma)). \end{aligned}$$

Assim, $N_{M/K} = N_{L/K} \circ N_{M/L}$. Similarmente, temos:

$$\begin{aligned} \mathrm{Tr}_{M/K}(\gamma) &= \mathrm{Tr}_{L(\gamma)/K}(\mathrm{Tr}_{M/L(\gamma)}(\gamma)) = \mathrm{Tr}_{L(\gamma)/K}([M : L(\gamma)]\gamma) = [M : L(\gamma)]\,\mathrm{Tr}_{L(\gamma)/K}(\gamma) \\ &= [M : L(\gamma)]\,\mathrm{Tr}_{L/K}(\mathrm{Tr}_{L(\gamma)/L}(\gamma)) \\ &= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{L(\gamma)/L}([M : L(\gamma)]\gamma)) \\ &= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\gamma)). \end{aligned}$$

Assim, $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$. Isso conclui a demonstração. □

Devido ao Teorema 1.18, nós conseguimos obter diversas informações sobre o polinômio característico, o polinômio minimal, o traço e a norma de elementos em uma extensão integral de um domínio integralmente fechado:

Corolário 1.30. *Sejam A um domínio integralmente fechado, $K = Q(A)$, L uma extensão finita de K de grau n e B um subanel de $\overline{A}^L$ que contém A. Então, para todo $\gamma \in B$, temos:*

(a) $P_{\gamma,K} \in A[x]$, $F_{\gamma,L/K} \in A[x]$, $N_{L/K}(\gamma) \in A$ *e* $\mathrm{Tr}_{L/K}(\gamma) \in A$.

(b) $N_{L/K}(\gamma)$ *é um múltiplo de* γ *em* B.

(c) $\gamma \in B^\times$ *se e só se* $N_{L/K}(\gamma) \in A^\times$.

(d) Se $N_{L/K}(\gamma)$ *for irredutível em* A*, então* γ *será irredutível em* B.

(e) Se $\alpha, \beta \in B$ *forem associados em* B*, então* $N_{L/K}(\alpha)$ *e* $N_{L/K}(\beta)$ *serão associados em* A.

Demonstração. Se $\gamma = 0$, os resultados são óbvios. Suponhamos então $\gamma \neq 0$, e seja $n = [L : K]$.

(a) Temos que $P_\gamma \in A[x]$ pelo Teorema 1.18. Pela Proposição 1.27, F_γ é uma potência de P_γ, e portanto esse polinômio também está em $A[x]$ pelo Teorema 1.18. Consequentemente, a norma e o traço de γ estão em A, já que são, a menos de sinal, coeficientes de F_γ.

(b) Temos $F_\gamma(\gamma) = 0$. Escrevamos $F_\gamma(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$, onde $a_0, \ldots, a_{n-1} \in A$. Então $0 = F_\gamma(\gamma) = a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1} + \gamma^n$, o que mostra que $\gamma \mid a_0$ em B. Mas $a_0 = (-1)^n N(\gamma)$, logo $\gamma \mid N(\gamma)$ em B, como gostaríamos.

(c) Pelo item (b), $\gamma \mid N(\gamma)$ em B, assim $N(\gamma) \in A^\times \Rightarrow \gamma \in B^\times$. Por outro lado, se $\gamma \in B^\times$, então $\gamma^{-1} \in B$, e $\gamma\gamma^{-1} = 1 \Rightarrow N(\gamma)N(\gamma^{-1}) = N(1) = 1^n = 1$. Como $N(\gamma), N(\gamma^{-1}) \in A$ pelo item (a), concluímos que $N(\gamma) \in A^\times$.

(d) Se γ for redutível em B, teremos $\gamma = \alpha\beta$, para alguns $\alpha, \beta \in B \setminus B^\times$, e então temos $N(\gamma) = N(\alpha)N(\beta)$. Pelo item (c), concluímos que $N(\alpha), N(\beta) \in A \setminus A^\times$, o que mostra que $N(\gamma)$ não será irredutível em A nesse caso.

(e) Sendo α e β associados em B, existe $u \in B^\times$ tal que $\alpha = u\beta$. Então $N(\alpha) = N(u)N(\beta)$. Pelo item (c), $N(u) \in A^\times$, e portanto $N(\alpha)$ e $N(\beta)$ são associados em A, como desejávamos.

□

1.4. Discriminante e Base Integral

Outra noção importante no estudo de extensões finitas de corpos é a de **discriminante**:

Definição (Discriminante de uma n-upla)**.** Seja L/K uma extensão finita de grau n. Dados $\alpha_1, \ldots, \alpha_n \in L$, o **discriminante** da n-upla $(\alpha_1, \ldots, \alpha_n)$ é definido por:

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

Quando a extensão L/K estiver clara, indicaremos o discriminante de $\alpha_1, \ldots, \alpha_n$ simplesmente por $\Delta(\alpha_1, \ldots, \alpha_n)$.

O discriminante se comporta bem por transformações lineares:

Proposição 1.31. *Sejam $\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_n \in L$, e suponhamos que, para $1 \leq i \leq n$, nós tenhamos $\gamma_i = \sum_{j=1}^n c_{ij}\alpha_j$, onde $c_{i1}, \ldots, c_{in} \in K$. Então*

$$\Delta_{L/K}(\gamma_1, \ldots, \gamma_n) = (\det(c_{ij}))^2 \Delta_{L/K}(\alpha_1, \ldots, \alpha_n).$$

Em particular, se $\alpha_1, \ldots, \alpha_n$ formarem uma base de L/K e se $T\colon L^n \to L^n$ for um operador K-linear, teremos:

$$\Delta_{L/K}(T(\alpha_1, \ldots, \alpha_n)) = (\det T)^2 \Delta_{L/K}(\alpha_1, \ldots, \alpha_n).$$

Demonstração. Notemos que, para $1 \leq i, j \leq n$, temos

$$\gamma_i \gamma_j = \left(\sum_{r=1}^n c_{ir}\alpha_r\right)\left(\sum_{s=1}^n c_{js}\alpha_s\right) = \sum_{r=1}^n \sum_{s=1}^n c_{ir}c_{js}\alpha_r\alpha_s.$$

Tomando o traço, obtemos $\mathrm{Tr}(\gamma_i\gamma_j) = \sum_{r=1}^n \sum_{s=1}^n c_{ir}c_{js}\,\mathrm{Tr}(\alpha_r\alpha_s)$. Desse modo, temos a igualdade de matrizes $(\mathrm{Tr}(\gamma_i\gamma_j)) = (c_{ij})(\mathrm{Tr}(\alpha_i\alpha_j))(c_{ij})^\intercal$. Tomando o determinante, obtemos a igualdade desejada. □

Consideremos a partir de agora L/K separável. Então temos exatamente n K-imersões de L, e podemos escrever o traço de um elemento em função dessas imersões. Denotaremos por $\sigma_1, \ldots, \sigma_n$ tais imersões. Essas imersões também podem ser usadas no cálculo do discriminante:

Proposição 1.32. *Sejam $\alpha_1, \ldots, \alpha_n \in L$ quaisquer. Então $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = (\det(\sigma_i(\alpha_j)))^2$.*

Demonstração. Sabemos que, para $1 \leq i, j \leq n$, vale

$$\mathrm{Tr}(\alpha_i\alpha_j) = \sum_{r=1}^n \sigma_r(\alpha_i\alpha_j) = \sum_{r=1}^n \sigma_r(\alpha_i)\sigma_r(\alpha_j).$$

Então temos a igualdade de matrizes $(\mathrm{Tr}(\alpha_i\alpha_j)) = (\sigma_i(\alpha_j))^\intercal(\sigma_i(\alpha_j))$. Tomando o determinante, obtemos a igualdade desejada. □

A partir disso podemos também, fixado um elemento $\alpha \in L$, associar o discriminante da n-upla $(1, \alpha, \ldots, \alpha^{n-1})$ com o discriminante de seu polinômio característico. Lembremos da definição de discriminante de um polinômio:

Definição (Discriminante de um Polinômio)**.** Seja $f(x) \in K[x]$ um polinômio mônico de grau n, e sejam $\alpha_1, \ldots, \alpha_n$ as n raízes de f num fecho algébrico Ω, contadas com as respectivas multiplicidades. Então o **discriminante** de f, denotado por $\Delta(f)$, é definido como sendo:

$$\Delta(f) \coloneqq \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Proposição 1.33. *Seja $\alpha \in L$ qualquer. Então temos:*

$$\begin{aligned}\Delta_{L/K}(1,\alpha,\ldots,\alpha^{n-1}) &= \prod_{1\le i<j\le n}(\sigma_j(\alpha)-\sigma_i(\alpha))^2 = \Delta(F_{\alpha,L/K}) \\ &= (-1)^{\binom{n}{2}} N_{L/K}(F'_{\alpha,L/K}(\alpha)),\end{aligned}$$

onde $F'_{\alpha,L/K}$ denota a derivada formal do polinômio $F_{\alpha,L/K}$.

Demonstração. Pela proposição acima, temos

$$\Delta(1,\alpha,\ldots,\alpha^{n-1}) = (\det(\sigma_i(\alpha^{j-1})))^2 = (\det(\sigma_i(\alpha)^{j-1}))^2.$$

Mas a matriz $(\sigma_i(\alpha)^{j-1})$ é uma matriz de Vandermonde, logo seu determinante é

$$\det(\sigma_i(\alpha)^{j-1}) = \prod_{1\le i<j\le n}(\sigma_j(\alpha)-\sigma_i(\alpha)).$$

Disto segue a primeira igualdade. Por outro lado, a igualdade

$$\prod_{1\le i<j\le n}(\sigma_j(\alpha)-\sigma_i(\alpha))^2 = \Delta(F_\alpha)$$

segue diretamente da definição do discriminante de um polinômio e do fato de que $F_\alpha(x) = \prod_{i=1}^n (x-\sigma_j(\alpha))$. Finalmente, mostremos a última igualdade. Pela regra de Leibniz, temos

$$F'_\alpha(x) = \sum_{j=1}^n (x-\sigma_1(\alpha))\cdots\widehat{(x-\sigma_j(\alpha))}\cdots(x-\sigma_n(\alpha)).$$

Assim, para $1 \le i \le n$ nós temos:

$$\begin{aligned}F'_\alpha(\sigma_i(\alpha)) &= \sum_{j=1}^n (\sigma_i(\alpha)-\sigma_1(\alpha))\cdots\widehat{(\sigma_i(\alpha)-\sigma_j(\alpha))}\cdots(\sigma_i(\alpha)-\sigma_n(\alpha)) \\ &= (\sigma_i(\alpha)-\sigma_1(\alpha))\cdots\widehat{(\sigma_i(\alpha)-\sigma_i(\alpha))}\cdots(\sigma_i(\alpha)-\sigma_n(\alpha)).\end{aligned}$$

Desse modo:

$$\begin{aligned}N(F'_\alpha(\alpha)) &= \prod_{i=1}^n \sigma_i(F'_\alpha(\alpha)) = \prod_{i=1}^n F'_\alpha(\sigma_i(\alpha)) \\ &= \prod_{i=1}^n [(\sigma_i(\alpha)-\sigma_1(\alpha))\cdots\widehat{(\sigma_i(\alpha)-\sigma_i(\alpha))}\cdots(\sigma_i(\alpha)-\sigma_n(\alpha))] \\ &= \prod_{1\le i<j\le n}(-1)^{1+2+\cdots+(n-1)}(\sigma_i(\alpha)-\sigma_j(\alpha))^2 \\ &= \prod_{1\le i<j\le n}(-1)^{\binom{n}{2}}(\sigma_i(\alpha)-\sigma_j(\alpha))^2 \\ &= (-1)^{\binom{n}{2}}\Delta(F_\alpha).\end{aligned}$$

Finalmente, obtemos que $\Delta(F_\alpha) = (-1)^{\binom{n}{2}} N(F'_\alpha(\alpha))$, como queríamos. □

Com o resultado acima, conseguimos mostrar que o discriminante é uma espécie de "determinante" no sentido de que ele determina se uma n-upla de L forma uma base da extensão L/K:

Teorema 1.34. *Sejam $\beta_1,\ldots,\beta_n \in L$. Então $\Delta_{L/K}(\beta_1,\ldots,\beta_n) \neq 0$ se e só se $\{\beta_1,\ldots,\beta_n\}$ for uma base de L/K.*

Demonstração. Tomemos $\alpha \in L$ elemento primitivo da extensão L/K. Como cada K-imersão de L é determinada inteiramente por α, temos $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ distintos dois a dois. Isso mostra, pela proposição acima, que $\Delta(1, \alpha, \ldots, \alpha^{n-1}) \neq 0$. Como $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de L/K, existe uma única transformação K-linear $T\colon L^n \to L^n$ tal que $T(1, \alpha, \ldots, \alpha^{n-1}) = (\beta_1, \ldots, \beta_n)$, e $\{\beta_1, \ldots, \beta_n\}$ será uma base de L/K se e só se $\det T \neq 0$. Pela Proposição 1.31, temos

$$\Delta(\beta_1, \ldots, \beta_n) = (\det T)^2 \Delta(1, \alpha, \ldots, \alpha^{n-1}),$$

de onde segue o resultado desejado. □

Nosso objetivo agora é associar uma base $\{\beta_1, \ldots, \beta_n\}$ de L/K a uma **base dual** $\{\beta_1', \ldots, \beta_n'\}$, que satisfaça $\mathrm{Tr}(\beta_i \beta_j') = \delta_{ij}$, para todos $1 \leq i, j \leq n$. Isso será uma consequência do seguinte lema:

Lema 1.35. *Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de L/K. Para quaisquer $c_1, \ldots, c_n \in K$, existe um único $\alpha \in L$ que satisfaz $\mathrm{Tr}_{L/K}(\beta_i \alpha) = c_i$, para todo $1 \leq i \leq n$.*

Demonstração. Seja $\alpha = \sum_{j=1}^{n} a_j \beta_j$, onde $a_1, \ldots, a_n \in K$. Então, para $1 \leq i \leq n$, temos:

$$\beta_i \alpha = \sum_{j=1}^{n} a_j \beta_i \beta_j \Rightarrow \mathrm{Tr}(\beta_i \alpha) = \sum_{j=1}^{n} a_j \, \mathrm{Tr}(\beta_i \beta_j).$$

Assim, procuramos $a_1, \ldots, a_n \in K$ tais que

$$\begin{bmatrix} \mathrm{Tr}(\beta_1^2) & \mathrm{Tr}(\beta_1\beta_2) & \ldots & \mathrm{Tr}(\beta_1\beta_n) \\ \mathrm{Tr}(\beta_2\beta_1) & \mathrm{Tr}(\beta_2^2) & \ldots & \mathrm{Tr}(\beta_2\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\beta_n\beta_1) & \mathrm{Tr}(\beta_n\beta_2) & \ldots & \mathrm{Tr}(\beta_n^2) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}.$$

Como $\det(\mathrm{Tr}(\beta_i \beta_j)) = \Delta(\beta_1, \ldots, \beta_n) \neq 0$ pelo Teorema 1.34, o sistema acima tem uma única solução $(a_1, \ldots, a_n) \in K^n$, o que mostra que existe um único $\alpha \in L$ satisfazendo as condições do enunciado. □

Teorema 1.36. *Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de L/K. Então existe uma única base $\{\beta_1', \ldots, \beta_n'\}$ de L/K tal que, para todos $1 \leq i, j \leq n$, valha $\mathrm{Tr}(\beta_i \beta_j') = \delta_{ij}$. Além disso, para todo $\alpha \in L$ temos:*

$$\alpha = \sum_{j=1}^{n} \mathrm{Tr}_{L/K}(\beta_j \alpha) \beta_j'.$$

*A base $\{\beta_1', \ldots, \beta_n'\}$ é chamada de **base dual** da base $\{\beta_1, \ldots, \beta_n\}$.*

Demonstração. A existência e a unicidade dos elementos $\beta_1', \ldots, \beta_n' \in L$ seguem do lema acima. Seja agora $\alpha = \sum_{j=1}^{n} a_j \beta_j'$, onde $a_1, \ldots, a_n \in K$. Então, para $1 \leq i \leq n$, temos:

$$\mathrm{Tr}(\beta_i \alpha) = \sum_{j=1}^{n} a_j \, \mathrm{Tr}(\beta_i \beta_j') = \sum_{j=1}^{n} a_j \delta_{ij} = a_i.$$

Assim, $\alpha = \sum_{j=1}^{n} \mathrm{Tr}(\beta_j \alpha) \beta_j'$. Em particular, se $\alpha = 0$, temos $a_1 = a_2 = \cdots = a_n = 0$, logo $\{\beta_1', \ldots, \beta_n'\}$ é um conjunto LI e portanto uma base de L/K. Portanto, todo $\alpha \in L$ pode ser escrito na forma acima. □

Suponhamos a partir de agora que A seja um domínio integralmente fechado com corpo de frações $K = Q(A)$ e que L seja uma extensão finita e separável de K de grau n. Chamemos $B = \overline{A}^L$. Se $\{\gamma_1, \ldots, \gamma_n\}$ for uma base de L/K, então é claro que para todo $d \in A \setminus \{0\}$ o conjunto $\{d\gamma_1, \ldots, d\gamma_n\}$ é também uma base de L/K. Pelo Teorema 1.16, $L = (A \setminus \{0\})^{-1}B$. Assim, podemos tomar d de forma que cada $d\gamma_i$ esteja em B. Isso mostra que podemos escolher uma base $\{\beta_1, \ldots, \beta_n\}$ de L/K com $\beta_1, \ldots, \beta_n \in B$.

Teorema 1.37. *Suponhamos que $\beta_1, \ldots, \beta_n \in B$ formem uma base de L/K, e que $\{\beta'_1, \ldots, \beta'_n\}$ seja sua base dual. Então B está entre dois A-módulos livres de posto n:*

$$A\beta_1 + \cdots + A\beta_n \subseteq B \subseteq A\beta'_1 + \cdots + A\beta'_n.$$

Em particular, se A for um anel noetheriano então B será um A-módulo finitamente gerado, e portanto um anel noetheriano.

Demonstração. $\{\beta_1, \ldots, \beta_n\}$ e $\{\beta'_1, \ldots, \beta'_n\}$ são conjuntos LI sobre $K = Q(A)$, logo também são LI sobre A pela Proposição 1.6. Isso mostra que os módulos indicados são de fato A-módulos livres de posto n.

Como cada $\beta_i \in B$, é claro que $A\beta_1 + \cdots + A\beta_n \subseteq B$. Por outro lado, se $\alpha \in B$ nós temos, para $1 \leq j \leq n$, $\beta_j\alpha \in B$. Então, pelo item (a) do Corolário 1.30, temos $\mathrm{Tr}(\beta_j\alpha) \in A$. Assim, pelo teorema acima, $\alpha = \sum_{j=1}^n \mathrm{Tr}(\beta_j\alpha)\beta'_j \in A\beta'_1 + \cdots + A\beta'_n$, mostrando as desigualdades desejadas.

Suponhamos agora A noetheriano. Então $A\beta'_1 + \cdots + A\beta'_n$, sendo finitamente gerado, é um A-módulo noetheriano. Sendo B um A-submódulo desse módulo, vemos que B também é um A-módulo noetheriano. Como os ideais de B são A-submódulos, é fácil ver que B é um anel noetheriano. □

No caso em que A é um DIP, podemos concluir de fato que B é um A-módulo livre de posto n. Para isso, recordemos alguns resultados de módulos livres sobre domínios de ideais principais, cujas demonstrações podem ser encontradas na Seção I.5 de [1]:

Teorema 1.38. *Sejam A um DIP, M um A-módulo livre de posto n e M' um submódulo de M. Então:*

(a) M' é um A-módulo livre de posto $q \leq n$.

(b) Existem uma base $\{\beta_1, \ldots, \beta_n\}$ de M e elementos $a_1, \ldots, a_q \in A$ tais que $a_1 \mid a_2 \mid \cdots \mid a_q$ e $\{a_1\beta_1, \ldots, a_q\beta_q\}$ é uma base de M'. Além disso, temos um isomorfismo de A-módulos:

$$M/M' \cong A/(a_1A) \times \cdots \times A/(a_qA) \times \underbrace{A \times \cdots \times A}_{n-q \text{ vezes}}.$$

Com esse teorema em mãos, nós obtemos:

Teorema 1.39. *Sejam A um DIP, $K = Q(A)$, L uma extensão separável de K de grau n e $B = \overline{A}^L$. Então B é um A-módulo livre de posto n. Uma base qualquer da extensão B/A é chamada de **base integral** da extensão B/A.*

Além disso, para um anel intermediário $A \subseteq R \subseteq L$ são equivalentes:

(i) $R \subseteq B$.

(ii) R é um A-módulo livre de posto $q \leq n$.

(iii) R é um A-módulo finitamente gerado.

Nesse caso, $q = n$ se e somente se $L = Q(R)$.

Demonstração. Pelo Teorema 1.37, B está entre dois A-módulos livres de posto n, e portanto deve ser um A-módulo livre de posto n pelo teorema acima. $(i) \Rightarrow (ii)$ segue diretamente do fato de B ser um A-módulo livre de posto n e do teorema acima, $(ii) \Rightarrow (iii)$ é óbvia e $(iii) \Rightarrow (i)$ segue diretamente do Corolário 1.12. Provemos agora que $q = n$ se e só se $L = Q(R)$:

$(\Rightarrow)$: Suponhamos $q = n$. Então existem $r_1, \ldots, r_n \in R$ linearmente independentes sobre A. Mas isso equivale a $r_1, \ldots, r_n \in R \subseteq L$ serem linearmente independentes sobre $Q(A) = K$, e como $[L : K] = n$ vemos que $Kr_1 + \cdots + Kr_n = L$. Como $A \subseteq R$ e $K = Q(A)$, concluímos que $L = Q(R)$.

$(\Leftarrow)$: Suponhamos $L = Q(R)$. Notemos que $(A \setminus \{0\})^{-1}R$ é um anel intermediário da extensão L/K, e portanto é um corpo. Como $Q(R) = L$, vemos que $L = (A \setminus \{0\})^{-1}R$. Seja γ um elemento primitivo da extensão L/K, ou seja, $L = K(\gamma)$. Como $L = (A \setminus \{0\})^{-1}R$, existem $r \in R$ e $s \in A \setminus \{0\}$ tais que $\gamma = r/s$. Então é claro que $L = K(r)$. Desse modo, $1, r, r^2, \ldots, r^{n-1}$ são elementos linearmente independentes sobre K, e portanto sobre A. Isso prova que $q \geq n$. Mas $q \leq n$, logo $q = n$. □

Voltemos a considerar o caso em que A é apenas um domínio integralmente fechado (não necessariamente um DIP). Conseguimos mais algumas informações acerca do discriminante:

Proposição 1.40. *Para quaisquer $\alpha_1, \ldots, \alpha_n \in B$, temos $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) \in A$.*

Demonstração. Segue diretamente da definição do discriminante de uma n-upla e do Corolário 1.30 que $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)) \in A$. □

Proposição 1.41. *Suponhamos que $\beta_1, \ldots, \beta_n \in B$ formem uma base de L/K, e denotemos $d := \Delta(\beta_1, \ldots, \beta_n) \in A$. Então $dB \subseteq A\beta_1 + \cdots + A\beta_n$.*

Demonstração. Isso é equivalente a termos $B \subseteq Ad^{-1}\beta_1 + \cdots + Ad^{-1}\beta_n$. Pelo Teorema 1.37, sabemos que $B \subseteq A\beta_1' + \cdots + A\beta_n'$. Assim, basta mostrarmos que vale:

$$A\beta_1' + \cdots + A\beta_n' \subseteq Ad^{-1}\beta_1 + \cdots + Ad^{-1}\beta_n.$$

Seja $1 \leq k \leq n$. Note que definimos $\beta_k' = \sum_{j=1}^n a_j\beta_j$, de modo que tenhamos

$$\begin{bmatrix} \mathrm{Tr}(\beta_1^2) & \mathrm{Tr}(\beta_1\beta_2) & \ldots & \mathrm{Tr}(\beta_1\beta_n) \\ \mathrm{Tr}(\beta_2\beta_1) & \mathrm{Tr}(\beta_2^2) & \ldots & \mathrm{Tr}(\beta_2\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\beta_n\beta_1) & \mathrm{Tr}(\beta_n\beta_2) & \ldots & \mathrm{Tr}(\beta_n^2) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = e_k.$$

Assim, pela regra de Kramer, cada coeficiente a_ℓ de β_k' é dado por um elemento de A quocientado por $\det(Tr(\beta_i\beta_j)) = d$. Então cada coeficiente de β_k' está em $d^{-1}A$, e portanto

$$\beta_k' \in Ad^{-1}\beta_1 + \cdots + Ad^{-1}\beta_n.$$

Com isso, concluímos a demonstração. □

A Proposição 1.40 nos garante que a definição a seguir faz sentido:

Definição (Ideal Discriminante)**.** Seja R um anel tal que $A \subseteq R \subseteq B$. Então o **ideal discriminante** de R/A, denotado $\mathfrak{d}_{R/A}$, é o ideal de A gerado pelos elementos da forma $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n)$, onde $\alpha_1, \ldots, \alpha_n$ percorrem todos os elementos de R.

Proposição 1.42. *Seja R um anel tal que $A \subseteq R \subseteq B$, e suponhamos que R seja um A-módulo livre com base $\beta_1, \ldots, \beta_n$. Então:*

(a) $\mathfrak{d}_{R/A}$ *é um ideal principal, gerado por* $\Delta_{L/K}(\beta_1, \ldots, \beta_n)$.

Além disso, para quaisquer elementos $\alpha_1, \ldots, \alpha_n \in R$, *temos:*

(b) $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = a^2 \Delta_{L/K}(\beta_1, \ldots, \beta_n)$, *para algum* $a \in A$.

(c) $\{\alpha_1, \ldots, \alpha_n\}$ *será uma base de* R *como* A*-módulo se e só se* $a \in A^\times$.

Demonstração. Escrevamos, para cada i, $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$, com cada $a_{ij} \in A$. Então pela Proposição 1.31 temos $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = a^2 \Delta_{L/K}(\beta_1, \ldots, \beta_n)$, para $a = \det(a_{ij}) \in A$. Isso prova (a) e (b). Para provar (c), notemos que $\alpha_1, \ldots, \alpha_n$ será uma base de R se e só se a matriz (a_{ij}) for inversível, ou seja, se e só se $a \in A^\times$. □

Um exemplo importante da proposição acima é o caso em que $R = A[\beta]$, para algum $\beta \in B$ elemento primitivo da extensão L/K. Com efeito:

Proposição 1.43. *Para qualquer* $\beta \in B$, *as seguintes condições são equivalentes:*

(i) $L = K(\beta)$.

(ii) $1, \beta, \ldots, \beta^{n-1}$ *formam uma base do* A*-módulo* $A[\beta]$.

Nesse caso, $\mathfrak{d}_{A[\beta]/A}$ *é gerado pelo elemento* $\Delta_{L/K}(1, \beta, \ldots, \beta^{n-1})$.

Demonstração. $(i) \Rightarrow (ii)$: Suponhamos que $L = K(\beta)$. Temos $1, \beta, \ldots, \beta^{n-1}$ LI sobre K, e portanto também sobre A pela Proposição 1.6. Além disso, é claro que esses elementos geram $A[\beta]$, provando essa implicação.

$(ii) \Rightarrow (i)$: Suponhamos que $1, \beta, \ldots, \beta^{n-1}$ formem uma base do A-módulo $A[\beta]$. Sendo esses elementos linearmente independentes sobre A, eles também o são sobre K, pela Proposição 1.6. Como eles formam um conjunto de $n = [L : K]$ elementos, eles formam uma base de L/K, e portanto $L = K(\beta)$, como desejado.

A última afirmação segue da proposição acima. □

1.5. Extensões de Ideais

Nesta seção, vemos como podemos associar os ideais do anel maior e do anel menor em uma extensão de anéis. Começamos com a definição a seguir:

Definição (Restrição de Ideais/Extensão de Ideais/Ideal sobre o Outro)**.** Seja B/A uma extensão de anéis.

- Se $\mathfrak{A} \lhd B$, dizemos que $\mathfrak{A} \cap A \lhd A$ é a **restrição** de $\mathfrak{A}$ ao anel A.
- Se $\mathfrak{a} \lhd A$, dizemos que $\mathfrak{a}B \lhd B$ é a **extensão** de $\mathfrak{a}$ ao anel B.
- Dizemos que um ideal $\mathfrak{A} \lhd B$ está **sobre** $\mathfrak{a}$ se $\mathfrak{a} = \mathfrak{A} \cap A$, ou seja, se $\mathfrak{a}$ for a restrição de $\mathfrak{A}$ a A, e denotamos $\mathfrak{A} \mid \mathfrak{a}$.

Proposição 1.44. *(a) Se* $\mathfrak{A} \lhd B$ *for um ideal próprio de* B, *então sua restrição* $\mathfrak{A} \cap A$ *será um ideal próprio de* A.

(b) Se $\mathfrak{P} \lhd B$ *for um ideal primo, então sua restrição* $\mathfrak{P} \cap A \lhd A$ *será um ideal primo.*

(c) Se $\mathfrak{A} \lhd B$ for um ideal sobre $\mathfrak{a} \lhd A$, então a inclusão canônica $A \hookrightarrow B$ induz uma inclusão $A/\mathfrak{a} \hookrightarrow B/\mathfrak{A}$, dada por $x + \mathfrak{a} \mapsto x + \mathfrak{A}$.

Demonstração. (a) Se $\mathfrak{A} \lhd B$ for um ideal próprio, então $1 \notin \mathfrak{A} \Rightarrow 1 \notin \mathfrak{A} \cap A$, mostrando que $\mathfrak{A} \cap A$ é um ideal próprio de A.

(b) Pelo item (a), $\mathfrak{P} \cap A$ será um ideal próprio de A. Suponhamos agora que $x, y \in A$ sejam tais que $xy \in \mathfrak{P} \cap A$. Então, como $\mathfrak{P}$ é primo, $x \in \mathfrak{P}$ ou $y \in \mathfrak{P}$, e portanto $x \in \mathfrak{P} \cap A$ ou $y \in \mathfrak{P} \cap A$. Isso prova que $\mathfrak{P} \cap A$ é um ideal primo de A.

(c) Essa função está bem-definida e é injetora, pois dados $x, y \in A$ quaisquer nós temos:

$$x + \mathfrak{A} = y + \mathfrak{A} \iff x - y \in \mathfrak{A} \iff x - y \in \mathfrak{A} \cap A = \mathfrak{a} \iff x + \mathfrak{a} = y + \mathfrak{a}.$$

Finalmente, essa função é claramente um homomorfismo.

□

Observação 1.45. *A inclusão $A/\mathfrak{a} \hookrightarrow B/\mathfrak{A}$ do item (c) dessa proposição nos permite ver $A/\mathfrak{a}$ como um subanel de $B/\mathfrak{A}$ (ou o que é o mesmo, ver $B/\mathfrak{A}$ como uma extensão de $A/\mathfrak{a}$). Faremos isso diretamente daqui para a frente, e nos referiremos à inclusão $A/\mathfrak{a} \hookrightarrow B/\mathfrak{A}$ como a* ***inclusão canônica*** *de $A/\mathfrak{a}$ em $B/\mathfrak{A}$.*

Um problema das aplicações de extensão e restrição de ideais é que elas não necessariamente são inversas uma da outra. Obviamente, $(\mathfrak{A} \cap A)B \subseteq \mathfrak{A}B = \mathfrak{A}$, e $\mathfrak{a}B \cap A \supseteq \mathfrak{a}$, mas as inclusões contrárias podem não valer. Assim, não é tão simples o problema de, dado um ideal $\mathfrak{a} \lhd A$, encontrarmos $\mathfrak{A} \lhd B$ que esteja sobre $\mathfrak{A}$. Esse ideal pode nem existir!

Denotemos o conjunto dos ideais de A por $\mathscr{I}$ e o conjunto dos ideais de B por $\mathscr{J}$. Então as operações de extensão e restrição de ideais nos dão duas funções $\varepsilon\colon \mathscr{I} \to \mathscr{J}$ e $\rho\colon \mathscr{J} \to \mathscr{I}$, que como já vimos podem não ser inversas uma da outra. No entanto, temos as seguintes propriedades, cujas demonstrações são diretas:

Proposição 1.46. *As funções ε e ρ satisfazem as seguintes propriedades (onde temos $\mathfrak{a}, \mathfrak{b} \in \mathscr{I}, \mathfrak{A}, \mathfrak{B} \in \mathscr{J}$ quaisquer:*

(a) ε e ρ preservam inclusões, isto é, se $\mathfrak{a} \subseteq \mathfrak{b}$ então $\varepsilon\mathfrak{a} \subseteq \varepsilon\mathfrak{b}$, e se $\mathfrak{A} \subseteq \mathfrak{B}$ então $\rho\mathfrak{A} \subseteq \rho\mathfrak{B}$.

(b) $\varepsilon(\mathfrak{a} + \mathfrak{b}) = \varepsilon\mathfrak{a} + \varepsilon\mathfrak{b}$.

(c) $\varepsilon(\mathfrak{a}\mathfrak{b}) = \varepsilon\mathfrak{a} \cdot \varepsilon\mathfrak{b}$.

(d) $\rho(\mathfrak{A} \cap \mathfrak{B}) = \rho\mathfrak{A} \cap \rho\mathfrak{B}$.

(e) $\rho(\sqrt{\mathfrak{A}}) = \sqrt{\rho\mathfrak{A}}$.

(f) $\rho\varepsilon\mathfrak{a} \supseteq \mathfrak{a}$, e vale a igualdade se e só se $\mathfrak{a}$ estiver na imagem de ρ.

(g) $\varepsilon\rho\mathfrak{A} \subseteq \mathfrak{A}$, e vale a igualdade se e só se $\mathfrak{A}$ estiver na imagem de ε.

(h) $\varepsilon\rho\varepsilon = \varepsilon$ e $\rho\varepsilon\rho = \rho$.

(i) ε será injetora se e só $\rho\varepsilon = \mathrm{id}_{\mathscr{I}}$, se e só se ρ for sobrejetora.

(j) ρ será injetora se e só $\varepsilon\rho = \mathrm{id}_{\mathscr{J}}$, se e só se ε for sobrejetora.

(k) ε e ρ induzem aplicações bijetoras, inversas entre si, entre os conjuntos $\rho(\mathscr{J})$ e $\varepsilon(\mathscr{I})$.

(l) Se $\mathfrak{a}$ e $\mathfrak{b}$ forem ideais coprimos, suas extensões $\varepsilon\mathfrak{a}$ e $\varepsilon\mathfrak{b}$ também serão ideais coprimos.

Será importante para nós estudar as propriedades de ε e ρ no caso em que A é um domínio e que $B = S^{-1}A$, para algum conjunto multiplicativo $S \subseteq A \setminus \{0\}$. Se tivermos $S = A \setminus \{0\}$, $B = Q(A)$ é seu corpo de frações, e temos $\mathscr{J} = \{0, B\}$. Assim, é claro que ε é sobrejetora e ρ é injetora. No caso geral, vale o seguinte:

Proposição 1.47. *(a) Para todo $\mathfrak{a} \lhd A$ nós temos $\mathfrak{a} \cdot S^{-1}A = S^{-1}\mathfrak{a}$. Em particular, $\mathfrak{a} \cdot S^{-1}A = S^{-1}A$ se e só se $\mathfrak{a} \cap S \neq \emptyset$.*

(b) ε é sempre sobrejetora e ρ é sempre injetora nesse caso, e temos $\varepsilon\rho = \mathrm{id}_{\mathscr{J}}$. Em particular, para todo $\mathfrak{A} \lhd S^{-1}A$ nós temos $(\mathfrak{A} \cap A) \cdot S^{-1}A = \mathfrak{A}$.

Demonstração. (a) É claro.

(b) Pelo item (j) da proposição acima, basta mostrar que ε é sobrejetora. Mas isso é verdade, já que pela teoria de localização todo ideal de $S^{-1}A$ é da forma $S^{-1}\mathfrak{a} = \mathfrak{a} \cdot S^{-1}A = \varepsilon(\mathfrak{a})$, para algum $\mathfrak{a} \lhd A$.

□

Sendo A um domínio, o mapa de localização $A \to S^{-1}A$ é uma inclusão. Sabemos da teoria de localização que existe uma bijeção entre os ideais primos de A que não intersectam S e os ideais primos de $S^{-1}A$. Mostraremos que nesse caso ε e ρ são bijeções entre esses conjuntos. O fato de ε ser uma bijeção não é uma novidade, dado que a proposição que acabamos de mostrar nos diz que $\varepsilon\mathfrak{a} = S^{-1}\mathfrak{a}$ e essa é justamente a correspondência dada pela teoria de localização. O mais interessante é o fato da restrição ρ ser sua inversa:

Teorema 1.48. *(a) Seja $\mathfrak{P} \lhd S^{-1}A$ primo. Então $\mathfrak{P} \cap A$ é um ideal primo de A que não intersecta S, e nós temos $(\mathfrak{P} \cap A) \cdot S^{-1}A = \mathfrak{P}$.*

(b) Seja $\mathfrak{p}$ um ideal primo de A que não intersecta S. Então $\mathfrak{p} \cdot S^{-1}A = S^{-1}\mathfrak{p}$ é um ideal primo de $S^{-1}A$, e $(\mathfrak{p} \cdot S^{-1}A) \cap A = (S^{-1}\mathfrak{p}) \cap A = \mathfrak{p}$.

(c) As aplicações ε e ρ induzem aplicações bijetoras, inversas entre si, entre o conjunto dos ideais primos de A que não intersectam S e o conjunto dos ideais primos de $S^{-1}A$.

Demonstração. (a) É claro que $\mathfrak{P} \cap S = \emptyset$, caso contrário teríamos $1 \in \mathfrak{P} \Rightarrow \mathfrak{P} = S^{-1}A$. Assim, $\mathfrak{P} \cap A \lhd A$ é primo que não intersecta S. A última igualdade segue do item (b) da proposição anterior.

(b) Pela teoria de localização sabemos que $S^{-1}\mathfrak{p}$ é um ideal primo de $S^{-1}A$. Assim, basta mostrarmos que $(S^{-1}\mathfrak{p}) \cap A = \mathfrak{p}$. A igualdade $(\supseteq)$ é clara. Para a igualdade contrária, tomemos $x \in (S^{-1}\mathfrak{p}) \cap A$. Então $x = p/s$, para $p \in \mathfrak{p}$ e $s \in S$, e $sx = p \in \mathfrak{p}$. Como $\mathfrak{p}$ é primo e $s \notin \mathfrak{p}$, devemos ter $x \in \mathfrak{p}$, como desejado.

(c) Segue diretamente dos itens anteriores.

□

Dado um ideal $\mathfrak{a} \lhd A$ podemos considerar o homomorfismo canônico $A/\mathfrak{a} \to S^{-1}A/S^{-1}\mathfrak{a}$ dado por $x + \mathfrak{a} \mapsto x + S^{-1}\mathfrak{a}$. O núcleo desse homomorfismo é igual ao conjunto $\{x + \mathfrak{a} \colon x \in (S^{-1}\mathfrak{a}) \cap A\}$, e portanto ele será uma inclusão se e só se valer $(S^{-1}\mathfrak{a}) \cap A = \mathfrak{a}$, ou seja, se e só se $S^{-1}\mathfrak{a} \mid \mathfrak{a}$.

Corolário 1.49. *Se $\mathfrak{p} \lhd A$ for um primo que não intersecta S, então o homomorfismo canônico $A/\mathfrak{p} \to S^{-1}A/S^{-1}\mathfrak{p}$ será uma inclusão. Se $\mathfrak{p}$ for um ideal maximal, esse homomorfismo será um isomorfismo, e portanto $A/\mathfrak{p} \cong S^{-1}A/S^{-1}\mathfrak{p}$.*

Demonstração. Esse homomorfismo é uma inclusão porque para $\mathfrak{p}$ primo que não intersecta S nós temos $(S^{-1}\mathfrak{p}) \cap A = \mathfrak{p}$ pelo Teorema 1.48. Suponhamos agora $\mathfrak{p}$ maximal, e seja $a/s \in S^{-1}A$ qualquer. Queremos mostrar que $a/s + S^{-1}\mathfrak{p}$ está na imagem do homomorfismo. Nós temos $sA + \mathfrak{p} = A$. Em particular, $a = sx + p$ para alguns $x \in A$, $p \in \mathfrak{p}$, e assim em $S^{-1}A$ temos $a/s = x + p/s \Rightarrow a/s + S^{-1}\mathfrak{p} = x + S^{-1}\mathfrak{p}$, que está na imagem desse homomorfismo, como queríamos. □

O seguinte resultado, envolvendo localização, não precisa de nenhuma hipótese sobre a extensão B/A.

Proposição 1.50. *Sejam B/A uma extensão de anéis, S um conjunto multiplicativo de A e $\mathfrak{p} \lhd A$ um primo que não intersecta S. Então os ideais primos de B sobre $\mathfrak{p}$ estão em bijeção com os ideais primos de $S^{-1}B$ sobre o ideal primo $S^{-1}\mathfrak{p} \lhd S^{-1}A$. Nessa bijeção, um ideal $\mathfrak{P} \lhd B$ sobre $\mathfrak{p}$ é levado em $S^{-1}\mathfrak{P}$.*

Em particular, isso ocorre se $S = A \setminus \mathfrak{p}$, de modo que os ideais primos de B sobre $\mathfrak{p}$ estão em bijeção com os ideais primos de $B_\mathfrak{p}$ sobre $\mathfrak{p}_\mathfrak{p}$, bijeção esta dada por $\mathfrak{P} \mapsto \mathfrak{P}_\mathfrak{p}$.

Demonstração. Seja $\mathfrak{P} \lhd B$ sobre $\mathfrak{p}$. Então $S^{-1}\mathfrak{P} \cap S^{-1}A = S^{-1}(\mathfrak{P} \cap A) = S^{-1}\mathfrak{p}$. Além disso, $S^{-1}\mathfrak{P}$ é um ideal primo de $S^{-1}B$, pois $\mathfrak{P}$ é um ideal primo de B que não intersecta S.

Por outro lado, se um ideal primo $\mathfrak{Q} \lhd S^{-1}B$ estiver sobre $S^{-1}\mathfrak{p}$, então $\mathfrak{Q} = S^{-1}\mathfrak{P}$ para um ideal primo $\mathfrak{P}$ de B que não intersecta S. Nós temos $S^{-1}(\mathfrak{P} \cap A) = S^{-1}\mathfrak{P} \cap S^{-1}A = S^{-1}\mathfrak{p}$. Como $\mathfrak{p}$ e $\mathfrak{P} \cap A$ são primos de A que não intersectam S, a bijeção entre os ideais primos de A que não intersectam S e os ideais primos de $S^{-1}A$ nos permite concluir que $\mathfrak{p} = \mathfrak{P} \cap A$. □

Essa proposição é especialmente útil para reduzir o problema de provar que uma propriedade vale para todos os ideais primos de um anel para provar que ela vale apenas para os ideais maximais desse anel. Outra utilidade interessante é conseguir reduzir o problema inicial para um anel local.

Com esse resultado em mãos podemos mostrar que, dado $\mathfrak{p} \lhd A$ primo, a existência de um ideal primo de B sobre $\mathfrak{p}$ é equivalente à existência de um ideal qualquer sobre $\mathfrak{p}$. Lembremos que $\rho\varepsilon\,\mathfrak{p} = \mathfrak{p}$ é equivalente a $\mathfrak{p}$ estar na imagem de ρ. Comecemos com o seguinte lema:

Lema 1.51. *Sejam $\mathfrak{a}, \mathfrak{p} \lhd A$ ideais de A que não intersectam S, onde $\mathfrak{p}$ é primo. Suponhamos que $S^{-1}\mathfrak{a} \subseteq S^{-1}\mathfrak{p}$. Então $\mathfrak{a} \subseteq \mathfrak{p}$.*

Demonstração. Seja $a \in \mathfrak{a}$ qualquer. Então $a/1 \in S^{-1}\mathfrak{a} \subseteq S^{-1}\mathfrak{p}$, e portanto $a/1 = p/s$ para alguns $p \in \mathfrak{p}$, $s \in S$. Isso significa que existe $t \in S$ com $ast = pt \in \mathfrak{p}$. Como $\mathfrak{p}$ é primo e $s, t \notin \mathfrak{p}$, concluímos que $a \in \mathfrak{p}$. Desse modo, $\mathfrak{a} \subseteq \mathfrak{p}$, como queríamos. □

Teorema 1.52. *Seja B/A uma extensão de anéis e seja $\mathfrak{p} \lhd A$ primo. Então existe um primo $\mathfrak{P} \lhd B$ sobre $\mathfrak{p}$ se e só se $\mathfrak{p}B \cap A = \mathfrak{p}$.*

Demonstração. Observemos que a implicação ($\Rightarrow$) é imediata, já que isso implica que $\mathfrak{p} = \rho\mathfrak{P}$. Assim, provemos a implicação ($\Leftarrow$). Suponhamos que $\mathfrak{p}B \cap A = \mathfrak{p}$, e localizemos por $S = A \setminus \mathfrak{p}$. Pela Proposição 1.50, basta mostrarmos que existe um ideal primo de $B_\mathfrak{p}$ sobre $\mathfrak{p}_\mathfrak{p}$. Como vale a igualdade $\mathfrak{p}B \cap A = \mathfrak{p}$, temos $\mathfrak{p}B \cap S = \emptyset$, e portanto sua localização $(\mathfrak{p}B)_\mathfrak{p}$ é um ideal próprio de $B_\mathfrak{p}$. Tomemos um ideal maximal de $B_\mathfrak{p}$ que contém o ideal $(\mathfrak{p}B)_\mathfrak{p}$. Ele é da forma $\mathfrak{P}_\mathfrak{p}$, para algum $\mathfrak{P} \lhd B$ primo que não intersecta S. Provemos que $\mathfrak{P} \mid \mathfrak{p}$. Como $\mathfrak{P} \cap S = \emptyset$ e $S = A \setminus \mathfrak{p}$, nós temos $\mathfrak{P} \cap A \subseteq \mathfrak{p}$. Como $(\mathfrak{p}B)_\mathfrak{p} \subseteq \mathfrak{P}_\mathfrak{p}$, o Lema 1.51 nos garante que $\mathfrak{p}B \subseteq \mathfrak{P}$, e assim $\mathfrak{p} = \mathfrak{p}B \cap A \subseteq \mathfrak{P} \cap A$. Provamos assim que $\mathfrak{P} \cap A = \mathfrak{p}$, e assim $\mathfrak{P}$ é um ideal primo de B sobre $\mathfrak{p}$. □

No caso em que B/A é uma extensão integral de domínios, nós podemos obter mais informações:

Teorema 1.53. *Seja B/A uma extensão integral de domínios. Então:*

(a) Se $\mathfrak{A} \lhd B$ for um ideal não-nulo de B, $\mathfrak{A} \cap A$ será um ideal não-nulo de A.

(b) Se $\mathfrak{A} \lhd B$ e $\mathfrak{a} \lhd A$ forem tais que $\mathfrak{A} \mid \mathfrak{a}$, então $B/\mathfrak{A}$ será uma extensão integral de $A/\mathfrak{a}$.

(c) $B^\times \cap A = A^\times$.

(d) B será um corpo se e só se A for um corpo.

(e) Um ideal primo $\mathfrak{P}$ de B será um ideal maximal de B se e só se $\mathfrak{P} \cap A$ for um ideal maximal de A. Em particular, se todo ideal primo não-nulo de A for maximal, todo ideal primo não-nulo de B também será maximal.

Demonstração. (a) Suponhamos $\mathfrak{A} \neq 0$, e tomemos $\alpha \in \mathfrak{A}$ não-nulo. Como B/A é integral, temos $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$, para alguns $a_0, \ldots, a_{n-1} \in A$. Podemos supor sem perda de generalidade $a_0 \neq 0$, pois B é um domínio. Assim, nós temos $a_0 \in \alpha B \subseteq \mathfrak{A}$, e portanto $a_0 \in \mathfrak{A} \cap A$ é não-nulo.

(b) Consideremos a projeção canônica $\pi\colon B \to B/\mathfrak{A}$. Como B é integral sobre A, pela Proposição 1.11 o anel $B/\mathfrak{A}$ é integral sobre $\pi(A)$. Notemos agora que $\pi(A)$ é igual a $A/\mathfrak{a}$, com a identificação da Observação 1.45. Então $B/\mathfrak{A}$ é integral sobre $A/\mathfrak{a}$, como gostaríamos.

(c) É claro que $A^\times \subseteq B^\times \cap A$. Seja agora $u \in B^\times \cap A$. Como B/A é integral, u^{-1} é integral sobre A, e assim $a_0 + a_1/u + \cdots + a_{n-1}/u^{n-1} + 1/u^n = 0$, para alguns $a_0, \ldots, a_{n-1} \in A$. Multiplicando essa equação por u^{n-1}, obtemos:

$$a_0u^{n-1} + a_1u^{n-2} + \cdots + a_{n-1} + u^{-1} = 0 \Rightarrow u^{-1} = -a_{n-1} - \ldots - a_0u^{n-1} \in A.$$

Assim, o inverso de u está em A, o que mostra que $u \in A^\times$. Concluímos que $B^\times \cap A \subseteq A^\times$, e portanto $A^\times = B^\times \cap A$.

(d) Se B for um corpo, $B^\times = B \setminus \{0\} \Rightarrow A^\times = B^\times \cap A = B \setminus \{0\} \cap A = A \setminus \{0\}$, pelo item (c). Logo A é um corpo. Se A for um corpo, os únicos ideais de A serão 0 e A. Se $\mathfrak{A} \lhd B$ for não-nulo, então pelo item (a) o ideal $\mathfrak{A} \cap A \lhd A$ será não-nulo, de modo que $\mathfrak{A} \cap A = A$. Mas então $1 \in \mathfrak{A} \Rightarrow \mathfrak{A} = B$. Logo os únicos ideais de B são 0 e B, e portanto B é um corpo.

(e) Seja $\mathfrak{P} \lhd B$ primo. Pelo item (b), o domínio $B/\mathfrak{P}$ é integral sobre $A/(\mathfrak{P} \cap A)$. Assim, pelo item (d), $B/\mathfrak{P}$ será um corpo se e só se $A/(\mathfrak{P} \cap A)$ for um corpo. Ou seja, $\mathfrak{P}$ será um ideal maximal de B se e só se $\mathfrak{P} \cap A$ for um ideal maximal de A.

□

Com a hipótese de B/A ser uma extensão integral de domínios, nós podemos garantir que todo ideal primo de A possui um primo de B sobre ele, resultado clássico conhecido como **lying-over**. Ele será uma consequência direta do seguinte teorema:

Teorema 1.54. *Sejam B/A uma extensão integral de domínios e $\mathfrak{p} \lhd A$ primo. Então:*

(a) Para todo ideal $\mathfrak{A} \lhd B$ tal que $\mathfrak{A} \cap A \subseteq \mathfrak{p}$, existe um ideal primo $\mathfrak{P} \lhd B$ sobre $\mathfrak{p}$ com $\mathfrak{A} \subseteq \mathfrak{P}$.

(b) Os ideais primos $\mathfrak{P} \lhd B$ sobre $\mathfrak{p}$ são os elementos maximais do conjunto $\{\mathfrak{A} \lhd B\colon\ \mathfrak{A} \cap A \subseteq \mathfrak{p}\}$.

Demonstração. (a) Seja $S = A \setminus \mathfrak{p}$, e consideremos $\mathfrak{A} \lhd B$ com $\mathfrak{A} \cap A \subseteq \mathfrak{p}$. Então $\mathfrak{A} \cap S = \emptyset$, e portanto $\mathfrak{A}_\mathfrak{p}$ é um ideal próprio de $B_\mathfrak{p}$. Podemos tomar um ideal maximal de $B_\mathfrak{p}$ que contém $\mathfrak{A}_\mathfrak{p}$. Ele é da forma $\mathfrak{P}_\mathfrak{p}$, para algum ideal primo $\mathfrak{P} \lhd B$. Como B/A é integral, $B_\mathfrak{p}/A_\mathfrak{p}$ também é integral pela Proposição 1.15. Assim, pelo item (e) do Teorema 1.53, $\mathfrak{P}_\mathfrak{p} \cap A_\mathfrak{p}$ é um ideal maximal de $A_\mathfrak{p}$. Mas $A_\mathfrak{p}$ é um anel local com anel maximal $\mathfrak{p}_\mathfrak{p}$, e portanto $\mathfrak{P}_\mathfrak{p} \cap A_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$. Desse modo, $\mathfrak{P}_\mathfrak{p}$ é um ideal primo sobre $\mathfrak{p}_\mathfrak{p}$, e pela Proposição 1.50 nós concluímos que $\mathfrak{P}$ é um ideal primo sobre $\mathfrak{p}$. Finalmente, temos $\mathfrak{A}_\mathfrak{p} \subseteq \mathfrak{P}_\mathfrak{p} \Rightarrow \mathfrak{A} \subseteq \mathfrak{P}$, pelo Lema 1.51. Assim, $\mathfrak{P}$ é o ideal primo desejado.

(b) Pelo item (a), se $\mathfrak{A} \lhd B$ for tal que $\mathfrak{A} \cap A \subseteq \mathfrak{p}$, então existirá $\mathfrak{P} \lhd B$ primo com $\mathfrak{A} \subseteq \mathfrak{P}$ e $\mathfrak{P} \cap A = \mathfrak{p}$. Isso mostra que todos os elementos maximais desse conjunto são ideais primos sobre $\mathfrak{p}$.

Provaremos agora que todo primo $\mathfrak{P} \lhd B$ sobre $\mathfrak{P}$ é um elemento maximal desse conjunto. Para isso, suponhamos que $\mathfrak{A} \lhd B$ seja tal que $\mathfrak{A} \cap A \subseteq \mathfrak{p}$ e $\mathfrak{P} \subseteq \mathfrak{A}$. Queremos mostrar que $\mathfrak{A} = \mathfrak{P}$. Seja $\mathfrak{Q} \lhd B$ primo sobre $\mathfrak{p}$ com $\mathfrak{A} \subseteq \mathfrak{Q}$. Então $\mathfrak{P} \subseteq \mathfrak{A} \subseteq \mathfrak{Q}$. Localizando em relação a $\mathfrak{p}$, temos que $\mathfrak{P}_\mathfrak{p}$ e $\mathfrak{Q}_\mathfrak{p}$ são ambos ideais primos de $B_\mathfrak{p}$ sobre $\mathfrak{p}_\mathfrak{p}$, pela Proposição 1.50, com $\mathfrak{P}_\mathfrak{p} \subseteq \mathfrak{Q}_\mathfrak{p}$. Mas pelo item (e) do Teorema 1.53, $\mathfrak{P}_\mathfrak{p}$ e $\mathfrak{Q}_\mathfrak{p}$ são ambos maximais. Isso implica que $\mathfrak{P}_\mathfrak{p} = \mathfrak{Q}_\mathfrak{p}$, e portanto em $\mathfrak{P} = \mathfrak{Q}$ pelo Lema 1.51. Então $\mathfrak{P} \subseteq \mathfrak{A} \subseteq \mathfrak{Q} = \mathfrak{P} \Rightarrow \mathfrak{A} = \mathfrak{P}$, como desejado.

□

Aplicando o item (a) do teorema acima para $\mathfrak{A} = 0$, obtemos imediatamente:

Corolário 1.55. *(Lying Over) Sejam B/A uma extensão integral de domínios e $\mathfrak{p} \lhd A$ primo. Então existe um ideal primo $\mathfrak{P} \lhd B$ sobre $\mathfrak{p}$.*

Por lying-over, todo primo $\mathfrak{p} \lhd A$ está na imagem de ρ, e portanto em particular vale a igualdade $\mathfrak{p}\,B \cap A = \mathfrak{p}$. Notemos que se $\mathfrak{A} \lhd B$ está sobre $\mathfrak{p}$, então $\mathfrak{A} \supseteq \varepsilon\rho\,\mathfrak{A} = \varepsilon\,\mathfrak{p} = \mathfrak{p}\,B$. Isso, juntamente com o Teorema 1.54, nos dá:

Corolário 1.56. *Sejam B/A uma extensão integral de domínios e $\mathfrak{p} \lhd A$ primo. Então o conjunto dos ideais de B sobre $\mathfrak{p}$ tem como elemento minimal o ideal $\mathfrak{p}\,B$ e como elementos maximais os ideais primos de B sobre $\mathfrak{p}$.*

Capítulo 2

Inteiros Algébricos

Nesse capítulo, definiremos o principal objeto de estudo da Teoria Algébrica dos Números: os chamados **anéis de inteiros algébricos**. Iremos utilizar os resultados do Capítulo 1 para deduzir propriedades importantes desses anéis. Também estudaremos com mais profundidade dois tipos especiais de anéis de inteiros algébricos: os associados a corpos quadráticos e ciclotômicos.

2.1. Definição e Propriedades

Denotemos por $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ o fecho algébrico $\overline{\mathbb{Q}}^{\mathbb{C}}$ de $\mathbb{Q}$ em $\mathbb{C}$, e por $\mathcal{O}_{\mathbb{C}}$ o fecho integral $\overline{\mathbb{Z}}^{\mathbb{C}}$ de $\mathbb{Z}$ em $\mathbb{C}$. Então $\mathcal{O}_{\mathbb{C}}$ é um subanel de $\overline{\mathbb{Q}}$, e de fato é igual ao fecho integral de $\mathbb{Z}$ em $\overline{\mathbb{Q}}$.

Definição (Número Algébrico/Inteiro Algébrico)**.** Chamamos de **número algébrico** um elemento de $\overline{\mathbb{Q}}$, e de **inteiro algébrico** um elemento de $\mathcal{O}_{\mathbb{C}}$.

Assim como temos a inclusão $\mathbb{Z} \subseteq \mathbb{Q}$ dos números inteiros nos números racionais, podemos associar a cada extensão finita $K \subseteq \mathbb{C}$ de $\mathbb{Q}$ um "anel de inteiros" $\mathcal{O}_K \subseteq K$, de forma que essa inclusão tenha propriedades parecidas com a inclusão de $\mathbb{Z}$ em $\mathbb{Q}$:

Definição (Corpo de Números Algébricos/Anel de Inteiros Algébricos)**.** Dizemos que um subcorpo $K \subseteq \mathbb{C}$ é um **corpo de números algébricos**, ou simplesmente um **corpo de números**, se ele for uma extensão finita de $\mathbb{Q}$. Nesse caso, o subanel $\mathcal{O}_K \coloneqq \overline{\mathbb{Z}}^K \subseteq K$ é chamado de **anel de inteiros algébricos** de K.

Observação 2.1. *Notemos que $\mathcal{O}_K = K \cap \mathcal{O}_{\mathbb{C}}$, e portanto os elementos de $\mathcal{O}_K$ são exatamente os inteiros algébricos que estão em K, justificando a nomenclatura "anel de inteiros algébricos de K".*

Como a inclusão $\mathcal{O}_K \subseteq K$ deve generalizar a inclusão $\mathbb{Z} \subseteq \mathbb{Q}$, esperamos que valha $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Isso de fato é verdade, pois $\mathbb{Z}$ é integralmente fechado pelo Teorema 1.14. Como nós podemos falar em um "anel de inteiros" para cada extensão finita de $\mathbb{Q}$, é comum na literatura se referir a um elemento de $\mathbb{Z}$ como um **inteiro racional**.

Muitos resultados do Capítulo 1 têm uma consequência imediata sobre inteiros algébricos. Como todo corpo de números algébricos é uma extensão algébrica de $\mathbb{Q}$, o Teorema 1.16 nos dá:

Teorema 2.2. *Seja K um corpo de números algébricos. Então $Q(\mathcal{O}_K) = (\mathbb{Z}\setminus\{0\})^{-1}\mathcal{O}_K = K$.*

Como $\mathbb{Z}$ é integralmente fechado, o Corolário 1.30 nos permite concluir:

Corolário 2.3. *Sejam K um corpo de números algébricos e R um subanel de $\mathcal{O}_K$. Então, se $\gamma \in R$, temos:*

(a) $P_{\gamma,\mathbb{Q}} \in \mathbb{Z}[x]$, $F_{\gamma,K/\mathbb{Q}} \in \mathbb{Z}[x]$, $N_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$ *e* $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$.

(b) $N_{K/\mathbb{Q}}(\gamma)$ *é um múltiplo de* γ *em* R.

(c) $\gamma \in R^\times$ *se e só se* $|N_{K/\mathbb{Q}}(\gamma)| = 1$.

(d) Se $|N_{K/\mathbb{Q}}(\gamma)|$ *for um número primo, então* γ *será irredutível em* R.

(e) Se $\alpha, \beta \in R$ *forem associados em* R, *então* $N_{K/\mathbb{Q}}(\alpha) = \pm N_{K/\mathbb{Q}}(\beta)$.

Podemos ainda aplicar o Teorema 1.39 para o DIP $\mathbb{Z}$. Com isso, obtemos o famoso **Teorema da Base Integral**:

Teorema 2.4. *Seja* K *um corpo de números algébricos com* $[K : \mathbb{Q}] = n$. *Então:*

1. *(Teorema da Base Integral)* $\mathcal{O}_K$ *é um* $\mathbb{Z}$*-módulo livre de posto* n. *Uma base qualquer da extensão* $\mathcal{O}_K/\mathbb{Z}$ *é chamada de* ***base integral*** *de* $\mathcal{O}_K$, *ou ainda de base integral do corpo* K.

2. *Para qualquer subanel* R *de* K, *são equivalentes:*

   (i) $R \subseteq \mathcal{O}_K$.

   (ii) R *é um* $\mathbb{Z}$*-módulo livre de posto* $q \leq n$.

   (iii) R *é um* $\mathbb{Z}$*-módulo finitamente gerado.*

   Nesse caso, $q = n$ *se e somente se* $K = Q(R)$. *Se isso ocorrer, dizemos que* R *é uma de* K.

Observação 2.5. *Em geral, achar bases integrais explicitamente não é um problema simples. Nós faremos isso em alguns casos particulares, como para corpos quadráticos e ciclotômicos.*

Estudemos agora como ficam os resultados associados ao discriminante para anéis de inteiros algébricos. Devido à Proposição 1.40, temos:

Proposição 2.6. *Seja* K *um corpo de números algébricos com* $[K : \mathbb{Q}] = n$. *Para quaisquer* $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, *temos* $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

Seja R uma ordem de K. Então podemos aplicar a Proposição 1.42 para concluir que os discriminantes de duas bases de R como $\mathbb{Z}$-módulo diferem pelo quadrado de uma unidade de $\mathbb{Z}$. Mas $\mathbb{Z}^\times = \{-1, 1\}$, e $(-1)^2 = 1^2 = 1$. Portanto, todas as bases de R como $\mathbb{Z}$-módulo possuem o mesmo discriminante. Então obtemos:

Teorema 2.7. *Seja* K *um corpo de números com* $[K : \mathbb{Q}] = n$ *e seja* R *uma ordem de* K. *Então existe* $d_K(R) \in \mathbb{Z}$ *tal que, para toda base* $\{\beta_1, \ldots, \beta_n\}$ *de* R *como* $\mathbb{Z}$*-módulo, nós tenhamos* $\Delta_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = d_K(R)$. *Além disso,* $\mathfrak{d}_{R/\mathbb{Z}} = d_K(R)\,\mathbb{Z}$, *e para todos* $\alpha_1, \ldots, \alpha_n \in R$ *nós temos* $\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = a^2 d_K(R)$ *para algum* $a \in \mathbb{Z}$.

Em particular, existe $d_K \in \mathbb{Z}$, *chamado de* ***discriminante*** *do corpo* K, *que é igual ao discriminante de toda base integral de* $\mathcal{O}_K$, *e* $\mathfrak{d}_{\mathcal{O}_K/\mathbb{Z}} = d_K\,\mathbb{Z}$.

O resultado acima pode ser usado para encontrar bases integrais: basta acharmos $\beta_1, \ldots, \beta_n$ em $\mathcal{O}_K$ tais que $\Delta(\beta_1, \ldots, \beta_n) \neq 0$ seja mínimo em módulo. Note em particular que se encontrarmos $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ tais que $\Delta(\beta_1, \ldots, \beta_n)$ seja livre de quadrados então $\beta_1, \ldots, \beta_n$ formarão uma base integral de $\mathcal{O}_K$.

Exemplo 2.8. *Consideremos $K = \mathbb{Q}(\beta)$, onde β é uma raiz do polinômio irredutível $P(x) = x^3 + x^2 - 2x + 8$. Provaremos que $\{1, \beta, 4\beta^{-1}\}$ formam uma base integral de $\mathcal{O}_K$. Denotemos $\alpha := 4\beta^{-1}$. Observemos que $x^3 P(1/x) = 8x^3 - 2x^2 + x + 1$. Assim:*

$$8(\beta^{-1})^3 - 2(\beta^{-1})^2 + \beta^{-1} + 1 = 0.$$

Desse modo:

$$0 = 8(\alpha/4)^3 - 2(\alpha/4)^2 + (\alpha/4) + 1 = \frac{\alpha^3 - 2\alpha^2 + 4\alpha + 16}{16} \Rightarrow \alpha^3 - 2\alpha^2 + 4\alpha + 16 = 0.$$

Isso prova que $4\beta^{-1} = \alpha \in \mathcal{O}_K$. Calculemos agora $\Delta(1, \beta, 4\beta^{-1})$. Sabemos que $\{1, \beta, \beta^2\}$ forma uma base de $K/\mathbb{Q}$. Notemos que

$$\beta^3 + \beta^2 - 2\beta + 8 = 0 \Rightarrow \beta^2 + \beta - 2 + 8\beta^{-1} = 0 \Rightarrow 4\beta^{-1} = -\frac{1}{2}\beta^2 - \frac{1}{2}\beta + 1.$$

De forma similar, encontramos $16\beta^{-2} = \frac{1}{2}\beta^2 - \frac{5}{2}\beta - 1$. Com isso, analisando as matrizes de multiplicação na base $\{1, \beta, \beta^2\}$, nós obtemos:

$$\mathrm{Tr}(\beta) = -1,\ \mathrm{Tr}(\beta^2) = 5,\ \mathrm{Tr}(4\beta^{-1}) = 1,\ \mathrm{Tr}(16\beta^{-2}) = -3.$$

Assim:

$$\begin{aligned}
\Delta(1, \beta, 4\beta^{-1}) &= \det \begin{pmatrix} \mathrm{Tr}(1\cdot 1) & \mathrm{Tr}(1\cdot\beta) & \mathrm{Tr}(1\cdot 4\beta^{-1}) \\ \mathrm{Tr}(\beta\cdot 1) & \mathrm{Tr}(\beta\cdot\beta) & \mathrm{Tr}(\beta\cdot 4\beta^{-1}) \\ \mathrm{Tr}(4\beta^{-1}\cdot 1) & \mathrm{Tr}(4\beta^{-1}\cdot\beta) & \mathrm{Tr}(4\beta^{-1}\cdot 4\beta^{-1}) \end{pmatrix} \\
&= \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\beta) & \mathrm{Tr}(4\beta^{-1}) \\ \mathrm{Tr}(\beta) & \mathrm{Tr}(\beta^2) & \mathrm{Tr}(4) \\ \mathrm{Tr}(4\beta^{-1}) & \mathrm{Tr}(4) & \mathrm{Tr}(16\beta^{-2}) \end{pmatrix} \\
&= \det \begin{pmatrix} 3 & -1 & 1 \\ -1 & 5 & 12 \\ 1 & 12 & -3 \end{pmatrix} \\
&= -503.
\end{aligned}$$

Note que -503 é um número primo. Em particular, é livre de quadrados. Assim, concluímos que $\{1, \beta, 4\beta^{-1}\}$ é de fato uma base integral de $\mathcal{O}_K$, e $d_K = -503$.

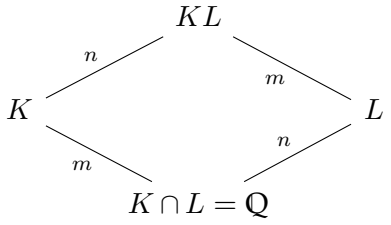
Um critério útil para construir bases integrais de um corpo a partir de bases integrais de corpos mais simples é o seguinte teorema, que será utilizado para encontrar bases integrais de corpos ciclotômicos:

Teorema 2.9. *Sejam K, L extensões galoisianas finitas de $\mathbb{Q}$ de graus m e n respectivamente, tais que $K \cap L = \mathbb{Q}$. Sejam ainda $\{\alpha_1, \ldots, \alpha_m\}$ e $\{\beta_1, \ldots, \beta_n\}$ bases integrais de K e de L, respectivamente. Suponhamos que d_K e d_L sejam primos entre si. Então o conjunto*

$$\mathcal{B} := \{\alpha_i\beta_j : 1 \le i \le m,\ 1 \le j \le n\}$$

é uma base integral de KL, e $d_{KL} = d_K^n d_L^m$.

Demonstração. Como $K/\mathbb{Q}$ e $L/\mathbb{Q}$ são galoisianas, a extensão $KL/\mathbb{Q}$ também é galoisiana, e como $K \cap L = \mathbb{Q}$ nós temos $\mathrm{Gal}(KL/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$. Em particular, $[KL : \mathbb{Q}] = mn$. Desse modo, temos o seguinte diagrama:



Como os α_i's geram K como $\mathbb{Q}$-espaço e os β_j's geram L como $\mathbb{Q}$-espaço, é fácil ver que o conjunto $\mathcal{B}$ dos produtos $\alpha_i\beta_j$ gera KL como $\mathbb{Q}$-espaço. Como $|\mathcal{B}| = mn = [KL : \mathbb{Q}]$, nós concluímos que $\mathcal{B}$ é uma base da extensão $KL/\mathbb{Q}$.

É claro que $\mathcal{O}_K, \mathcal{O}_L \subseteq \mathcal{O}_{KL}$. Assim, cada α_i e cada β_j estão em $\mathcal{O}_{KL}$, de modo que todos os elementos de $\mathcal{B}$ estão em $\mathcal{O}_{KL}$. Dessa forma, para provarmos que $\mathcal{B}$ é base integral de KL, basta mostrarmos que esse conjunto gera $\mathcal{O}_{KL}$ como $\mathbb{Z}$-módulo.

Seja $\gamma \in \mathcal{O}_{KL}$. Podemos escrever unicamente $\gamma = \sum_{i=1}^m \sum_{j=1}^n a_{ij}\alpha_i\beta_j$, com cada $a_{ij} \in \mathbb{Q}$. Mostraremos que cada $a_{ij} \in \mathbb{Z}$, o que nos dará o resultado desejado. Definindo, para $1 \leq j \leq n$, $\theta_j := \sum_{i=1}^m a_{ij}\alpha_i \in K$, nós temos $\gamma = \sum_{j=1}^n \theta_j\beta_j$. Denotemos $\mathrm{Gal}(KL/K) = \{\sigma_1, \ldots, \sigma_n\}$ e $\mathrm{Gal}(KL/L) = \{\tau_1, \ldots, \tau_m\}$. Então é fácil verificar que valem a igualdades:

$$\mathrm{Gal}(KL/\mathbb{Q}) = \{\sigma_k\tau_\ell \colon 1 \leq k \leq n,\ 1 \leq \ell \leq m\},\ \text{e}\ \ \mathrm{Gal}(L/\mathbb{Q}) = \{\sigma_1|_L, \ldots, \sigma_n|_L\}$$

Assim, definindo $T := (\sigma_i(\beta_j)) \in M_n(L)$, a Proposição 1.32 nos garante que

$$(\det T)^2 = \Delta(\beta_1, \ldots, \beta_n) = d_L.$$

Consideremos ainda os vetores $a := (\sigma_1(\gamma), \ldots, \sigma_n(\gamma)) \in (KL)^n$ e $b := (\theta_1, \ldots, \theta_n) \in K^n$. Então

$$Tb = \begin{bmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) & \cdots & \sigma_1(\beta_n) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) & \cdots & \sigma_2(\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \sigma_n(\beta_2) & \cdots & \sigma_n(\beta_n) \end{bmatrix} \begin{bmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_n \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^n \sigma_1(\beta_j)\theta_j \\ \sum_{j=1}^n \sigma_2(\beta_j)\theta_j \\ \vdots \\ \sum_{j=1}^n \sigma_n(\beta_j)\theta_j \end{bmatrix} = \begin{bmatrix} \sigma_1\left(\sum_{j=1}^n \beta_j\theta_j\right) \\ \sigma_2\left(\sum_{j=1}^n \beta_j\theta_j\right) \\ \vdots \\ \sigma_n\left(\sum_{j=1}^n \beta_j\theta_j\right) \end{bmatrix} = a,$$

uma vez que os σ_i fixam os θ_j's. Desse modo, $(\mathrm{adj}\, T)a = (\mathrm{adj}\, T)Tb = (\det T)b$. Agora, $\mathrm{adj}\, T$ é uma matriz com entradas em $\mathcal{O}_L$, já que cada $\beta_j \in \mathcal{O}_L$, e portanto cada $\sigma_i(\beta_j) \in \mathcal{O}_L$ (esse elemento satisfaz o mesmo polinômio mônico que β_j, já que os σ_i fixam $\mathbb{Q}$). Do mesmo modo, as entradas de a estão em $\mathcal{O}_{KL}$. Assim, $(\det T)b = (\mathrm{adj}\, T)a$ tem entradas em $\mathcal{O}_{KL}$. Como T tem entradas em $\mathcal{O}_L$, $\det T \in \mathcal{O}_L$. Logo $d_Lb = (\det T)[(\det T)b]$ tem entradas em $\mathcal{O}_{KL}$. Mas $d_L \in \mathbb{Z}$ e $b \in K^n$, de modo que $d_Lb \in K$. Então d_Lb tem entradas em $\mathcal{O}_{KL} \cap K = \mathcal{O}_K$.

Isso prova que, para $1 \leq j \leq n$, o elemento $d_L\theta_j = \sum_{i=1}^m (d_La_{ij})\alpha_i$ está em $\mathcal{O}_K$. Como $\alpha_1, \ldots, \alpha_m$ formam uma base integral de $\mathcal{O}_K$, isso significa que cada $d_La_{ij} \in \mathbb{Z}$. De forma análoga, se prova que cada $d_Ka_{ij} \in \mathbb{Z}$. Como d_K e d_L são primos entre si, existem $r, s \in \mathbb{Z}$ tais que $d_Kr + d_Ls = 1$. Desse modo, $a_{ij} = d_Ka_{ij}r + d_La_{ij}s \in A$. Isso prova que $\gamma = \sum_{i=1}^m \sum_{j=1}^n a_{ij}\alpha_i\beta_j$ está no $\mathbb{Z}$-módulo gerado por $\mathcal{B}$, e concluímos que $\mathcal{B}$ é base integral de KL, como desejado. Calculemos agora o discriminante dessa base integral. Como

$$\mathrm{Gal}(KL/\mathbb{Q}) = \{\sigma_k\tau_\ell \colon 1 \leq k \leq n,\ 1 \leq \ell \leq m\},$$

a Proposição 1.32 nos diz que esse discriminante é o quadrado do determinante da matriz de tamanho $mn \times mn$ dada por $\tilde{M} := (\sigma_k\tau_\ell(\alpha_i\beta_j)) = (\sigma_k(\beta_j) \cdot \tau_\ell(\alpha_i))$. Note que podemos trocar a ordem dos elementos da base integral e das imersões, pois isso altera apenas o sinal do determinante da matriz obtida, e quando elevado ao quadrado esse sinal desaparece. Desse modo, consideremos a matriz M obtida ordenando a base integral e as imersões na seguinte ordem:

$$\alpha_1\beta_1, \alpha_2\beta_1, \ldots, \alpha_m\beta_1, \alpha_1\beta_2, \alpha_2\beta_2, \ldots, \alpha_m\beta_2, \ldots, \alpha_1\beta_n, \alpha_2\beta_n, \ldots, \alpha_m\beta_n,\ \text{e}$$
$$\sigma_1\tau_1, \sigma_1\tau_2, \ldots, \sigma_1\tau_m, \sigma_2\tau_1, \sigma_2\tau_2, \ldots, \sigma_2\tau_m, \ldots, \sigma_n\tau_1, \sigma_n\tau_2, \ldots, \sigma_n\tau_m.$$

A matriz M pode ser pensada como uma matriz $n \times n$ por blocos de tamanho $m \times m$. Vendo

desse jeito, temos $M = (M_{ij})$, de modo que para cada $1 \leq i, j \leq n$ tenhamos

$$\begin{aligned} M_{ij} &= \begin{bmatrix} \sigma_i\tau_1(\alpha_1\beta_j) & \sigma_i\tau_1(\alpha_2\beta_j) & \cdots & \sigma_i\tau_1(\alpha_m\beta_j) \\ \sigma_i\tau_2(\alpha_1\beta_j) & \sigma_i\tau_2(\alpha_2\beta_j) & \cdots & \sigma_i\tau_2(\alpha_m\beta_j) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_i\tau_m(\alpha_1\beta_j) & \sigma_i\tau_m(\alpha_2\beta_j) & \cdots & \sigma_i\tau_m(\alpha_m\beta_j) \end{bmatrix} \\ &= \begin{bmatrix} \sigma_i(\beta_j)\cdot\tau_1(\alpha_1) & \sigma_i(\beta_j)\cdot\tau_1(\alpha_2) & \cdots & \sigma_i(\beta_j)\cdot\tau_1(\alpha_m) \\ \sigma_i(\beta_j)\cdot\tau_2(\alpha_1) & \sigma_i(\beta_j)\cdot\tau_2(\alpha_2) & \cdots & \sigma_i(\beta_j)\cdot\tau_2(\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_i(\beta_j)\cdot\tau_m(\alpha_1) & \sigma_i(\beta_j)\cdot\tau_m(\alpha_2) & \cdots & \sigma_i(\beta_j)\cdot\tau_m(\alpha_m) \end{bmatrix} \\ &= \sigma_i(\beta_j)\cdot\begin{bmatrix} \tau_1(\alpha_1) & \tau_1(\alpha_2) & \cdots & \tau_1(\alpha_m) \\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \cdots & \tau_2(\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_m(\alpha_1) & \tau_m(\alpha_2) & \cdots & \tau_m(\alpha_m) \end{bmatrix} \end{aligned}$$

Chamemos de P a matriz $m \times m$ dada por $(\tau_i(\alpha_j))$. Então a conta acima nos mostra que vale $M_{ij} = \sigma_i(\beta_j)\cdot P$, e assim:

$$\begin{aligned} M &= \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ M_{n1} & M_{n2} & \cdots & M_{nn} \end{bmatrix} \\ &= \begin{bmatrix} \sigma_1(\beta_1)\cdot P & \sigma_1(\beta_2)\cdot P & \cdots & \sigma_1(\beta_n)\cdot P \\ \sigma_2(\beta_1)\cdot P & \sigma_2(\beta_2)\cdot P & \cdots & \sigma_2(\beta_n)\cdot P \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\beta_1)\cdot P & \sigma_n(\beta_2)\cdot P & \cdots & \sigma_n(\beta_n)\cdot P \end{bmatrix} \\ &= \begin{bmatrix} \sigma_1(\beta_1)\cdot \mathrm{Id} & \sigma_1(\beta_2)\cdot \mathrm{Id} & \cdots & \sigma_1(\beta_n)\cdot \mathrm{Id} \\ \sigma_2(\beta_1)\cdot \mathrm{Id} & \sigma_2(\beta_2)\cdot \mathrm{Id} & \cdots & \sigma_2(\beta_n)\cdot \mathrm{Id} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\beta_1)\cdot \mathrm{Id} & \sigma_n(\beta_2)\cdot \mathrm{Id} & \cdots & \sigma_n(\beta_n)\cdot \mathrm{Id} \end{bmatrix} \cdot \begin{bmatrix} P & 0 & \cdots & 0 \\ 0 & P & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P \end{bmatrix}, \end{aligned}$$

onde Id denota a matriz identidade $m \times m$. Chamemos as matrizes acima de C e D respectivamente. Assim, $M = CD$, e $\det M = \det C \cdot \det D$. Abrindo a expressão para o determinante de uma matriz, nós podemos encontrar que $\det C = (\det Q)^m$ e $\det D = (\det P)^n$, onde $Q = (\sigma_i(\beta_j))$ é uma matriz $n \times n$. Agora, a Proposição 1.32 nos diz que $(\det P)^2 = d_K$ e $(\det Q)^2 = d_L$. Finalmente, concluímos que o discriminante da base integral $\mathcal{B}$ é:

$$(\det M)^2 = (\det C)^2 \cdot (\det D)^2 = (\det Q)^{2m} \cdot (\det P)^{2n} = d_K^n d_L^m.$$

□

Consideremos agora um $\mathbb{Z}$-submódulo qualquer $M \subseteq \mathcal{O}_K$ de posto n. Como $\mathcal{O}_K$ é livre, sabemos que M é livre pelo Teorema 1.38. Argumentando do mesmo modo que nas demonstrações das Proposições 1.42 e 2.7, vemos que existe $d_K(M) \in \mathbb{Z}$ que é igual ao discriminante de qualquer base de M. Pela Proposição 1.42, existe um inteiro positivo k_M tal que $d_K(M) = k_M^2 d_K$. Chamamos k_M de **índice** de M. A justificativa para essa nomenclatura é dada pelo resultado abaixo:

Teorema 2.10. *Sejam K um corpo de números e $M \subseteq \mathcal{O}_K$ um $\mathbb{Z}$-submódulo de posto n. Então k_M é igual ao índice $(\mathcal{O}_K : M)$, onde consideramos $\mathcal{O}_K$ e M como grupos aditivos. Em particular, esse índice é finito.*

Demonstração. Seja $\{\beta_1, \dots, \beta_n\}$ uma base integral de K. Como $M \subseteq \mathcal{O}_K$ é um $\mathbb{Z}$-módulo de posto n, pelo Teorema 1.38 vemos que existem $a_1, \dots, a_n \in \mathbb{N}$ tais que $\{a_1\beta_1, \dots, a_n\beta_n\}$ é uma base de M. Assim, $k_M^2 d_K = d_K(M) = \Delta(a_1\beta_1, \dots, a_n\beta_n)$. Mas pela Proposição 1.31 nós temos:

$$\Delta(a_1\beta_1, \dots, a_n\beta_n) = (a_1 \cdots a_n)^2 \Delta(\beta_1, \dots, \beta_n) = (a_1 \cdots a_n)^2 d_K.$$

Assim, concluímos que $k_M = |a_1 \cdots a_n|$. Por outro lado, pelo Teorema 1.38, nós temos um isomorfismo de grupos abelianos:

$$\mathcal{O}_K / M \cong \mathbb{Z} / (a_1 \mathbb{Z}) \times \cdots \times \mathbb{Z} / (a_n \mathbb{Z}),$$

de modo que $(\mathcal{O}_K : M) = |\mathcal{O}_K / M| = |a_1| \cdots |a_n| = |a_1 \cdots a_n| = k_M$, como queríamos. □

Esse resultado se aplica em particular para as ordens de K. Entre essas ordens estão os anéis da forma $R = \mathbb{Z}[\alpha]$, onde $\alpha \in \mathcal{O}_K$ é um elemento primitivo da extensão $K / \mathbb{Q}$ (veja a Proposição 1.43). Chamamos esses anéis de **ordens principais** de K. Eles possuem $\mathbb{Z}$-base formada pelos elementos $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. Nesse caso, denotaremos também $k_{\mathbb{Z}[\alpha]}$ por k_α, e o chamaremos de **índice** de α.

Em geral, as ordens principais de K são subanéis próprios de $\mathcal{O}_K$. Ainda assim, esses anéis são "suficientemente grandes" no sentido de que conseguimos achar representantes de classes de ideais maximais pertencentes a eles. Mais especificamente:

Corolário 2.11. *Sejam $\alpha \in \mathcal{O}_K$ um elemento primitivo da extensão $K / \mathbb{Q}$ e $\mathfrak{p} \lhd \mathcal{O}_K$ maximal tal que $k_\alpha \notin \mathfrak{p}$. Então, para todo $\gamma \in \mathcal{O}_K$, existe $\gamma' \in \mathbb{Z}[\alpha]$ tal que $\gamma' \equiv \gamma \pmod{\mathfrak{p}}$.*

Demonstração. Como $\mathfrak{p}$ é maximal, $\mathfrak{p} + k_\alpha \mathcal{O}_K = \mathcal{O}_K$. Mas pelo Teorema de Lagrange temos $k_\alpha \mathcal{O}_K \subseteq \mathbb{Z}[\alpha]$. Assim, temos $\mathfrak{p} + \mathbb{Z}[\alpha] = \mathcal{O}_K$, o que conclui a demonstração. □

O Teorema 2.10 também se aplica para os ideais não-nulos de $\mathcal{O}_K$. De fato, seja $\{\beta_1, \dots, \beta_n\}$ uma base integral de $\mathcal{O}_K$. Dado um ideal não-nulo $\mathfrak{a} \lhd \mathcal{O}_K$, tomando $a \in \mathfrak{a}$ não-nulo nós vemos que $\{a\beta_1, \dots, a\beta_n\} \subseteq \mathfrak{a}$ é um conjunto linearmente independente sobre $\mathbb{Z}$. Assim, $\mathfrak{a}$ tem posto n. Pelo Teorema 2.10, $|\mathcal{O}_K / \mathfrak{a}| = (\mathcal{O}_K : \mathfrak{a}) = k_\mathfrak{a}$ é finito. Nós denotamos esse inteiro positivo por $\mathfrak{N}(\mathfrak{a})$, e o chamamos de **norma** de $\mathfrak{a}$. Isso define uma função $\mathfrak{N}$: {Ideais de $\mathcal{O}_K$} $\to \mathbb{N}^*$, chamada de **norma de ideais**, que será estudada com mais detalhes no Capítulo 4. Notemos ainda que $\mathfrak{N}(\mathfrak{a})^2 d_K = d_K(\mathfrak{a})$.

Como todo ideal primo não-nulo de $\mathbb{Z}$ é maximal, segue do Teorema 1.53:

Teorema 2.12. *Seja K um corpo de números algébricos. Então todo ideal primo não-nulo de $\mathcal{O}_K$ é maximal.*

Terminamos a seção observando que, como consequência da transitividade da integrabilidade de extensões, vemos que se K, L forem corpos de números com $K \subseteq L$ então $\overline{\mathcal{O}_K}^L = \mathcal{O}_L$.

2.2. Corpos Quadráticos

Os corpos de números algébricos mais simples são os corpos quadráticos:

Definição (Corpo Quadrático)**.** Dizemos que um corpo de números algébricos K é um **corpo quadrático** se $[K : \mathbb{Q}] = 2$.

Notemos que se K for um corpo quadrático então todo $\alpha \in K \setminus \mathbb{Q}$ será um elemento primitivo dessa extensão. É fácil mostrar que todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z} \setminus \{0, 1\}$ é livre de quadrados. De fato, vale o seguinte:

Teorema 2.13. *Seja $\mathcal{D} = \{d \in \mathbb{Z}\setminus\{0,1\} \mid d \text{ é livre de quadrados}\}$, e seja $\mathcal{L}_2$ o conjunto dos corpos quadráticos. Então $f\colon \mathcal{D} \to \mathcal{L}_2$ dado por $d \mapsto \mathbb{Q}(\sqrt{d})$ é uma bijeção. Mais do que isso, se d_1 e d_2 pertencerem a $\mathcal{D}$, então $\mathbb{Q}(\sqrt{d_1}) \cong \mathbb{Q}(\sqrt{d_2}) \iff d_1 = d_2$.*

Se $K = \mathbb{Q}(\sqrt{d})$ é uma extensão quadrática com $d \in \mathcal{D}$, então $\{1, \sqrt{d}\}$ é uma base dessa extensão. Seja $\alpha = a + b\sqrt{d} \in K$ qualquer. Então:

$$\begin{aligned} \alpha \cdot 1 &= a + b\sqrt{d}, \\ \alpha \cdot \sqrt{d} &= bd + a\sqrt{d}. \end{aligned}$$

Dessa forma, a matriz de multiplicação por α nessa base é

$$M_\alpha = \begin{bmatrix} a & bd \\ b & a \end{bmatrix}.$$

Então, em relação à extensão $K/\mathbb{Q}$:

$$F_\alpha(x) = \det(x\,\mathrm{Id} - M_\alpha) = \det\begin{pmatrix} x-a & -bd \\ -b & x-a \end{pmatrix} = x^2 - 2ax + (a^2 - db^2).$$

Assim, $\mathrm{Tr}(a + b\sqrt{d}) = 2a$ e $N(a + b\sqrt{d}) = a^2 - db^2$. Note que se $d < 0$ então sempre vale $N(a + b\sqrt{d}) \geq 0$, com igualdade se e só se $a = b = 0$. Nosso objetivo agora é determinar, para $K = \mathbb{Q}(\sqrt{d})$, o anel $\mathcal{O}_K$. Comecemos com o seguinte lema:

Lema 2.14. *Seja $K = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$. Então*

$$\mathcal{O}_K = \left\{ \frac{m}{2} + \frac{n}{2}\sqrt{d} \colon m, n \in \mathbb{Z},\ m^2 - dn^2 \equiv 0 \pmod 4 \right\}.$$

Demonstração. ($\subseteq$) Seja $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$, onde $a, b \in \mathbb{Q}$. Então, pelo Corolário 2.3, nós temos $F_\alpha(x) \in \mathbb{Z}[x]$. Como já vimos, $F_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$. Disso tiramos que $2a \in \mathbb{Z}$ e que $a^2 - db^2 \in \mathbb{Z}$. Seja $r = a^2 - db^2$. Dessa forma, $4a^2 - 4db^2 = 4r$, ou seja, $d(2b)^2 = (2a)^2 - 4r \in \mathbb{Z}$, pois $2a, r \in \mathbb{Z}$. Podemos escrever $2b = p/q$, com $p, q \in \mathbb{Z}$, $q \neq 0$, primos entre si. Então $d(2b)^2 \in \mathbb{Z} \Rightarrow q^2 \mid dp^2 \Rightarrow q^2 \mid d$, já que $\mathrm{mdc}(p, q) = 1$. Como d é livre de quadrados, concluímos que $q = \pm 1$, de modo que $2b$ é inteiro. Portanto, $m \coloneqq 2a$ e $n \coloneqq 2b$ são números inteiros, e como vimos temos $m^2 - dn^2 = 4r \equiv 0 \pmod 4$. Isso mostra que $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$ está no conjunto da direita do enunciado.

($\supseteq$) Seja $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$, onde $m, n \in \mathbb{Z}$ satisfazem $m^2 - dn^2 \equiv 0 \pmod 4$. Então

$$F_\alpha(x) = x^2 - mx + \frac{m^2 - dn^2}{4}$$

Como $m^2 - dn^2 \equiv 0 \pmod 4$, temos $F_\alpha(x) \in \mathbb{Z}[x]$, e como $F_\alpha(\alpha) = 0$, temos $\alpha \in \mathcal{O}_K$. □

Podemos agora determinar $\mathcal{O}_K$:

Teorema 2.15. *Seja $K = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$. Então:*

(a) Se $d \equiv 2, 3 \pmod 4$, então $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ tem base integral $\{1, \sqrt{d}\}$ e discriminante $d_K = 4d$.

(b) Se $d \equiv 1 \pmod 4$, então $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ tem base integral $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ e discriminante $d_K = d$.

Demonstração. (a) É imediato verificar que os elementos 1 e $\sqrt{d}$ estão em $\mathcal{O}_K$, utilizando o lema anterior. Assim, $\mathbb{Z}+\mathbb{Z}\cdot\sqrt{d} \subseteq \mathcal{O}_K$. Seja agora $\alpha \in \mathcal{O}_K$. Então, pelo lema anterior,

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \in \mathcal{O}_K, \text{ com } m^2 - dn^2 \equiv 0 \pmod 4.$$

Se $d \equiv 2 \pmod 4$, então $m^2 \equiv 0 \pmod 2$, e assim m é par. Logo $4 \mid dn^2$, e como d é livre de quadrados temos $2 \mid n$. Isso mostra que n também é par, e assim

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \in \mathbb{Z}+\mathbb{Z}\cdot\sqrt{d}.$$

Se $d \equiv 3 \pmod 4$, então $m^2 + n^2 \equiv 0 \pmod 4$. Como o quadrado de um ímpar deixa resto 1 na divisão por 4, a única possibilidade é termos $m \equiv n \equiv 0 \pmod 2$. Assim:

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \in \mathbb{Z}+\mathbb{Z}\cdot\sqrt{d}.$$

Logo, em ambos os casos, temos $\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}\cdot\sqrt{d}$. Isso mostra que $\{1, \sqrt{d}\}$ é base integral de $\mathcal{O}_K$, e portanto:

$$d_K = \Delta(1, \sqrt{d}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

(b) É imediato verificar que os elementos 1 e $\frac{1+\sqrt{d}}{2}$ estão em $\mathcal{O}_K$, utilizando o lema anterior. Assim, $\mathbb{Z}+\mathbb{Z}\cdot\frac{1+\sqrt{d}}{2} \subseteq \mathcal{O}_K$. Seja agora $\alpha \in \mathcal{O}_K$. Então, pelo lema anterior,

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \in \mathcal{O}_K, \text{ com } m^2 - dn^2 \equiv 0 \pmod 4.$$

Como $d \equiv 1 \pmod 4$, temos $m^2 \equiv n^2 \pmod 4$. Logo m e n possuem a mesma paridade, e podemos escrever $m = 2k + n$, com $k \in \mathbb{Z}$. Assim:

$$\alpha = \frac{2k+n}{2} + \frac{n}{2}\sqrt{d} = k + n\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}+\mathbb{Z}\cdot\frac{1+\sqrt{d}}{2}.$$

Logo temos $\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}\cdot\frac{1+\sqrt{d}}{2}$. Isso mostra que $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ é base integral de $\mathcal{O}_K$, e portanto:

$$\begin{aligned} d_K = \Delta\left(1, \frac{1+\sqrt{d}}{2}\right) &= \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) \\ \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) & \mathrm{Tr}\left(\frac{1+d+2\sqrt{d}}{4}\right) \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d. \end{aligned}$$

□

Observação 2.16. *Note que podemos encontrar todas as bases integrais de $\mathcal{O}_K$ usando o discriminante: Se $\alpha, \beta \in \mathcal{O}_K$, então $\{\alpha, \beta\}$ será uma base de $\mathcal{O}_K$ se e só se $\Delta(\alpha, \beta) = 4d$, se $d \equiv 2$ ou $3 \pmod 4$, e se e só se $\Delta(\alpha, \beta) = d$, se $d \equiv 1 \pmod 4$.*

Esse resultado nos permite exibir exemplos de domínios que não são integralmente fechados:

Exemplo 2.17. *O domínio $\mathbb{Z}[\sqrt{d}]$, para $d \in \mathcal{D}$ congruente a 1 módulo 4, não é integralmente fechado. De fato, é claro que seu corpo de frações é $K = Q(\sqrt{d})$, e que, como $\mathbb{Z}[\sqrt{d}]/\mathbb{Z}$ é uma extensão integral:*

$$\overline{\mathbb{Z}[\sqrt{d}]}^K = \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \supsetneq \mathbb{Z}[\sqrt{d}].$$

Em particular, $\mathbb{Z}[\sqrt{d}]$ não é um DFU. De fato, este mesmo argumento funciona para mostrar que qualquer ordem própria de um corpo de números algébricos não é integralmente fechada.

É interessante se perguntar quando $\mathcal{O}_K$ é um DFU, um DIP ou um domínio euclidiano, para podermos deduzir propriedades mais profundas desse anel. Às vezes, $\mathcal{O}_K$ não é nem mesmo um DFU:

Exemplo 2.18. *Sendo $K = \mathbb{Q}(\sqrt{-5})$, o anel $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ não é um DFU. De fato, temos que*

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

são duas fatorações distintas de 6 nesse anel. Temos $N(2) = 4$, $N(3) = 9$, e $N(1+\sqrt{-5}) = N(1-\sqrt{-5}) = 6$. Assim, pelos itens (c) e (e) do corolário 2.3, os elementos 2, 3, $1+\sqrt{-5}$ e $1-\sqrt{-5}$ não são unidades em $\mathcal{O}_K$, e 2 e 3 não são associados a $1+\sqrt{-5}$ nem a $1-\sqrt{-5}$. Assim, basta provarmos que esses quatro elementos são irredutíveis em $\mathcal{O}_K$. Se algum desses elementos não fosse irredutível, então garantiríamos a existência de um elemento em $\mathcal{O}_K$ com norma ± 2 ou ± 3, o que é impossível, pois não existem $a, b \in \mathbb{Z}$ tais que $N(a+b\sqrt{-5}) = a^2 + 5b^2$ seja igual a ± 2 ou ± 3. Assim, $\mathcal{O}_K$ não é um DFU.

Analisemos agora a questão de $\mathcal{O}_K$ ser um domínio euclidiano. O melhor candidato à "função grau" é a norma absoluta $|N_{K/\mathbb{Q}}|$, pois já sabemos de antemão que essa é uma função com valores naturais que é multiplicativa e que só se anula em 0.

Teorema 2.19. *Seja $K = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$.*

(a) As seguintes condições são equivalentes:

(i) $\mathcal{O}_K$ é euclidiano em relação à norma absoluta.

(ii) Para qualquer $\lambda \in K$, existe $q \in \mathcal{O}_K$ tal que $|N_{K/\mathbb{Q}}(\lambda - q)| < 1$.

(iii) Para quaisquer $r, s \in \mathbb{Q}$, existem $m, n \in \mathbb{Z}$ tais que:

$$\begin{cases} |(r-m)^2 - d(s-n)^2| < 1, & \text{se } d \equiv 2,3 \pmod 4; \\ |(r-m+\frac{s-n}{2})^2 - d(\frac{s-n}{2})^2| < 1, & \text{se } d \equiv 1 \pmod 4. \end{cases}$$

(b) $\mathcal{O}_K$ é euclidiano com a norma absoluta se $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 13\}$, e isso não acontece para nenhum outro valor negativo de $d \in \mathcal{D}$.

Demonstração. (a) (i)⇒(ii): Suponhamos que valha (i). Seja $\lambda \in K$ qualquer. Pelo Teorema 2.2, temos $L = \mathbb{Q}(\mathcal{O}_K)$, logo $\lambda = a/b$ para alguns $a, b \in \mathcal{O}_K$, $b \neq 0$. Por hipótese, existem $q, r \in \mathcal{O}_K$ tais que $a = bq + r$ e $|N(r)| < |N(b)|$. Assim:

$$|N(\lambda - q)| = \left|N\left(\frac{a}{b} - q\right)\right| = \left|N\left(\frac{r}{b}\right)\right| = \frac{|N(r)|}{|N(b)|} < 1,$$

provando (ii).

(ii)⇒(i) Suponhamos que valha (ii). Sejam $a, b \in \mathcal{O}_K$ quaisquer, $b \neq 0$. Então existe

$q \in \mathcal{O}_K$ tal que $|N(a/b - q)| < 1$. Chamemos $r := a - bq \in \mathcal{O}_K$. Assim, $a = bq + r$ e temos:

$$\left|N\left(\frac{a}{b} - q\right)\right| < 1 \Rightarrow \left|N\left(\frac{r}{b}\right)\right| < 1 \Rightarrow \frac{|N(r)|}{|N(b)|} < 1 \Rightarrow |N(r)| < |N(b)|,$$

provando (i).

(ii) $\iff$ (iii): Basta, se $d \equiv 2, 3 \pmod 4$, tomar $\lambda = r + s\sqrt{d} \in K$ e $q = m + n\sqrt{d} \in \mathcal{O}_K$, e notar que a desigualdade em (iii) equivale a termos $|N(\lambda - q)| < 1$. Da mesma forma, se $d \equiv 1 \pmod 4$, basta tomar $\lambda = r + s\left(\frac{1+\sqrt{d}}{2}\right) \in K$ e $q = m + n\left(\frac{1+\sqrt{d}}{2}\right) \in \mathcal{O}_K$ e notar que a desigualdade em (iii) equivale a termos $|N(\lambda - q)| < 1$.

(b) Provaremos que para esses valores de d vale (iii), e que para qualquer outro valor negativo de $d \in \mathcal{D}$ não vale (iii):

Caso 1: $d < 0$. Chamemos $\ell = -d > 0$. Como observado anteriormente, nesse caso a norma é sempre não-negativa, então podemos ignorar os valores absolutos em (iii).

Caso 1.1: $d \equiv 2, 3 \pmod 4$. Suponhamos $\ell < 3$. Sejam $r, s \in \mathbb{Q}$. Então existem inteiros $m, n \in \mathbb{Z}$ tais que $|r - m| \leq 1/2$ e $|s - n| \leq 1/2$. Então:

$$(r-m)^2 + \ell(s-n)^2 < \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2 = 1,$$

logo vale (iii). Assim, se $d \in \{-2, -1\}$, $\mathcal{O}_K$ é domínio euclidiano. Se $\ell \geq 5$, tomemos $r = s = 1/2$. Então, para quaisquer $m, n \in \mathbb{Z}$, temos $|r - m| \geq 1/2$ e $|s - n| \geq 1/2$. Assim:

$$(r-m)^2 + \ell(s-n)^2 \geq \left(\frac{1}{2}\right)^2 + 5\left(\frac{1}{2}\right)^2 = \frac{3}{2} > 1,$$

mostrando que nesse caso não vale (iii), e assim $\mathcal{O}_K$ não é domínio euclidiano.

Caso 1.2: $d \equiv 1 \pmod 4$. Suponhamos $\ell \leq 11$. Sejam $r, s \in \mathbb{Q}$. Então existe um inteiro n tal que $|s - n| \leq 1/2$. Queremos agora achar $m \in \mathbb{Z}$ tal que

$$\left|r - m + \frac{s-n}{2}\right| \leq 1/2,$$

ou seja,

$$-\frac{1}{2} \leq r - m + \frac{s-n}{2} \leq \frac{1}{2} \iff r + \frac{s-n-1}{2} \leq m \leq r + \frac{s-n+1}{2}.$$

Como a diferença entre os números nos extremos da última desigualdade é de 1, podemos tomar m como sendo um número inteiro no intervalo correspondente. Para esses valores de m e n, temos:

$$\left(r - m + \frac{s-n}{2}\right)^2 + \ell\left(\frac{s-n}{2}\right)^2 \leq \left(\frac{1}{2}\right)^2 + 11\left(\frac{1}{4}\right)^2 = \frac{15}{16} < 1,$$

logo vale (iii). Assim, se $d \in \{-11, -7, -3\}$, $\mathcal{O}_K$ é domínio euclidiano. Se $\ell \geq 15$, tomemos $r = s = 1/2$. Sejam $m, n \in \mathbb{Z}$. Se $n \notin \{0, 1\}$, então $s - n > 1$, e portanto

$$\ell\left(\frac{s-n}{2}\right)^2 > 15\left(\frac{1}{2}\right)^2 = \frac{15}{4} > 1,$$

o que já mostra que não temos a desigualdade de (iii). Se $n = 0$ ou $n = 1$, então é claro que os valores de m que minimizam $\left|r - m + \frac{s-n}{2}\right|$ são $m = 1$ e $m = 0$, respectivamente. De qualquer forma, vemos que $\left|r - m + \frac{s-n}{2}\right| \geq \frac{1}{4}$. Assim:

$$\left(r - m + \frac{s-n}{2}\right)^2 + \ell(s-n)^2 \geq \left(\frac{1}{4}\right)^2 + 15\left(\frac{1}{4}\right)^2 = 1,$$

mostrando que nesse caso não vale (iii), e $\mathcal{O}_K$ não é domínio euclidiano.

Caso 2: $d > 0$:

Caso 2.1: $d \in \{2, 3\}$. Dados $r, s \in \mathbb{Q}$, sejam $m, n \in \mathbb{Z}$ tais que $|r - m| \leq 1/2$ e $|s - n| \leq 1/2$. Assim, como $d > 0$:

$$\left|(r-m)^2 - d(s-n)^2\right| \leq \max\left\{(r-m)^2, d(s-n)^2\right\}.$$

Mas

$$(r-m)^2 \leq \left(\frac{1}{2}\right)^2 = \frac{1}{4} \text{ e } d(s-n)^2 \leq 3\left(\frac{1}{2}\right)^2 = \frac{3}{4},$$

portanto vale (iii), e $\mathcal{O}_K$ é domínio euclidiano.

Caso 2.2: $d \in \{5, 13\}$. Dados $r, s \in \mathbb{Q}$, sejam $m, n \in \mathbb{Z}$ tais que $\left|r - m + \frac{s-n}{2}\right| \leq 1/2$ e $|s - n| \leq 1/2$ (podemos achar tais inteiros procedendo como no Caso 1.2). Como $d > 0$:

$$\left|\left(r - m + \frac{s-n}{2}\right)^2 - d\left(\frac{s-n}{2}\right)^2\right| \leq \max\left\{\left(r - m + \frac{s-n}{2}\right)^2, d\left(\frac{s-n}{2}\right)^2\right\}.$$

Mas

$$\left(r - m + \frac{s-n}{2}\right)^2 \leq \left(\frac{1}{2}\right)^2 = \frac{1}{4} \text{ e } d\left(\frac{s-n}{2}\right)^2 \leq 13\left(\frac{1}{4}\right)^2 = \frac{13}{16},$$

portanto vale (iii), e $\mathcal{O}_K$ é domínio euclidiano.

□

Observação 2.20. *Pode-se provar que, se $d \in \{6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$, então $\mathcal{O}_K$ também é euclidiano com relação à norma absoluta, e esses valores, junto com os do teorema acima, são os únicos valores de $d \in \mathcal{D}$ tais que isso acontece (veja [18]).*

Podemos ainda nos perguntar para que valores de d o anel $\mathcal{O}_K$ será um DIP ou um DFU. De fato, veremos mais adiante que $\mathcal{O}_K$ será um DIP se e só se for um DFU, e isso não vale apenas para corpos quadráticos, mas para anéis de inteiros algébricos em geral.

Pelo item (c) do Corolário 2.3, um elemento $u \in \mathcal{O}_K$ será uma unidade se e só se $N(u) = \pm 1$. Sabemos que todo elemento de $\mathcal{O}_K$ é da forma $a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$, se $d \equiv 2, 3 \pmod 4$, e é da forma $a + b\left(\frac{1+\sqrt{d}}{2}\right)$, se $d \equiv 1 \pmod 4$. No caso em que $d < 0$, vemos que a norma "cresce rapidamente" em função de a e de b. Com isso, é fácil caracterizarmos os elementos inversíveis de $\mathcal{O}_K$, para obter:

Teorema 2.21. *Seja $K = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$ e $d < 0$.*

(a) Se $d = -1$, então $\mathcal{O}_K^\times = \{1, i, -i, -1\}$ é gerado por i.

(b) Se $d = -3$, então $\mathcal{O}_K^\times = \{1, \zeta, \zeta^2, \zeta^3 = -1, \zeta^4, \zeta^5\}$ é gerado por $\zeta = \frac{1+\sqrt{-3}}{2}$, uma raiz sexta primitiva da unidade.

(c) Se $d \notin \{-1, -3\}$, então $\mathcal{O}_K^\times = \{1, -1\}$.

A determinação dos grupos de unidades dos corpos quadráticos com $d > 0$ será feita na Seção 7.5.

Exemplo 2.22. *Com os resultados acima, podemos dar uma boa caracterização do anel $\mathbb{Z}[i]$ dos inteiros de Gauss. Sabemos que os inversíveis desse anel são os elementos $\pm 1, \pm i$. Além disso, sendo $\mathbb{Z}[i]$ um domínio euclidiano, ele é um DFU, e portanto as noções de irredutível e primo coincidem. Afirmamos que os irredutíveis/primos desse anel, a menos de associados, são:*

- *Os primos de $\mathbb{N}$ congruentes a 3 módulo 4;*
- *$1 + i$;*
- *Os elementos da forma $a \pm bi$, com $1 \leq a < b$ naturais tais que $a^2 + b^2$ é um primo de $\mathbb{N}$ congruente a 1 módulo 4.*

Além disso, na lista acima não existem dois elementos associados entre si, e para cada primo $p \in \mathbb{Z}$ congruente a 1 módulo 4 os naturais a e b são únicos.

Para mostrar isso, seja $x + yi \in \mathbb{Z}[i]$ primo. Então $x + yi \mid N(x + yi) = x^2 + y^2$. Assim, $x + yi$ divide algum primo $p \in \mathbb{N}$ que aparece na fatoração de $x^2 + y^2$. Disso concluímos que para encontrarmos os primos de $\mathbb{Z}[i]$ basta encontrarmos os primos de $\mathbb{Z}[i]$ que dividem um primo de $\mathbb{N}$.

- *Se $p = 2$: Notemos que $2 = -i(1 + i)^2$, e $N(1 + i) = 2$, provando que $1 + i$ é o único primo em $\mathbb{Z}[i]$ que divide 2 a menos de associados.*
- *Se p deixa resto 3 na divisão por 4: Temos $x + yi \mid p \Rightarrow N(x + yi) = x^2 + y^2 \mid N(p) = p^2$. Sendo $x + yi$ primo, devemos ter $N(x + yi) = p$ ou $N(x + yi) = p^2$. Mas $x^2 + y^2$ não pode deixar resto 3 na divisão por 4, assim $N(x + yi) = p^2 = N(p)$. Escrevamos $p = (x + yi)\gamma$ para algum $\gamma \in \mathbb{Z}[i]$. Então $N(p) = N(x + yi)N(\gamma) \Rightarrow N(\gamma) = 1 \Rightarrow \gamma \in \mathbb{Z}[i]^\times$. Isso prova que $x + yi$ é associado de p, e assim p é primo de $\mathbb{Z}[i]$.*
- *Se p deixa resto 1 na divisão por 4: provemos que p não é primo. Para isso, notemos que, utilizando o Teorema de Wilson:*

$$\begin{aligned} p \mid (p-1)! + 1 &= \left(1 \cdots \frac{p-1}{2}\right)\left(\left(-\frac{p-1}{2}\right) \cdots (-1)\right) \\ &= (-1)^{(p-1)/2}\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1 \\ &= \left(\left(\frac{p-1}{2}\right)!\right)^2 + 1. \end{aligned}$$

Chamemos $w = \left(\frac{p-1}{2}\right)!$. Então $p \nmid w + i$ e $p \nmid w - i$, mas $p \mid w^2 + 1 = (w + i)(w - i)$. Isso prova que p não é primo, e portanto existe $a + bi$ primo não associado a p tal que $a + bi \mid p$. Multiplicando por algum dos inversíveis $\pm 1, \pm i$ se necessário, podemos supor $1 \leq a < b$.

Assim como no item anterior, concluímos que $a^2 + b^2 \mid p^2$. Como $a + bi$ não é associado a p, nós devemos ter $a^2 + b^2 = p$, e assim $p = (a + bi)(a - bi)$. Sendo $N(a - bi) = p$, vemos que $a - bi$ também é um primo de $\mathbb{Z}[i]$. É fácil ver, simplesmente multiplicando pelos inversíveis de $\mathbb{Z}[i]$, que $a + bi$ e $a - bi$ não são associados. Isso termina a prova da nossa afirmação.

2.3. Corpos ciclotômicos

Outro tipo importante de corpo de números é aquele gerado por uma raiz da unidade. Comecemos relembrando algumas definições e enunciando alguns resultados básicos sem demonstração:

Definição (Raiz da Unidade/Extensão Ciclotômica/Corpo Ciclotômico)**.** Seja K um corpo. Dizemos que um elemento ζ de um fecho algébrico de K é uma **raiz da unidade** se $\zeta^n = 1$ para algum n inteiro positivo. Se n for o menor inteiro positivo tal que isso ocorra, dizemos que ζ é uma **raiz primitiva** n-ésima da unidade.

Uma **extensão ciclotômica** de K é um corpo da forma $K(\zeta)$, onde ζ é uma raiz da unidade, e dizemos que um corpo é um **corpo ciclotômico** se ele for da forma $\mathbb{Q}(\zeta)$ para alguma raiz da unidade $\zeta \in \mathbb{C}$.

Denotemos por $W(K)$, $W_n(K)$ e $\mathscr{P}_n(K)$ os conjuntos das raízes da unidade em K, das raízes n-ésima da unidade em K e das raízes n-ésimas primitivas da unidade em K, respectivamente. O conjunto $W(K)$ também é chamado de **grupo de torção** de K, já que esse é o subgrupo dos elementos de ordem finita de $K^\times$. Note que temos as inclusões $\mathscr{P}_n(K) \subseteq W_n(K) \subseteq W(K) \subseteq K^\times$. Uma propriedade conhecida da teoria dos grupos abelianos finitos é que se G for um grupo abeliano finito então existe um elemento γ em G de ordem $\operatorname{mmc}(\operatorname{ordem}(g)\colon g \in G)$. Utilizando isso, podemos obter:

Proposição 2.23. *Todo subgrupo finito G de $K^\times$ é cíclico e igual a $W_m(K)$, sendo $m = |G|$.*

Nós temos ainda a seguinte equivalência:

Proposição 2.24. *Seja p a característica de K. Então são equivalentes:*

(i) $|W_n(K)| = n$.

(ii) $\mathscr{P}_n(K) \neq \emptyset$.

(iii) $p \nmid n$ *e* $x^n - 1$ *se fatora em fatores lineares de* $K[x]$.

Nesse caso, $\mathscr{P}_d(K) \neq \emptyset$ para todo $d \mid n$, e[1] $W_n(K) = \bigsqcup_{d|n} \mathscr{P}_d(K)$.

Suponhamos que $\zeta \in K$ seja uma raiz primitiva n-ésima da unidade. Então é claro que $W_n(K) = \langle\zeta\rangle$ é isomorfo ao grupo aditivo $\mathbb{Z}/n\mathbb{Z}$, com isomorfismo $k + n\mathbb{Z} \mapsto \zeta^k$. Como os geradores de $\mathbb{Z}/n\mathbb{Z}$ são as $\varphi(n)$ classes dos inteiros primos com n, vemos que $W_n(K)$ tem $\varphi(n)$ geradores, da forma ζ^k para $1 \leq k \leq n$ e $\operatorname{mdc}(k, n) = 1$. Assim, $|\mathscr{P}_n(K)| = \varphi(n)$. Sendo $W_n(K) = \bigsqcup_{d|n} \mathscr{P}_d(K)$, concluímos que

$$n = |W_n(K)| = \sum_{d|n} |\mathscr{P}_d| = \sum_{d|n} \varphi(d).$$

Assim, obtemos um famoso resultado da Teoria Elementar dos Números. Associemos a cada $k \in \mathbb{Z}$ o endomorfismo de $W_n(K)$ dado por $\nu \mapsto \nu^k$. Esse endomorfismo só depende da classe de k módulo n, e será um automorfismo se e só se $\operatorname{mdc}(k, n) = 1$. Isso define um isomorfismo $(\mathbb{Z}/n\mathbb{Z})^\times \to \operatorname{Aut}(W_n(K))$, como é fácil verificar.

Dados K um corpo e $n \geq 1$, supondo que a característica de K não divida n sempre existirá uma raiz primitiva n-ésima da unidade ζ num fecho algébrico de K. Então a extensão $K(\zeta)/K$ é "bem-comportada":

[1] A notação $\bigsqcup_{\lambda\in\Lambda} C_\lambda$ indica uma união disjunta. Isto é, indica que os conjuntos C_λ são disjuntos dois a dois.

Teorema 2.25. *Seja K um corpo e seja n um inteiro positivo não divisível pela característica de K. Seja $L = K(\zeta)$, onde ζ é uma raiz primitiva n-ésima da unidade num fecho algébrico de K. Então L/K é uma extensão galoisiana, e $\mathrm{Gal}(L/K)$ é canonicamente isomorfo a um subgrupo de $(\mathbb{Z}/n\mathbb{Z})^\times$. Em particular, $\mathrm{Gal}(L/K)$ é abeliano de ordem divisora de $\varphi(n)$.*

Demonstração. L é extensão galoisiana de K, pois é o corpo de decomposição do polinômio $x^n - 1$, que é separável já que a característica de K não divide n pela Proposição 2.24. Dado um automorfismo $\sigma \in \mathrm{Gal}(L/K)$, é fácil ver que $\sigma(\zeta)$ também é raiz primitiva n-ésima da unidade, de modo que $\sigma|_{W_n(K)} \in \mathrm{Aut}(W_n(K))$. Como todo automorfismo de $\mathrm{Gal}(L/K)$ está totalmente determinado pela imagem de ζ, temos uma inclusão $\mathrm{Gal}(L/K) \to \mathrm{Aut}(W_n(K))$ dada por $\sigma \mapsto \sigma|_{W_n(K)}$. Mas como já vimos $\mathrm{Aut}(W_n(K))$ é canonicamente isomorfo a $(\mathbb{Z}/n\mathbb{Z})^\times$, mostrando que $\mathrm{Gal}(L/K)$ é canonicamente isomorfo a um subgrupo de $(\mathbb{Z}/n\mathbb{Z})^\times$. □

No caso $K = \mathbb{Q}$, obtemos um resultado ainda melhor:

Teorema 2.26. *Seja $\zeta \in \mathbb{C}$ uma raiz primitiva n-ésima da unidade. Então $K = \mathbb{Q}(\zeta)$ é uma extensão galoisiana de $\mathbb{Q}$, com $\mathrm{Gal}(K/\mathbb{Q})$ canonicamente isomorfo a $(\mathbb{Z}/n\mathbb{Z})^\times$. Assim, $\mathrm{Gal}(K/\mathbb{Q})$ é abeliano de ordem $\varphi(n)$. Além disso, o polinômio minimal $P_{\zeta,\mathbb{Q}}$ é igual a $\Phi_n(x) := \prod_{\eta \in \mathscr{P}_n(\mathbb{C})}(x - \eta)$.*

Demonstração. Provaremos que se p é um primo que não divide n e se θ é uma raiz primitiva n-ésima da unidade, então θ e θ^p possuem o mesmo polinômio minimal. Com esse resultado, podemos mostrar que para todo k primo com n o polinômio minimal de ζ^k será $P_{\zeta,\mathbb{Q}}$. Com efeito, seja $k = p_1 p_2 \cdots p_m$ para $p_1, p_2, \ldots, p_m$ primos. Como $\mathrm{mdc}(k, n) = 1$, nenhum desses primos divide n. Aplicando esse resultado a ζ e p_1, concluímos que o polinômio minimal de ζ^{p_1} é $P_{\zeta,\mathbb{Q}}$. Aplicando novamente esse resultado a ζ^{p_1} e p_2, concluímos que o polinômio minimal de $(\zeta^{p_1})^{p_2} = \zeta^{p_1 p_2}$ é $P_{\zeta,\mathbb{Q}}$. Continuando dessa forma, concluímos que o polinômio minimal de $\zeta^k = \zeta^{p_1 \cdots p_m}$ é $P_{\zeta,\mathbb{Q}}$.

Desse modo, $P_{\zeta,\mathbb{Q}}$ será o polinômio minimal dos $\varphi(n)$ números da forma ζ^k com $\mathrm{mdc}(k, n) = 1$, isto é, as $\varphi(n)$ raízes primitivas n-ésimas da unidade. Então $\varphi(n) \leq \partial\, P_{\zeta,\mathbb{Q}} = [L : \mathbb{Q}] \leq \varphi(n)$ pelo teorema anterior, e assim $P_{\zeta,\mathbb{Q}} = [K : \mathbb{Q}] = \varphi(n)$. Desse modo, as raízes de $P_{\zeta,\mathbb{Q}}$ são exatamente as raízes primitivas n-ésimas da unidade, o que mostra que $P_{\zeta,\mathbb{Q}}(x) = \Phi_n(x) = \prod_{\eta \in \mathscr{P}_n(\mathbb{C})}(x - \eta)$.

Mostremos então que vale o resultado desejado. Se esse não fosse o caso, então θ e θ^p teriam polinômio minimais distintos, digamos P e Q respectivamente. Como θ e θ^p são raízes de $x^n - 1$, eles são inteiros algébricos, e portanto $P, Q \in \mathbb{Z}[x]$. Desse modo, $x^n - 1 = P(x)Q(x)f(x)$, para algum $f \in \mathbb{Z}[x]$. Notemos que θ é raiz de $Q(x^p)$, e portanto temos $Q(x^p) = P(x)g(x)$ para algum $g \in \mathbb{Z}[x]$. Passando a $\mathbb{F}_p[x]$, nós temos $x^n - \overline{1} = \overline{P}(x)\overline{Q}(x)\overline{f}(x)$ e $\overline{P}(x)\overline{g}(x) = \overline{Q(x^p)} = \overline{Q}(x)^p$. Essa última igualdade nos diz que $\overline{P}$ e $\overline{Q}$ possuem um fator comum $\overline{D} \in \mathbb{F}_p[x]$. Mas então $\overline{D}^2 \mid x^n - \overline{1}$ um absurdo já que $x^n - \overline{1}$ é separável em $\mathbb{F}_p[x]$ (pois $p \nmid n$). Isso conclui a demonstração. □

Definição (n-ésimo Corpo Ciclotômico/Polinômio Ciclotômico)**.** Definimos o **n-ésimo corpo ciclotômico** como sendo $\mathbb{Q}(\zeta)$, onde $\zeta \in \mathbb{C}$ é uma raiz primitiva n-ésima da unidade. Além disso, chamamos o polinômio $\Phi_n(x) \in \mathbb{Z}[x]$, minimal de ζ, de **n-ésimo polinômio ciclotômico**.

As igualdades $W_n(\mathbb{C}) = \bigsqcup_{d|n} \mathscr{P}_d(\mathbb{C})$ e $\Phi_n(x) = \prod_{\eta \in \mathscr{P}_n(\mathbb{C})}(x - \eta)$ nos dão diretamente:

Corolário 2.27. *Para todo n inteiro positivo, nós temos $x^n - 1 = \prod_{d|n} \Phi_d(x)$.*

Esse corolário nos dá um método prático para calcular Φ_n por recorrência, utilizando a igualdade $\Phi_n(x) = (x^n - 1)/\prod_{d|n,\ d<n} \Phi_d(x)$. É claro que $\Phi_1(x) = x - 1$. Assim, para cada número primo p, temos $\Phi_p(x) = (x^p - 1)/\Phi_1(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1$. Isso mostra em

particular que esses polinômios são irredutíveis, fato conhecido e usualmente demonstrado pelo critério de Eisenstein. Mais geralmente, é fácil determinar explicitamente $\Phi_{p^r}(x)$, para $r \geq 1$:

$$\begin{aligned} x^{p^r}-1 &= \Phi_1(x)\Phi_p(x)\cdots\Phi_{p^{r-1}}(x)\Phi_{p^r}(x) = (x^{p^{r-1}}-1)\Phi_{p^r}(x) \\ &\Rightarrow \Phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = x^{(p-1)p^{r-1}} + \cdots + x^{2p^{r-1}} + x^{p^{r-1}} + 1. \end{aligned}$$

Consideremos agora o corpo $\mathbb{Q}(\zeta)$, para ζ raiz primitiva n-ésima da unidade, e procuremos calcular o polinômio característico, o traço e a norma de um elemento qualquer desse corpo. Observemos que $1, \zeta, \ldots, \zeta^{\varphi(n)-1}$ formam uma base da extensão $\mathbb{Q}(\zeta)/\mathbb{Q}$, e portanto um elemento genérico de $\mathbb{Q}(\zeta)$ se escreve como $\gamma = a_0 + a_1\zeta + \cdots + a_{\varphi(n)}\zeta^{\varphi(n)-1}$, para $a_0, a_1, \ldots, a_{\varphi(n)} \in \mathbb{Q}$. Sabemos que o grupo de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}$ é composto pelos automorfismos $\zeta \mapsto \zeta^k$, onde $1 \leq k \leq n$ e $\mathrm{mdc}(k,n) = 1$. Sendo assim, os conjugados de γ são os elementos da forma

$$a_0 + a_1\zeta^k + \cdots + a_{\varphi(n)}\zeta^{(\varphi(n)-1)k}, \text{ para } 1 \leq k \leq n \text{ e } \mathrm{mdc}(k,n) = 1.$$

Portanto, o polinômio característico de γ é dado por

$$F_\gamma(x) = \prod_{\substack{1\leq k\leq n \\ \mathrm{mdc}(k,n)=1}} (x - (a_0 + a_1\zeta^k + \cdots + a_{\varphi(n)}\zeta^{(\varphi(n)-1)k})).$$

Além disso, o traço de γ é

$$\mathrm{Tr}(\gamma) = \sum_{\substack{1\leq k\leq n \\ \mathrm{mdc}(k,n)=1}} (a_0 + a_1\zeta^k + \cdots + a_{\varphi(n)}\zeta^{(\varphi(n)-1)k})$$

e a norma de γ é

$$N(\gamma) = \prod_{\substack{1\leq k\leq n \\ \mathrm{mdc}(k,n)=1}} (a_0 + a_1\zeta^k + \cdots + a_{\varphi(n)}\zeta^{(\varphi(n)-1)k}).$$

Observe que $\mathrm{Tr}(\gamma)$ e $N(\gamma)$ são polinômio simétricos nas raízes primitivas da unidade, e portanto podem ser determinados como polinômios nos coeficientes de Φ_n.

Mostraremos que o anel de inteiros algébricos de um corpo ciclotômico $K = \mathbb{Q}(\zeta)$ tem base integral $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$. Note que basta provarmos que

$$\mathcal{O}_K = \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\cdot\zeta + \cdots + \mathbb{Z}\cdot\zeta^{\varphi(n)-1}.$$

Entretanto, postergaremos essa demonstração para a Seção 5.3, pois necessitamos de um maquinário maior. Por ora, mostraremos apenas alguns fatos que nos serão úteis mais adiante.

Consideremos p primo ímpar, $\zeta \in \mathbb{C}$ uma raiz primitiva p-ésima da unidade e $K = \mathbb{Q}(\zeta)$. Estudemos K e $\mathcal{O}_K$. Nesse caso, temos $p-1$ raízes primitivas p-ésimas da unidade, a saber $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, e como visto acima temos $\Phi_p(x) = x^{p-1} + \cdots + x + 1$. Existem exatamente $p-1$ automorfismos $\sigma_1, \ldots, \sigma_{p-1} \colon K \to K$, com $\sigma_j(\zeta) = \zeta^j$ para $1 \leq j \leq p-1$ (note que $\sigma_1 = \mathrm{id}_K$). Começamos com o seguinte resultado:

Lema 2.28. *Os elementos $\zeta - 1, \ldots, \zeta^{p-1} - 1$ são raízes do polinômio*

$$\psi_p := x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1} \in \mathbb{Z}[x],$$

que é irredutível em $\mathbb{Q}[x]$.

Demonstração. Basta notar que

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = \frac{\sum_{j=1}^{p}\binom{p}{j}x^j}{x} = \sum_{j=1}^{p}\binom{p}{j}x^{j-1} = \psi_p(x).$$

Assim, é claro que $\zeta - 1, \ldots, \zeta^{p-1} - 1$ são raízes de ψ_p. A irredutibilidade de ψ_p segue da irredutibilidade de Φ_p. □

Como cada ζ^j, $\zeta^j - 1$ são elementos primitivos de $K/\mathbb{Q}$, seus polinômios característicos coincidem com seus minimais, isto é, com Φ_p e com ψ_p respectivamente. Como sabemos Φ_p e ψ_p explicitamente, é fácil calcular a norma e o traço desses elementos. Para $1 \leq j \leq p-1$ nós temos:

$$\begin{array}{lll} \mathrm{Tr}(\zeta^j) = -1; & \mathrm{Tr}(\zeta^j - 1) = -p; & \mathrm{Tr}(1-\zeta^j) = p; \\ N(\zeta^j) = 1; & N(\zeta^j - 1) = p; & N(1-\zeta^j) = p. \end{array} \tag{2.1}$$

Note que de fato $N(\zeta) = 1$ vale para ζ raiz n-ésima da unidade para n qualquer, já que $\zeta^n = 1$. A partir dessas equações nós conseguimos calcular o discriminante do que mostraremos futuramente ser a base integral de uma extensão ciclotômica de grau potência de primo:

Proposição 2.29. *Sejam $p \in \mathbb{Z}$ primo, $r \geq 1$ inteiro e $\zeta \in \mathbb{C}$ uma raiz primitiva p^r-ésima da unidade. Consideremos o corpo ciclotômico $K = \mathbb{Q}(\zeta)$. Suponhamos ainda que $r \geq 2$ caso $p = 2$, pois senão $K = \mathbb{Q}$. Então:*

$$\Delta_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}) = (-1)^{\frac{\varphi(p^r)}{2}} p^{p^{(r-1)}(rp-r-1)}.$$

Demonstração. Notemos que como ζ é elemento primitivo da extensão $K/\mathbb{Q}$, temos $F_\zeta = P_\zeta = \Phi_{p^r}$. Como vimos, vale a igualdade $x^{p^r} - 1 = (x^{p^{r-1}} - 1)\Phi_{p^r}(x)$. Assim, derivando os dois lados dessa equação obtemos

$$p^r x^{p^r - 1} = p^{r-1}x^{p^{r-1}-1}\Phi_{p^r}(x) + (x^{p^{r-1}} - 1)\Phi'_{p^r}(x).$$

Avaliando em ζ, obtemos:

$$p^r \zeta^{p^r-1} = (\zeta^{p^{r-1}} - 1)\Phi'_{p^r}(\zeta) \Rightarrow \Phi'_{p^r}(\zeta) = \frac{p^r\zeta^{-1}}{\zeta^{p^{r-1}} - 1} = \frac{p^r\zeta^{-1}}{\xi - 1},$$

onde $\xi := \zeta^{p^{r-1}}$ é uma raiz primitiva p-ésima da unidade. Consideremos primeiramente o caso p ímpar. Aplicando $N_{K/\mathbb{Q}}$, obtemos:

$$\begin{aligned} N_{K/\mathbb{Q}}(\Phi'_{p^r}(\zeta)) = \frac{N_{K/\mathbb{Q}}(p^r\zeta^{-1})}{N_{K/\mathbb{Q}}(\xi - 1)} &= \frac{p^{r\varphi(p^r)} \cdot N_{K/\mathbb{Q}}(\zeta)^{-1}}{N_{\mathbb{Q}(\xi)/\mathbb{Q}}(N_{K/\mathbb{Q}(\xi)}(\xi - 1))} \\ &= \frac{p^{r\varphi(p^r)} \cdot 1}{N_{\mathbb{Q}(\xi)/\mathbb{Q}}((\xi-1)^{\varphi(p^r)/\varphi(p)})} \\ &= \frac{p^{r\varphi(p^r)}}{p^{\varphi(p^r)/\varphi(p)}} \\ &= p^{r(p-1)p^{r-1} - p^{r-1}} \\ &= p^{p^{r-1}(rp-r-1)}, \end{aligned}$$

onde utilizamos (2.1) e as propriedades da norma. Sendo assim, pela Proposição 1.33 nós temos:

$$\begin{aligned} \Delta(1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}) &= (-1)^{\binom{\varphi(p^r)}{2}} N_{K/\mathbb{Q}}(\Phi'_{p^r}(\zeta)) \\ &= (-1)^{\frac{\varphi(p^r)}{2}} p^{p^{r-1}(rp-r-1)}, \end{aligned}$$

já que $\varphi(p^r)$ é par, e portanto a paridade de $\binom{\varphi(p^r)}{2}$ é a mesma de $\varphi(p^r)/2$.

Consideremos agora $p = 2$. Nesse caso, $r \geq 2$ e ξ é uma raiz primitiva 2-ésima da unidade, ou seja, $\xi = -1$. Assim, nós temos:

$$\begin{aligned} N_{K/\mathbb{Q}}(\Phi'_{2^r}(\zeta)) = \frac{N_{K/\mathbb{Q}}(2^r\zeta^{-1})}{N_{K/\mathbb{Q}}(-2)} &= \frac{2^{r\varphi(2^r)} \cdot N_{K/\mathbb{Q}}(\zeta)^{-1}}{(-2)^{\varphi(2^r)}} \\ &= \frac{2^{r\varphi(2^r)} \cdot 1}{(-2)^{\varphi(2^r)}} \\ &= (-1)^{\varphi(2^r)} 2^{(r-1)\varphi(2^r)} \\ &= 2^{2^{r-1}(r-1)}, \end{aligned}$$

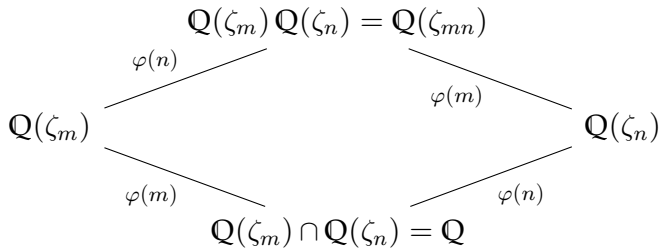
por (2.1), pelas propriedades da norma e observando que $\varphi(2^r)$ é par. Sendo assim, pela Proposição 1.33, nós temos:

$$\begin{aligned} \Delta(1, \zeta, \ldots, \zeta^{\varphi(2^r)-1}) &= (-1)^{\binom{\varphi(2^r)}{2}} N_{K/\mathbb{Q}}(\Phi'_{2^r}(\zeta)) \\ &= (-1)^{\frac{\varphi(2^r)}{2}} 2^{2^{r-1}(r-1)}. \end{aligned}$$

Note que essa expressão é a desejada substituindo $p = 2$. □

Outro fato importante é a relação entre diferentes corpos ciclotômicos:

Proposição 2.30. *Sejam $m, n > 1$ inteiros positivos primos entre si, e sejam $\zeta_m, \zeta_n, \zeta_{mn} \in \mathbb{C}$ raízes primitivas m-ésima, n-ésima e mn-ésima da unidade, respectivamente. Então valem as igualdades $\mathbb{Q}(\zeta_m)\,\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$ e $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.*



Além disso, se denotarmos por $\xi_1, \ldots, \xi_{\varphi(m)}$ as raízes m-ésimas primitivas da unidade e por $\eta_1, \ldots, \eta_{\varphi(n)}$ as raízes n-ésimas primitivas da unidade, então o conjunto das raízes mn-ésimas da unidade é igual a $\{\xi_i\eta_j \colon 1 \leq i \leq \varphi(m),\ 1 \leq j \leq \varphi(n)\}$. Em particular:

$$\Phi_{mn}(x) = \prod_{i=1}^{\varphi(m)} \prod_{j=1}^{\varphi(n)} (x - \xi_i\eta_j).$$

Demonstração. Consideremos o grupo multiplicativo $\mathbb{C}^\times$. Como ζ_m tem ordem m, ζ_n tem ordem n e $\mathrm{mdc}(m, n) = 1$, um resultado conhecido da teoria de grupos abelianos nos diz que $\zeta' := \zeta_m\zeta_n$ tem ordem $\mathrm{mmc}(m, n) = mn$. Consequentemente, $\mathbb{Q}(\zeta') = \mathbb{Q}(\zeta_{mn})$, já que ζ' é uma potência inteira de ζ e vice-versa. Assim, basta mostrarmos que $\mathbb{Q}(\zeta_m)\,\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta')$, o que é claro. Podemos agora concluir que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$, já que essa é a condição para valer

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)\,\mathbb{Q}(\zeta_n)/\,\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\,\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\,\mathbb{Q}),$$

que sabemos ser verdade já que $(\mathbb{Z}/mn\,\mathbb{Z})^\times \cong (\mathbb{Z}/m\,\mathbb{Z})^\times \times (\mathbb{Z}/n\,\mathbb{Z})^\times$.

Para a segunda afirmação, como já vimos o produto de uma raiz primitiva m-ésima da unidade com uma raiz primitiva$n$-ésima da unidade é uma raiz primitiva mn-ésima da unidade. Assim, cada $\xi_i\eta_j$ é uma raiz primitiva mn-ésima da unidade, e é um exercício simples verificar que esses produtos são distintos dois a dois. Como $\varphi(m)\varphi(n) = \varphi(mn)$, o conjunto dos $\xi_i\eta_j$ está contido em $\mathscr{P}_{mn}(\mathbb{C})$ e tem o mesmo número de elementos que esse conjunto. Assim, os dois conjuntos coincidem. A expressão para $\Phi_{mn}(x)$ é então imediata. □

Estudemos agora extensões ciclotômicas em corpos de característica $p > 0$. Devido à Proposição 2.24, dado n inteiro positivo só podem existir raízes primitivas n-ésimas da unidade em alguma extensão de um corpo de característica p se $p \nmid n$. Se esse for o caso, tais raízes da unidade sempre existirão. No caso de corpos finitos, nós temos uma caracterização para suas extensões ciclotômicas:

Teorema 2.31. *Sejam $p \in \mathbb{N}$ um primo, $q = p^r$ e n um inteiro positivo tal que $p \nmid n$. Chamemos de f_q a ordem de $\overline{q}$ no grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^\times$. Então existem raízes primitivas n-ésimas da unidade em $\mathbb{F}_{q^{f_q}}$, e essa é a menor extensão de $\mathbb{F}_q$ tal que isso ocorre. Em particular, sendo ζ uma raiz primitiva n-ésima da unidade, temos $\mathbb{F}_q[\zeta] = \mathbb{F}_{q^{f_q}}$, e portanto o polinômio minimal de ζ em $\mathbb{F}_q$ tem grau f_q.*

Demonstração. Pela Proposição 2.24, para garantirmos a existência de uma (e portanto de todas) raiz primitiva da unidade em uma extensão $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$, é necessário e suficiente que $x^n - 1$ se fatore em fatores lineares de $\mathbb{F}_{q^m}[x]$, ou seja, que o corpo de decomposição de $x^n - 1$ esteja contido em $\mathbb{F}_{q^m}[x]$. Assim, basta mostrarmos que $\mathbb{F}_{q^{f_q}}$ é o corpo de decomposição de $x^n - 1$ sobre $\mathbb{F}_q$.

Comecemos notando que esse corpo de decomposição será da forma $\mathbb{F}_{q^k}$, para algum inteiro positivo k. Como $\mathbb{F}_{q^k}^\times$ é um grupo multiplicativo de ordem $q^k - 1$, temos $\zeta^{q^k-1} = 1$. Mas uma vez que a ordem de ζ nesse grupo é n, nós obtemos $n \mid q^k - 1$. Isso significa que $f_q \mid k$. Assim, $q^{f_q} - 1 \mid q^k - 1$, e $x^{q^{f_q}-1} - 1 \mid x^{q^k-1} - 1$. Como $\mathbb{F}_{q^{f_q}}$ é corpo de decomposição de $x^{q^{f_q}-1} - 1$ e $\mathbb{F}_{q^k}$ é corpo de decomposição de $x^{q^k-1} - 1$, concluímos que $\mathbb{F}_{q^{f_q}} \subseteq \mathbb{F}_{q^k}$.

Por outro lado, como $n \mid q^{f_q} - 1$, temos $x^n - 1 \mid x^{q^{f_q}-1} - 1$, e portanto o corpo de decomposição de $x^n - 1$ está contido no corpo de decomposição de $x^{q^{f_q}-1} - 1$. Mas o corpo de decomposição de $x^n - 1$ é $\mathbb{F}_{q^k}$, e o corpo de decomposição de $x^{q^{f_q}-1} - 1$ é $\mathbb{F}_{q^{f_q}}$. Assim, $\mathbb{F}_{q^k} \subseteq \mathbb{F}_{q^{f_q}}$.

Concluímos que o corpo de decomposição de $x^n - 1$ sobre $\mathbb{F}_q$ é $\mathbb{F}_{q^{f_q}}$. Portanto, essa é a menor extensão de $\mathbb{F}_q$ que possui raízes primitivas n-ésimas da unidade, pela Proposição 2.24. Finalmente, dada uma raiz primitiva n-ésima da unidade $\zeta \in \mathbb{F}_{q^{f_q}}$, por essa mesma proposição vale a igualdade $x^n - 1 = (x-1)(x-\zeta)\cdots(x-\zeta^{n-1})$ em $\mathbb{F}_{q^{f_q}}[x]$. Portanto, $\mathbb{F}_{q^{f_q}} = \mathbb{F}_p[\zeta]$. Em particular, o polinômio irredutível de ζ sobre $\mathbb{F}_q$ tem grau f_q. □

2.4. Algumas Aplicações

Nessa seção, mostraremos duas aplicações interessantes do estudo de corpos quadráticos e ciclotômicos. Um problema clássico de Teoria dos Números é o das **ternas pitagóricas**: encontrar as soluções inteiras da equação $x^2 + y^2 = z^2$. Esse problema pode ser resolvido sem utilizar inteiros algébricos, mas possui uma solução em certo sentido "mais natural" que se utiliza do anel dos inteiros de Gauss. Lembre que esse anel é um domínio euclidiano. Seja $d = \text{mdc}(x, y)$, e escrevamos $x = da$ e $y = db$. Então $x^2 + y^2 = z^2 \Rightarrow d \mid z$, e podemos escrever $z = dc$. Assim, nossa equação se torna $a^2 + b^2 = c^2$, e vale $\text{mdc}(a, b) = 1$.

Observemos agora que temos a fatoração $a^2 + b^2 = (a + bi)(a - bi)$ em $\mathbb{Z}[i]$, de modo que $(a + bi)(a - bi) = c^2$ é um quadrado perfeito. Encontremos os primos $\pi \in \mathbb{Z}[i]$ que podem dividir ambos $a + bi$ e $a - bi$. Um tal primo deve também dividir $(a + bi) + (a - bi) = 2a$ e $(a + bi) - (a - bi) = 2bi$. Assim, $\pi \mid 2a$ e $\pi \mid 2b$. Como a, b são primos entre si em $\mathbb{Z}$, concluímos que $\pi \mid 2$, e portanto a única possibilidade é termos $\pi = 1 + i$. Mas isso não pode acontecer! De fato, se esse fosse o caso então

$$1 + i \mid a + bi \Rightarrow 2 = N(1 + i) \mid N(a + bi) = a^2 + b^2,$$

logo concluiríamos que a e b são ambos ímpares já que $\text{mdc}(a, b) = 1$. Mas então nós teríamos que $c^2 = a^2 + b^2 \equiv 2 \pmod 4$, um absurdo! Isso mostra que $a + bi$ e $a - bi$ são primos entre si em $\mathbb{Z}[i]$.

Como $(a+bi)(a-bi)$ é um quadrado perfeito e $a+bi$ é primo com $a-bi$, nós devemos ter $a+bi = u\alpha^2$ para alguns $u \in \mathbb{Z}[i]^\times$, $\alpha \in \mathbb{Z}[i]$. Escrevamos $\alpha = m+ni$, para $m, n \in \mathbb{Z}$, e lembremos que $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$. Abrindo a expressão $a+bi = u(m+ni)^2$, nós encontramos:

$$(a,b) = \begin{cases} (m^2-n^2, 2mn), \text{ se } u = 1; \\ (n^2-m^2, -2mn), \text{ se } u = -1; \\ (-2mn, m^2-n^2), \text{ se } u = i; \\ (2mn, n^2-m^2), \text{ se } u = -i. \end{cases}$$

Notemos que, em qualquer caso, encontramos $c^2 = a^2+b^2 = (m^2-n^2)^2 + (2mn)^2 = (m^2+n^2)^2$, de modo que obtemos $c = \pm(m^2+n^2)$. Observemos que, a menos da ordem de a e de b e dos sinais de a, b, c, todas as soluções de $a^2+b^2 = c^2$ são da forma $(m^2-n^2, 2mn, m^2+n^2)$, para $m \geq n \geq 0$ inteiros. A partir disso, concluímos que todas as soluções da equação inicial $x^2+y^2 = z^2$ são, a menos de ordem e sinais, da forma $(x,y,z) = (d(m^2-n^2), 2dmn, d(m^2+n^2))$, para $m \geq n \geq 0$ inteiros e $d \geq 0$ inteiro.

Mostraremos agora uma aplicação do estudo de corpos ciclotômicos: o Pequeno Teorema de Wedderburn:

Teorema 2.32 (Pequeno Teorema de Wedderburn)**.** *Seja A um domínio finito. Então A é um corpo*[2]*.*

Demonstração. Dado $a \in A$ não-nulo, consideremos a função $L_a \colon A \to A$ dada por $L_a(x) = ax$ e a função $R_a \colon A \to A$ dada por $R_a(x) = xa$. Então, como A é domínio, essas funções são injetoras. Sendo A finito, essas funções são bijeções. Assim, existem $\ell, r \in A$ tais que $\ell a = ar = 1$. Mas desse modo $\ell = \ell(ar) = (\ell a)r = r$, e portanto a é inversível. Como $a \in A$ não-nulo é qualquer, provamos que A é um anel de divisão.

Assim, basta mostrarmos que todo anel de divisão finito A é um corpo. Faremos isso por indução na cardinalidade de A. Comecemos observando que A é simples, e portanto o seu centro $Z(A)$ é um corpo. Se $|A|$ for um primo, então $A = Z(A)$ é um corpo, pois como $(Z(A), +)$ é um subgrupo de $(A, +)$ vemos que $|Z(A)|$ divide $|A|$, e $|Z(A)| \geq 2$ já que $0, 1 \in Z(A)$. Assim, $|Z(A)| = |A|$ e temos a igualdade desejada.

Suponhamos então por indução que a ordem de A não é prima, e que todo anel com divisão de ordem menor que $|A|$ é um corpo. Em particular, todo subanel próprio não-nulo de A é um corpo. Chamemos $p \coloneqq |Z(A)|$. Então A é um espaço vetorial sobre $Z(A)$ com uma certa dimensão $n \geq 1$, de modo que $|A| = p^n$. Queremos mostrar que $n = 1$, pois então concluiremos que $A = Z(A)$ é um corpo.

Para cada $a \in A \setminus Z(A)$, o seu centralizador $Z_a \coloneqq \{z \in A \colon za = az\}$ é um anel tal que $Z(A) \subseteq Z_a \subsetneq A$. Assim, por hipótese Z_a é um corpo. Notemos que então A é um espaço vetorial sobre Z_a e Z_a é um espaço vetorial sobre $Z(A)$. Dessa forma, devemos ter $|Z_a| = p^{d_a}$ para algum d_a divisor próprio de n.

Consideremos a ação do grupo multiplicativo $A^\times$ sobre si mesmo, dada pela multiplicação de A. O centro dessa ação é $Z(A)^\times$, e o estabilizador de cada elemento $a \in A^\times$ é $Z_a^\times$. Seja $\{a_1, \ldots, a_k\}$ um conjunto de representantes das órbitas não-triviais. Então a equação de classes nos dá:

$$|A^\times| = |Z(A)^\times| + \sum_{j=1}^{k} [A^\times : Z_{a_j}^\times] \Rightarrow p^n - 1 = p - 1 + \sum_{j=1}^{k} \frac{p^n-1}{p^{d_{a_j}}-1}.$$

Agora, lembremos que vale $x^n - 1 = \prod_{d|n} \Phi_d(x)$, e que sendo $1 \leq j \leq k$ temos $x^{d_{a_j}} - 1 = \prod_{m|d_{a_j}} \Phi_m(x)$. Como $m \mid d_{a_j} \Rightarrow m \mid n$ e $m \neq n$, é fácil ver que $\Phi_n(x) \mid \frac{x^n-1}{x^{d_{a_j}}-1}$ em $\mathbb{Z}[x]$. Desse

[2]Nesse enunciado, consideramos que a princípio A não precisaria ser comutativo.

modo, $\Phi_n(p) \mid \frac{p^n-1}{p^{da_j}-1}$. Como também $\Phi_n(p) \mid p^n - 1$, concluímos a partir da equação de classes que $\Phi_n(p) \mid p-1$. Em particular, $|\Phi_n(p)| \leq p-1$.

Sejam agora $\zeta_1, \ldots, \zeta_{\varphi(n)}$ as raízes primitivas n-ésimas da unidade. Então

$$\Phi_n(p) = \prod_{j=1}^{\varphi(n)} (p - \zeta_j) \Rightarrow |\Phi_n(p)| = \left| \prod_{j=1}^{\varphi(n)} (p - \zeta_j) \right| = \prod_{j=1}^{\varphi(n)} |p - \zeta_j|.$$

Para cada $1 \leq j \leq \varphi(n)$ temos $|p - \zeta_j| \geq |p| - |\zeta_j| = p - 1 \geq 1$, e se a igualdade valer então p e ζ_j são colineares, ou seja, $\zeta_j \in \mathbb{R}$. Mas nesse caso $\zeta_j = \pm 1$, e portanto $\zeta_j = 1$ já que $|p - (-1)| = p + 1 > p - 1 = |p| - |-1|$. Desse modo, se $n > 1$ então temos $|p - \zeta_j| > p - 1 \geq 1$ para todo j, e assim

$$|\Phi_n(p)| = \prod_{j=1}^{\varphi(n)} |p - \zeta_j| > (p-1)^{\varphi(n)} \geq p - 1,$$

absurdo! Concluímos que $n = 1$, e que portanto $A = Z(A)$ é um corpo, como desejado. □

Existem diversas outras aplicações do estudo de corpos quadráticos e ciclotômicos na matemática. O conjunto $\mathbb{Z}[i]$ também pode ser utilizado, por exemplo, para provar o **Teorema dos Dois Quadrados**, que determina quais números inteiros positivos se escrevem como soma de dois quadrados perfeitos. Os corpos ciclotômicos, por sua vez, possuem uma importância histórica na resolução de casos particulares do Último Teorema de Fermat. Além disso, um estudo mais detalhado dos polinômios ciclotômicos nos permite solucionar de forma elementar um caso particular do famoso Teorema de Dirichlet sobre progressões aritméticas.

Teorema 2.33 (Teorema de Dirichlet sobre Progressões Aritméticas)**.** *Sejam a e n inteiros positivos primos entre si. Então existem infinitos primos da forma $nk + a$, para k variando nos naturais. Equivalentemente, existem infinitos primos congruentes a a módulo n.*

Esse teorema se demonstra utilizando métodos da Teoria Analítica dos Números. Entretanto, utilizando polinômios ciclotômicos pode-se demonstrar o caso em que $a = 1$, isto é:

Teorema 2.34 (Caso particular do Teorema de Dirichlet)**.** *Seja $n > 1$ um inteiro positivo. Então existem infinitos primos p tais que $p \equiv 1 \pmod{n}$.*

Uma demonstração desse resultado se encontra em [13].

Capítulo 3

Domínios de Dedekind e de Valoração Discreta

Como vimos, nem todo anel de inteiros algébricos é um DFU, como por exemplo $\mathbb{Z}[\sqrt{-5}]$. Apesar disso, como veremos neste capítulo, todo anel de inteiros algébricos ainda possui propriedades muito boas. A saber, ele é um **domínio de Dedekind**, isto é, ainda que não haja a unicidade da fatoração para os elementos de $\mathcal{O}_K$, vale um teorema de unicidade da fatoração para objetos um pouco diferentes: os ideais de $\mathcal{O}_K$. Com isso, vale a pena um estudarmos mais detalhadamente esse importante tipo de anel. Também estudaremos os **domínios de valoração discreta**, que são tipos especiais de DIP's. Como veremos, a cada domínio de valoração discreta nós podemos associar uma **valoração discreta**, uma função que possui diversas propriedades boas.

3.1. A Fatoração Única de Ideais

Definição (Domínio de Dedekind)**.** Seja A um domínio. Então A é chamado de **domínio de Dedekind** se for integralmente fechado, noetheriano e se todo ideal primo não-nulo de A for maximal.

O seguinte teorema diz que a propriedade de um anel ser um domínio de Dedekind é preservada em certos tipos de extensão:

Teorema 3.1. *Sejam A um domínio de Dedekind, $K = Q(A)$ e L uma extensão finita e separável de K. Então $B := \overline{A}^L$ é um domínio de Dedekind.*

Demonstração. Temos $Q(B) = L$, pelo Teorema 1.16. Além disso, $\overline{B}^L = B$, pelo Corolário 1.13. Logo B é integralmente fechado. Além disso, B é noetheriano pelo Teorema 1.37. Finalmente, todo ideal primo não-nulo de B é maximal, pelo item (e) do Teorema 1.53. □

É claro que $\mathbb{Z}$ é um domínio de Dedekind. Assim, o teorema acima nos dá diretamente o seguinte resultado, que mostra a importância de estudar domínios de Dedekind em Teoria Algébrica dos Números:

Teorema 3.2. *Seja K um corpo de números algébricos. Então $\mathcal{O}_K$ é um domínio de Dedekind.*

Sejam A um domínio qualquer e $K = Q(A)$ seu corpo de frações. Então podemos ver K como A-módulo com a multiplicação de K. Dados dois A-submódulos $M, N \subseteq K$, podemos definir os submódulos $M + N$ e $M \cap N$ de K da maneira usual. Como temos uma multiplicação em K, podemos definir também o produto MN, como sendo o submódulo formado pelas somas finitas de elementos da forma mn com $m \in M$ e $n \in N$. Essas operações são bem-comportadas, pois elas são associativas e comutativas, e além disso é fácil ver que temos, para $M, N, P \subseteq K$ submódulos:

- $M(N+P) = MN + MP$;
- $(M \cap N)(M+N) \subseteq MN$;
- $M(N \cap P) \subseteq MN \cap MP$;
- $M \cap (N+P) \supseteq (M \cap N) + (M \cap P)$;
- $M + (N \cap P) \subseteq (M+N) \cap (M+P)$.

Dessa forma, esses submódulos se comportam como ideais.

Definição (Ideal Fracionário)**.** Dizemos que um submódulo não-nulo $M \subseteq K$ é um **ideal fracionário** de A se existir $d \in A \setminus \{0\}$ tal que $dM \subseteq A$.

Nesse caso, é fácil ver que dM será um ideal $\mathfrak{a} \lhd A$, de modo que $M = d^{-1}\mathfrak{a}$ é a "fração" de um ideal de A por um elemento não-nulo de A. Notemos que os ideais de A coincidem com os ideais fracionários contidos em A. É importante também notar que todo submódulo não-nulo finitamente gerado de K é um ideal fracionário, pois basta escolher d de forma a "limpar os denominadores" de todos os geradores desse submódulo. Reciprocamente, num domínio noetheriano todo ideal fracionário M é finitamente gerado, pois se $dM \lhd A$ então dM é finitamente gerado. Assim:

Proposição 3.3. *Todo A-submódulo não-nulo finitamente gerado $M \subseteq K$ é um ideal fracionário de A. Além disso, se A for um domínio noetheriano, um submódulo não-nulo $M \subseteq K$ de A será um ideal fracionário de A se e somente se for um A-módulo finitamente gerado.*

Notação. Indicaremos o conjunto dos A-submódulos não-nulos de K por $\mathscr{M}(A)$, o conjunto dos ideais fracionários de A por $I(A)$, o conjunto dos ideais não-nulos de A por $\mathscr{J}(A)$ e o conjunto dos ideais primos não-nulos de A por $\mathscr{P}(A)$. Quando A estiver claro, denotaremos apenas $\mathscr{M}, I, \mathscr{J}$ e $\mathscr{P}$.

É fácil mostrar que o conjunto I é fechado por soma, interseção e produto.

Definição (Ideal Inversível)**.** Dizemos que $M \in \mathscr{M}$ é **inversível** se existir $N \in \mathscr{M}$ tal que $MN = A$. Nesse caso, dizemos que N é o **inverso** de M.

Com a operação de multiplicação, $\mathscr{M}$ se torna um monoide, com identidade A. Assim, se $M \in \mathscr{M}$ for inversível, seu inverso será único, e será denotado M^{-1}. Notemos ainda que I é um submonoide de $\mathscr{M}$.

Os submódulos gerados por um único elemento não-nulo sempre são fracionários inversíveis:

Proposição 3.4. *Seja $x \in K \setminus \{0\}$. Então o submódulo $xA \subseteq K$ é um ideal fracionário de A. Além disso, dado $y \in K \setminus \{0\}$, temos $(xA)(yA) = xyA$. Em particular, xA é inversível, com inverso $x^{-1}A$.*

Demonstração. É claro que $(xA)(yA) = xyA$, de onde segue também a última afirmação. Chamando $x = r/s$, onde $r, s \in A$, $s \neq 0$, temos $sx = r \in A$, e portanto $sxA \subseteq A$. Isso mostra que xA é um ideal fracionário de A. □

Essa proposição mostra que a seguinte definição faz sentido:

Definição (Ideal Fracionário Principal)**.** Chamaremos um ideal fracionário de A de **principal** se ele for da forma xA, para $x \in K \setminus \{0\}$.

O conjunto dos ideais fracionários principais de A forma um grupo, que será denotado por $P(A)$. Quando A estiver claro, denotaremos $P(A)$ apenas por P.

Nós temos uma caracterização melhor para o inverso de um módulo, utilizando o chamado **quociente** de um submódulo:

Definição (Quociente de um Submódulo)**.** Dado $M \subseteq K$ submódulo, definimos o **quociente** de M como sendo $(A : M) \coloneqq \{x \in K \mid xM \subseteq A\}$.

É fácil ver que $(A : M)$ também é um submódulo de K, e que ele satisfaz $(A : M)M \subseteq A$. Além disso, dado um ideal $\mathfrak{a} \lhd A$, temos claramente $A \subseteq (A : \mathfrak{a})$, e $(A : 0) = K$.

Proposição 3.5. *Seja $M \in \mathscr{M}$. Então:*

(a) $(A : M)$ é um ideal fracionário de A;

(b) Se M for um ideal fracionário de A, então $(A : M) \neq 0$;

(c) Se $A \neq K$, então $(A : K) = 0$, e K não é um ideal fracionário de A.

Demonstração. (a) Seja $c/d \in M$ não-nulo, com $c, d \in A$. Então $c = d(c/d) \in M \cap A \setminus \{0\}$. Observemos agora que $c(A : M) \subseteq M(A : M) \subseteq A$, e portanto $(A : M)$ é ideal fracionário.

(b) Seja $d \in A \setminus \{0\}$ tal que $dM \subseteq A$. Então $d \in (A : M)$, mostrando que $(A : M) \neq 0$.

(c) Suponhamos $A \neq K$. Seja $c/d \in (A : K)$, com $c, d \in A$. Então $(c/d)K \subseteq A$. Se $c \neq 0$, isso significa que $K \subseteq (d/c)A$. Mas $d/c = (c/d)(d^2/c^2) \in (c/d)K \subseteq A$, e portanto temos $K \subseteq (d/c)A \subseteq A$, um absurdo! Assim, temos $c = 0$, e $c/d = 0$. Ou seja, $(A : K) = 0$. Do item (b), concluímos que K não é ideal fracionário.

□

A proposição acima nos diz, em particular, que I também é fechado para o quociente.

Proposição 3.6. *Seja $M \in \mathscr{M}$ inversível. Então M é um A-módulo finitamente gerado, $M^{-1} = (A : M)$ e ambos M e M^{-1} são ideais fracionários. Além disso, $xM^{-1} \lhd A$ para todo $x \in M$.*

Demonstração. Como $M^{-1}M = A$, temos $M^{-1} \subseteq (A : M)$. Por outro lado,

$$(A : M) = (A : M)A = (A : M)MM^{-1} \subseteq AM^{-1} = M^{-1}.$$

Dessa forma, $M^{-1} = (A : M)$. Pela Proposição 3.5 já sabemos que $(A : M)$ é ideal fracionário. Mostremos agora que M é finitamente gerado. Como $(A : M)M = 1$, nós podemos escrever $1 = y_1z_1 + \cdots + y_mz_m$, para alguns $y_1, \ldots, y_m \in (A : M)$ e $z_1, \ldots, z_m \in M$. Afirmamos que $M = Az_1 + \cdots + Az_m$. De fato, dado $x \in M$ qualquer, temos:

$$x = (xy_1)z_1 + \cdots + (xy_m)z_m \in Az_1 + \cdots + Az_m,$$

pois pela definição de $(A : M)$ temos $xy_1, \ldots, xy_m \in A$. Sendo M finitamente gerado, temos M ideal fracionário. Por fim, basta notar que, dado $x \in M$, temos $xM^{-1} \subseteq MM^{-1} = A$. □

Chamemos de $J(A)$ o conjunto dos ideais fracionários inversíveis de A. Quando A estiver claro pelo contexto, denotaremos $J(A)$ apenas por J. Pelo resultado acima, nós temos $J \subseteq I$. Notemos que J munido da multiplicação forma um grupo abeliano, e é o maior grupo contido nos monoides I e $\mathscr{M}$. Notemos ainda que $P \subseteq J$.

Para o que segue, precisaremos de alguns resultados gerais sobre ideais primos e sobre anéis noetherianos:

Proposição 3.7. *Sejam $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \lhd A$ e $\mathfrak{p} \lhd A$ primo. Suponhamos que $\mathfrak{p} \supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_r$. Então temos $\mathfrak{p} \supseteq \mathfrak{a}_j$ para algum $1 \leq j \leq r$.*

Demonstração. Provaremos a contrapositiva: se $\mathfrak{p} \not\supseteq \mathfrak{a}_j$ para $1 \leq j \leq r$, então podemos escolher $a_j \in \mathfrak{a}_j \setminus \mathfrak{p}$. Mas então $a_1 \cdots a_r \in \mathfrak{a}_1 \cdots \mathfrak{a}_r \setminus \mathfrak{p}$, já que $\mathfrak{p}$ é primo, mostrando que $\mathfrak{p} \not\supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_r$. □

Teorema 3.8. *Seja A um anel noetheriano. Então para todo ideal $\mathfrak{a} \lhd A$ existem ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \lhd A$ tais que*

$$\mathfrak{p}_1\,\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a} \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_n\,.$$

Demonstração. É claro que A e os ideais primos de A possuem essa propriedade (basta tomar $n = 0$ e $n = 1$ respectivamente). Seja Ω o conjunto dos ideais de A que não possuem a propriedade acima. Queremos mostrar que $\Omega = \emptyset$. Suponhamos por absurdo que esse não seja o caso. Como A é noetheriano, existe $\mathfrak{b} \in \Omega$ maximal. Sabemos que $\mathfrak{b}$ é um ideal próprio e não-primo de A. Assim, existem $x, y \in A \setminus \mathfrak{b}$ tais que $xy \in \mathfrak{b}$. Como $\mathfrak{b} \subsetneq \mathfrak{b} + xA$ e $\mathfrak{b} \subsetneq \mathfrak{b} + yA$, segue da maximalidade de $\mathfrak{b}$ que existem ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s \lhd A$ tais que

$$\begin{aligned} \mathfrak{p}_1\,\mathfrak{p}_2 \cdots \mathfrak{p}_r &\subseteq \mathfrak{b} + xA \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r \text{ e} \\ \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s &\subseteq \mathfrak{b} + yA \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_s. \end{aligned}$$

Desse modo:

$$\begin{aligned} \mathfrak{p}_1\,\mathfrak{p}_2 \cdots \mathfrak{p}_r\,\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s &\subseteq (\mathfrak{b} + xA)(\mathfrak{b} + yA) \subseteq \mathfrak{b} \\ &\subseteq (\mathfrak{b} + xA) \cap (\mathfrak{b} + yA) \\ &\subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r \cap \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_s, \end{aligned}$$

mostrando que $\mathfrak{b} \notin \Omega$, um absurdo! Assim, $\Omega = \emptyset$, como queríamos. □

Como consequência desse resultado, nós temos:

Corolário 3.9. *Seja A um anel noetheriano. Então todo ideal não-nulo $\mathfrak{a} \lhd A$ contém o produto de um número finito de ideais primos não-nulos.*

Demonstração. Pelo teorema anterior, existem primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \lhd A$ com

$$\mathfrak{p}_1\,\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a} \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_n\,.$$

Como $\mathfrak{a}$ é não-nulo, a segunda inclusão nos mostra que nenhum desses primos é nulo, e assim temos o resultado desejado. □

Lema 3.10. *Seja A um domínio noetheriano tal que todos os ideais primos não-nulos de A sejam maximais. Então para todo $\mathfrak{p} \in \mathscr{P}$ nós temos $A \subsetneq (A : \mathfrak{p})$.*

Demonstração. Já sabemos que $A \subseteq (A : \mathfrak{p})$. Assim, devemos achar um elemento de $(A : \mathfrak{p})$ fora de A. Para isso, tomemos $d \in \mathfrak{p} \setminus \{0\}$ qualquer. Pelo Corolário 3.9 existem $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \lhd \mathscr{P}$ tais que

$$\mathfrak{p}_1\,\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq dA \subseteq \mathfrak{p}\,.$$

Podemos supor que r é mínimo. Como $\mathfrak{p}$ contém o produto $\mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{p}$ deve conter algum dos ideais $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ por 3.7. Suponhamos sem perda de generalidade que $\mathfrak{p} \supseteq \mathfrak{p}_1$. Sendo $\mathfrak{p}_1$ maximal, temos $\mathfrak{p} = \mathfrak{p}_1$. Pela minimalidade de r, nós temos $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq dA$, de modo que existe um elemento $c \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tal que $c/d \notin A$. Por outro lado,

$$c\,\mathfrak{p} \subseteq \mathfrak{p}_1\,\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq dA \Rightarrow (c/d)\,\mathfrak{p} \subseteq A \Rightarrow c/d \in (A : \mathfrak{p}).$$

Então c/d é o elemento procurado, completando a demonstração. □

Com os resultados acima em mãos, podemos demonstrar:

Teorema 3.11. *Seja A um domínio de Dedekind. Então:*

(a) Todo $\mathfrak{p} \in \mathscr{P}$ é inversível.

(b) Todo ideal não-nulo de A é produto de ideais primos de A. Consequentemente, todo ideal não-nulo de A é inversível.

(c) Todo ideal fracionário não-nulo de A é inversível. Desse modo, I é um grupo, ou seja, $J = I$.

Demonstração. (a) Devido à Proposição 3.6, queremos mostrar que $(A : \mathfrak{p})\,\mathfrak{p} = A$. Mas temos $\mathfrak{p} \subseteq (A : \mathfrak{p})\,\mathfrak{p} \lhd A$, então sendo $\mathfrak{p}$ maximal basta mostrarmos que $\mathfrak{p} \neq (A : \mathfrak{p})\,\mathfrak{p}$. Suponhamos por absurdo que $\mathfrak{p} = (A : \mathfrak{p})\,\mathfrak{p}$, e tomemos $c \in (A : \mathfrak{p})$. Isso significa que $c\,\mathfrak{p} \subseteq \mathfrak{p}$. Desse modo, para todo inteiro positivo m nós temos:

$$c^m\,\mathfrak{p} \subseteq c^{m-1}\,\mathfrak{p} \subseteq \cdots \subseteq c\,\mathfrak{p} \subseteq \mathfrak{p} \subseteq A.$$

Logo $A[c]\,\mathfrak{p} \subseteq A$. Fixemos $d \in \mathfrak{p} \setminus \{0\}$. Então $0 \neq A[c]d \subseteq A$, mostrando que $A[c]$ é um ideal fracionário de A. Como A é noetheriano, concluímos da Proposição 3.3 que $A[c]$ é um A-módulo finitamente gerado, de onde vemos que $A[c]/A$ é uma extensão integral, pelo Teorema 1.9. Em particular, $c \in \overline{A}^K = A$. Ou seja, $(A : \mathfrak{p}) \subseteq A$, um absurdo pelo Lema 3.10.

(b) Para cada $m \in \mathbb{N}$, definamos $\mathscr{J}_m$ como sendo o conjunto dos ideais não-nulos de A que contêm um produto de m elementos de $\mathscr{P}$. Dessa forma, $\{A\} = \mathscr{J}_0 \subseteq \mathscr{J}_1 \subseteq \mathscr{J}_2 \subseteq \cdots$, e $\bigcup_{n=0}^{\infty} \mathscr{J}_n = \mathscr{J}$, onde essa última igualdade segue do Corolário 3.9. Provaremos por indução em n que todo ideal em $\mathscr{J}_n$ é produto de elementos de $\mathscr{P}$. Como a afirmação é óbvia para $n = 0$ (basta tomar o produto vazio), suponhamos que a afirmação valha para $n = r - 1$, com $r \geq 1$, e tomemos $\mathfrak{a} \in \mathscr{J}_r \setminus \{A\}$. Pela definição de $\mathscr{J}_r$, existem $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathscr{P}$ tais que $\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Tomemos $\mathfrak{m} \lhd A$ maximal com $\mathfrak{m} \supseteq \mathfrak{a}$. Então $\mathfrak{m} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, e como $\mathfrak{m}$ é primo temos por 3.7 que $\mathfrak{m} \supseteq \mathfrak{p}_i$ para algum $1 \leq i \leq r$. Sem perda de generalidade, suponhamos $\mathfrak{m} \supseteq \mathfrak{p}_1$. Como $\mathfrak{p}_1$ é maximal, temos $\mathfrak{m} = \mathfrak{p}_1$. Sendo $\mathfrak{m}$ inversível por (a), podemos multiplicar a cadeia de continências $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a} \subseteq \mathfrak{m}$ por $\mathfrak{m}^{-1}$, para concluir que

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{m}^{-1}\mathfrak{a} \subseteq \mathfrak{m}^{-1}\mathfrak{m} = A.$$

Então $\mathfrak{m}^{-1}\mathfrak{a} \in \mathscr{J}_{r-1}$, e por hipótese existem $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \in \mathscr{P}$ tais que $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Multiplicando por $\mathfrak{m}$, chegamos em $\mathfrak{a} = \mathfrak{m}\mathfrak{q}_1 \cdots \mathfrak{q}_s$, provando que $\mathfrak{a}$ é produto de elementos de $\mathscr{P}$. Notemos ainda que, como todo ideal primo não-nulo de A é inversível, $\mathfrak{a}$ também o é, com $\mathfrak{a}^{-1} = \mathfrak{m}^{-1}\mathfrak{q}_1^{-1} \cdots \mathfrak{q}_s^{-1}$. Assim, por indução, provamos que todo ideal não-nulo de A é produto de ideais primos não-nulos de A, e também é inversível.

(c) Se $M \in I$, existe $d \in A \setminus \{0\}$ tal que $\mathfrak{a} := dM \lhd A$. Então $M = d^{-1}\mathfrak{a}$. Por (b), $\mathfrak{a}$ é inversível, logo M também o é, com inversa $M^{-1} = d\mathfrak{a}^{-1}$.

□

O item (b) do teorema acima afirma que todo ideal não-nulo $\mathfrak{a} \lhd A$ admite uma fatoração em ideais primos não-nulos de A. Juntando os primos que aparecem mais de uma vez nessa fatoração, encontramos a fatoração de $\mathfrak{a}$ como $\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$, onde $k_1, \ldots, k_r$ são inteiros positivos e $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathscr{P}$ são distintos dois a dois. Entretanto, o maquinário poderoso que ganhamos ao trabalhar com domínios de Dedekind não se baseia apenas na existência dessa fatoração, mas sim na sua unicidade:

Teorema 3.12 (Fatoração Única de Ideais em Domínios de Dedekind)**.** *Seja A um domínio de Dedekind. Então I é um grupo, e:*

(a) Todo ideal $\mathfrak{a} \in \mathscr{J}$ se escreve de modo único (a menos de ordem) na forma

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{k_i}, \text{ com } \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathscr{P} \text{ distintos dois a dois, e } k_1, \ldots, k_n \in \mathbb{N}^*.$$

(b) Todo ideal fracionário $M \in I$ se escreve de modo único (a menos de ordem) na forma

$$M = \prod_{i=1}^{n} \mathfrak{p}_i^{k_i}, \text{ com } \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathscr{P} \text{ distintos dois a dois, e } k_1, \ldots, k_n \in \mathbb{Z} \setminus \{0\}.$$

Demonstração. Notemos que (a) segue do teorema anterior e de (b). Assim, basta provar (b). Seja portanto $M \in I$, e tomemos $d \in A \setminus \{0\}$ tal que $dM \lhd A$. Desse modo, $M = d^{-1}(dM) = (dA)^{-1} \cdot dM$. Pelo Teorema 3.11, existem $\mathfrak{q}_1, \ldots, \mathfrak{q}_m, \mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n \in \mathscr{P}$ tais que $dA = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ e $dM = \mathfrak{q}_{m+1} \cdots \mathfrak{q}_n$. Assim, nós temos

$$M = (dA)^{-1} \cdot dM = \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_m^{-1}\, \mathfrak{q}_{m+1} \cdots \mathfrak{q}_n,$$

o que nos mostra a existência da fatoração de um ideal fracionário (basta juntar/cortar os primos que aparecem mais de uma vez). Assim, resta demonstrar a unicidade da fatoração. Para isso, suponhamos que tenhamos duas fatorações para M:

$$M = \prod_{j=1}^{k} \mathfrak{p}_j^{m_j} = \prod_{j=1}^{k} \mathfrak{p}_j^{n_j},$$

com $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ primos distintos e $m_1, \ldots, m_k, n_1, \ldots, n_k \in \mathbb{Z}$ (aqui, permitimos que os expoentes sejam nulos, para que tenhamos o mesmo conjunto de primos de ambos os lados). Queremos mostrar que $(m_1, \ldots, m_k) = (n_1, \ldots, n_k)$. Para isso, notemos que a igualdade acima implica que vale

$$\prod_{\substack{1 \le j \le k \\ m_j > n_j}} \mathfrak{p}_j^{m_j - n_j} = \prod_{\substack{1 \le j \le k \\ m_j < n_j}} \mathfrak{p}_j^{n_j - m_j}.$$

Notemos que nos dois produtórios acima todos os primos aparecem com expoentes positivos. Suponhamos por absurdo que $(m_1, \ldots, m_k) \neq (n_1, \ldots, n_k)$. Então pelo menos um dos produtórios acima é não-vazio, e portanto ambos os produtórios acima o são, já que senão teríamos uma igualdade entre A e um ideal próprio de A. Sem perda de generalidade, consideremos $m_1 > n_1$. Assim, $\mathfrak{p}_1$ aparece no lado esquerdo da igualdade acima. Isso implica que o produtório do lado direito está contido em $\mathfrak{p}_1$, e por 3.7 algum primo $\mathfrak{p}_i$ que aparece com expoente positivo no produtório da direita está contido em $\mathfrak{p}_1$. Temos $i \neq 1$, pois um mesmo primo não pode aparecer nos dois produtórios acima. Assim, $\mathfrak{p}_1 \neq \mathfrak{p}_i$. Mas $\mathfrak{p}_i$ é maximal, logo $\mathfrak{p}_1 = \mathfrak{p}_i$, absurdo! Isso termina a demonstração do teorema. □

Observação 3.13. *Nós utilizaremos também a notação $M = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$ para indicar a fatoração de M em ideais primos de A. Nessa notação, subentende-se que $\mathfrak{p}$ varia entre os ideais primos não-nulos de A e que cada $\nu_{\mathfrak{p}} \in \mathbb{Z}$. Note que esse será na verdade um produto finito, ou seja, temos $\nu_{\mathfrak{p}} \neq 0$ apenas para um número finito de ideais primos não-nulos $\mathfrak{p} \lhd A$.*

O que esse resultado nos diz na prática é que os ideais fracionários de um domínio de Dedekind têm um comportamento multiplicativo muito parecido com o do corpo de frações de um DFU: temos multiplicação, inverso e fatoração única. Na verdade, podemos pensar no grupo dos ideais fracionários de um domínio de Dedekind A como uma extensão da estrutura multiplicativa de A, com um elemento $x \in A$ identificado com o ideal principal xA. Notemos que o elemento neutro A corresponde ao elemento neutro 1. Essa "extensão" não é bem uma extensão, dado que elementos associados geram o mesmo ideal. Porém, isso na verdade é bom, pois elementos associados de A são essencialmente "a mesma coisa", e dessa forma conseguimos um teorema de fatoração única mais limpo (num DFU, os primos são únicos a menos de associados).

Essa semelhança de ideais fracionários com DFU's nos sugere que possamos definir divisibilidade nesse conjunto:

Definição (Divisibilidade em I)**.** Sejam $M, N \in I$. Então dizemos que M **divide** N, ou ainda que N é um **múltiplo** de M, se $N = \mathfrak{a}M$ para algum $\mathfrak{a} \in \mathscr{J}$. Denotamos $M \mid N$.

A divisibilidade, como esperado, se comporta bem, e nos dá uma relação mais estreita ainda entre ideais fracionários e DFU's:

Corolário 3.14. *Seja A um domínio de Dedekind, e sejam $M = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}, N = \mathfrak{p}_1^{\ell_1} \cdots \mathfrak{p}_r^{\ell_r}$, onde nós temos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathscr{P}, k_1, \ldots, k_r, \ell_1, \ldots, \ell_r \in \mathbb{Z}$. Então:*

(a) $MN = \mathfrak{p}_1^{k_1+\ell_1} \cdots \mathfrak{p}_r^{k_r+\ell_r}$.

(b) $M \supseteq N \iff M \mid N \iff k_1 \leq \ell_1, \ldots, k_r \leq \ell_r$.

(c) $\mathrm{mdc}(M, N) \coloneqq M + N = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$, *onde para* $1 \leq j \leq r$ *temos* $m_j = \min\{k_j, \ell_j\}$.

(d) $\mathrm{mmc}(M, N) \coloneqq M \cap N = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$, *onde para* $1 \leq j \leq r$ *temos* $n_j = \max\{k_j, \ell_j\}$.

(e) Seja $P \in I$ qualquer. Então valem as igualdades:

(i) $(M \cap N)(M + N) = MN$, *ou seja,* $\mathrm{mdc}(M, N)\,\mathrm{mmc}(M, N) = MN$.

(ii) $M(N + P) = MN + MP$, *ou seja,* $M \cdot \mathrm{mdc}(N, P) = \mathrm{mdc}(MN, MP)$.

(iii) $M(N \cap P) = MN \cap MP$, *ou seja,* $M \cdot \mathrm{mmc}(N, P) = \mathrm{mmc}(MN, MP)$.

(iv) $M \cap (N + P) = (M \cap N) + (M \cap P)$, *ou seja,*
$mmc(M, mdc(N, P)) = mdc(mmc(M, N), mmc(M, P))$.

(v) $M + (N \cap P) = (M + N) \cap (M + P)$, *ou seja,*
$mdc(M, mmc(N, P)) = mmc(mdc(M, N), mdc(M, P))$.

Demonstração. (a) É óbvio.

(b) É claro que valem as implicações $k_1 \leq \ell_1, \ldots, k_r \leq \ell_r \Rightarrow M \mid N \Rightarrow M \supseteq N$. Notemos agora que $M \supseteq N \Rightarrow A \supseteq NM^{-1}$. Assim, $NM^{-1} \lhd A$, e temos $N = (NM^{-1})M \Rightarrow M \mid N$. Suponhamos por fim que valha $M \mid N$. Então existe $\mathfrak{a} \lhd A$ com $N = \mathfrak{a}M$. A implicação restante segue do fato de que todos os expoentes da fatoração prima de $\mathfrak{a}$ são não-negativos e do item (a).

(c) Devido à fatoração única e ao item (b), $\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$ é o menor ideal fracionário que contém ambos M e N. Mas $M + N$ também possui essa propriedade, de onde tiramos a igualdade desejada.

(d) Devido à fatoração única e ao item (b), $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ é o maior ideal fracionário contido em ambos M e N. Mas $M \cap N$ também possui essa propriedade, de onde tiramos a igualdade desejada.

(e) (i) Segue dos itens anteriores e da igualdade $\min(m, n) + \max(m, n) = m + n$.

(ii) Segue dos itens anteriores e da igualdade $m \cdot \max(n, p) = \max(mn, mp)$. Notemos no entanto que essa igualdade de ideais fracionários vale para todo domínio A, e assim pode ser concluída diretamente.

(iii) Segue dos itens anteriores e da igualdade $m \cdot \min(n, p) = \min(mn, mp)$.

(iv) Segue dos itens anteriores e da igualdade $\min(m, \max(n, p)) = \max(\min(m, n), \min(m, p))$.

(v) Segue dos itens anteriores e da igualdade $\max(m, \min(n, p)) = \min(\max(m, n), \max(m, p))$.

□

Como consequência do item (b) desse corolário, nós obtemos:

Corolário 3.15. *Seja A um domínio de Dedekind. Então:*

(a) Para todo $\mathfrak{a} \in \mathscr{J}$, o conjunto dos ideais de A que contêm $\mathfrak{a}$ é finito.

(b) Para todo $\mathfrak{a} \in \mathscr{J}$, os ideais $\mathfrak{ap}$, onde $\mathfrak{p}$ percorre $\mathscr{P}$, são os elementos maximais do conjunto dos ideais de A que estão estritamente contidos em $\mathfrak{a}$.

(c) Sejam $\mathfrak{a} \in \mathscr{J}$ e $\mathfrak{p} \in \mathscr{P}$. Então $\mathfrak{a}/(\mathfrak{pa})$ é um $A/\mathfrak{p}$-espaço vetorial de dimensão 1.

Demonstração. Os itens (a) e (b) seguem imediatamente do resultado acima. Provemos (c). O anel $\mathfrak{a}/(\mathfrak{pa})$ é um $A/\mathfrak{p}$ espaço vetorial, pois é claro que $\mathfrak{p}$ anula esse A-módulo. Do item (b), vemos que $\mathfrak{a}/(\mathfrak{pa}) \neq 0$ é simples como A-módulo, e portanto também é simples como $A/\mathfrak{p}$-espaço. □

Ainda temos o seguinte teorema, que nos diz que os DIP's são exatamente os DFU's que são domínios de Dedekind:

Teorema 3.16. *Seja A um domínio. Então as seguintes condições são equivalentes:*

(i) A é um DIP.

(ii) A é um DFU e um domínio de Dedekind.

Demonstração. $(i) \Rightarrow (ii)$: Seja A um DIP. Então é claro que A também é um DFU, e em particular é integralmente fechado pelo Teorema 1.14. Além disso, como todo ideal de A é principal é claro que A é noetheriano e todo ideal primo não-nulo de A é maximal.

$(ii) \Rightarrow (i)$: Suponhamos que A seja um DFU e um domínio de Dedekind. Como todo ideal de A é produto de primos, basta mostrar que todo $\mathfrak{p} \in \mathscr{P}$ é principal. Para ver isso, seja $a \in \mathfrak{p} \setminus \{0\}$ qualquer. Sendo A um DFU, podemos escrever $a = z_1 \cdots z_r$ onde $z_1, \ldots, z_r \in A$ são irredutíveis. Sendo $\mathfrak{p}$ primo, existe $1 \leq j \leq r$ com $z_j \in \mathfrak{p}$, e portanto $z_j A \subseteq \mathfrak{p}$. Mas como A é um DFU, o ideal $z_j A$ é primo, e portanto maximal. Assim, $z_j A \subseteq \mathfrak{p} \Rightarrow z_j A = \mathfrak{p}$, mostrando que $\mathfrak{p}$ é principal, como desejado. □

Esse teorema nos permite afirmar, como havíamos comentado, que DIP's e DFU's são a mesma coisa quando tratamos de um anel de inteiros algébricos:

Teorema 3.17. *Seja K um corpo de números algébricos. Então $\mathcal{O}_K$ será um DIP se e só se for um DFU.*

Pelo que vimos, num domínio de Dedekind A o monoide $I(A)$ é um grupo. Note que utilizamos todas as hipóteses que caracterizam um domínio de Dedekind na demonstração do Teorema 3.11. Assim, pode-se perguntar se o fato de $I(A)$ ser um grupo implica em A ser um domínio de Dedekind. Isso de fato ocorre:

Teorema 3.18. *Seja A um domínio. Então as seguintes condições são equivalentes:*

(i) A é um domínio de Dedekind.

(ii) I é um grupo.

Demonstração. Já provamos que $(i) \Rightarrow (ii)$. Provemos que $(ii) \Rightarrow (i)$. Devemos verificar que A é noetheriano, integralmente fechado e que todo elemento de $\mathscr{P}$ é maximal:

- Seja $\mathfrak{a} \lhd A$. Se $\mathfrak{a} = 0$, é óbvio que $\mathfrak{a}$ é finitamente gerado. Suponhamos $\mathfrak{a} \neq 0$. Então $\mathfrak{a}$ é inversível, e portanto finitamente gerado pela Proposição 3.6. Assim, todo ideal de A é finitamente gerado, mostrando que A é noetheriano.

- Seja $c \in \overline{A}^K$. Então $A[c]$ é finitamente gerado, e portanto é um ideal fracionário de A. É fácil ver que $A[c]A[c] = A[c]$, e sendo $A[c]$ inversível concluímos que $A[c] = A$. Ou seja, $c \in A$.

- Seja $\mathfrak{p} \in \mathscr{P}$, e tomemos $\mathfrak{a} \lhd A$ tal que $\mathfrak{p} \subsetneq \mathfrak{a}$. Queremos mostrar que $\mathfrak{a} = A$. Fixemos $a \in \mathfrak{a} \setminus \mathfrak{p}$. Se $r \in \mathfrak{a}^{-1}\mathfrak{p}$, então $ar \in \mathfrak{a}\mathfrak{a}^{-1}\mathfrak{p} = \mathfrak{p}$. Como $\mathfrak{p}$ é primo, concluímos que $r \in \mathfrak{p}$. Ou seja, $\mathfrak{a}^{-1}\mathfrak{p} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a}^{-1} \subseteq A$. Mas $A \subseteq \mathfrak{a}^{-1}$, logo $A = \mathfrak{a}^{-1} \Rightarrow \mathfrak{a} = A$, como queríamos. Assim, $\mathfrak{p}$ é maximal.

Então A é domínio de Dedekind, como desejávamos. □

3.2. Propriedades dos Domínios de Dedekind

Pelo Teorema 3.12, se A for um domínio de Dedekind então o grupo dos ideais fracionários principais $P = P(A)$ é um subgrupo do grupo $I = I(A)$. Assim, podemos considerar o grupo quociente $\mathscr{C}\ell(A) := I/P$, que é chamado de **grupo de classes de ideais** de A. Quando A estiver claro, denotaremos esse grupo simplesmente por $\mathscr{C}\ell$. Além disso, denotaremos a classe de um elemento $M \in I$ por MP ou por $[M]$. O nome "grupo de classes de ideais" é devido ao seguinte resultado:

Proposição 3.19. *Dados $M, N \in I$, temos $MP = NP$ se e só se existirem $c, d \in A \setminus \{0\}$ tais que $cM = dN$. Além disso, a função $\pi\colon \mathscr{J} \to \mathscr{C}\ell$ dada por $\mathfrak{a} \mapsto \mathfrak{a}P$ é sobrejetora. Ou seja, toda classe de $\mathscr{C}\ell$ é a classe de algum ideal de A.*

Demonstração. Dados dois ideais fracionários $M, N \in I$, temos $MP = NP \iff M^{-1}N \in P$. Isso, por sua vez, acontecerá se e só se existir um $x \in K \setminus \{0\}$ tal que $M^{-1}N = xA$. Escrevendo $x = c/d$, com $c, d \in A \setminus \{0\}$, obtemos $M^{-1}N = (c/d)A \iff cM = dN$. Seja agora $MP \in \mathscr{C}\ell$ qualquer, com $M \in I$. Então existe $r \in A \setminus \{0\}$ tal que $rM \in \mathscr{J}$. Mas $r \cdot M = 1 \cdot (rM)$, logo pelo que provamos acima temos $MP = (rM)P = \pi(rM) \in \operatorname{im}\pi$, mostrando que π é sobrejetora. □

Definição (Número de Classes)**.** O número cardinal $|\mathscr{C}\ell|$ é chamado de o **número de classes** de A, e será denotado por h_A. Se $A = \mathcal{O}_K$ for o anel de inteiros algébricos de um corpo de números K, denotamos $h_{\mathcal{O}_K}$ simplesmente por h_K, e também o chamamos de **número de classes** de K.

Temos imediatamente o seguinte corolário:

Corolário 3.20. *Um domínio de Dedekind A será um DIP se e só se o grupo $\mathscr{C}\ell$ for trivial, ou seja, se e só se $h_A = 1$.*

No próximo capítulo, nós demostraremos o **Teorema da Finitude do Número de Classes**, que afirma que para todo corpo de números K o número h_K é finito.

Pelo que vimos, dado um domínio A teremos $J(A) = I(A)$ se e só se A for um domínio de Dedekind. Entretanto, mesmo se A não for um domínio de Dedekind, os conjuntos $J(A)$ e $P(A) \subseteq J(A)$ são grupos abelianos, e portanto podemos considerar o quociente $J(A)/P(A)$:

Definição (Grupo de Picard)**.** Dado um domínio A qualquer, definimos seu **grupo de Picard** $\operatorname{Pic}(A)$ como sendo o grupo abeliano dado pelo quociente $\operatorname{Pic}(A) := J(A)/P(A)$.

Denotaremos $\operatorname{Pic}(A)$ apenas por Pic se A estiver claro. É claro que se A for um domínio de Dedekind o grupo de Picard $\operatorname{Pic}(A)$ coincidirá com o grupo de classes $\mathscr{C}\ell(A)$.

Como já vimos, todo ideal fracionário de um domínio noetheriano é finitamente gerado. No caso de domínios de Dedekind, podemos melhorar isso, para garantir que todo ideal fracionário é gerado como A-módulo por dois elementos, podendo um deles ser previamente fixado. Comecemos com o seguinte teorema:

Teorema 3.21. *Seja A um domínio de Dedekind. Então para todos $M \in I$ e $\mathfrak{b} \in \mathscr{J}$ existe $x \in M$ tal que os ideais xM^{-1} e $\mathfrak{b}$ são coprimos.*

Demonstração. Seja $\mathfrak{b} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$ a fatoração prima de $\mathfrak{b}$. Se $r = 0$, $\mathfrak{b} = A$ e a afirmação é óbvia. Suponhamos então $r \geq 1$. Como $\mathfrak{b} \lhd A$, temos $k_1, \ldots, k_r > 0$. Queremos escolher x de modo que xM^{-1} e $\mathfrak{b}$ sejam coprimos. Pelo Corolário 3.14, isso significa que os primos que aparecem na fatoração de xM^{-1} e de $\mathfrak{b}$ devem ser todos distintos. Ou seja, queremos achar $x \in M$ de modo que $xM^{-1} \not\subseteq \mathfrak{p}_j$ para todo $1 \leq j \leq r$.

Definamos, para $1 \leq j \leq r$, $M_j := \mathfrak{p}_1 \cdots \mathfrak{p}_{j-1}\mathfrak{p}_{j+1} \cdots \mathfrak{p}_r M$. Notemos que $\mathfrak{p}_j M_j \subsetneq M_j$. Assim, podemos escolher $x_j \in M_j \setminus \mathfrak{p}_j M_j$. É claro que $x_j \in \mathfrak{p}_i M$ para $i \neq j$. Por outro lado, $x_j \notin \mathfrak{p}_j M$. De fato, se tivéssemos $x_j \in \mathfrak{p}_j M$, então teríamos $x_j M^{-1} \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, onde a última igualdade segue do fato dos ideais $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ serem coprimos. Assim, poderíamos concluir que $x_j \in \mathfrak{p}_1 \cdots \mathfrak{p}_r M = \mathfrak{p}_j M_j$, um absurdo!

Definamos $x := x_1 + x_2 + \cdots + x_r \in M$. Afirmamos que x satisfaz a condição desejada. Suponhamos por absurdo que $xM^{-1} \subseteq \mathfrak{p}_j$ para algum $1 \leq j \leq r$, e sem perda de generalidade tomemos $j = r$. Então $x \in \mathfrak{p}_r M$, e portanto $x_r = x - x_1 - \cdots - x_{r-1} \in \mathfrak{p}_r M$, um absurdo, concluindo a demonstração. □

Finalmente, podemos aplicar esse teorema para mostrar o que queríamos:

Corolário 3.22. *Sejam A um domínio de Dedekind, $M \in I$ e $y \in M \setminus \{0\}$. Então existe $x \in M$ tal que $M = xA + yA$.*

Demonstração. Temos $yM^{-1} \lhd A$. Assim, pelo teorema acima, existe um elemento $x \in M$ tal que $xM^{-1} + yM^{-1} = A$. Mas isso equivale a termos $xA + yA = M$. □

Outro resultado importante é que todo domínio de Dedekind com um número finito de ideais primos é um DIP:

Teorema 3.23. *Seja A um domínio de Dedekind com um número finito de ideais primos. Então A é um DIP.*

Demonstração. Como todo ideal de A é produto de ideais primos, basta mostrar que todo ideal primo de A é principal. Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ os ideais primos de A. Provaremos que $\mathfrak{p}_1$ é principal. O resto segue analogamente. Sabemos que $\mathfrak{p}_1^2 \subsetneq \mathfrak{p}_1$. Assim, podemos tomar $r_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$. Os ideais $\mathfrak{p}_1^2, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ são coprimos dois a dois, e portanto podemos aplicar o Teorema Chinês dos Restos para encontrar $r \in A$ tal que $r \equiv r_1 \pmod{\mathfrak{p}_1^2}$ e $r \equiv 1 \pmod{\mathfrak{p}_j}$ para $2 \leq j \leq n$. Desse modo, r é tal que $r \notin \mathfrak{p}_1^2$ e $r \notin \mathfrak{p}_j$ para $2 \leq j \leq n$, e portanto na fatoração prima de rA o primo $\mathfrak{p}_1$ aparece com expoente no máximo 1, e os primos $\mathfrak{p}_2, \ldots, \mathfrak{p}_n$ não aparecem. Disso concluímos que $rA \supseteq \mathfrak{p}_1$. Como a outra inclusão segue diretamente de $r \in \mathfrak{p}_1$, concluímos que $\mathfrak{p}_1 = rA$ é principal, como desejado. □

Terminaremos a seção vendo como domínios de Dedekind se comportam com localizações:

Proposição 3.24. *Sejam A um domínio de Dedekind e S um conjunto multiplicativo de A. Então $S^{-1}A$ é um domínio de Dedekind. Além disso, o mapa $I(A) \to I(S^{-1}A)$ dado por $M \mapsto S^{-1}M$ é um homomorfismo sobrejetor de grupos abelianos, e seu núcleo consiste dos ideais fracionários $M \in I(A)$ tais que $M \cap S \neq \emptyset$ e $M^{-1} \cap S \neq \emptyset$. Esse mapa induz um homomorfismo sobrejetor $\mathscr{C}\ell(A) \to \mathscr{C}\ell(S^{-1}A)$ dado por $[M] \mapsto [S^{-1}M]$.*

Demonstração. Sendo a localização de um domínio noetheriano, $S^{-1}A$ também é um domínio noetheriano. Como A é integralmente fechado, segue da Proposição 1.15 que $S^{-1}A$ também é integralmente fechado. Finalmente, um ideal primo de $S^{-1}A$ é da forma $S^{-1}\mathfrak{p}$ para algum $\mathfrak{p} \lhd A$ primo que não intersecta S. Como $\mathfrak{p}$ é maximal em A, pela correspondência da localização vemos que $S^{-1}\mathfrak{p}$ é maximal em $S^{-1}A$. Isso mostra que $S^{-1}A$ é domínio de Dedekind.

O fato da função indicada ser um homomorfismo de grupos equivale a termos, para todos $M, N \in I$, a igualdade $S^{-1}(MN) = (S^{-1}M)(S^{-1}N)$, que se verifica diretamente. Para mostrar que esse homomorfismo é sobrejetor, seja $N \in I(S^{-1}A)$ qualquer. Então existe $x \in S^{-1}A \setminus \{0\}$ tal que $xN \lhd S^{-1}A$. Dessa forma, existe $\mathfrak{a} \lhd A$ tal que $xN = S^{-1}\mathfrak{a}$. Portanto, nós vemos que $N = x^{-1}S^{-1}\mathfrak{a} = S^{-1}(x^{-1}\mathfrak{a})$ está na imagem do homomorfismo acima, já que $x^{-1}\mathfrak{a} \in I(A)$.

Falta mostrar que o núcleo desse homomorfismo é o conjunto dos ideais fracionários M de A tais que $M \cap S \neq \emptyset$ e $M^{-1} \cap S \neq \emptyset$. Suponhamos primeiramente que $M \cap S \neq \emptyset$ e que $M^{-1} \cap S \neq \emptyset$. Tomemos $s \in M \cap S$ e $x \in M^{-1} \cap S$. Sendo $r/t \in S^{-1}A$ qualquer, temos $r/t = (rs)/(ts) \in S^{-1}M$. Assim, $S^{-1}A \subseteq S^{-1}M$. Sendo agora $m/s \in S^{-1}M$ qualquer, temos $m/s = (mx)/(sx) \in S^{-1}A$, mostrando que $S^{-1}M \subseteq S^{-1}A$. Assim, $S^{-1}A = S^{-1}M$, e M está no núcleo desse homomorfismo.

Reciprocamente, suponhamos que M está nesse núcleo, ou seja, que $S^{-1}M = S^{-1}A$. Então $1 \in S^{-1}M$, e podemos escrever $1 = m/s$ para $m \in M$ e $s \in S$. Mas isso significa que $m = s$, e esse é um elemento de $M \cap S$. Além disso, notemos que a condição $S^{-1}M \subseteq S^{-1}A$. é equivalente a $S^{-1}A \subseteq S^{-1}M^{-1}$, e da mesma forma concluímos que $M^{-1} \cap S \neq \emptyset$, como queríamos.

Para ver que esse homomorfismo induz um homomorfismo $\mathscr{C}\ell(A) \to \mathscr{C}\ell(S^{-1}A)$ dado por $[M] \mapsto [S^{-1}M]$, mostremos que se $[M_1] = [M_2]$ então $[S^{-1}M_1] = [S^{-1}M_2]$. Como $[M_1] = [M_2]$, existe $x \in Q(A)$ tal que $xM_1 = M_2$. Localizando, vemos que $x(S^{-1}M_1) = S^{-1}M_2$, o que mostra que $[S^{-1}M_1] = [S^{-1}M_2]$. Assim, essa função está bem-definida, e o fato dela ser um homomorfismo sobrejetor segue do mapa $I(A) \to I(S^{-1}A)$ o ser. □

O seguinte resultado generaliza o Teorema 1.48 e o Corolário 1.49 para potências de primos:

Teorema 3.25. *Sejam A um domínio de Dedekind, S um conjunto multiplicativo de A e $\mathfrak{p} \lhd A$ um ideal primo não-nulo que não intersecta S. Então:*

(a) Para todo n inteiro positivo temos $S^{-1}\mathfrak{p}^n \cap A = \mathfrak{p}^n$.

(b) Para todo n inteiro positivo o homomorfismo canônico $A/\mathfrak{p}^n \to S^{-1}A/S^{-1}\mathfrak{p}^n$ dado por $x + \mathfrak{p}^n \mapsto x + S^{-1}\mathfrak{p}^n$ é um isomorfismo, e portanto nós temos $A/\mathfrak{p}^n \cong S^{-1}A/S^{-1}\mathfrak{p}^n$.

Demonstração. (a) É claro que $\mathfrak{p}^n \subseteq S^{-1}\mathfrak{p}^n \cap A$. Para a inclusão contrária, seja $a \in S^{-1}\mathfrak{p}^n \cap A$. Então $a = x/s$, para alguns elementos $x \in \mathfrak{p}^n$ e $s \in S$, e nós temos $sa = x \in \mathfrak{p}^n$. Assim, $\mathfrak{p}^n \mid (sa)A = (sA)(aA)$. Como $s \notin \mathfrak{p}$, temos $\mathfrak{p} \nmid sA$, e portanto $\mathfrak{p}^n \mid aA \Rightarrow a \in \mathfrak{p}^n$, o que prova que $S^{-1}\mathfrak{p}^n \cap A \subseteq \mathfrak{p}^n$, como queríamos.

(b) Comecemos observando que, para todo $s \in A \setminus \mathfrak{p}$, nós temos $sA + \mathfrak{p} = A$ pela maximalidade de $\mathfrak{p}$. Sendo sA coprimo com $\mathfrak{p}$, é fácil ver que sA também é coprimo com $\mathfrak{p}^n$, e portanto $sA + \mathfrak{p}^n = A$. Mostremos que o homomorfismo canônico definido acima é de fato um isomorfismo:

- Essa função está bem-definida: Sejam $x, y \in A$ tais que $x + \mathfrak{p}^n = y + \mathfrak{p}^n$. Então $x - y \in \mathfrak{p}^n \subseteq S^{-1}\mathfrak{p}^n$, e portanto $x + S^{-1}\mathfrak{p}^n = y + S^{-1}\mathfrak{p}^n$.
- Essa função é um homomorfismo: É claro.
- Essa função é injetora: Seja $x \in A$ tal que $x \in S^{-1}\mathfrak{p}^n$. Então, pelo item (a), temos $x \in \mathfrak{p}^n$, o que mostra a injetividade desse homomorfismo.
- Essa função é sobrejetora: Seja $y \in S^{-1}A$ qualquer. Então temos $y = a/s$, para alguns $a \in A$, $s \in S$. Como $A = sA + \mathfrak{p}^n$, existem $p \in \mathfrak{p}^n$ e $x \in A$ tais que $a = sx + p$, de modo que $y = a/s = x + p/s \Rightarrow y + S^{-1}\mathfrak{p}^n = x + S^{-1}\mathfrak{p}^n$, mostrando que esse homomorfismo é de fato sobrejetor.

□

3.3. Domínios de Valoração Discreta

Os domínios de valoração discreta são, em certo sentido, os domínios mais simples depois dos corpos:

Definição (Domínio de Valoração Discreta)**.** Um domínio A é chamado de **domínio de valoração discreta** (abreviamos DVD) se for um DIP local, e se seu único ideal maximal for não-nulo.

Sendo A um DVD com único ideal maximal $\mathfrak{p} \neq 0$, podemos escolher um gerador π do ideal principal $\mathfrak{p}$. Como os ideais maximais em um DIP são exatamente aqueles que são gerados por um elemento irredutível, vemos que π é o único elemento irredutível de A a menos de associados. Nós chamamos π (ou qualquer um de seus associados) de **normalizador** de A. Desse modo, todo elemento não-nulo de A se escreve de modo único como $u\pi^n$, onde $u \in A^\times = A \setminus \mathfrak{p}$ e $n \in \mathbb{N}$. A partir disso, é fácil ver que de fato todo elemento não-nulo de $K := Q(A)$ se escreve de modo único como $u\pi^n$, onde $u \in A^\times$ e $n \in \mathbb{Z}$. Assim, dado $x \in K \setminus \{0\}$, existe um único $n \in \mathbb{Z}$ para o qual $xA = \mathfrak{p}^n$. A partir disso, podemos definir uma função sobrejetora $v\colon K \to \mathbb{Z} \cup \{\infty\}$, que chamamos de **valoração** de A, dada por:

$$v(x) = \begin{cases} n, \text{se } x \neq 0 \text{ e } xA = \mathfrak{p}^n; \\ \infty, \text{ se } x = 0. \end{cases}$$

Podemos ainda denotar essa valoração por v_A, para especificar o domínio de valoração discreta com o qual começamos. Estendamos a soma de $\mathbb{Z}$ e a ordem de $\mathbb{Z}$ para o conjunto $\mathbb{Z} \cup \{\infty\}$ definindo, para todo $n \in \mathbb{Z}$, $n + \infty = \infty + n = \infty$ e $\infty > n$.

Dado $x \in K$ qualquer, chamaremos $v(x)$ de **valoração** de x. Dados $x, y \in K$ quaisquer, escrevamos $x = u_1\pi^{v(x)}$ e $y = u_2\pi^{v(y)}$, com $u_1, u_2 \in A^\times$. Então nós temos $xy = u_1u_2\pi^{v(x)+v(y)}$, o que nos dá a relação $v(xy) = v(x) + v(y)$. Suponhamos agora que $v(x) \leq v(y)$, sem perda de generalidade. Então $x + y = u_1\pi^{v(x)} + u_2\pi^{v(y)} = (u_1 + u_2\pi^{v(y)-v(x)})\pi^{v(x)}$. Como $u_1 + u_2\pi^{v(y)-v(x)} \in A$, nós concluímos que $v(x + y) \geq v(x)$. Isso nos dá a relação $v(x + y) \geq \min\{v(x), v(y)\}$.

Nós definimos, de forma geral, uma **valoração (exponencial) discreta** como uma função que tenha propriedades como as acima:

Definição (Valoração (Exponencial) Discreta)**.** Seja K um corpo. Uma **valoração (exponencial) discreta** de K é uma função sobrejetora $v\colon K \to \mathbb{Z} \cup \{\infty\}$ que verifica:

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$ (assim, $v\colon K^\times \to \mathbb{Z}$ é um morfismo de grupos);

(iii) (Propriedade não-arquimediana) $v(x + y) \geq \min\{v(x), v(y)\}$.

Toda valoração discreta tem as seguintes propriedades básicas, que decorrem diretamente da definição acima:

Lema 3.26. *Seja $v\colon K \to \mathbb{Z} \cup \{\infty\}$ uma valoração discreta. Então:*

(a) $v(\pm 1) = 0$, *e* $v(-x) = v(x)$ *para todo* $x \in K$.

(b) $v(x/y) = v(x) - v(y)$, *para todos* $x, y \in K$ *com* $y \neq 0$. *Em particular,* $v(y^{-1}) = -v(y)$.

(c) $v(x) \neq v(y) \Rightarrow v(x + y) = \min\{v(x), v(y)\}$.

(d) $v(x_1 + \cdots + x_n) = \min\{v(x_1), \ldots, v(x_n)\}$, *se* $v(x_i) \neq v(x_j)$ *para todos* $1 \leq i < j \leq n$.

(e) Se $x_1 + \cdots + x_n = 0$ *com* $n \geq 2$, *então existem* $1 \leq i < j \leq n$ *com* $v(x_i) = v(x_j)$.

Demonstração. (a) Como $v(1) = v(1 \cdot 1) = v(1) + v(1)$, temos $v(1) = 0$. Além disso, temos $0 = v(1) = v((-1) \cdot (-1)) = v(-1) + v(-1) = 2v(-1)$, e portanto $v(-1) = 0$. Finalmente, dado $x \in K$ qualquer, temos $v(-x) = v(x \cdot (-1)) = v(x) + v(-1) = v(x)$.

(b) Temos $v(x) = v(y \cdot (x/y)) = v(y) + v(x/y)$, de onde concluímos que $v(x/y) = v(x) - v(y)$. Note que podemos subtrair $v(y)$, pois $y \neq 0 \Rightarrow v(y) \in \mathbb{Z}$.

(c) Suponhamos sem perda de generalidade que $v(x) < v(y)$. Então queremos mostrar que $v(x+y) = v(x)$. Nós sabemos que $v(x+y) \geq v(x)$. Assim, é suficiente mostrarmos que $v(x+y) \leq v(x)$. Notemos que $v(x) \geq \min\{v(x+y), v(-y)\} = \min\{v(x+y), v(y)\}$. Como $v(x) < v(y)$, concluímos que devemos ter $v(x) \geq v(x+y)$, e assim $v(x+y) = v(x)$.

(d) Segue facilmente por indução a partir do item anterior.

(e) Suponhamos sem perda de generalidade que $v(x_1) \leq v(x_2) \leq \cdots \leq v(x_n)$. Se todas essas desigualdades fossem estritas, então pelo item acima nós poderíamos concluir que $v(x_1) = v(0) = \infty \Rightarrow x_1 = 0$. Mas então $v(x_2) > v(x_1) = \infty$, um absurdo!

□

Da mesma forma que partindo de um domínio de valoração discreta nós conseguimos construir uma valoração discreta associada a ele, partindo de uma valoração discreta nós conseguimos construir um domínio de valoração discreta associado a ela:

Proposição 3.27. *(a) Seja $v\colon K \to \mathbb{Z} \cup \{\infty\}$ uma valoração discreta. Então o conjunto*

$$\mathcal{O}_v \coloneqq \{a \in K\colon v(a) \geq 0\}$$

é um domínio de valoração discreta, com único ideal maximal

$$\mathfrak{p}_v \coloneqq \{a \in K\colon v(a) > 0\} = \{a \in K\colon v(a) \geq 1\}.$$

(b) As operações $A \mapsto v_A$ e $v \mapsto \mathcal{O}_v$ são inversas uma da outra, isto é, $v_{\mathcal{O}_v} = v$ e $\mathcal{O}_{v_A} = A$. Assim, temos uma bijeção entre os domínios de valoração discreta e as valorações discretas.

Demonstração. (a) Dados $a, b \in \mathcal{O}_v$, nós temos $v(a+b) \geq \min\{v(a), v(b)\} \geq 0$ e $v(ab) = v(a) + v(b) \geq 0$, o que mostra que $a+b, ab \in \mathcal{O}_v$. Além disso, como vimos temos $v(0) = \infty$ e $v(\pm 1) = 0$, de modo que $0, \pm 1 \in \mathcal{O}_v$. Isso prova que $\mathcal{O}_v$ é um anel. Agora, dados $a, b \in \mathfrak{p}_v$ e $x \in \mathcal{O}_v$, temos $v(a+b) \geq \min\{v(a), v(b)\} > 0$ e $v(ax) = v(a) + v(x) > 0$, de modo que $a+b, ax \in \mathfrak{p}_v$. Isso prova que $\mathfrak{p}_v$ é um ideal de $\mathcal{O}_v$. Como v é sobrejetora, existe $\pi \in K$ com $v(\pi) = 1$. Assim, $\pi \in \mathfrak{p}_v \setminus \{0\}$, o que mostra que $\mathfrak{p}_v \neq 0$.

Observemos agora que $\mathcal{O}_v^\times$ é o conjunto dos elementos $u \in K$ tais que $v(u) \geq 0$ e $v(u^{-1}) \geq 0$. Como $v(u^{-1}) = -v(u)$, vemos que isso ocorre se e só se $v(u) = 0$. Assim, nós temos $\mathcal{O}_v^\times = \{a \in K\colon v(a) = 0\}$. Mas então $\mathcal{O}_v^\times = \mathcal{O}_v \setminus \mathfrak{p}_v$, o que mostra que $\mathcal{O}_v$ é anel local com único ideal maximal $\mathfrak{p}_v$.

Falta mostrar que $\mathcal{O}_v$ é um DIP. Para isso, seja $\mathfrak{a} \lhd \mathcal{O}_v$ um ideal não-nulo. Então existe $a \in \mathfrak{a} \setminus \{0\}$ tal que $v|_{\mathfrak{a}}\colon \mathfrak{a} \to \mathbb{N} \cup \{\infty\}$ assume seu mínimo em a. Seja $b \in \mathfrak{a} \setminus \{0\}$ qualquer. Pela escolha de a, temos $v(b) \geq v(a)$. Assim:

$$v(a\pi^{v(b)-v(a)}b^{-1}) = v(a) + (v(b) - v(a))v(\pi) + v(b^{-1}) = v(a) + v(b) - v(a) - v(b) = 0,$$

de modo que $u \coloneqq a\pi^{v(b)-v(a)}b^{-1} \in \mathcal{O}_v^\times$. Logo $b = au^{-1}\pi^{v(b)-v(a)} \in a\mathcal{O}_v$, provando que $\mathfrak{a} \subseteq a\mathcal{O}_v$, e portanto que $\mathfrak{a} = a\mathcal{O}_v$. Concluímos que $\mathcal{O}_v$ é um DIP, e assim um DVD.

(b) Seja $v\colon K \to \mathbb{Z}\cup\{\infty\}$ uma valoração discreta. Tomemos, como no item acima, $\pi \in K$ tal que $v(\pi) = 1$. Dado $x \in K \setminus \{0\}$ qualquer, nós temos:

$$v(\pi^{v(x)}x^{-1}) = v(x)v(\pi) + v(x^{-1}) = v(x) - v(x) = 0.$$

Assim, $u := \pi^{v(x)}x^{-1} \in \mathcal{O}_v^\times$, de modo que $x = u^{-1}\pi^{v(x)}$. Isso mostra tanto que vale $K = Q(\mathcal{O}_v)$ quanto que $v_{\mathcal{O}_v}$ coincide com v em $K^\times$. Como $v(0) = \infty = v_{\mathcal{O}_v}(0)$, vemos que $v = v_{\mathcal{O}_v}$.

Reciprocamente, sejam A um DVD, $K = Q(A)$ e π um normalizador de A. Então $\mathcal{O}_{v_A}$ é o conjunto dos $x \in K$ tais que $v_A(x) \geq 0$, onde $v_A(x)$ é tal que $xA = \pi^{v_A(x)}A$. Mas é claro que

$$x \in A \iff xA \subseteq A \iff \pi^{v_A(x)}A \subseteq A \iff \pi^{v_A(x)} \in A \iff v_A(x) \geq 0$$

(lembre que $\pi \notin A^\times$). Assim, vemos que $\mathcal{O}_{v_A} = A$, como queríamos.

□

Notemos que todos os ideais de um DVD A com ideal maximal $\mathfrak{p}$ são da forma $\mathfrak{p}^n$, para $n \geq 0$. Além disso, sendo $v = v_A$, nós temos $\mathfrak{p}^n = \{a \in K\colon v(a) \geq n\}$. A partir desses ideais, nós podemos definir:

Definição (Grupos de Unidades)**.** Com as notações acima, definimos $U^{(0)} := A^\times$ e, para cada $n \geq 1$, $U^{(n)} := 1 + \mathfrak{p}^n$. Para cada $n \in \mathbb{N}$, nós chamamos $U^{(n)}$ de **n-ésimo grupo de unidades**, e $U^{(1)}$ de **grupo principal de unidades**.

Os grupos de unidade possuem as seguintes propriedades:

Proposição 3.28. *(a) Para todo $n \in \mathbb{N}$, $U^{(n)}$ é um grupo multiplicativo. Além disso, temos que $U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \cdots$.*

(b) Para todo $n \geq 1$, $U^{(0)}/U^{(n)}$ é canonicamente isomorfo ao grupo multiplicativo $(A/\mathfrak{p}^n)^\times$. Em particular, $U^{(0)}/U^{(1)}$ é canonicamente isomorfo ao grupo multiplicativo $(A/\mathfrak{p})^\times$ do corpo $A/\mathfrak{p}$.

(c) Para todo $n \geq 1$, $U^{(n)}/U^{(n+1)}$ é canonicamente isomorfo ao grupo aditivo do corpo $A/\mathfrak{p}$.

Essa proposição segue diretamente do seguinte resultado mais geral:

Lema 3.29. *Seja R um domínio local, com único ideal maximal $\mathfrak{m} \neq 0$. Então:*

(a) Para todo $i \geq 1$, $U_i := 1 + \mathfrak{m}^i = \{1 + a\colon a \in \mathfrak{m}^i\}$ é um subgrupo do grupo $U_0 := R^\times$ das unidades de R, e temos que $U_0 \supseteq U_1 \supseteq U_2 \supseteq \cdots$.

(b) Para todo $i \geq 1$, U_0/U_i é canonicamente isomorfo ao grupo multiplicativo $(R/\mathfrak{m}^i)^\times$. Em particular, U_0/U_1 é canonicamente isomorfo ao grupo multiplicativo $(R/\mathfrak{m})^\times$ do corpo $R/\mathfrak{m}$.

(c) Para todo $i \geq 1$, U_i/U_{i+1} é canonicamente isomorfo ao grupo aditivo do $R/\mathfrak{m}$-espaço $\mathfrak{m}^i/\mathfrak{m}^{i+1}$.

(d) Se R for um domínio de Dedekind, então para todo $i \geq 1$ o grupo aditivo de $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ será isomorfo ao grupo aditivo do corpo $R/\mathfrak{m}$.

Demonstração. (a) Fixemos $i \geq 1$. É fácil ver que $1 \in U_i$ e que U_i é fechado para a multiplicação. Mostremos agora que U_i também é fechado por inversão. Como R é local, temos $R^\times = R \setminus \mathfrak{m}$, e portanto $U_i = 1 + \mathfrak{m}^i \subseteq R \setminus \mathfrak{m} = R^\times = U_0$. Assim, todo elemento de U_i é inversível. Seja $u \in U_i$ qualquer. Então $u^{-1} \equiv uu^{-1} = 1 \pmod{\mathfrak{m}^i}$, mostrando que $u^{-1} \in 1 + \mathfrak{m}^i = U_i$. Isso prova que, para cada $i \geq 1$, U_i é um subgrupo de U_0. Finalmente, as inclusões $U_1 \supseteq U_2 \supseteq \cdots$ são claras, já que $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots$.

(b) Consideremos o mapa $U_0/U_i \to (R/\mathfrak{m}^i)^\times$ dado por $uU_i \mapsto u + \mathfrak{m}^i$. É uma verificação direta mostrar que essa função está bem-definida e é um isomorfismo de grupos.

(c) Consideremos o mapa $U_i/U_{i+1} \to \mathfrak{m}^i/\mathfrak{m}^{i+1}$ dado por $uU_{i+1} \mapsto (u-1) + \mathfrak{m}^{i+1}$. É uma verificação direta mostrar que essa função está bem-definida e é um isomorfismo de grupos.

(d) Se R for um domínio de Dedekind, então $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ é um $R/\mathfrak{m}$-espaço de dimensão 1, pelo Corolário 3.15. Desse modo, $\mathfrak{m}^i/\mathfrak{m}^{i+1} \cong R/\mathfrak{m}$ como $R/\mathfrak{m}$-espaços, e em particular como grupos abelianos.

□

Outra propriedade importante de um DVD é que ele não admite anéis intermediários entre ele e seu corpo de frações. De fato, seja A um DVD com $K = Q(A)$, e suponhamos que $A \subsetneq R \subseteq K$. Então existe $x \in R \setminus A$, e ele é da forma $x = u\pi^{v(x)}$, onde $u \in A^\times$ e $\pi \in A$ é um normalizador. Como $x \notin A$, vemos que $v(x) < 0$, de modo que $\pi^{-1} = xu^{-1}\pi^{-(v(x)+1)} \in R$. Assim, é claro que $R = K$.

Os domínios de valoração discreta surgem naturalmente no estudo dos domínios de Dedekind, devido ao seguinte resultado:

Teorema 3.30. *Sejam A um domínio de Dedekind e $\mathfrak{p} \lhd A$ primo não-nulo. Então $A_\mathfrak{p}$ é um DVD, com único ideal maximal $\mathfrak{p}_\mathfrak{p}$.*

Demonstração. Sabemos que $A_\mathfrak{p}$ é um anel local com único ideal maximal $\mathfrak{p}_\mathfrak{p}$. Como todos os primos de A são maximais, $\mathfrak{p}_\mathfrak{p}$ é de fato o único ideal primo de $A_\mathfrak{p}$. Pela Proposição 3.24, $A_\mathfrak{p}$ é um domínio de Dedekind. Finalmente, concluímos do Teorema 3.23 que $A_\mathfrak{p}$ é um DIP. □

Assim, toda localização de um domínio de Dedekind por um ideal primo não-nulo é um DVD. Vale também a volta para domínios noetherianos. Para demostrá-la, utilizaremos um resultado da teoria de localização, cujo enunciado relembramos aqui:

Teorema 3.31. *Seja A um domínio. Então para todo ideal $\mathfrak{a} \lhd A$ nós temos $\mathfrak{a} = \bigcap_\mathfrak{m} \mathfrak{a}_\mathfrak{m} = \bigcap_\mathfrak{p} \mathfrak{a}_\mathfrak{p}$, onde $\mathfrak{m}$ percorre todos os ideais maximais de A e $\mathfrak{p}$ percorre todos os ideais primos de A. Em particular, $A = \bigcap_\mathfrak{m} A_\mathfrak{m} = \bigcap_\mathfrak{p} A_\mathfrak{p}$.*

Com isso, podemos demonstrar:

Teorema 3.32. *Seja A um domínio noetheriano. Então A é um domínio de Dedekind se e somente se, para todos os ideais primos $\mathfrak{p} \lhd A$ não-nulos, as localizações $A_\mathfrak{p}$ forem domínios de valoração discreta.*

Demonstração. ($\Rightarrow$): É consequência direta do Teorema 3.30.

($\Leftarrow$): Suponhamos que A seja um domínio noetheriano tal que para todo $\mathfrak{p} \lhd A$ primo não-nulo nós tenhamos $A_\mathfrak{p}$ um DVD. Queremos mostrar que A é um domínio de Dedekind. Assim, queremos mostrar que A é integralmente fechado e que todo ideal primo não-nulo de A é maximal. Se A for um corpo, é claro que A será um domínio de Dedekind. Suponhamos então que A não seja um corpo. Pelo Teorema 3.31, vale a igualdade:

$$\bigcap_{\mathfrak{p} \neq 0} A_\mathfrak{p} = A, \tag{3.1}$$

já que $A_0 = Q(A)$ e assim pode ser ignorado na interseção. Denotemos $K = Q(A)$. Então K é o corpo de frações de todas as localizações de A. Seja $x \in \overline{A}^K$ qualquer. Então em particular $x \in \overline{A_\mathfrak{p}}^K$ para todo $\mathfrak{p} \lhd A$ primo não-nulo. Como $A_\mathfrak{p}$ é um DVD por hipótese, vemos que $A_\mathfrak{p}$ é

integralmente fechado, e portanto $\overline{A_\mathfrak{p}}^K = A_\mathfrak{p}$. Assim, $x \in A_\mathfrak{p}$ para todo $\mathfrak{p} \lhd A$ primo não-nulo, e por (3.1) nós concluímos que $x \in A$. Isso mostra que A é integralmente fechado.

Suponhamos agora que $\mathfrak{p} \subseteq \mathfrak{q}$ sejam dois ideais primos não-nulos de A. Então $\mathfrak{p}_\mathfrak{q} \subseteq \mathfrak{q}_\mathfrak{q}$ são ideais primos não-nulos de $A_\mathfrak{q}$. Mas sendo $A_\mathfrak{q}$ um DVD, vemos que seu único ideal primo não-nulo é $\mathfrak{q}_\mathfrak{q}$, e portanto $\mathfrak{p}_\mathfrak{q} = \mathfrak{q}_\mathfrak{q}$. Concluímos portanto que $\mathfrak{p} = \mathfrak{p}_\mathfrak{q} \cap A = \mathfrak{q}_\mathfrak{q} \cap A = \mathfrak{q}$. Isso prova que todo ideal primo não-nulo de A é maximal, o que termina a demonstração. □

Dado um domínio de Dedekind A, para cada ideal primo não-nulo $\mathfrak{p} \lhd A$ nós temos um DVD $A_\mathfrak{p}$. Associada a esse DVD nós temos a valoração discreta $v_\mathfrak{p} := v_{A_\mathfrak{p}}$, chamada de **valoração $\mathfrak{p}$-ádica**. As valorações $\mathfrak{p}$-ádicas se relacionam com a fatoração dos ideais fracionários principais de A:

Proposição 3.33. *Seja A um domínio de Dedekind com corpo de frações $K = Q(A)$. Seja $x \in K^\times$, e suponhamos que a fatoração de xA em ideais primos de A seja $xA = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$. Então, para cada ideal primo não-nulo $\mathfrak{p} \lhd A$, nós temos $\nu_\mathfrak{p} = v_\mathfrak{p}(x)$. Ou seja, o expoente de $\mathfrak{p}$ na fatoração prima de xA é a valoração discreta $v_\mathfrak{p}(x)$.*

Demonstração. Localizando a igualdade $xA = \prod_\mathfrak{q} \mathfrak{q}^{\nu_\mathfrak{q}}$ por $\mathfrak{p}$, nós obtemos $xA_\mathfrak{p} = \prod_\mathfrak{q} \mathfrak{q}_\mathfrak{p}^{\nu_\mathfrak{q}}$. Notemos que $\mathfrak{q}_\mathfrak{p} = A_\mathfrak{p}$ para todo $\mathfrak{q} \neq \mathfrak{p}$, já que $\mathfrak{p}$ é maximal. Assim, vale $xA_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^{\nu_\mathfrak{p}}$. Mas isso é exatamente o mesmo que dizer que $v_\mathfrak{p}(x) = \nu_\mathfrak{p}$. □

Consideremos agora, para $p \in \mathbb{N}$ primo, o ideal primo não-nulo $p\mathbb{Z} \lhd \mathbb{Z}$. Denotaremos a localização $\mathbb{Z}_{p\mathbb{Z}}$ simplesmente por $\mathbb{Z}_{(p)}$. Notemos que

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ p \nmid b \right\}.$$

Esse é um DVD, com único ideal maximal

$$p\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ p \mid a,\ p \nmid b \right\}$$

e grupo de unidades

$$\mathbb{Z}_{(p)}^\times = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ p \nmid a, b \right\}.$$

Denotamos sua valoração discreta associada por $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Ela é chamada de **valoração p-ádica** de $\mathbb{Q}$. É fácil ver pela proposição acima que v_p pode ser calculada da seguinte forma: dado $x \in \mathbb{Q}^\times$, podemos escrevê-lo de modo único como $x = p^\nu a/b$, onde $p \nmid a, b$. Nós temos então $v_p(x) = \nu$. As valorações p-ádicas são importantíssimas em Teoria Algébrica dos Números, como veremos mais adiante.

Capítulo 4

Extensões de Domínios de Dedekind

Ao estendermos $\mathbb{Z}$ para um corpo de inteiros algébricos $\mathcal{O}_K$, alguns elementos primos de $\mathbb{N}$ deixam de ser primos em $\mathcal{O}_K$, enquanto outros continuam primos. Como vimos no Exemplo 2.22, os primos $p \in \mathbb{N}$ com $p \equiv 3 \pmod 4$ continuam primos em $\mathbb{Z}[i]$, enquanto 2 e os primos $p \in \mathbb{N}$ tais que $p \equiv 1 \pmod 4$ se tornam elementos redutíveis nesse anel. É interessante notar também que todos os primos $p \equiv 1 \pmod 4$ se decompõe como produto de dois primos não-associados, enquanto que $2 = -i(1+i)^2$ é o único dos primos de $\mathbb{N}$ que não é livre de quadrados em $\mathbb{Z}[i]$. Esse evento pode ser visto em termos de ideais: dado um ideal primo $p\mathbb{Z} \lhd \mathbb{Z}$, como $p\mathcal{O}_K$ se fatora em ideais primos do domínio de Dedekind $\mathcal{O}_K$?

4.1. Norma de ideais

Ao longo desta seção, K sempre denotará um corpo de números algébricos com $[K : \mathbb{Q}] = n$. Lembre que no Capítulo 2 nós mostramos que a função $\mathfrak{N}\colon \{\text{Ideais de } \mathcal{O}_K\} \to \mathbb{N}^*$ dada por $\mathfrak{N}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ está bem-definida, e que satisfaz $\mathfrak{N}(\mathfrak{a})^2 d_K = d_K(\mathfrak{a})$. Nosso objetivo nessa seção é estudar um pouco melhor essa função, que será fundamental na demonstração do Teorema da Finitude do Número de Classes. Ela generaliza a norma $N_{K/\mathbb{Q}}$ no seguinte sentido:

Teorema 4.1. *(a) Todo ideal não-nulo $\mathfrak{a}$ de $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n, e para toda base $\{\alpha_1, \ldots, \alpha_n\}$ deste $\mathbb{Z}$-módulo temos $\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \mathfrak{N}(\mathfrak{a})^2 d_K$.*

(b) Para todo $\alpha \in \mathcal{O}_K \setminus \{0\}$, temos $\mathfrak{N}(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$.

Demonstração. (a) Já foi demonstrado.

(b) Seja $\{\beta_1, \ldots, \beta_n\}$ uma base integral de $\mathcal{O}_K$. Então $\{\alpha\beta_1, \ldots, \alpha\beta_n\}$ é claramente uma base do ideal $\alpha\mathcal{O}_K$ como $\mathbb{Z}$-módulo. Mas então, por (a) e pela Proposição 1.31:

$$\begin{aligned} \mathfrak{N}(\alpha\mathcal{O}_K)^2 d_K &= \Delta(\alpha\beta_1, \ldots, \alpha\beta_n) = \Delta(T_\alpha(\beta_1, \ldots, \beta_n)) \\ &= (\det T_\alpha)^2 \Delta(\beta_1, \ldots, \beta_n) = N(\alpha)^2 d_K. \end{aligned}$$

Isso nos dá $\mathfrak{N}(\alpha\mathcal{O}_K) = |N(\alpha)|$, como desejado.

□

Todo ideal primo de $\mathcal{O}_K$ está associado a um primo de $\mathbb{N}$:

Teorema 4.2. *Seja $\mathfrak{p}$ um ideal primo não-nulo de $\mathcal{O}_K$. Então:*

(a) $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, onde p é o único número primo de $\mathbb{N}$ no ideal $\mathfrak{p}$.

(b) $\mathcal{O}_K/\mathfrak{p}$ é uma extensão finita do corpo $\mathbb{F}_p$, de grau $[\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] \leq n$.

Demonstração. (a) Sendo $\mathfrak{p} \lhd \mathcal{O}_K$ maximal, temos que $\mathfrak{p} \cap \mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, pelo item (e) do Teorema 1.53. Então temos $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, para algum primo $p \in \mathbb{N}$. Assim, é claro que $p \in \mathfrak{p}$, o que não ocorre para nenhum outro primo de $\mathbb{N}$.

(b) Como $\mathfrak{p} \mid p\mathbb{Z}$, temos a inclusão canônica $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$, de modo que podemos ver $\mathcal{O}_K/\mathfrak{p}$ como extensão de $\mathbb{F}_p$. Essa extensão tem grau no máximo $[K : \mathbb{Q}] = n$. Em particular, é finita.

□

Definição (Grau de Inércia)**.** Nas notações do teorema acima, o número inteiro positivo dado pelo grau $[\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$ é chamado o **grau de inércia** de $\mathfrak{p}$, que denotamos por $f_\mathfrak{p}$.

A norma de ideais é multiplicativa:

Teorema 4.3. *(a) Para todo ideal primo não-nulo $\mathfrak{p}$ de $\mathcal{O}_K$ temos $\mathfrak{N}(\mathfrak{p}) = p^{f_\mathfrak{p}}$, onde p é o único número primo de $\mathbb{N}$ em $\mathfrak{p}$.*

(b) Para quaisquer ideais não-nulos $\mathfrak{a}, \mathfrak{b}$ de $\mathcal{O}_K$, temos $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\,\mathfrak{N}(\mathfrak{b})$.

(c) $\mathfrak{N}(\mathfrak{a}) = 1$ se e só se $\mathfrak{a} = \mathcal{O}_K$.

Demonstração. (a) Pelo teorema acima, $[\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] = f_\mathfrak{p}$. Assim, $\mathfrak{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = p^{f_\mathfrak{p}}$.

(b) Sejam $\mathfrak{b}$ um ideal não-nulo de $\mathcal{O}_K$ e $\mathfrak{p}$ um ideal primo não-nulo de $\mathcal{O}_K$. Então $\mathfrak{b}/(\mathfrak{bp})$ é um $\mathcal{O}_K/\mathfrak{p}$-espaço vetorial de dimensão 1 pelo Corolário 3.15, e portanto tem $|\mathcal{O}_K/\mathfrak{p}| = \mathfrak{N}(\mathfrak{p})$ elementos. Agora, $\mathcal{O}_K/\mathfrak{b} \cong \frac{\mathcal{O}_K/(\mathfrak{bp})}{\mathfrak{b}/(\mathfrak{bp})}$. Assim: $|\mathcal{O}_K/\mathfrak{b}| = \frac{|\mathcal{O}_K/(\mathfrak{bp})|}{|\mathfrak{b}/(\mathfrak{bp})|} \Rightarrow \mathfrak{N}(\mathfrak{bp}) = \mathfrak{N}(\mathfrak{b})\,\mathfrak{N}(\mathfrak{p})$. Pelo Teorema 3.12, todo ideal não-nulo $\mathfrak{a}$ de $\mathcal{O}_K$ é da forma $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, onde $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ são ideais primos não-nulos de $\mathcal{O}_K$. Então é fácil ver por indução em m que vale a igualdade $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1) \cdots \mathfrak{N}(\mathfrak{p}_m)$, de segue a multiplicatividade de $\mathfrak{N}$.

(c) Para todo ideal primo $\mathfrak{p}$, $\mathfrak{N}(\mathfrak{p}) = p^{f_\mathfrak{p}}$ é um múltiplo de p, logo pela fórmula acima o único jeito de termos $\mathfrak{N}(\mathfrak{a}) = 1$ é se $m = 0$, ou seja, se $\mathfrak{a} = \mathcal{O}_K$, e é claro que $\mathfrak{N}(\mathcal{O}_K) = 1$.

□

Com isso, podemos mostrar que a norma de ideais é mais similar ainda à norma de um elemento:

Corolário 4.4. *Seja $\mathfrak{a}$ um ideal não-nulo de $\mathcal{O}_K$. Então:*

(a) $\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$. Equivalentemente, o ideal $\mathfrak{N}(\mathfrak{a})\mathcal{O}_K$ é um múltiplo de $\mathfrak{a}$.

(b) Se $\mathfrak{N}(\mathfrak{a})$ for um número primo, então $\mathfrak{a}$ será um ideal primo.

(c) Se $\mathfrak{a}$ for um múltiplo do ideal $\mathfrak{b}$ e $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})$, então $\mathfrak{a} = \mathfrak{b}$.

Demonstração. (a) O grupo aditivo $\mathcal{O}_K/\mathfrak{a}$ tem ordem $\mathfrak{N}(\mathfrak{a})$. Assim, $\mathfrak{N}(\mathfrak{a}) \cdot (1 + \mathfrak{a}) = \mathfrak{a}$, o que mostra que $\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$.

(b) Escrevamos $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, onde $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ são ideais primos não-nulos de $\mathcal{O}_K$. Então, como vimos, $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1) \cdots \mathfrak{N}(\mathfrak{p}_m) = p_1^{f(\mathfrak{p}_1)} \cdots p_m^{f(\mathfrak{p}_m)}$, onde $p_1, \ldots, p_m \in \mathbb{N}$ são primos. Então é claro que $\mathfrak{N}(\mathfrak{a})$ só pode ser prima se $m = 1$, e nesse caso $\mathfrak{a}$ é um ideal primo de $\mathcal{O}_K$.

(c) Se $\mathfrak{a}$ for um múltiplo de $\mathfrak{b}$, então existe $\mathfrak{c}$ ideal não-nulo de $\mathcal{O}_K$ tal que $\mathfrak{a} = \mathfrak{bc}$. Então temos $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})\,\mathfrak{N}(\mathfrak{c})$. Como $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})$, concluímos que $\mathfrak{N}(\mathfrak{c}) = 1$, o que nos garante que $\mathfrak{c} = \mathcal{O}_K$, e portanto $\mathfrak{a} = \mathfrak{b}$.

□

O seguinte corolário será essencial na prova da finitude de h_K:

Corolário 4.5. *Para todo m inteiro positivo, existe somente um número finito de ideais não-nulos $\mathfrak{a}$ de $\mathcal{O}_K$ tais que $\mathfrak{N}(\mathfrak{a}) = m$.*

Demonstração. Pelo item (a) do corolário anterior, $\mathfrak{N}(\mathfrak{a}) = m \Rightarrow \mathfrak{a} \mid m\mathcal{O}_K$. Mas pelo item (a) do Corolário 3.15, o conjunto dos ideais que dividem $m\mathcal{O}_K$ é finito, o que prova o corolário. □

A norma de ideais ainda pode ser usada para deduzir a **identidade fundamental** em sua versão mais simples. Ela nos dá informações sobre como um primo de $\mathbb{N}$ se decompõe em ideais primos de $\mathcal{O}_K$:

Corolário 4.6. *Seja $p \in \mathbb{N}$ um número primo tal que a fatoração de $p\mathcal{O}_K$ em ideais primos seja $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. Denotemos ainda $f_{\mathfrak{p}_j} = f_j$, para $1 \leq j \leq g$. Então:*

(a) $\mathfrak{p}_1 \ldots, \mathfrak{p}_g$ são os únicos ideais primos de $\mathcal{O}_K$ que contêm p.

(b) (Identidade Fundamental) $\sum_{j=1}^{g} e_j f_j = n$.

Demonstração. (a) Dado um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$, temos $p \in \mathfrak{p} \iff \mathfrak{p} \mid p\mathcal{O}_K$, e pela unicidade da fatoração obtemos o resultado desejado.

(b) Temos $N(p) = p^n$, logo pelo item (b) do Teorema 4.1 temos $\mathfrak{N}(p\mathcal{O}_K) = |N(p)| = p^n$. Então:

$$p^n = \mathfrak{N}(p\mathcal{O}_K) = \mathfrak{N}(\mathfrak{p}_1)^{e_1} \cdots \mathfrak{N}(\mathfrak{p}_g)^{e_g} = (p^{f(\mathfrak{p}_1)})^{e_1} \cdots (p^{f(\mathfrak{p}_g)})^{e_g} = p^{\sum_{j=1}^{g} e_j f_j},$$

e portanto $\sum_{j=1}^{g} e_j f_j = n$, como queríamos.

□

4.2. O Teorema da Finitude do Número de Classes

Seja K um corpo de números. Denotaremos por $\mathscr{J}$ o conjunto de ideais não-nulos de $\mathcal{O}_K$ e por $\mathscr{C}\ell$ o grupo de classes de ideais de $\mathcal{O}_K$. Com o maquinário que nós desenvolvemos, já é possível demonstrar o Teorema da Finitude do Número de Classes. Tudo o que falta são dois lemas técnicos, um que relaciona ideais de $\mathscr{J}$ com classes de $\mathscr{C}\ell$ e outro que garante que certo conjunto de inteiros positivos é limitado superiormente, e que no fundo nada mais é do que uma aplicação esperta do Princípio da Casa dos Pombos. Definamos, para qualquer $\mathfrak{a} \in \mathscr{J}$, o número

$$t(\mathfrak{a}) := \min\{\mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\alpha\mathcal{O}_K) \colon \alpha \in \mathfrak{a} \setminus \{0\}\}.$$

Para qualquer $\alpha \in \mathfrak{a} \setminus \{0\}$, temos que $\mathfrak{a} \mid \alpha\mathcal{O}_K$. Logo, pela multiplicatividade da norma de ideais, $\mathfrak{N}(\mathfrak{a}) \mid \mathfrak{N}(\alpha\mathcal{O}_K)$, o que mostra que $t(\mathfrak{a})$ é o mínimo de um conjunto de inteiros positivos, sendo portanto bem-definido e um inteiro positivo. Além disso, pelo item (c) do Corolário 4.4 temos que $t(\mathfrak{a}) = 1$ se e só se $\mathfrak{a} = \alpha\mathcal{O}_K$ para algum $\alpha \in \mathfrak{a} \setminus \{0\}$, ou seja, se e só se $\mathfrak{a}$ for principal. Por outro lado, dada uma classe $\mathfrak{B} \in \mathscr{C}\ell$, definimos:

$$u(\mathfrak{B}) := \min\{\mathfrak{N}(\mathfrak{b}) \colon \mathfrak{b} \in \mathscr{J} \cap \mathfrak{B}\}.$$

Pela Proposição 3.19, a interseção $\mathscr{J} \cap \mathfrak{B}$ é não-vazia, o que mostra que $u(B)$ está bem-definido. Note que $u(B)$ é um inteiro positivo. Temos uma importante relação entre as duas funções t e u:

Lema 4.7. *Sejam $\mathfrak{B} \in \mathscr{C}\ell$ e $\mathfrak{a} \in \mathscr{J}$ tais que $\mathfrak{a}^{-1} \in \mathfrak{B}$. Então $u(\mathfrak{B}) = t(\mathfrak{a})$. Em particular, temos*

$$\{t(\mathfrak{a})\colon \mathfrak{a} \in \mathscr{J}\} = \{u(\mathfrak{B})\colon \mathfrak{B} \in \mathscr{C}\ell\}.$$

Demonstração. Seja $\alpha \in \mathfrak{a} \setminus \{0\}$ tal que $t(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\alpha\mathcal{O}_K)$. Então $\alpha\mathfrak{a}^{-1} \in \mathscr{J} \cap \mathfrak{B}$, pela Proposição 3.19 e usando que $\alpha\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$. Notemos que

$$(\alpha\mathfrak{a}^{-1})\mathfrak{a} = \alpha\mathcal{O}_K \Rightarrow \mathfrak{N}(\alpha\mathfrak{a}^{-1})\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\alpha\mathcal{O}_K),$$

e portanto:

$$u(\mathfrak{B}) \leq \mathfrak{N}(\alpha\mathfrak{a}^{-1}) = \mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\alpha\mathcal{O}_K) = t(\mathfrak{a}).$$

Por outro lado, seja $\mathfrak{b} \in \mathscr{J} \cap \mathfrak{B}$ tal que $u(\mathfrak{B}) = \mathfrak{N}(\mathfrak{b})$. Então, como $\mathfrak{a}^{-1}, \mathfrak{b} \in \mathfrak{B}$, existe $\beta \in K \setminus \{0\}$ tal que $\beta\mathfrak{a}^{-1} = \mathfrak{b}$. Mas então $\beta\mathcal{O}_K = \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$. Disso tiramos que $\beta \in \mathfrak{a} \setminus \{0\}$. Além disso,

$$\mathfrak{N}(\beta\mathcal{O}_K) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})u(\mathfrak{B}).$$

Logo:

$$t(\mathfrak{a}) \leq \mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\beta\mathcal{O}_K) = u(\mathfrak{B}).$$

Então de fato temos $u(\mathfrak{B}) = t(\mathfrak{a})$. Para a última afirmação basta notar, de um lado, que para $\mathfrak{a} \in \mathscr{J}$ temos $t(\mathfrak{a}) = u([\mathfrak{a}^{-1}])$, e de outro que, se $\mathfrak{B} \in \mathscr{C}\ell$, então existe um $\mathfrak{a} \in \mathfrak{B}^{-1} \cap \mathscr{J}$. Assim, $\mathfrak{a}^{-1} \in \mathfrak{B}$, e temos $u(\mathfrak{B}) = t(\mathfrak{a})$. □

Ainda temos um último lema técnico a provar antes de chegarmos ao resultado desejado:

Lema 4.8. *Existe uma constante $C > 0$ tal que $t(\mathfrak{a}) \leq C$, para todo $\mathfrak{a} \in \mathscr{J}$.*

Demonstração. Sejam $\sigma_1, \ldots, \sigma_n$ as imersões de K, e seja $\{\beta_1, \ldots, \beta_n\}$ uma base integral de K. Definamos

$$C \coloneqq \prod_{j=1}^{n}\left(\sum_{i=1}^{n}|\sigma_j(\beta_i)|\right).$$

Mostraremos que, para todo $\mathfrak{a} \in \mathscr{J}$, temos $t(\mathfrak{a}) \leq C$, o que terminará a demonstração. Tomemos $\mathfrak{a} \in \mathscr{J}$ qualquer. Então existe k inteiro positivo tal que $k^n \leq \mathfrak{N}(\mathfrak{a}) < (k+1)^n$. Definamos

$$\mathscr{L} \coloneqq \left\{\sum_{i=1}^{n} d_i\beta_i \mid d_1, \ldots, d_n \in \{0, \ldots, k\}\right\}.$$

Notemos que $|\mathscr{L}| = (k+1)^n > \mathfrak{N}(\mathfrak{a})$, logo pelo Princípio da Casa dos Pombos existem $\lambda, \nu \in \mathscr{L}$ distintos tais que $\lambda + \mathfrak{a} = \nu + \mathfrak{a}$. Então temos

$$\lambda - \nu = \sum_{i=1}^{n} a_i\beta_i \in \mathfrak{a}, \text{ onde } a_1, \ldots, a_n \in \{-k, \ldots, k\}.$$

Assim:

$$\begin{aligned}
|N(\lambda-\nu)| = \left|\prod_{j=1}^{n}\sigma_j(\lambda-\nu)\right| &= \left|\prod_{j=1}^{n}\sigma_j\Big(\sum_{i=1}^{n}a_i\beta_i\Big)\right| = \prod_{j=1}^{n}\left|\sum_{i=1}^{n}a_i\sigma_j(\beta_i)\right| \\
&\leq \prod_{j=1}^{n}\left(\sum_{i=1}^{n}|a_i||\sigma_j(\beta_i)|\right) \leq \prod_{j=1}^{n}\left(\sum_{i=1}^{n}k|\sigma_j(\beta_i)|\right) \\
&= k^n\prod_{j=1}^{n}\left(\sum_{i=1}^{n}|\sigma_j(\beta_i)|\right) = k^nC \leq \mathfrak{N}(\mathfrak{a})C.
\end{aligned}$$

Concluímos finalmente do item (b) do Teorema 4.1 que

$$t(\mathfrak{a}) \leq \mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}((\lambda-\nu)\mathcal{O}_K) = \mathfrak{N}(\mathfrak{a})^{-1}|N(\lambda-\nu)| \leq C.$$

□

Enfim, chegamos ao resultado que tanto almejávamos:

Teorema 4.9 (Finitude do Número de Classes)**.** *O número de classes h_K é finito.*

Demonstração. Pelo Lema 4.8, o conjunto $\{t(\mathfrak{a})\colon \mathfrak{a} \in \mathscr{J}\}$ é limitado superiormente por um $C > 0$. Mas pelo Lema 4.7 esse conjunto é igual a $\{u(\mathfrak{B})\colon \mathfrak{B} \in \mathscr{C}\ell\}$, que portanto também é limitado por C. Seja agora $\mathfrak{B} \in \mathscr{C}\ell$. Então existe $\mathfrak{b} \in \mathfrak{B}$ tal que $\mathfrak{N}(\mathfrak{b}) \leq C$. Mas pelo Corolário 4.5, existe um número finito m de ideais de $\mathscr{J}$ tais que $\mathfrak{N}(\mathfrak{b}) \leq C$. Assim, $\mathfrak{B}$ é a classe de um desses m ideais. Isso mostra que $\mathscr{C}\ell$ é finito, como desejávamos. □

Um corolário direto deste teorema é:

Corolário 4.10. *Para todo $\mathfrak{a} \in \mathscr{J}$, $\mathfrak{a}^{h_K}$ é um ideal principal.*

A demonstração que demos não é totalmente satisfatória para o cálculo efetivo de h_K, pois a constante C que encontramos no lema acima é muito grande. Como veremos mais adiante, podemos diminuir essa constante para a chamada **cota de Minkowski**:

$$\mu_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|d_K|},$$

onde r_2 é a metade do número de imersões σ de K tais que $\sigma(K) \not\subseteq \mathbb{R}$ (pode-se mostrar que o número de tais imersões é sempre par, ou seja, r_2 é inteiro).

Com a cota de Minkowski em mãos, podemos determinar h_K da seguinte forma: como vimos, cada classe de ideais de K contém um ideal com norma no máximo μ_K. Mas existe um número finito m de ideais não-nulos de $\mathcal{O}_K$ com norma menor ou igual a μ_K. Nós podemos então determinar quais são esses ideais e verificar quantas classes de ideais distintas eles nos fornecem. O resultado encontrado será h_K.

Exemplo 4.11. *Como exemplo prático, vamos calcular o número de classes de alguns corpos quadráticos. Sendo $K = \mathbb{Q}(\sqrt{d})$, notemos que K possui duas imersões complexas se $d < 0$ e nenhuma imersão complexa se $d > 0$. Assim, $r_2 = 1$ se $d < 0$ e $r_2 = 0$ se $d > 0$, e a cota de Minkowski para K se torna:*

$$\mu_K = \begin{cases} \frac{2}{\pi}\sqrt{|d_K|}, & \text{se } d < 0; \\ \frac{1}{2}\sqrt{|d_K|}, & \text{se } d > 0. \end{cases}$$

Como $d_K = 4d$ se $d \equiv 2, 3 \pmod 4$ e $d_K = d$ se $d \equiv 1 \pmod 4$, nós obtemos:

$$\mu_K = \begin{cases} \frac{2}{\pi}\sqrt{|4d|} = \frac{4\sqrt{|d|}}{\pi}, & \text{se } d < 0 \text{ e } d \equiv 2, 3 \pmod 4; \\ \frac{2\sqrt{|d|}}{\pi}, & \text{se } d < 0 \text{ e } d \equiv 1 \pmod 4; \\ \frac{1}{2}\sqrt{4d} = \sqrt{d}, & \text{se } d > 0 \text{ e } d \equiv 2, 3 \pmod 4; \\ \frac{\sqrt{d}}{2}, & \text{se } d > 0 \text{ e } d \equiv 1 \pmod 4. \end{cases}$$

Com isso, nós obtemos que $\mu_K < 2 \iff d \in \{-7, -3, -2, -1, 2, 3, 5, 13\}$. Assim, para esses valores de d toda classe de ideais de K contém um ideal de norma menor que 2, ou seja, igual a 1. Mas sabemos que o único ideal de norma 1 em $\mathcal{O}_K$ é $\mathcal{O}_K$! Assim, nesse caso vemos que K é um DIP. Observe que já havíamos concluído que esses corpos quadráticos eram DIP's (de fato,

domínios euclidianos) no Teorema 2.19. Note que também havíamos concluído nesse teorema que para $d = -11$ tínhamos $K = \mathbb{Q}(\sqrt{-11})$ um DIP, embora $\mu_K = \frac{2\sqrt{11}}{\pi} \cong 2,11 > 2$.

Utilizando a cota de Minkowski, a estratégia para verificar que $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ é um DIP é mostrar que todos os ideais de norma 2 em $\mathcal{O}_K$ são principais. Lembremos que se $\mathfrak{N}(\mathfrak{a}) = 2$ então $\mathfrak{a} \mid 2\mathcal{O}_K$. Assim, basta analisarmos a fatoração prima de $2\mathcal{O}_K$ para encontrarmos os ideais de norma 2. Como veremos na Seção 5.2, temos um método para encontrarmos essa fatoração prima. Aplicando este método, vemos que o ideal $2\mathcal{O}_K$ é primo. Assim, não existe nenhum ideal de norma 2 em $\mathcal{O}_K$, e concluímos que $\mathcal{O}_K$ é um DIP.

De forma mais geral, o método de olhar para a fatoração prima de $2\mathcal{O}_K$ funcionará se tivermos $2 \leq \mu_K < 3 \iff d \in \{-19, -15, -11, -5, 6, 7, 17, 21, 29, 33\}$. Pela identidade fundamental, nós temos duas opções para a fatoração de $2\mathcal{O}_K$ em corpos quadráticos: ou $2\mathcal{O}_K$ é um ideal primo ou $2\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2$ para $\mathfrak{p}_1, \mathfrak{p}_2 \lhd \mathcal{O}_K$ primos (que podem ser distintos ou não). Para os valores de d indicados acima, se $2\mathcal{O}_K$ for primo então $\mathcal{O}_K$ será um DIP (foi o que ocorreu para $d = -11$).

Supondo agora que $2\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2$, vemos que $\mathfrak{p}_1$ e $\mathfrak{p}_2$ serão os únicos ideais de $\mathcal{O}_K$ com norma 2. Desse modo, temos $\mathscr{C}\ell = \{[1], [\mathfrak{p}_1], [\mathfrak{p}_2]\}$. Assim, $h_K \leq 3$. A outra forma de termos $h_K = 1$ é se os ideais $\mathfrak{p}_1$ e $\mathfrak{p}_2$ forem ambos principais. Também é interessante observar que se $\mathfrak{p}_1 = \mathfrak{p}_2$, então sabemos que $h_K \leq 2$. Faremos agora uma análise mais detalhada para determinar h_K para $d \in \{-19, -15, -11, -5, 6, 7, 17, 21, 29, 33\}$, utilizando os resultados da Seção 5.2:

- *Como $-19, -11, 21, 29 \equiv 5 \pmod 8$, vemos que $2\mathcal{O}_K$ é primo para esses valores de d. Assim, nesses casos $\mathcal{O}_K$ é um DIP.*

- *Como $2 \mid 6$ e $-5, 7 \equiv 3 \pmod 4$, vemos que nesse caso $2\mathcal{O}_K$ é o quadrado de um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$. De fato, nós temos:*

$$2\mathcal{O}_K = \begin{cases} (2\mathcal{O}_K + (\sqrt{-5} - 1)\mathcal{O}_K)^2, & \text{se } d = -5; \\ (2\mathcal{O}_K + \sqrt{6}\,\mathcal{O}_K)^2, & \text{se } d = 6; \\ (2\mathcal{O}_K + (\sqrt{7} - 1)\mathcal{O}_K)^2, & \text{se } d = 7. \end{cases}$$

  Assim, nesses casos temos $h_K = 1$ ou $h_K = 2$, sendo que $h_K = 1$ se $\mathfrak{p}$ for principal e $h_K = 2$ se $\mathfrak{p}$ não for principal. Da multiplicidade da norma de ideais e do fato de que $\mathfrak{N}(2\mathcal{O}_K) = |N(2)| = 4$, nós vemos que $\mathfrak{N}(\mathfrak{p}) = 2$ em qualquer um dos três casos. Lembremos que $\mathfrak{p}$ é principal se e só se $t(\mathfrak{p}) = 1$, isto é, se e só se existir $\alpha \in \mathfrak{p}$ não-nulo tal que $|N(\alpha)| = \mathfrak{N}(\mathfrak{p}) = 2$. Assim, basta encontrarmos os elementos de $\mathcal{O}_K$ de norma ± 2 e verificar se eles estão em $\mathfrak{p}$. Escrevendo $\alpha = a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$, temos $N(\alpha) = a^2 - db^2$.

  Para $d = -5$, buscamos $a, b \in \mathbb{Z}$ tais que $a^2 + 5b^2 = \pm 2$. Mas é fácil ver que tais elementos não existem! Assim, concluímos que $\mathfrak{p}$ não é principal, e portanto $h_K = 2$ nesse caso (note que poderíamos também concluir isso do fato de que $\mathbb{Z}[\sqrt{-5}]$ não é um DFU, como já havíamos visto).

  Para $d = 6$, buscamos $a, b \in \mathbb{Z}$ tais que $a^2 - 6b^2 = \pm 2$. Vemos que $(a, b) = (2, 1)$ é uma solução, e que $\alpha = 2 + \sqrt{6} \in 2\mathcal{O}_K + \sqrt{6}\mathcal{O}_K = \mathfrak{p}$. Assim, $\mathfrak{p}$ é principal e temos $h_K = 1$. Desse modo, $\mathcal{O}_K$ é um DIP nesse caso.

  Para $d = 7$, buscamos $a, b \in \mathbb{Z}$ tais que $a^2 - 7b^2 = \pm 2$. Vemos que $(a, b) = (3, 1)$ é uma solução, e que $\alpha = 3 + \sqrt{7} = 4 + (\sqrt{7} - 1) \in 2\mathcal{O}_K + (\sqrt{7} - 1)\mathcal{O}_K = \mathfrak{p}$. Assim, $\mathfrak{p}$ é principal e temos $h_K = 1$. Desse modo, $\mathcal{O}_K$ é um DIP nesse caso.

- *Como $-15, 17, 33 \equiv 1 \pmod 8$, vemos que nesse caso $2\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2$ para $\mathfrak{p}_1, \mathfrak{p}_2 \lhd \mathcal{O}_K$ primos distintos. De fato, nós temos:*

$$2\mathcal{O}_K = \begin{cases} \left(2\mathcal{O}_K + \frac{\sqrt{-15}+1}{2}\,\mathcal{O}_K\right) \cdot \left(2\mathcal{O}_K + \frac{\sqrt{-15}-1}{2}\,\mathcal{O}_K\right), & \text{se } d = -15; \\ \left(2\mathcal{O}_K + \frac{\sqrt{17}+1}{2}\,\mathcal{O}_K\right) \cdot \left(2\mathcal{O}_K + \frac{\sqrt{17}-1}{2}\,\mathcal{O}_K\right), & \text{se } d = 17; \\ \left(2\mathcal{O}_K + \frac{\sqrt{33}+1}{2}\,\mathcal{O}_K\right) \cdot \left(2\mathcal{O}_K + \frac{\sqrt{33}-1}{2}\,\mathcal{O}_K\right), & \text{se } d = 33. \end{cases}$$

Da multiplicidade da norma de ideais e do fato de que $\mathfrak{N}(2\mathcal{O}_K) = 4$*, nós vemos que* $\mathfrak{N}(\mathfrak{p}_1) = \mathfrak{N}(\mathfrak{p}_2) = 2$ *em qualquer um dos três casos. Como* $\mathfrak{p}_1\,\mathfrak{p}_2 = 2\mathcal{O}_K$ *é um ideal principal, nós temos* $[\mathfrak{p}_1][\mathfrak{p}_2] = [1]$*, de onde se vê facilmente que* $\mathfrak{p}_1$ *será um ideal principal se e só se* $\mathfrak{p}_2$ *o for. Como no caso anterior,* $\mathfrak{p}_1$ *ser principal equivale à existência de* $\alpha \in \mathfrak{p}_1$ *não-nulo com* $|N(\alpha)| = 2$*. Escrevendo* $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right)$ *com* $a, b \in \mathbb{Z}$*, nós temos* $N(\alpha) = a^2 + ab + b^2 \cdot \frac{1-d}{4}$*.*

Para $d = -15$*, buscamos* $a, b \in \mathbb{Z}$ *tais que* $a^2 + ab + 4b^2 = \pm 2$*. Mas é fácil ver que tais elementos não existem! Assim, concluímos que* $\mathfrak{p}_1$*, e portanto* $\mathfrak{p}_2$*, não são principais. Devemos agora determinar se* $h_K = 2$ *ou se* $h_K = 3$*, isto é, se* $[\mathfrak{p}_1] = [\mathfrak{p}_2]$ *ou se* $[\mathfrak{p}_1] \neq [\mathfrak{p}_2]$*. Como* $[\mathfrak{p}_2] = [\mathfrak{p}_1]^{-1}$*, nós temos* $[\mathfrak{p}_1] = [\mathfrak{p}_2] \iff [\mathfrak{p}_1]^2 = [1]$*. Desse modo, o problema se resume a determinar se* $\mathfrak{p}_1^2$ *é um ideal principal de* $\mathcal{O}_K$*. Chamando* $\beta := \frac{1+\sqrt{-15}}{2}$*, nós temos* $\mathfrak{p}_1 = 2\mathcal{O}_K + \beta\mathcal{O}_K$*, e portanto* $\mathfrak{p}_1^2 = 4\mathcal{O}_K + 2\beta\mathcal{O}_K + \beta^2\mathcal{O}_K$*. Como* $\beta^2 = \beta - 4$*, temos então* $\mathfrak{p}_1^2 = 4\mathcal{O}_K + 2\beta\mathcal{O}_K + (\beta - 4)\mathcal{O}_K$*. É claro que* $4\mathcal{O}_K + (\beta - 4)\mathcal{O}_K = 4\mathcal{O}_K + \beta\mathcal{O}_K$*, e portanto* $\mathfrak{p}_1^2 = 4\mathcal{O}_K + 2\beta\mathcal{O}_K + \beta\mathcal{O}_K = 4\mathcal{O}_K + \beta\mathcal{O}_K$*.*

Como $\mathfrak{N}(\mathfrak{p}_1^2) = 2^2 = 4$*, buscamos agora por* $a, b \in \mathbb{Z}$ *tais que* $a^2 + ab + 4b^2 = \pm 4$*. Vemos que* $(a, b) = (0, 1)$ *é uma solução, e que* $\alpha = \beta \in \mathfrak{p}_1^2$*. Assim,* $\mathfrak{p}_1^2 = \beta\mathcal{O}_K$ *é principal, o que mostra que* $[\mathfrak{p}_1] = [\mathfrak{p}_2]$*. Concluímos que* $h_K = 2$*.*

Para $d = 17$*, buscamos* $a, b \in \mathbb{Z}$ *tais que* $a^2 + ab - 4b^2 = \pm 2$*. Vemos que* $(a, b) = (1, 1)$ *é uma solução, e que* $\alpha = 1 + \frac{1+\sqrt{17}}{2} = 2 + \frac{\sqrt{17}-1}{2} \in 2\mathcal{O}_K + \frac{\sqrt{17}-1}{2}\,\mathcal{O}_K = \mathfrak{p}_2$*. Assim,* $\mathfrak{p}_2$ *é principal, e portanto* $\mathfrak{p}_1$ *também o é. Concluímos que* $h_K = 1$*, de modo que* $\mathcal{O}_K$ *é um DIP nesse caso.*

Para $d = 33$*, buscamos* $a, b \in \mathbb{Z}$ *tais que* $a^2 + ab - 8b^2 = \pm 2$*. Vemos que* $(a, b) = (2, 1)$ *é uma solução, e que* $\alpha = 2 + \frac{1+\sqrt{33}}{2} \in 2\mathcal{O}_K + \frac{\sqrt{33}+1}{2}\,\mathcal{O}_K = \mathfrak{p}_1$*. Assim,* $\mathfrak{p}_1$ *é principal, e portanto* $\mathfrak{p}_2$ *também o é. Concluímos que* $h_K = 1$*, de modo que* $\mathcal{O}_K$ *é um DIP nesse caso.*

Assim, vemos que $h_K = 1$ *para* $d = -19, -11, 6, 7, 17, 21, 29, 33$ *e* $h_K = 2$ *para* $d = -15, -5$*.*

Para finalizar a seção, mostraremos como a teoria que desenvolvemos pode ser utilizada para resolver uma equação diofantina concreta:

Exemplo 4.12. *Na introdução, falamos sobre como a Teoria Algébrica dos Números aparece naturalmente no estudo das equações diofantinas. Caso o anel de inteiros algébricos necessário para resolver uma equação diofantina não seja um DFU, entretanto, não está claro como devemos prosseguir. Como já vimos,* $\mathbb{Z}[\sqrt{-5}]$ *não é um DFU. No entanto, veremos como resolver a equação diofantina* $y^3 = x^2 + 5$ *utilizando este anel. Este exemplo se encontra em [5]. Como vimos no exemplo acima,* $h_K = 2$ *para* $K = \mathbb{Q}(\sqrt{-5})$*. Além disso, pelo item* (c) *do Teorema 2.21,* $\mathbb{Z}[\sqrt{-5}]^\times = \{1, -1\}$*.*

Consideremos a equação diofantina $y^3 = x^2 + 5$*. Se* x *fosse ímpar, nós obteríamos que* $y^3 \equiv 1 + 5 = 6 \pmod 8$*, o que não é possível. Logo* x *é par, e portanto* y *é ímpar. Se* $y \equiv 0 \pmod 5$*, então* $x^2 \equiv 0 \pmod 5$*, logo* $x \equiv 0 \pmod 5$*. Mas então* $5 \equiv x^2 + 5 = y^3 \equiv 0 \pmod{25}$*, absurdo! Logo* $y \not\equiv 0 \pmod 5$*.*

Em $\mathbb{Z}[\sqrt{-5}]$*, temos* $y^3 = (x + \sqrt{-5})(x - \sqrt{-5})$*. Denotemos* $\mathfrak{a} := \langle x + \sqrt{-5}\rangle$ *e* $\mathfrak{b} := \langle x - \sqrt{-5}\rangle$*. Então temos a igualdade de ideais* $\langle y\rangle^3 = \langle x + \sqrt{-5}\rangle\langle x - \sqrt{-5}\rangle = \mathfrak{a}\mathfrak{b}$*. Suponhamos que exista um ideal primo não-nulo* $\mathfrak{p} \lhd \mathcal{O}_K$ *que divide* $\mathfrak{a}$ *e* $\mathfrak{b}$*. Então* $\mathfrak{p} \ni (x + \sqrt{-5}) - (x - \sqrt{-5}) = 2\sqrt{-5}$*. Assim,* $\mathfrak{p}$ *divide* $\langle 2\sqrt{-5}\rangle = \langle 2\rangle\langle\sqrt{-5}\rangle$*. É simples verificar*[1] *que* $\langle 2\rangle = \langle 2, \sqrt{-5} - 1\rangle^2$*, e pela multiplicatividade da norma de ideais e pelo Teorema 4.1 temos*

$$\mathfrak{N}(\langle 2, \sqrt{-5} - 1\rangle)^2 = \mathfrak{N}(\langle 2\rangle) = |N(2)| = |2^2| = 4 \Rightarrow \mathfrak{N}(\langle 2, \sqrt{-5} - 1\rangle) = 2,$$

que é um número primo, logo pelo item (b) *do Corolário 4.4 o ideal* $\langle 2, \sqrt{-5} - 1\rangle$ *é primo.*

[1] Alternativamente, podemos utilizar os resultados da Seção 5.2 no que segue.

Além disso, $\mathfrak{N}(\langle\sqrt{-5}\rangle) = |N(\sqrt{-5})| = 5$*, logo pelo mesmo corolário o ideal* $\langle\sqrt{-5}\rangle$ *é primo. Assim, temos a fatoração em ideais primos:*

$$\langle 2\sqrt{-5}\rangle = \langle 2, \sqrt{-5}-1\rangle^2\langle\sqrt{-5}\rangle.$$

Logo $\mathfrak{p} = \langle 2, \sqrt{-5}-1\rangle$ *ou* $\mathfrak{p} = \langle\sqrt{-5}\rangle$*. Se* $\mathfrak{p} = \langle 2, \sqrt{-5}-1\rangle$*, então*

$$\mathfrak{p} \mid \langle y\rangle \Rightarrow 2 = \mathfrak{N}(\mathfrak{p}) \mid \mathfrak{N}(\langle y\rangle) = |N(y)| = y^2.$$

Mas y *é ímpar, absurdo! Se* $\mathfrak{p} = \langle\sqrt{-5}\rangle$*, temos*

$$\mathfrak{p} \mid \langle y\rangle \Rightarrow 5 = \mathfrak{N}(\mathfrak{p}) \mid \mathfrak{N}(\langle y\rangle) = |N(y)| = y^2.$$

Mas y *não é múltiplo de* 5*, absurdo! Isso mostra que os ideais* $\mathfrak{a}$ *e* $\mathfrak{b}$ *são primos entre si. Assim, como* $\langle y\rangle^3 = \mathfrak{ab}$*, existem ideais* $\mathfrak{c}$ *e* $\mathfrak{d}$ *de* $\mathbb{Z}[\sqrt{-5}]$ *tais que* $\mathfrak{a} = \mathfrak{c}^3$ *e* $\mathfrak{b} = \mathfrak{d}^3$*. Pelo Corolário 4.10,* $[\mathfrak{c}^2] = [1]$*, logo como* $\mathfrak{a}$ *é principal:*

$$\mathfrak{a} = \mathfrak{c}^3 \Rightarrow [1] = [\mathfrak{a}] = [\mathfrak{c}]^3 = [\mathfrak{c}]^2[\mathfrak{c}] = [1][\mathfrak{c}] = [\mathfrak{c}].$$

Isso mostra que $\mathfrak{c}$ *é principal. Então existem* $a, b \in \mathbb{Z}$ *tais que* $\mathfrak{c} = \langle a + b\sqrt{-5}\rangle$*, ou seja,*

$$\langle x + \sqrt{-5}\rangle = \mathfrak{a} = \mathfrak{c}^3 = \langle a + b\sqrt{-5}\rangle^3.$$

Assim, os elementos $x + \sqrt{-5}$ *e* $(a + b\sqrt{-5})^3$ *são associados. Como* $\mathbb{Z}[\sqrt{-5}]^\times = \{1, -1\}$*, temos:*

$$x + \sqrt{-5} = \pm(a + b\sqrt{-5})^3 = \pm((a^3 - 15ab^2) + (3a^2b - 5b^3)\sqrt{-5}).$$

Então

$$\pm 1 = 3a^2b - 5b^3 = b(3a^2 - 5b^2) \Rightarrow |b| = |3a^2 - 5b^2| = 1.$$

Assim, $b = \pm 1$*, e devemos ter:*

$$3a^2 - 5 = \pm 1 \Rightarrow 3a^2 = 6 \text{ ou } 3a^2 = 4,$$

o que é impossível. Portanto, a equação $y^3 = x^2 + 5$ *não tem soluções inteiras.*

4.3. Extensões de Ideais Primos em Domínios de Dedekind

Seja A um domínio de Dedekind com corpo de frações $K = Q(A)$. Seja L uma extensão finita e separável de K de grau n, e seja $B = \overline{A}^L$. Então B também é um domínio de Dedekind, pelo Teorema 3.1. Fixemos um ideal primo não-nulo $\mathfrak{p} \lhd A$. Então $\mathfrak{p}\,B \lhd B$ admite uma fatoração única em ideais primos de B, digamos $\mathfrak{p}\,B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. Essa fatoração se relaciona diretamente com os ideais que estão sobre $\mathfrak{p}$. De fato:

Proposição 4.13. *Nas condições acima, nós temos:*

(a) $g \geq 1$.

(b) $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ *são exatamente os ideais primos sobre* $\mathfrak{p}$.

(c) O conjunto dos ideais de B *sobre* $\mathfrak{p}$ *é igual ao conjunto de divisores de* $\mathfrak{p}\,B$ *diferentes de* B.

Demonstração. (a) Como essa extensão é integral, pelo Corolário 1.56 temos $\mathfrak{p}B \cap A = \mathfrak{p}$. Se $g = 0$, então $\mathfrak{p}B = B$. Assim, $\mathfrak{p} = \mathfrak{p}B \cap A = B \cap A = A$, um absurdo! Isso mostra que $g \geq 1$.

(b) Segue diretamente de (a) e (c).

(c) Seja $\mathfrak{A} \lhd B$ um ideal sobre $\mathfrak{p}$. Pelo Corolário 1.56, nós temos $\mathfrak{A} \supseteq \mathfrak{p}B$, o que implica em $\mathfrak{A} \mid \mathfrak{p}B$ pelo Corolário 3.14. Suponhamos agora que $\mathfrak{A} \lhd B$ seja um divisor de $\mathfrak{p}B$ diferente de B. Então, pelo Corolário 3.14, temos $\mathfrak{A} \supseteq \mathfrak{p}B$, e portanto $A \supsetneq \mathfrak{A} \cap A \supseteq \mathfrak{p}B \cap A = \mathfrak{p}$. Como $\mathfrak{p}$ é maximal, temos $\mathfrak{A} \cap A = \mathfrak{p}$, como desejado.

□

Notemos que, dado $\mathfrak{A} \lhd B$ sobre um ideal primo $\mathfrak{p} \lhd A$, o anel quociente $B/\mathfrak{A}$ pode ser considerado tanto como A-módulo quanto como $A/\mathfrak{p}$-espaço, já que $\mathfrak{p}B \subseteq \mathfrak{A} \Rightarrow \mathfrak{p}$ anula $B/\mathfrak{A}$. O $A/\mathfrak{p}$-espaço $B/\mathfrak{A}$ tem sempre dimensão finita:

Proposição 4.14. *Para todo ideal $\mathfrak{A} \lhd B$ sobre $\mathfrak{p}$, $B/\mathfrak{A}$ é um $A/\mathfrak{p}$-espaço vetorial de dimensão finita.*

Demonstração. B é um A-módulo finitamente gerado pelo Teorema 1.37. Assim, é claro que $B/\mathfrak{A}$ é finitamente gerado sobre $A/\mathfrak{p}$, sendo portanto um $A/\mathfrak{p}$-espaço de dimensão finita. □

Definição (Número de Decomposição/Índice de Ramificação/Grau de Inércia)**.** Seja $\mathfrak{p} \lhd A$ primo. Definimos o **número de decomposição** g de $\mathfrak{p}$ em B (ou em K) como sendo igual à quantidade de primos de B sobre $\mathfrak{p}$. Sendo $\mathfrak{P} \mid \mathfrak{p}$ primo, podemos denotar ainda $g = g(\mathfrak{P} \mid \mathfrak{p}) = g_{\mathfrak{p}}$.

Para cada $\mathfrak{P} \lhd B$ primo não-nulo, definimos o **índice de ramificação** de $\mathfrak{P}$ como o maior inteiro $e(\mathfrak{P} \mid \mathfrak{p})$ tal que $\mathfrak{P}^e$ divide $\mathfrak{p}B$. Também denotamos $e(\mathfrak{P} \mid \mathfrak{p}) = e_{\mathfrak{P}}$, se $\mathfrak{p}$ estiver claro.

Além disso, se $\mathfrak{P} \mid \mathfrak{p}$, definimos o **grau de inércia** $f(\mathfrak{P} \mid \mathfrak{p})$ de $\mathfrak{P}$ como sendo o inteiro positivo $[B/\mathfrak{P} : A/\mathfrak{p}]$. Se $\mathfrak{P}$ não estiver sobre $\mathfrak{p}$, definiremos $f(\mathfrak{P} \mid \mathfrak{p}) = 0$. Também denotamos $f(\mathfrak{P} \mid \mathfrak{p}) = f_{\mathfrak{P}}$, se $\mathfrak{p}$ estiver claro.

Notemos que, das definições acima, nós temos $\mathfrak{p}B = \prod_{\mathfrak{P}} \mathfrak{P}^{e_{\mathfrak{P}}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$, onde $\mathfrak{P}$ varia entre os primos não-nulos de B. O índice de ramificação e o grau de inércia são multiplicativos:

Proposição 4.15. *Sejam C/B e B/A extensões integrais de domínios de Dedekind, e sejam $\mathfrak{p} \lhd A$, $\mathfrak{P}' \lhd B$ e $\mathfrak{P} \lhd C$ primos não-nulos. Então temos $e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P} \mid \mathfrak{P}') \cdot e(\mathfrak{P}' \mid \mathfrak{p})$ e $f(\mathfrak{P} \mid \mathfrak{p}) = f(\mathfrak{P} \mid \mathfrak{P}') \cdot f(\mathfrak{P}' \mid \mathfrak{p})$.*

Demonstração. Podemos supor que $\mathfrak{P} \mid \mathfrak{P}'$ e $\mathfrak{P}' \mid \mathfrak{p}$, pois caso contrário ambas as igualdades se reduzirão a $0 = 0$. A multiplicatividade do grau de inércia segue da multiplicatividade dos graus de extensão de corpos: $[C/\mathfrak{P} : A/\mathfrak{p}] = [C/\mathfrak{P} : B/\mathfrak{P}'][B/\mathfrak{P}' : A/\mathfrak{p}]$. Para a multiplicatividade do índice de ramificação, escrevamos $\mathfrak{p}B = \mathfrak{P}'^{e(\mathfrak{P}'|\mathfrak{p})}\mathfrak{A}'$, para $\mathfrak{P}' \nmid \mathfrak{A}'$, e $\mathfrak{P}'C = \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{P}')}\mathfrak{A}$, para $\mathfrak{P} \nmid \mathfrak{A}$. Então nós temos:

$$\mathfrak{p}C = (\mathfrak{p}B)C = (\mathfrak{P}'^{e(\mathfrak{P}'|\mathfrak{p})}\mathfrak{A}')C = (\mathfrak{P}'C)^{e(\mathfrak{P}'|\mathfrak{p})}(\mathfrak{A}'C) = \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{P}')e(\mathfrak{P}'|\mathfrak{p})}\mathfrak{A}^{e(\mathfrak{P}'|\mathfrak{p})}(\mathfrak{A}'C).$$

Agora, $\mathfrak{P} \nmid \mathfrak{A}$, e como $\mathfrak{P}' \nmid \mathfrak{A}'$ vemos que $\mathfrak{P}'C$ e $\mathfrak{A}'C$ são coprimos devido ao item (l) da Proposição 1.46. Mas $\mathfrak{P} \mid \mathfrak{P}'C$, o que mostra que $\mathfrak{P} \nmid \mathfrak{A}'C$. Portanto, ambos $\mathfrak{A}$ e $\mathfrak{A}'C$ não são múltiplos de $\mathfrak{P}$, e concluímos que $e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P} \mid \mathfrak{P}')e(\mathfrak{P}' \mid \mathfrak{p})$, como queríamos. □

Nosso próximo objetivo é mostrar que vale a **identidade fundamental**, uma generalização da identidade fundamental vista na Seção 4.1. A identidade fundamental no caso mais geral afirma que, para todo primo não-nulo $\mathfrak{p} \lhd A$, temos $\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} = n = [L : K]$. Naquele caso particular, utilizamos propriedades da norma de ideais para obter o resultado desejado. Aqui, adotaremos outra estratégia. Comecemos mostrando que o grau de inércia, o índice de ramificação e o número de decomposição são invariantes por localização:

Proposição 4.16. *Sejam S um conjunto multiplicativo de A e $\mathfrak{p} \lhd A$ um ideal primo não-nulo que não intersecta S. Então, sendo $\mathfrak{p}\,B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ a fatoração prima de $\mathfrak{p}\,B$ em B, temos:*

$$(S^{-1}\,\mathfrak{p}) \cdot S^{-1}B = S^{-1}(\mathfrak{p}\,B) = (S^{-1}\mathfrak{P}_1)^{e_1} \cdots (S^{-1}\mathfrak{P}_g)^{e_g}.$$

Em particular, dado $\mathfrak{P} \mid \mathfrak{p}$ primo, $g(\mathfrak{P} \mid \mathfrak{p}) = g(S^{-1}\mathfrak{P} \mid S^{-1}\,\mathfrak{p})$ e $e(\mathfrak{P} \mid \mathfrak{p}) = e(S^{-1}\mathfrak{P} \mid S^{-1}\,\mathfrak{p})$. Além disso, dado $\mathfrak{P} \mid \mathfrak{p}$, temos $B/\mathfrak{P} \cong S^{-1}B/S^{-1}\mathfrak{P}$ canonicamente, e esse isomorfismo restrito a $A/\,\mathfrak{p}$ induz um isomorfismo $A/\,\mathfrak{p} \cong S^{-1}A/S^{-1}\,\mathfrak{p}$. Em particular, $f(\mathfrak{P} \mid \mathfrak{p}) = f(S^{-1}\mathfrak{P} \mid S^{-1}\,\mathfrak{p})$.

Demonstração. A primeira parte segue diretamente da Proposição 3.24, enquanto a segunda parte segue diretamente do Corolário 1.49, já que $\mathfrak{P} \lhd B$ é maximal. □

Finalmente, provemos a identidade fundamental:

Teorema 4.17. *(Identidade Fundamental) Sejam A um domínio de Dedekind, $K = Q(A)$, L uma extensão finita e separável de K de grau n e $B = \overline{A}^L$. Seja $\mathfrak{p} \lhd A$ um primo não-nulo e sejam $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ os ideais primos de B sobre $\mathfrak{p}$. Então temos:*

$$\sum_{j=1}^{g} e(\mathfrak{P}_j \mid \mathfrak{p}) f(\mathfrak{P}_j \mid \mathfrak{p}) = \dim_{A/\,\mathfrak{p}} B/(\mathfrak{p}\,B) = n.$$

Demonstração. Denotemos, para $1 \leq j \leq g$, $e_j := e(\mathfrak{P}_j \mid \mathfrak{p})$ e $f_j := f(\mathfrak{P}_j \mid \mathfrak{p})$. Então sabemos que $\mathfrak{p}\,B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ é a fatoração prima de $\mathfrak{p}\,B$ em B. A prova de que $\sum_{j=1}^{g} e_j f_j = \dim_{A/\,\mathfrak{p}} B/(\mathfrak{p}\,B)$ é parecida com a do Teorema 4.3: seja $\mathfrak{A} \lhd B$ tal que $\mathfrak{A} \mid \mathfrak{p}\,B$, e seja $1 \leq j \leq g$ tal que o ideal $\mathfrak{A}\,\mathfrak{P}_j \lhd B$ esteja sobre $\mathfrak{p}$. Notemos que $\mathfrak{A}\,/\,\mathfrak{A}\,\mathfrak{P}_j$ é um $B/\mathfrak{P}_j$-espaço vetorial de dimensão 1, devido ao Corolário 3.15. Desse modo, como $B/\mathfrak{P}_j$ é um $A/\,\mathfrak{p}$-espaço de dimensão f_j, $\mathfrak{A}\,/\,\mathfrak{A}\,\mathfrak{P}_j$ também é um $A/\,\mathfrak{p}$-espaço vetorial de dimensão f_j. Agora, $B/\,\mathfrak{A} \cong (B/\,\mathfrak{A}\,\mathfrak{P}_j)/(\mathfrak{A}\,/\,\mathfrak{A}\,\mathfrak{P}_j)$, e portanto

$$\dim_{A/\,\mathfrak{p}} B/\,\mathfrak{A}\,\mathfrak{P}_j = \dim_{A/\,\mathfrak{p}} B/\,\mathfrak{A} + \dim_{A/\,\mathfrak{p}} \mathfrak{A}\,/\,\mathfrak{A}\,\mathfrak{P}_j = \dim_{A/\,\mathfrak{p}} B/\,\mathfrak{A} + f_j.$$

Finalmente, vemos que para obter $\dim_{A/\,\mathfrak{p}} B/\,\mathfrak{p}\,B$ basta começar com $\mathfrak{A} = B$ e repetir esse processo e_j vezes para cada $\mathfrak{P}_j$, para $1 \leq j \leq g$, para obter:

$$\begin{aligned}
\dim_{A/\,\mathfrak{p}} B/\,\mathfrak{p}\,B &= \dim_{A/\,\mathfrak{p}} B/(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g - 1}) + f_g \\
&= \dim_{A/\,\mathfrak{p}} B/(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g - 2}) + 2f_g \\
&= \cdots \\
&= \dim_{A/\,\mathfrak{p}} B/(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_{g-1}^{e_{g-1}}) + e_g f_g \\
&= \cdots \\
&= \dim_{A/\,\mathfrak{p}} B/\mathfrak{P}_1 + (e_1 - 1)f_1 + \cdots + e_g f_g \\
&= e_1 f_1 + \cdots + e_g f_g \\
&= \sum_{j=1}^{g} e_j f_j.
\end{aligned}$$

Provaremos agora que $\dim_{A/\,\mathfrak{p}} B/\,\mathfrak{p}\,B = n$. Nós sabemos que $B = \overline{A}^L$ tem posto n, pelo Teorema 1.39. Observe que não necessariamente B é um A-módulo livre, pois A pode não ser um DIP. Assumiremos inicialmente que B seja um A-módulo livre, com uma base $\{\beta_1, \ldots, \beta_n\}$. Seja $\pi\colon B \to B/\,\mathfrak{p}\,B$ a projeção canônica. Então é claro que $\pi\beta_1, \ldots, \pi\beta_n$ geram $B/\,\mathfrak{p}\,B$ como $A/\,\mathfrak{p}$-espaço. Mostraremos que esses elementos também são linearmente independentes, o que provará que $\dim_{A/\,\mathfrak{p}} B/\,\mathfrak{p}\,B = n$. Suponhamos que $a_1, \ldots, a_n \in A$ sejam tais que $\sum_{j=1}^{n} \pi a_j \cdot \pi\beta_j = 0$. Isso significa que $\sum_{j=1}^{n} a_j\beta_j \in \mathfrak{p}\,B$, e portanto temos $\sum_{j=1}^{n} a_j\beta_j = \sum_{k=1}^{m} p_k b_k$, para alguns

$p_1, \ldots, p_m \in \mathfrak{p}$ e $b_1, \ldots, b_m \in B$. Como $\beta_1, \ldots, \beta_n$ geram B nós podemos, para $1 \leq k \leq m$, escrever $b_k = \sum_{j=1}^{n} c_{kj}\beta_j$, onde cada $c_{kj} \in A$. Desse modo:

$$\sum_{j=1}^{n} a_j\beta_j = \sum_{k=1}^{m} p_k b_k = \sum_{k=1}^{m} p_k \left(\sum_{j=1}^{n} c_{kj}\beta_j \right) = \sum_{j=1}^{n} \left(\sum_{k=1}^{m} p_k c_{kj} \right) \beta_j.$$

Como o conjunto $\{\beta_1, \ldots, \beta_n\}$ é linearmente independente, concluímos que para $1 \leq j \leq n$ nós temos $a_j = \sum_{k=1}^{m} p_k c_{kj} \in \mathfrak{p}$, e portanto cada $\pi a_j = 0$, mostrando a independência linear dos $\pi\beta_j$.

Suponhamos agora que B não seja necessariamente um A-módulo livre. Localizemos por $S = A \setminus \mathfrak{p}$. Então $K = Q(A_\mathfrak{p})$, $L = Q(B_\mathfrak{p})$ e $\overline{A_\mathfrak{p}}^L = (\overline{A}^L)_\mathfrak{p} = B_\mathfrak{p}$. Pelo Teorema 3.30, o anel $A_\mathfrak{p}$ é um DIP, e portanto $B_\mathfrak{p}$ é um $A_\mathfrak{p}$-módulo livre pelo Teorema 1.39. Assim, podemos aplicar o que acabamos de provar ao ideal $(\mathfrak{p}\,B)_\mathfrak{p}$. Finalmente:

$$n = \dim_{A_\mathfrak{p}/\,\mathfrak{p}_\mathfrak{p}} B_\mathfrak{p}/(\mathfrak{p}\,B)_\mathfrak{p} = \sum_{j=1}^{g((\mathfrak{P}_j)_\mathfrak{p} \mid \mathfrak{p}_\mathfrak{p})} e_j((\mathfrak{P}_j)_\mathfrak{p} \mid \mathfrak{p}_\mathfrak{p}) f((\mathfrak{P}_j)_\mathfrak{p} \mid \mathfrak{p}_\mathfrak{p}) = \sum_{j=1}^{g} e_j f_j,$$

onde na última igualdade utilizamos a proposição acima. □

A partir da identidade fundamental, conseguimos dividir a decomposição de um ideal primo de A em primos de B em alguns casos especiais:

Definição (Tipos de Decomposição)**.** Seja $\mathfrak{p} \lhd A$ primo. Então dizemos que $\mathfrak{p}$ é:

- **Decomposto** em L (ou B) quando $g \geq 2$, e **não-decomposto** em L (ou B) quando $g = 1$.
- **Ramificado** em L (ou B) quando existir um primo $\mathfrak{P} \mid \mathfrak{p}$ tal que $e(\mathfrak{P} \mid \mathfrak{p}) > 1$ ou quando a extensão $(B/\mathfrak{P})/(A/\,\mathfrak{p})$ for inseparável.
- **Totalmente decomposto** em L (ou B) quando $g = n$, ou seja, $e(\mathfrak{P} \mid \mathfrak{p}) = f(\mathfrak{P} \mid \mathfrak{p}) = 1$ para todo ideal primo $\mathfrak{P} \mid \mathfrak{p}$. Nesse caso, a decomposição de $\mathfrak{p}\,B$ é da forma $\mathfrak{P}_1 \cdots \mathfrak{P}_n$.
- **Totalmente inerte** em L (ou B) quando $f(\mathfrak{P} \mid \mathfrak{p}) = n$ para algum primo $\mathfrak{P} \mid \mathfrak{p}$. Nesse caso, $g = 1$ e $e(\mathfrak{P} \mid \mathfrak{p}) = 1$, e portanto $\mathfrak{p}\,B = \mathfrak{P}$ é o único ideal de B sobre $\mathfrak{p}$.
- **Totalmente ramificado** em L (ou B) quando $e(\mathfrak{P} \mid \mathfrak{p}) = n$ para algum primo $\mathfrak{P} \mid \mathfrak{p}$. Nesse caso, $g = 1$ e $f(\mathfrak{P} \mid \mathfrak{p}) = 1$, e portanto $\mathfrak{p}\,B = \mathfrak{P}^n$.

Além disso, dizemos que uma extensão de corpos L/K é **ramificada** se existir algum primo $\mathfrak{p} \lhd A$ ramificado em B, e dizemos que L/K é **não-ramificada** caso contrário.

No caso em que $A = \mathbb{Z}$, $B = \mathcal{O}_L$ e $\mathfrak{p} = p\mathbb{Z}$, para $p \in \mathbb{N}$ primo, diremos simplesmente que p é decomposto, ramificado, etc. para indicar que o ideal $p\mathbb{Z}$ é decomposto, ramificado, etc.

Observação 4.18. *Notemos que caso $n = 2$, pela identidade fundamental, todo $\mathfrak{p} \lhd A$ será totalmente decomposto, totalmente inerte ou totalmente ramificado. Além disso, observemos que $B/\mathfrak{P}$ sempre será uma extensão separável de $A/\,\mathfrak{p}$ se $A/\,\mathfrak{p}$ for perfeito, como é o caso se A for um corpo de números algébricos (já que nessas condições vale que $|A/\,\mathfrak{p}| = \mathfrak{N}(\mathfrak{p}) < \infty$).*

Exemplo 4.19. *Na extensão $\mathbb{Z}[i]/\,\mathbb{Z}$, os primos $p \in \mathbb{N}$ totalmente decompostos em $\mathbb{Z}[i]$ são aqueles com $p \equiv 1 \pmod 4$, os primos totalmente inertes são aqueles com $p \equiv 3 \pmod 4$ e o único primo totalmente ramificado é 2.*

Outra convenção que utilizaremos é a de chamar um primo $\mathfrak{p} \lhd A$ de "primo de K", e um primo $\mathfrak{P} \lhd B$ de "primo de L".

4.4. Fatorando Ideais Primos

Sejam A um domínio de Dedekind com corpo de frações $K = Q(A)$. Seja L uma extensão finita e separável de K de grau n, e seja $B = \overline{A}^L$. Nessa seção mostraremos que, dado um ideal $\mathfrak{p} \lhd A$ coprimo com um certo ideal de A, nós temos uma fórmula para calcular a fatoração de $\mathfrak{p}\,B$ em ideais primos de B. Em particular, caso B seja **monogêneo** sobre A, ou seja, se $B = A[\gamma]$ para algum $\gamma \in B$, então essa fórmula valerá para todos os ideais de A. Começamos com a seguinte definição:

Definição (Condutor)**.** Dados dois anéis $R \subseteq S$, nós chamamos de **condutor** de R em S o conjunto $\mathfrak{f} := \{x \in R \colon xS \subseteq R\}$.

É fácil ver da definição acima que o condutor $\mathfrak{f}$ de R em S é o maior ideal de S contido em R, e que esse é também um ideal de R. Além disso, notemos que $\mathfrak{f} = S$ se e somente se $1 \in \mathfrak{f}$, ou seja, se e só se $S \subseteq R \iff R = S$. Assim, se $R \subsetneq S$ então $\mathfrak{f}$ é um ideal próprio de S.

Similarmente à definição de ordem que demos para um anel de inteiros algébricos, temos:

Definição (Ordem de uma Extensão de Anéis)**.** Um anel R com $A \subseteq R \subseteq B$ é chamado de **ordem** de L/K se R contiver uma base $\{r_1, \ldots, r_n\}$ da extensão L/K, ou equivalentemente se R for um A-módulo de posto n ou se $Q(R) = L$. Uma ordem R será chamada de **principal** se for da forma $R = A[\gamma]$, para algum $\gamma \in B$.

Proposição 4.20. *Seja R uma ordem da extensão L/K. Consideremos o condutor $\mathfrak{f}$ de R em B. Então $\mathfrak{f} \neq 0$.*

Demonstração. Sabemos que B é um A-módulo finitamente gerado. Sejam $b_1, \ldots, b_m \in B$ para os quais $B = Ab_1 + \cdots + Ab_m$. Por hipótese, existem $r_1, \ldots, r_n \in R$ que formam uma base da extensão L/K. Assim nós podemos escrever, para $1 \leq i \leq m$, $b_i = \sum_{j=1}^{n} \frac{a_{ij}}{s_{ij}} \cdot r_j$, onde cada $a_{ij} \in A$ e cada $s_{ij} \in A \setminus \{0\}$. Chamemos $s := \prod_{i=1}^{m} \prod_{j=1}^{n} s_{ij}$. Então $s \neq 0$ e s "limpa os denominadores" de todos os b_i, isto é, para todo $1 \leq i \leq m$ vemos que sb_i é uma combinação linear dos r_j's com coeficientes em A, e portanto $sb_i \in R$. Como todo elemento de B é combinação linear dos b_i's com coeficientes em A, concluímos que $sB \subseteq R$. □

Com isso, nós conseguimos obter a fórmula desejada para a fatoração de um ideal primo de A em B.

Teorema 4.21. *Seja $\gamma \in B$ um elemento primitivo da extensão L/K, e consideremos o condutor $\mathfrak{f}$ de $A[\gamma]$ em B. Seja $\mathfrak{p} \lhd A$ um ideal primo tal que os ideais $\mathfrak{p}\,B$ e $\mathfrak{f}$ sejam primos entre si, isto é, $\mathfrak{p}\,B + \mathfrak{f} = B$. Denotemos $P = P_{\gamma,K}$, e sejam $P_1, \ldots, P_g \in A[x]$ polinômios mônicos tais que $\overline{P} = \overline{P}_1^{e_1} \cdots \overline{P}_g^{e_g}$ seja a fatoração prima de $\overline{P}$ em $(A/\mathfrak{p})[x]$. Então a fatoração de $\mathfrak{p}\,B$ em ideais primos distintos de B é $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, onde para $1 \leq j \leq g$ temos $\mathfrak{P}_j = \mathfrak{p}\,B + P_j(\gamma)B$. Assim, $e(\mathfrak{P}_j \mid \mathfrak{p}) = e_j$. Além disso, para $1 \leq j \leq g$ temos $f(\mathfrak{P}_j \mid \mathfrak{p}) = \partial\, P_j$.*

Demonstração. A ideia da demonstração é a seguinte cadeia de isomorfismos de anéis:

$$\frac{B}{\mathfrak{p}\,B} \cong \frac{A[\gamma]}{\mathfrak{p}\,A[\gamma]} \cong \frac{A[x]}{\langle P(x)\rangle + \mathfrak{p}\,A[x]} \cong \frac{(A/\mathfrak{p})[x]}{\langle \overline{P}(x)\rangle} \cong \prod_{j=1}^{g} \frac{(A/\mathfrak{p})[x]}{\langle \overline{P}_j(x)\rangle^{e_j}}.$$

- $\frac{B}{\mathfrak{p}\,B} \cong \frac{A[\gamma]}{\mathfrak{p}\,A[\gamma]}$ é um isomorfismo, dado por $a + \mathfrak{p}\,B \leftarrow\!\shortmid a + \mathfrak{p}\,A[\gamma]$: Por hipótese, sabemos que $\mathfrak{p}\,B + \mathfrak{f} = B$, e como $\mathfrak{f} \subseteq A[\gamma]$, nós temos $\mathfrak{p}\,B + A[\gamma] = B$, de modo que a restrição da projeção canônica $B \to B/\mathfrak{p}\,B$ a $A[\gamma]$ é sobrejetora. O núcleo dessa restrição é $\mathfrak{p}\,B \cap A[\gamma]$. Então basta provarmos que $\mathfrak{p}\,B \cap A[\gamma] = \mathfrak{p}\,A[\gamma]$. A inclusão ($\supseteq$) é clara. Para a outra inclusão, notemos que, como $\mathfrak{f}$ e $\mathfrak{p}\,B$ são coprimos, podemos escrever $\mathfrak{f} = \mathfrak{Q}_1 \cdots \mathfrak{Q}_m$ onde

$\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m$ são primos que não dividem $\mathfrak{p}\,B$, e portanto não estão sobre $\mathfrak{p}$. Sejam $\mathfrak{q}_1 := \mathfrak{Q}_1 \cap A, \ldots, \mathfrak{q}_m := \mathfrak{Q}_m \cap A$. Então $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ são ideais primos de A diferentes de $\mathfrak{p}$. Notemos agora que

$$\mathfrak{f} \cap A = (\mathfrak{Q}_1 \cdots \mathfrak{Q}_m) \cap A \supseteq (\mathfrak{Q}_1 \cap A) \cdots (\mathfrak{Q}_m \cap A) = \mathfrak{q}_1 \cdots \mathfrak{q}_m\,.$$

Então $\mathfrak{f} \cap A$ é um produto de ideais primos de A distintos de $\mathfrak{p}$, e portanto $\mathfrak{f} \cap A$ é primo com $\mathfrak{p}$, ou seja, $\mathfrak{p} + (\mathfrak{f} \cap A) = A$. Em particular, $1 \in \mathfrak{p} + \mathfrak{f}$. Desse modo:

$$\begin{aligned}
\mathfrak{p}\,B \cap A[\gamma] \subseteq (\mathfrak{p}+\mathfrak{f})(\mathfrak{p}\,B \cap A[\gamma]) &= \mathfrak{p}(\mathfrak{p}\,B \cap A[\gamma]) + \mathfrak{f}(\mathfrak{p}\,B \cap A[\gamma]) \\
&\subseteq \mathfrak{p}\,A[\gamma] + \mathfrak{p}\,B\mathfrak{f} \\
&= \mathfrak{p}\,A[\gamma] + \mathfrak{p}\,\mathfrak{f} \\
&\subseteq \mathfrak{p}\,A[\gamma] + \mathfrak{p}\,A[\gamma] \\
&= \mathfrak{p}\,A[\gamma],
\end{aligned}$$

mostrando a outra inclusão. Assim, temos o primeiro isomorfismo desejado.

- $\frac{A[\gamma]}{\mathfrak{p}\,A[\gamma]} \cong \frac{A[x]}{\langle P(x)\rangle + \mathfrak{p}\,A[x]}$ é um isomorfismo, dado por

$$f(\gamma) + \mathfrak{p}\,A[\gamma] \leftarrow\!\shortmid f(x) + (\langle P(x)\rangle + \mathfrak{p}\,A[x]).$$

  A verificação de que essa função é um isomorfismo é direta.

- $\frac{A[x]}{\langle P(x)\rangle + \mathfrak{p}\,A[x]} \cong \frac{(A/\mathfrak{p})[x]}{\overline{P}(x)}$ é um isomorfismo, dado por

$$f(x) + (\langle P(x)\rangle + \mathfrak{p}\,A[x]) \mapsto \overline{f}(x) + \langle \overline{P}(x)\rangle.$$

  A verificação de que essa função é um isomorfismo é direta.

- $\frac{(A/\mathfrak{p})[x]}{\langle \overline{P}(x)\rangle} \cong \prod_{j=1}^{g} \frac{(A/\mathfrak{p})[x]}{\langle \overline{P}_j(x)\rangle^{e_j}}$ é um isomorfismo, dado por

$$\overline{f}(x) + \langle \overline{P}(x)\rangle \mapsto (\overline{f}(x) + \langle \overline{P}_1(x)\rangle^{e_1}, \ldots, \overline{f}(x) + \langle \overline{P}_g(x)\rangle^{e_g}).$$

  Esse isomorfismo segue diretamente do Teorema Chinês dos Restos.

Denotemos $R := \frac{(A/\mathfrak{p})[x]}{\langle \overline{P}(x)\rangle}$ e, para $1 \le j \le g$, $R_j := \frac{(A/\mathfrak{p})[x]}{\langle \overline{P}_j(x)\rangle^{e_j}}$. Observemos que, para $1 \le j \le g$, os ideais primos de R_j correspondem aos ideais primos de $(A/\mathfrak{p})[x]$ que contêm $\langle \overline{P}_j(x)\rangle^{e_j}$, pelo Teorema da Correspondência. Como $A/\mathfrak{p}$ é um corpo, $(A/\mathfrak{p})[x]$ é um DIP, assim é fácil ver que o único ideal primo de $(A/\mathfrak{p})[x]$ que contém $\langle \overline{P}_j(x)\rangle^{e_j}$ é $\langle \overline{P}_j(x)\rangle$. Essa análise nos mostra que o único ideal primo de R_j é $\hat{\mathfrak{P}}_j := \langle \overline{P}_j(x)\rangle / \langle \overline{P}_j(x)\rangle^{e_j}$.

Assim, o anel produto $R_1 \times \cdots \times R_g$ possui exatamente g ideais primos, a saber os ideais $\tilde{\mathfrak{P}}_1, \ldots, \tilde{\mathfrak{P}}_g$, onde para $1 \le j \le g$ nós temos:

$$\tilde{\mathfrak{P}}_j := R_1 \times \cdots \times R_{j-1} \times \hat{\mathfrak{P}}_j \times R_{j+1} \times \cdots \times R_g.$$

Notemos que, dado um elemento $\overline{f}(x) + \langle \overline{P}(x)\rangle \in R$ qualquer, a imagem desse elemento em $R_1 \times \cdots \times R_g$ estará em $\tilde{\mathfrak{P}}_j$ se e só se $\overline{f}(x) + \langle \overline{P}_j(x)\rangle^{e_j} \in \hat{\mathfrak{P}}_j$, isto é, se e só se $\overline{f}(x) \in \langle \overline{P}_j(x)\rangle$. Isso nos diz que o ideal primo de R correspondente a $\tilde{P}_j$ é o ideal $\mathfrak{P}'_j := \langle \overline{P}_j(x)\rangle / \langle \overline{P}(x)\rangle$. Assim, o anel R tem exatamente g ideais primos não-nulos, a saber $\mathfrak{P}'_1 := \langle \overline{P}_1(x)\rangle / \langle \overline{P}(x)\rangle, \ldots, \mathfrak{P}'_g := \langle \overline{P}_g(x)\rangle / \langle \overline{P}(x)\rangle$.

Consideremos agora $\overline{f}(x) + \langle \overline{P}(x)\rangle \in R$. Ele é levado no elemento $f(x) + (\langle P(x)\rangle + \mathfrak{p}\,A[x]) \in \frac{A[x]}{\langle P(x)\rangle + \mathfrak{p}\,A[x]}$, que por sua vez é levado em $f(\gamma) + \mathfrak{p}\,A[\gamma] \in \frac{A[\gamma]}{\mathfrak{p}\,A[\gamma]}$, que é levado em $f(\gamma) + \mathfrak{p}\,B \in \frac{B}{\mathfrak{p}\,B}$.

Com isso, é fácil ver que cada ideal primo $\mathfrak{P}'_j$ de R é levado no ideal primo $P_j(\gamma)A[\gamma]/\mathfrak{p}\,B$ de $\frac{B}{\mathfrak{p}\,B}$. Isso mostra que o anel $\frac{B}{\mathfrak{p}\,B}$ tem exatamente g ideais primos não-nulos, a saber:

$$\overline{\mathfrak{P}}_1 \coloneqq P_1(\gamma)A[\gamma]/\mathfrak{p}\,B, \ldots, \overline{\mathfrak{P}}_g \coloneqq P_g(\gamma)A[\gamma]/\mathfrak{p}\,B.$$

Podemos utilizar o Teorema da Correspondência para concluir que os ideais primos de B que contêm $\mathfrak{p}\,B$ são exatamente os g ideais dados pelas pré-imagens dos $\overline{\mathfrak{P}}_j$'s pela projeção canônica $B \to B/\mathfrak{p}\,B$:

$$\mathfrak{P}_1 \coloneqq P_1(\gamma)A[\gamma] + \mathfrak{p}\,B, \ldots, \mathfrak{P}_g \coloneqq P_g(\gamma)A[\gamma] + \mathfrak{p}\,B.$$

Afirmamos que, para $1 \leq j \leq g$, nós temos $\mathfrak{P}_j = \mathfrak{p}\,B + P_j(\gamma)B$. A inclusão ($\subseteq$) é clara. Seja agora $p + P_j(\gamma)b$ qualquer, com $p \in \mathfrak{p}\,B$ e $b \in B$. Como $\mathfrak{p}\,B + A[\gamma] = B$, existem $q \in \mathfrak{p}\,B$, $a \in A[\gamma]$ tais que $b = q + a$. Assim:

$$p + P_j(\gamma)b = p + P_j(\gamma)(q + a) = (p + P_j(\gamma)q) + P_j(\gamma)a \in \mathfrak{p}\,B + P_j(\gamma)A[\gamma],$$

mostrando a inclusão inversa. Assim, o que fizemos até agora nos permite concluir que os ideais primos de B que contêm (e portanto que dividem) $\mathfrak{p}\,B$ são exatamente os g ideais:

$$\mathfrak{P}_1 \coloneqq \mathfrak{p}\,B + P_1(\gamma)B, \ldots, \mathfrak{P}_g \coloneqq \mathfrak{p}\,B + P_g(\gamma)B.$$

Notemos agora que $\tilde{\mathfrak{P}}_1^{e_1} \cdots \tilde{\mathfrak{P}}_g^{e_g} = 0$ em $R_1 \times \cdots \times R_g$, logo a partir dos isomorfismos indicados vemos que $\overline{\mathfrak{P}}_1^{e_1} \cdots \overline{\mathfrak{P}}_g^{e_g} = 0$ em $\frac{B}{\mathfrak{p}\,B}$, ou seja, que $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \subseteq \mathfrak{p}\,B$. Assim, temos $e_j \leq e(\mathfrak{P}_j \mid \mathfrak{p})$, para todo $1 \leq j \leq g$. Notemos agora que, para $1 \leq j \leq g$, nós temos um isomorfismo de $A/\mathfrak{p}$-espaços $\frac{B}{\mathfrak{P}_j} \cong \frac{B/\mathfrak{p}\,B}{\mathfrak{P}_j/\mathfrak{p}\,B}$. Como o isomorfismo $\frac{B}{\mathfrak{p}\,B} \cong \frac{(A/\mathfrak{p})[x]}{\langle \overline{P}(x)\rangle}$ leva $\overline{\mathfrak{P}_j} = \mathfrak{P}_j/\mathfrak{p}\,B$ em $\mathfrak{P}'_j = \langle \overline{P}_j(x)\rangle/\langle \overline{P}(x)\rangle$, nós temos:

$$\frac{B}{\mathfrak{P}_j} \cong \frac{B/\mathfrak{p}\,B}{\mathfrak{P}_j/\mathfrak{p}\,B} \cong \frac{(A/\mathfrak{p})[x]/\langle \overline{P}(x)\rangle}{\langle \overline{P}_j(x)\rangle/\langle \overline{P}(x)\rangle} \cong \frac{(A/\mathfrak{p})[x]}{\langle \overline{P}_j(x)\rangle}.$$

Como $\overline{P}_j(x)$ é um polinômio irredutível de $(A/\mathfrak{p})[x]$ temos que $(A/\mathfrak{p})[x]/\langle \overline{P}_j(x)\rangle$ é uma extensão de grau $\partial\,\overline{P}_j = \partial\,P_j$ de $A/\mathfrak{p}$. Isso mostra que $[B/\mathfrak{P}_j \colon A/\mathfrak{p}] = \partial\,P_j$, isto é, $f(\mathfrak{P}_j \mid \mathfrak{p}) = \partial\,P_j$. Agora, pela identidade fundamental:

$$n = \sum_{j=1}^{g} e(\mathfrak{P}_j \mid \mathfrak{p})\, f(\mathfrak{P}_j \mid \mathfrak{p}) \geq \sum_{j=1}^{g} e_j\ \partial\,P_j = \partial\,P = n.$$

Com isso, concluímos por fim que $e(\mathfrak{P}_j \mid \mathfrak{p}) = e_j$ para todo $1 \leq j \leq n$, o que termina a demonstração. □

Um caso particular importante é quando B é monogêneo sobre A:

Teorema 4.22. *Suponhamos que exista $\gamma \in B$ tal que $B = A[\gamma]$. Seja $\mathfrak{p} \lhd A$ primo não-nulo. Denotemos $P = P_{\gamma,K}$, e sejam $P_1, \ldots, P_g \in A[x]$ polinômios mônicos tais que $\overline{P} = \overline{P}_1^{e_1} \cdots \overline{P}_g^{e_g}$ seja a fatoração prima de $\overline{P}$ em $(A/\mathfrak{p})[x]$. Então a fatoração de $\mathfrak{p}\,B$ em ideais primos distintos de B é $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, onde para $1 \leq j \leq g$ temos $\mathfrak{P}_j = \mathfrak{p}\,B + P_j(\gamma)B$. Assim, $e(\mathfrak{P}_j \mid \mathfrak{p}) = e_j$. Além disso, para $1 \leq j \leq g$, $f(\mathfrak{P}_j \mid \mathfrak{p}) = \partial\,P_j$.*

Como consequência direta desse resultado, nós temos:

Corolário 4.23. *Supondo $B = A[\gamma]$:*

(a) $\mathfrak{p}$ será totalmente decomposto em L se e só se $\overline{P}$ se fatorar em $(A/\mathfrak{p})[x]$ em fatores lineares distintos $x - \overline{a}_j \in (A/\mathfrak{p})[x]$, para $1 \leq j \leq n$. Nesse caso, $\mathfrak{p}\,B = \mathfrak{P}_1 \cdots \mathfrak{P}_n$, com cada $\mathfrak{P}_j$ igual a $\mathfrak{p}\,B + (\beta - a_j)B$.

(b) $\mathfrak{p}$ *será totalmente inerte em* L *se e só se* $\overline{P}$ *for irredutível em* $(A/\mathfrak{p})[x]$*. Nesse caso,* $\mathfrak{p}B \lhd B$ *é primo.*

(c) $\mathfrak{p}$ *será totalmente ramificado em* L *se e só se tivermos* $\overline{P} = (x-\overline{a})^n$ *para algum* $a \in A/\mathfrak{p}$*. Nesse caso,* $\mathfrak{p}B = (\mathfrak{p}B + (\beta - a)B)^n$*, e* $\mathfrak{p}B + (\beta - a)B$ *é o único ideal primo de* B *sobre* $\mathfrak{p}$*.*

Nesse contexto, temos um critério simples para verificar se um ideal primo é ramificado:

Corolário 4.24. *Supondo* $B = A[\gamma]$*, as seguintes condições são equivalentes:*

(i) $\mathfrak{p}$ *é ramificado em* L*.*

(ii) O polinômio $\overline{P} \in (A/\mathfrak{p})[x]$ *é inseparável.*

(iii) $\Delta(P) \in \mathfrak{p}$*.*

(iv) $\mathfrak{p} \mid \mathfrak{d}_{B/A}$

Em particular, se $A = \mathbb{Z}$*,* $B = \mathcal{O}_L$ *e* $\mathfrak{p} = p\mathbb{Z}$*, isso equivale a* $p \mid d_L$*.*

Demonstração. $(i) \iff (ii)$: Seja $\overline{P} = \overline{P}_1^{e_1} \cdots \overline{P}_g^{e_g}$ a fatoração prima de $\overline{P}$ em irredutíveis de $(A/\mathfrak{p})[x]$. O polinômio $\overline{P}$ é inseparável se e só se para algum $1 \leq j \leq g$ tivermos $e_j > 1$ ou $\overline{P}_j$ inseparável, o que equivale a termos $\mathfrak{p}$ ramificado em L devido ao Teorema 4.22 (note que pela demonstração que fizemos a extensão $(B/\mathfrak{P})/(A/\mathfrak{p})$ é isomorfa a $\frac{(A/\mathfrak{p})[x]}{\langle \overline{P}_j(x)\rangle}/(A/\mathfrak{p})$).

$(ii) \iff (iii)$: Como o discriminante de um polinômio de grau n é um polinômio simétrico com coeficientes inteiros nas suas raízes, existe $D \in \mathbb{Z}[x_1, \ldots, x_n]$ tal que:

$$\Delta(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n) = D(c_0, \ldots, c_{n-1}),$$

para todos $c_0, \ldots, c_{n-1}$ em algum corpo. Sejam $a_1, \ldots, a_n \in A$ tais que

$$P(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n.$$

Então nós temos que $\overline{P}(x) = (a_0 + \mathfrak{p}) + (a_1 + \mathfrak{p})x + \cdots + (a_{n-1} + \mathfrak{p})x^{n-1} + x^n$, e portanto

$$\Delta(\overline{P}) = D(a_0 + \mathfrak{p}, \ldots, a_{n-1} + \mathfrak{p}) = D(a_0, \ldots, a_{n-1}) + \mathfrak{p} = \Delta(P) + \mathfrak{p},$$

mostrando que $\Delta(\overline{P}) = 0 \iff \Delta(P) \in \mathfrak{p}$. Como $\Delta(\overline{P}) = 0$ equivale a $\overline{P}$ ser separável, temos a equivalência desejada.

$(iii) \iff (iv)$: Devido às proposições 1.43 e 1.33, temos $\mathfrak{d}_{B/A} = \Delta(1, \gamma, \ldots, \gamma^{n-1})A = \Delta(P)A$. Sendo assim, $\Delta(P) \in \mathfrak{p} \iff \mathfrak{d}_{B/A} \subseteq \mathfrak{p} \iff \mathfrak{p} \mid \mathfrak{d}_{B/A}$.

Finalmente, para o caso particular basta notar que $\mathfrak{d}_{\mathcal{O}_L/\mathbb{Z}} = d_L\mathbb{Z}$ pelo Teorema 2.7. □

No caso em que B não é monogênico sobre A nós podemos, utilizando localização, obter resultados semelhantes aos anteriores se nos restringirmos aos ideais primos não-nulos $\mathfrak{p} \lhd A$ tais que $\Delta(P) \notin \mathfrak{p}$:

Corolário 4.25. *Sejam* $\gamma \in B$ *elemento primitivo da extensão* L/K *e* $P = P_{\gamma,K}$*. Então, se* $\mathfrak{p} \lhd A$ *primo não-nulo for tal que* $\Delta(P) \notin \mathfrak{p}$*, nós temos:*

(a) $1, \gamma, \ldots, \gamma^{n-1}$ *formam uma base do* $A_\mathfrak{p}$*-módulo* $B_\mathfrak{p}$*.*

(b) $\mathfrak{p}$ *não é ramificado em* L*.*

(c) $\overline{P} \in (A/\mathfrak{p})[x]$ *é separável.*

(d) Sejam $P_1, \dots, P_g \in A[x]$ *irredutíveis mônicos tais que* $\overline{P} = \overline{P}_1 \cdots \overline{P}_g$. *Então valem as afirmações* (a) *e* (b) *do Teorema 4.22 com* $e_1 = \cdots = e_g = 1$.

Demonstração. (a) Nós temos $B_\mathfrak{p} = \overline{A_\mathfrak{p}}^L$ devido à Proposição 1.15. Pelo Teorema 3.30, $A_\mathfrak{p}$ é um DIP, e portanto por 1.39 $B_\mathfrak{p}$ é um $A_\mathfrak{p}$-módulo livre de posto n. Seja $\{\beta_1, \dots, \beta_n\}$ uma base de $B_\mathfrak{p}$ como $A_\mathfrak{p}$-módulo. Seja $M \in M_n(A_\mathfrak{p})$ a matriz que satisfaz

$$M \cdot \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^{n-1} \end{bmatrix}$$

Essa matriz existe já que $\beta_1, \dots, \beta_n$ formam uma base de $B_\mathfrak{p}$ e $1, \gamma, \dots, \gamma^{n-1} \in B_\mathfrak{p}$. Então nós temos $\Delta(P) = \Delta(1, \gamma, \dots, \gamma^{n-1}) = (\det M)^2 \Delta(\beta_1, \dots, \beta_n)$, devido às proposições 1.31 e 1.33. Mas $\Delta(P) \in A \setminus \mathfrak{p} \subseteq A_\mathfrak{p} \setminus \mathfrak{p}_\mathfrak{p} = A_\mathfrak{p}^\times$. Assim, a igualdade acima nos diz que temos $\det M \in A_\mathfrak{p}^\times$. Segue da Proposição 1.42 que $1, \gamma, \dots, \gamma^{n-1}$ formam uma base de $B_\mathfrak{p}$ como $A_\mathfrak{p}$-módulo, como desejávamos.

Observemos que como $L = K(\gamma)$ e $B_\mathfrak{p} = A_\mathfrak{p}[\gamma]$ pelo que acabamos de mostrar, podemos aplicar os resultados anteriores dessa seção.

(b) Como vimos, $\Delta(P) \notin \mathfrak{p}_\mathfrak{p}$. Desse modo, o Corolário 4.24 nos diz que $\mathfrak{p}_\mathfrak{p}$ não é ramificado em $B_\mathfrak{p}$. Mas isso significa que $\mathfrak{p}$ não é ramificado em B, pela Proposição 4.16.

(c) Também pelo Corolário 4.24, podemos concluir que o polinômio induzido por P no corpo $(A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p})[x]$ é separável. Mas $A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ é canonicamente isomorfo a $A/\mathfrak{p}$, devido ao Corolário 1.49. Desse modo, $\overline{P} \in (A/\mathfrak{p})[x]$ é separável.

(d) Com a identificação $(A/\mathfrak{p})[x] = (A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p})[x]$, o Teorema 4.22 nos diz que a fatoração de $\mathfrak{p}_\mathfrak{p} B_\mathfrak{p}$ em ideais primos de $B_\mathfrak{p}$ é $\mathfrak{Q}_1^{e_1} \cdots \mathfrak{Q}_g^{e_g}$, onde para $1 \le j \le g$ temos $\mathfrak{Q}_j = \mathfrak{p}_\mathfrak{p} B_\mathfrak{p} + P_j(\gamma) B_\mathfrak{p}$, de modo que $e(\mathfrak{Q}_j \mid \mathfrak{p}_\mathfrak{p}) = e_j$, e que além disso $f(\mathfrak{Q}_j \mid \mathfrak{p}_\mathfrak{p}) = \partial P_j$.

Seja $\mathfrak{p} B = \mathfrak{P}_1^{\ell_1} \cdots \mathfrak{P}_r^{\ell_r}$ a fatoração prima de $\mathfrak{p} B$ em B. Pela Proposição 4.16, temos então

$$(\mathfrak{P}_1)_\mathfrak{p}^{\ell_1} \cdots (\mathfrak{P}_r)_\mathfrak{p}^{\ell_r} = \mathfrak{p}_\mathfrak{p} B_\mathfrak{p} = \mathfrak{Q}_1^{e_1} \cdots \mathfrak{Q}_g^{e_g}\,.$$

Por unicidade, concluímos que $r = g$ e que os ideais primos e expoentes que aparecem são iguais a menos de ordenação. Assim, podemos supor que $\mathfrak{Q}_j = (\mathfrak{P}_j)_\mathfrak{p}$ e que $\ell_j = e_j$, para $1 \le j \le g$. Isso já nos garante que $e(\mathfrak{P}_j \mid \mathfrak{p}) = e_j$, e que $f(\mathfrak{P}_j \mid \mathfrak{p}) = f(\mathfrak{Q}_j \mid \mathfrak{p}_\mathfrak{p}) = \partial P_j$.

Agora, nós temos $(\mathfrak{P}_j)_\mathfrak{p} = \mathfrak{p}_\mathfrak{p} B_\mathfrak{p} + P_j(\gamma) B_\mathfrak{p} = (\mathfrak{p} B + P_j(\gamma) B)_\mathfrak{p}$. Assim:

$$\mathfrak{P}_j = (\mathfrak{P}_j)_\mathfrak{p} \cap B = (\mathfrak{p} B + P_j(\gamma) B)_\mathfrak{p} \cap B.$$

Provaremos que se $\mathfrak{A} \lhd B$ é tal que $\mathfrak{p} B \subseteq \mathfrak{A}$, então $\mathfrak{A}_\mathfrak{p} \cap B = \mathfrak{A}$. Por um lado, é claro que $\mathfrak{A}_\mathfrak{p} \cap B \supseteq \mathfrak{A}$. Seja agora $x \in \mathfrak{A}_\mathfrak{p} \cap B$. Então $x = y/s$, para alguns $y \in \mathfrak{A}$, $s \in A \setminus \mathfrak{p}$. Sendo $\mathfrak{p} \lhd A$ maximal, temos $\mathfrak{p} + sA = A$, e portanto existem $p \in \mathfrak{p}$ e $a \in A$ tais que $1 = p + sa$. Desse modo:

$$x = (p + sa)x = px + sax = px + ya \in \mathfrak{p} B + \mathfrak{A} = \mathfrak{A}\,.$$

Portanto, $\mathfrak{A}_\mathfrak{p} \cap B = \mathfrak{A}$. Em particular, tomando $\mathfrak{A} = \mathfrak{p} B + P_j(\gamma) B$, nós concluímos que $\mathfrak{P}_j = (\mathfrak{p} B + P_j(\gamma) B)_\mathfrak{p} \cap B = \mathfrak{p} B + P_j(\gamma) B$, como queríamos.

□

Os primos não-nulos $\mathfrak{p} \lhd A$ tais que $\Delta(P_{\gamma,K}) \in \mathfrak{p}$ podem não ser os mesmos para diferentes escolhas de γ. Assim, para cada escolha de γ temos um conjunto C_γ de primos não-nulos de A que contêm o elemento $\Delta(P_{\gamma,K})$. Pelo corolário acima, é claro que o conjunto dos primos ramificados de A está contido na interseção de todos os C_γ. Uma observação importante é que cada C_γ é finito, pois:

$$\mathfrak{p} \in C_\gamma \iff \Delta(P_{\gamma,K}) \in \mathfrak{p} \iff \mathfrak{p} \mid \Delta(P_{\gamma,K})A = \mathfrak{d}_{A[\gamma]/A},$$

e $\Delta(P_{\gamma,K})A$ tem um número finito de divisores pelo Corolário 3.15. Em particular, concluímos que o número de ideais primos não-nulos de A que se ramificam em L é finito.

Corolário 4.26. *Existe apenas um número finito de ideais primos não-nulos $\mathfrak{p} \lhd A$ que se ramificam em L. Cada $\mathfrak{p}$ deste tipo divide $\mathfrak{d}_{A[\gamma]/A}$, para todo γ elemento primitivo de L/K.*

De fato, utilizando técnicas mais avançadas, pode-se mostrar uma condição necessária e suficiente para um ideal primo não-nulo $\mathfrak{p} \lhd A$ se ramificar em L:

Teorema 4.27. *Seja $\mathfrak{p} \lhd A$ primo não-nulo, e suponhamos que para todo $\mathfrak{P} \mid \mathfrak{p}$ a extensão $(B/\mathfrak{P})/(A/\mathfrak{p})$ seja separável. Então $\mathfrak{p}$ é ramificado em L se e só se $\mathfrak{p} \mid \mathfrak{d}_{B/A}$.*

Em particular, dados $p \in \mathbb{N}$ e um corpo de números algébricos L, p será ramificado em L se e só se $p \mid d_L$.

Para uma demonstração desse fato, veja por exemplo a Seção III.2 de [2] ou o Capítulo 12 de [3]. Estudemos agora os ideais totalmente ramificados da extensão B/A. Quando B/A era uma extensão gerada por um elemento, nós tínhamos o item (c) do Corolário 4.23 para nos dar informações. No entanto, um ideal primo $\mathfrak{p}$ totalmente ramificado satisfaz $\Delta(P_{\gamma,K}) \in \mathfrak{p}$ para todo γ elemento primitivo de L/K, de modo que não podemos adotar a mesma estratégia que utilizamos nos últimos resultados. O que fazemos nesse caso é mostrar a seguinte generalização do critério de Eisenstein:

Teorema 4.28. *Sejam $\mathfrak{p} \lhd A$ primo e suponhamos que $L = K(\gamma)$ para um elemento $\gamma \in B$ raiz de um polinômio mônico $P(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + x^m \in A[x]$ tal que $a_0, a_1, \ldots, a_{m-1} \in \mathfrak{p}$ e $a_0 \notin \mathfrak{p}^2$. Então P é irredutível em $K[x]$ (note que isso significa que $P = P_{\gamma,K}$), $m = [L : K] = n$ e $\mathfrak{p}B = \mathfrak{P}^n$, onde $\mathfrak{P} = \mathfrak{p}B + \gamma B$ é um ideal primo de B. Em particular, $\mathfrak{p}$ é totalmente ramificado em L.*

Demonstração. Sejam $\mathfrak{P} \lhd B$ primo sobre $\mathfrak{p}$ e $e = e(\mathfrak{P} \mid \mathfrak{p})$. Por hipótese, $a_0A = \mathfrak{p}\mathfrak{a}$, para algum $\mathfrak{a} \lhd B$ tal que $\mathfrak{p} \nmid \mathfrak{a}$. Sendo $\mathfrak{p}$ e $\mathfrak{a}$ coprimos, pelo item (l) da Proposição 1.46 temos $\mathfrak{p}B$ e $\mathfrak{a}B$ coprimos. Em particular, $\mathfrak{P} \nmid \mathfrak{a}B$, de modo que o ideal $a_0B = (\mathfrak{p}\mathfrak{a})B = (\mathfrak{p}B)(\mathfrak{a}B)$ se escreve como $a_0B = \mathfrak{P}^e\mathfrak{A}$ para $\mathfrak{A} \lhd B$ tal que $\mathfrak{P} \nmid \mathfrak{A}$. Notemos que

$$\gamma^m = -a_0 - a_1\gamma - \cdots - a_{m-1}\gamma^{m-1} \in \mathfrak{p}B \subseteq \mathfrak{P}.$$

Assim, $\gamma^m \in \mathfrak{P} \Rightarrow \gamma \in \mathfrak{P}$, já que $\mathfrak{P}$ é primo. Mais do que isso, notemos que para $1 \leq m \leq n-1$ temos $a_i \in \mathfrak{p} \subseteq \mathfrak{P}^e$, de modo que

$$a_0 = -\gamma^m - a_1\gamma - \cdots - a_{m-1}\gamma^{m-1} \in -\gamma^m - \mathfrak{P}^{e+1}.$$

Como $\mathfrak{P}^{e+1} \nmid a_0B$, temos $a_0 \notin \mathfrak{P}^{e+1}$, e portanto $\gamma^m \notin \mathfrak{P}^{e+1}$. Disso e do fato de que $\gamma^m \in \mathfrak{P}^m$ concluímos que $m \leq e$. Por outro lado, $P_{\gamma,K} \mid P$ em $K[x] \Rightarrow n = [L : K] = \partial P_{\gamma,K} \leq \partial P = m$. Mas da identidade fundamental nós sabemos que $e \leq n$. Assim, $m \leq e \leq n \leq m$, de forma que $m = n = e$. Isso mostra que $\partial P = \partial P_{\gamma,K} = n$, e então $P = P_{\gamma,K}$ é irredutível. Também concluímos da identidade fundamental que a fatoração de $\mathfrak{p}B$ em primos de B é $\mathfrak{p}B = \mathfrak{P}^n$.

Resta provarmos que $\mathfrak{P} = \mathfrak{p}B + \gamma B$. Observemos que $\mathfrak{P}^n = \mathfrak{p}B \subseteq \mathfrak{p}B + \gamma B$. Além disso, como $\mathfrak{p} \subseteq \mathfrak{P}$ e $\gamma \in \mathfrak{P}$, nós temos $\mathfrak{p}B + \gamma B \subseteq \mathfrak{P}$. Desse modo, $\mathfrak{p}B + \gamma B = \mathfrak{P}^j$ para algum $1 \leq j \leq n$. Suponhamos por absurdo $j \geq 2$. Então $\gamma \in \mathfrak{P}^j \Rightarrow \gamma^n \in \mathfrak{P}^{jn} \subseteq \mathfrak{P}^{n+1}$, um absurdo como já havíamos visto. Logo $\mathfrak{p}B + \gamma B = \mathfrak{P}$, terminando a demonstração. □

O teorema acima nos dá uma condição suficiente para garantirmos que um ideal primo $\mathfrak{p} \lhd A$ é totalmente ramificado em B. Mostraremos também que essa condição é necessária. Nós sabemos que $A_\mathfrak{p}$ é um DVD com único ideal maximal $\mathfrak{p}_\mathfrak{p}$. Supondo que $\mathfrak{p}$ seja totalmente ramificado em B, $B_\mathfrak{p}$ também será um DVD. De fato, seja $\mathfrak{P} \mid \mathfrak{p}$ primo. Então $\mathfrak{p}\,B = \mathfrak{P}^n$. Todo primo de $B_\mathfrak{p}$ é da forma $\mathfrak{Q}_\mathfrak{p}$, para $\mathfrak{Q} \lhd B$ primo não-nulo com $\mathfrak{Q} \cap (A \setminus \mathfrak{p}) = \emptyset$. Assim, $\mathfrak{Q} \cap A \subseteq \mathfrak{p}$ é primo não-nulo, e como A é domínio de Dedekind concluímos que $\mathfrak{Q} \cap A = \mathfrak{p}$. Logo $\mathfrak{Q} \mid \mathfrak{p} \Rightarrow \mathfrak{Q} = \mathfrak{P}$. Desse modo, $B_\mathfrak{p}$ é de fato um DVD, com único ideal maximal $\mathfrak{P}_\mathfrak{p}$. Notemos ainda que $\mathfrak{p}_\mathfrak{p}\,B_\mathfrak{p} = \mathfrak{P}_\mathfrak{p}^n$.

Teorema 4.29. *Nas condições acima, seja $\pi \in B_\mathfrak{p}$ um normalizador. Denotemos por v a valoração associada ao DVD $A_\mathfrak{p}$ e por w a valoração associada ao DVD $B_\mathfrak{p}$. Então:*

(a) Sejam $a_0, a_1, \ldots, a_{n-1} \in K$ quaisquer, não todos nulos. Definamos $\alpha := \sum_{i=0}^{n-1} a_i\pi^i \in L$. Então $w(\alpha) = \min\{n \cdot v(a_i) + i \colon 0 \leq i \leq n-1\}$. Em particular, $\alpha \neq 0$.

(b) $L = K(\pi)$.

(c) $1, \pi, \pi^2, \cdots, \pi^{n-1}$ formam uma base do A_p-módulo $B_\mathfrak{p}$. Em particular, $B_\mathfrak{p} = A_\mathfrak{p}[\pi]$.

(d) $P_{\pi,K}(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n$, onde $c_0, c_1, \ldots, c_{n-1} \in \mathfrak{p}_\mathfrak{p}$ e $c_0 \notin \mathfrak{p}_\mathfrak{p}^2$.

Demonstração. (a) Comecemos observando que para $0 \leq i \leq n-1$ qualquer, nós temos:

$$\begin{aligned}(a_i\pi^i)B_\mathfrak{p} &= (a_iB_\mathfrak{p})(\pi^iB_\mathfrak{p}) = ((a_iA_\mathfrak{p})B_\mathfrak{p}) \cdot \pi^iB_\mathfrak{p} \\ &= (\mathfrak{p}_\mathfrak{p}^{v(a_i)}\,B_\mathfrak{p}) \cdot \pi^iB_\mathfrak{p} = (\mathfrak{p}_\mathfrak{p}\,B_\mathfrak{p})^{v(a_i)} \cdot \pi^iB_\mathfrak{p} \\ &= (\mathfrak{P}_\mathfrak{p}^n)^{v(a_i)} \cdot \pi^iB_\mathfrak{p} = \mathfrak{P}_\mathfrak{p}^{n\cdot v(a_i)} \cdot \pi^iB_\mathfrak{p} \\ &= (\pi B_\mathfrak{p})^{n\cdot v(a_i)} \cdot \pi^iB_\mathfrak{p} = \pi^{n\cdot v(a_i)+i}B_\mathfrak{p}.\end{aligned}$$

Assim, $w(a_i\pi^i) = n \cdot v(a_i) + i$, para $0 \leq i \leq n-1$. É fácil ver que esses valores são distintos dois a dois, e portanto pelo item (d) do Lema 3.26 nós concluímos que:

$$\begin{aligned}w(\alpha) = w\left(\sum_{i=0}^{n-1} a_i\pi^i\right) &= \min\{w(a_i\pi^i) \colon 0 \leq i \leq n-1\} \\ &= \min\{n \cdot v(a_i) + i \colon 0 \leq i \leq n-1\},\end{aligned}$$

como queríamos. Em particular, $\alpha \neq 0$.

(b) Uma vez que $\{1, \pi, \pi^2, \ldots, \pi^{n-1}\}$ tem n elementos e $[L : K] = n$, basta mostrar que esse conjunto é linearmente independente. Mas isso segue do "em particular" do item (a)!

(c) Por (b), todo elemento α de L/K se escreve de modo único como $\alpha = \sum_{i=0}^{n-1} a_i\pi^i$, para alguns $a_0, \ldots, a_{n-1} \in K$. Desse modo, queremos mostrar que se $\alpha \in B_\mathfrak{p}$ então $a_0, \ldots, a_{n-1} \in A_\mathfrak{p}$. Assim, suponhamos que $\alpha \in B_\mathfrak{p}$. Logo $w(\alpha) \geq 0$. Por (a), nós temos a igualdade $w(\alpha) = \min\{n \cdot v(a_i) + i \colon 0 \leq i \leq n-1\}$. Isso mostra que, para $0 \leq i \leq n-1$,

$$n \cdot v(a_i) + i \geq 0 \Rightarrow v(a_i) \geq -\frac{i}{n} > -1 \Rightarrow v(a_i) \geq 0.$$

Mas isso significa que $a_i \in A_\mathfrak{p}$, como gostaríamos.

(d) Seja $P_{\pi,K}(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n \in K[x]$. Como $P_{\pi,K}(\pi) = 0$, nós temos

$$\pi^n = -\sum_{i=0}^{n-1} c_i\pi^i \Rightarrow \min\{n \cdot v(c_i) + i \colon 0 \leq i \leq n-1\} = n,$$

devido ao item (a). Assim, para $0 \leq i \leq n-1$, temos $v(c_i) \geq (n-i)/n > 0 \Rightarrow v(c_i) \geq 1$, o que mostra que $c_i \in \mathfrak{p}_\mathfrak{p}$. Notemos ainda que, para $1 \leq i \leq n-1$, $n \cdot v(c_i) + i > n \cdot 1 = n$.

Logo para o mínimo acima ser n ele deve ocorrer para $i = 0$. Ou seja, $n \cdot v(c_0) = n$, e concluímos que $v(c_0) = 1 \Rightarrow c_0 \notin \mathfrak{p}_{\mathfrak{p}}^2$, como desejado.

□

Como consequência direta do teorema acima, nós temos a recíproca do Teorema 4.28:

Corolário 4.30. *Se $\mathfrak{p} \lhd A$ é primo totalmente ramificado em B e $\mathfrak{P} \lhd B$ é o único ideal primo de B sobre $\mathfrak{p}$, então existe $\gamma \in B$ tal que $L = K(\gamma)$ e γ é raiz de um polinômio $P(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in A[x]$ tal que $a_0, a_1, \ldots, a_{n-1} \in \mathfrak{p}$ e $a_0 \notin \mathfrak{p}^2$.*

Demonstração. Seja π um gerador do ideal $\mathfrak{P}_{\mathfrak{p}} \lhd B_{\mathfrak{p}}$. Então o teorema acima nos diz que $L = K(\pi)$, que $\{1, \pi, \ldots, \pi^{n-1}\}$ é base do $A_{\mathfrak{p}}$-módulo $B_{\mathfrak{p}}$ e que $P_{\pi,K} = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n$ é tal que $c_0, \ldots, c_{n-1} \in \mathfrak{p}_{\mathfrak{p}}$ e $c_0 \notin \mathfrak{p}_{\mathfrak{p}}^2$. Como $\pi \in \mathfrak{P}_{\mathfrak{p}}$, nós temos $\pi = \gamma/s$ para alguns $\gamma \in \mathfrak{P}$ e $s \in A \setminus \mathfrak{p}$. Então $\gamma \in B$ é tal que $L = K(\gamma)$.

Agora, como cada $c_0, \ldots, c_{n-1} \in \mathfrak{p}_{\mathfrak{p}}$, nós podemos escrever, para $0 \leq i \leq n-1$, $c_i = b_i/s_i$ para alguns $b_i \in \mathfrak{p}$ e $s_i \in A \setminus \mathfrak{p}$. Como $c_0 \notin \mathfrak{p}_{\mathfrak{p}}^2$, nós devemos ter $b_0 \notin \mathfrak{p}^2$. Assim:

$$\begin{aligned} 0 = c_0 + c_1\pi + \cdots + c_{n-1}\pi^{n-1} + \pi^n &= \frac{b_0}{s_0} + \frac{b_1}{s_1}\frac{\gamma}{s} + \cdots + \frac{b_{n-1}}{s_{n-1}}\left(\frac{\gamma}{s}\right)^{n-1} + \left(\frac{\gamma}{s}\right)^n \\ &= \frac{a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1} + \gamma^n}{s^n s_0 s_1 \cdots s_{n-1}} \\ &\Rightarrow \quad a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1} + \gamma^n = 0, \end{aligned}$$

onde para $0 \leq i \leq n-1$ definimos $a_i \coloneqq b_i s^{n-i} s_0 \cdots \widehat{s_i} \cdots s_{n-1} \in A$. Para $0 \leq i \leq n-1$ nós temos $b_i \in \mathfrak{p}$, logo $a_i \in \mathfrak{p}$. Além disso, como $\mathfrak{p}$ é primo, $s^n s_1 \cdots s_{n-1} \notin \mathfrak{p}$, e portanto $a_0B = (b_0B)(s^n s_1 \cdots s_{n-1}B)$ não é múltiplo de $\mathfrak{p}^2$, já que $\mathfrak{p}^2 \nmid b_0B$ e $\mathfrak{p} \nmid s^n s_1 \cdots s_{n-1}B$. Finalmente, basta tomar $P(x) \coloneqq a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in A[x]$. □

Capítulo 5

Decomposição em Corpos Quadráticos e Ciclotômicos

Nesse capítulo, aplicaremos os resultados do capítulo anterior para estudar como os ideais primos de $\mathbb{Z}$ se fatoram em ideais primos de corpos quadráticos e ciclotômicos. Para estudarmos as extensões de corpos quadráticos, provaremos a famosa **Lei de Reciprocidade Quadrática**.

5.1. A Lei de Reciprocidade Quadrática

Seja $d \in \mathcal{D}$ congruente a 2 ou 3 módulo 4, e $K = \mathbb{Q}(\sqrt{d})$. Então $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. O polinômio minimal de $\sqrt{d}$ em relação a $\mathbb{Q}$ é $P(x) := P_{\sqrt{d},\mathbb{Q}}(x) = x^2 - d$. Assim, pelo Teorema 4.22, para estudarmos como um número primo $p \in \mathbb{N}$ se decompõe em $\mathcal{O}_K$ devemos analisar como o polinômio $x^2 - \overline{d}$ se fatora em $\mathbb{F}_p[x]$. Sendo esse um polinômio de segundo grau, temos apenas duas opções: ou esse polinômio possui uma raiz em $\mathbb{F}_p$ ou então ele é irredutível. Mas a existência de uma raiz desse polinômio em $\mathbb{F}_p$ equivale a dizer que existe uma raiz quadrada de $\overline{d}$ em $\mathbb{F}_p$, isto é, que existe $a \in \mathbb{Z}$ tal que $a^2 \equiv d \pmod{p}$. A existência ou não de tal $a \in \mathbb{Z}$ é o que abordaremos nessa seção.

É interessante notar que os resultados provados aqui possuem enunciados elementares, aparecendo naturalmente em Teoria Elementar dos Números no estudo de congruências quadráticas. De fato, embora a Lei de Reciprocidade Quadrática seja demonstrada aqui utilizando inteiros algébricos, ela possui demonstrações elementares (veja por exemplo os livros [1] ou [5]). Essa discussão motiva a seguinte definição:

Definição (Resíduo Quadrático)**.** Seja n um inteiro positivo. Dizemos que um inteiro $a \in \mathbb{Z}$ (ou sua classe $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$) é um **resíduo quadrático** módulo n (ou em $\mathbb{Z}/n\mathbb{Z}$) se existir $r \in \mathbb{Z}$ tal que $r^2 \equiv a \pmod{n}$ (equivalentemente, se existir $\overline{r} \in \mathbb{Z}/n\mathbb{Z}$ tal que $\overline{r}^2 = \overline{a}$).

Denotaremos o conjunto de resíduos quadráticos módulo n por $\mathrm{RQ}(n)$. Note que podemos ver $\mathrm{RQ}(n)$ tanto como um subconjunto de $\mathbb{Z}$ quanto de $\mathbb{Z}/n\mathbb{Z}$, dependendo da definição de resíduo quadrático utilizada. A forma de enxergarmos $\mathrm{RQ}(n)$ ficará clara pelo contexto. A seguinte notação é bastante útil:

Definição (Símbolo de Legendre)**.** Denotemos por $\mathcal{P}$ o conjunto dos números primos ímpares em $\mathbb{Z}$. O **símbolo de Legendre** é uma função $\left(\frac{\cdot}{\cdot}\right) : \mathbb{Z} \times \mathcal{P} \to \{-1, 0, 1\}$, com $(a, p) \mapsto \left(\frac{a}{p}\right)$, de modo que, dados $p \in \mathbb{Z}$ um primo ímpar e $a \in \mathbb{Z}$ qualquer, nós tenhamos:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{se } p \mid a; \\ 1, & \text{se } p \nmid a \text{ e } a \in \mathrm{RQ}(p); \\ -1, & \text{se } p \nmid a \text{ e } a \notin \mathrm{RQ}(p). \end{cases}$$

Assim, nosso problema inicial se reduz a conseguir calcular os símbolos de Legendre para quaisquer $(a,p) \in \mathbb{Z} \times \mathcal{P}$. O **critério de Euler** nos ajudará nessa tarefa:

Proposição 5.1. *(a) Seja p um primo ímpar, e seja g um gerador do grupo multiplicativo $\mathbb{F}_p^\times$. Então o conjunto de resíduos quadráticos de $\mathbb{F}_p$ é dado por*

$$\mathrm{RQ}(p) = \{\overline{0}\} \cup \{g^{2k} \colon 0 \leq k \leq (p-3)/2\}.$$

Em particular, $|\mathrm{RQ}(p)| = (p+1)/2$.

(b) (Critério de Euler) Se $(a,p) \in \mathbb{Z} \times \mathcal{P}$, então $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Demonstração. (a) Segue facilmente por teoria de grupos abelianos.

(b) Se $p \mid a$, essa igualdade é clara. Suponhamos que $p \nmid a$. Então temos $\overline{a} = g^m$ para $0 \leq m \leq p-2$. Assim, $\overline{a}^{(p-1)/2} = g^{m(p-1)/2}$. Se m for par, $m(p-1)/2 \equiv 0 \pmod{p-1}$, e nesse caso $\overline{a}^{(p-1)/2} = g^0 = \overline{1}$. Se m for ímpar, $m(p-1)/2 \equiv (p-1)/2 \pmod{p-1}$, e nesse caso $\overline{a}^{(p-1)/2} = g^{(p-1)/2} = -\overline{1}$ (note que $g^{(p-1)/2}$ é uma raiz de $x^2 - \overline{1}$ diferente de 1, e esse polinômio se fatora como $(x+\overline{1})(x-\overline{1})$, de onde $g^{(p-1)/2} = -\overline{1}$).

Utilizando o item (a) e o que acabamos de mostrar, concluímos que se a for resíduo quadrático então m é par, e portanto $a^{(p-1)/2} \equiv 1 = \left(\frac{a}{p}\right) \pmod{p}$, e que se a não for resíduo quadrático então m é ímpar, e portanto $a^{(p-1)/2} \equiv -1 = \left(\frac{a}{p}\right) \pmod{p}$.

□

O símbolo de Legendre possui as seguintes propriedades:

Proposição 5.2. *Seja p um primo ímpar e sejam $a, b \in \mathbb{Z}$ quaisquer. Então:*

(a) Se $a \equiv b \pmod{p}$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) Se $p \nmid a$, então $\left(\frac{a^2}{p}\right) = 1$.

(c) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Desse modo, $-1 \in \mathrm{RQ}(p) \iff p \equiv 1 \pmod{4}$.

(d) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Desse modo, o símbolo de Legendre induz um homomorfismo de grupos multiplicativos $\mathbb{F}_p^\times \to \{-1,1\}$ dado por $a \mapsto \left(\frac{a}{p}\right)$.

Demonstração. Os itens (a) e (b) são imediatos da definição.

(c) Pelo Critério de Euler, $\left(\frac{-1}{p}\right)$ deixa resto $(-1)^{(p-1)/2}$ módulo p. Mas como $\left(\frac{-1}{p}\right) = \pm 1$, temos que vale a igualdade já que $p > 2$. Assim:

$$-1 \in \mathrm{RQ}(p) \iff \left(\frac{-1}{p}\right) = 1 \iff (-1)^{(p-1)/2} = 1 \iff p \equiv 1 \pmod{4}.$$

(d) Se $p \mid a$ ou $p \mid b$, o resultado é óbvio. Suponhamos então que $p \nmid a, b$. Pelo Critério de Euler,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} \cdot b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Mas como $\left(\frac{ab}{p}\right) = \pm 1$ e $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \pm 1$, deve valer a igualdade desejada já que $p > 2$.

□

Finalmente, provemos a famosa Lei de Reciprocidade Quadrática:

Teorema 5.3 (Lei de Reciprocidade Quadrática)**.** *Sejam p, q primos ímpares distintos. Então:*

(a) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. *Isto é:*

- *Se $p \equiv 1 \pmod 4$ ou $q \equiv 1 \pmod 4$, então $p \in \mathrm{RQ}(q) \iff q \in \mathrm{RQ}(p)$.*
- *Se $p \equiv q \equiv 3 \pmod 4$, então $p \in \mathrm{RQ}(q) \iff q \notin \mathrm{RQ}(p)$.*

(b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. *Isto é,* $2 \in \mathrm{RQ}(p) \iff p \equiv \pm 1 \pmod 8$.

Demonstração. (a) Seja $\zeta \in \mathbb{C}$ uma raiz primitiva p-ésima da unidade. Consideremos a **soma de Gauss**[1] $S := \sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)\zeta^a \in \mathbb{Z}[\zeta]$. Então $S^2 = (-1)^{\frac{p-1}{2}}p$. De fato:

$$\begin{aligned} S^2 = \left(\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)\zeta^a\right)^2 &= \sum_{a,b\in\mathbb{F}_p}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\zeta^{a+b} = \sum_{n\in\mathbb{F}_p}\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a}{p}\right)\left(\frac{n-a}{p}\right)\zeta^n \\ &= \sum_{n\in\mathbb{F}_p}\zeta^n\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a(n-a)}{p}\right) = \sum_{n\in\mathbb{F}_p}\zeta^n\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a^2}{p}\right)\left(\frac{a^{-1}n-1}{p}\right) \\ &= \sum_{n\in\mathbb{F}_p}\zeta^n\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a^{-1}n-1}{p}\right). \end{aligned}$$

Assim, para determinar S^2 basta calcular a soma $\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a^{-1}n-1}{p}\right)$ para cada $n \in \mathbb{F}_p$. Para $n = 0$, todas as parcelas dessa soma são $\left(\frac{-1}{p}\right)$, de modo que essa soma é igual a $(p-1)\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}(p-1)$ pelo Critério de Euler. Para $n \in \mathbb{F}_p^\times$, vemos que quando a varia o número $a^{-1}n$ percorre todo $\mathbb{F}_p^\times$. Então nesse caso:

$$\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a^{-1}n-1}{p}\right) = \sum_{a\in\mathbb{F}_p^\times}\left(\frac{a-1}{p}\right) = \sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right) - \left(\frac{-1}{p}\right) = -\left(\frac{-1}{p}\right) = -(-1)^{\frac{p-1}{2}},$$

já que temos exatamente $(p-1)/2$ resíduos quadráticos e $(p-1)/2$ resíduos não-quadráticos em $\mathbb{F}_p^\times$ pelo item (a) da Proposição 5.1, e portanto a soma $\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)$, formada por uma parcela igual a 0, $(p-1)/2$ parcelas iguais a 1 e $(p-1)/2$ parcelas iguais a -1, é igual a 0. Assim:

$$\begin{aligned} S^2 = \sum_{n\in\mathbb{F}_p}\zeta^n\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a^{-1}n-1}{p}\right) &= (-1)^{\frac{p-1}{2}}(p-1) - \sum_{n=1}^{p-1}\zeta^n(-1)^{\frac{p-1}{2}} \\ &= (-1)^{\frac{p-1}{2}}(p-1) - (-1)^{\frac{p-1}{2}}\sum_{n=1}^{p-1}\zeta^n \\ &= (-1)^{\frac{p-1}{2}}(p-1) - (-1)^{\frac{p-1}{2}}(-1) \\ &= (-1)^{\frac{p-1}{2}}p, \end{aligned}$$

[1] Aqui, por simplicidade de notação, identificaremos $\mathbb{F}_p$ com seu conjunto de representantes $\{0, 1, \ldots, p-1\} \subseteq \mathbb{Z}$.

como desejávamos. Calculemos agora $\overline{S}^{q-1}$ no anel $A := \mathbb{Z}[\zeta]/(q\,\mathbb{Z}[\zeta])$. Observemos que como $S^2 = \pm p$ e $\mathrm{mdc}(p,q) = 1$, temos que $\overline{p} \in \mathbb{F}_q^\times \subseteq A^\times$, e portanto $\overline{S} \in A^\times$. Como A é um anel de característica q, nós temos:

$$\begin{aligned}\overline{S}^q = \left(\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)\overline{\zeta}^a\right)^q &= \sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)^q\overline{\zeta}^{aq} = \sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)\overline{\zeta}^{aq}\\ &= \sum_{a\in\mathbb{F}_p}\left(\frac{q}{p}\right)\left(\frac{aq}{p}\right)\overline{\zeta}^{aq} = \left(\frac{q}{p}\right)\overline{S},\end{aligned}$$

uma vez que quando a percorre $\mathbb{F}_p$, aq também percorre $\mathbb{F}_p$. Como $\overline{S} \in A^\times$, concluímos que $\overline{S}^{q-1} = \left(\frac{q}{p}\right)$ em A. Com as identidades $S^2 = (-1)^{\frac{p-1}{2}}p$ e $\overline{S}^{q-1} = \left(\frac{q}{p}\right)$, já temos tudo o que precisamos para provar a igualdade desejada. Basta notar que, pelo Critério de Euler:

$$\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) \equiv \left((-1)^{\frac{p-1}{2}}p\right)^{\frac{q-1}{2}} = (S^2)^{\frac{q-1}{2}} = S^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{qA}.$$

Mas por outro lado, $\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$, e portanto

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{qA} \Rightarrow (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

já que ambos esses valores são ± 1 e $q > 2$. Finalmente, essa última igualdade é equivalente à igualdade desejada (basta multiplicar por $\left(\frac{p}{q}\right) = \pm 1$ de ambos os lados).

(b) Seja $\zeta \in \mathbb{C}$ uma raiz oitava primitiva da unidade, e denotemos $\omega := \zeta + \zeta^{-1}$. Então $\omega^2 = 2$. De fato:

$$\omega^2 = (\zeta+\zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2\zeta\zeta^{-1} = \zeta^2 + \zeta^6 + 2 = \zeta^2(1+\zeta^4) + 2 = 2,$$

Assim, pelo Critério de Euler:

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv \omega^{p-1} \pmod{p\,\mathbb{Z}[\zeta]}.$$

Logo basta calcularmos $\overline{\omega}^{p-1}$. Como $\mathrm{mdc}(2,p) = 1$, temos $2 \in \mathbb{F}_p^\times \subseteq (\mathbb{Z}[\zeta]/p\,\mathbb{Z}[\zeta])^\times$. Como $\omega^2 = 2$, temos $\overline{\omega} \in (\mathbb{Z}[\zeta]/p\,\mathbb{Z}[\zeta])^\times$. Agora:

$$\overline{\omega}^p = (\overline{\zeta}+\overline{\zeta}^{-1})^p = \overline{\zeta}^p + \overline{\zeta}^{-p} = \begin{cases}\overline{\zeta}+\overline{\zeta}^{-1} = \overline{\omega}, \text{ se } p \equiv 1 \pmod 8;\\ \overline{\zeta}^3+\overline{\zeta}^5 = \overline{\zeta}^4\overline{\omega} = -\overline{\omega}, \text{ se } p \equiv \pm 3 \pmod 8.\end{cases}$$

Note que então temos $\overline{\omega}^p = (-1)^{\frac{p^2-1}{8}}\overline{\omega}$, para todo primo ímpar p, e como $\overline{\omega} \in (\mathbb{Z}[\zeta]/p\,\mathbb{Z}[\zeta])^\times$ temos $\overline{\omega}^{p-1} = (-1)^{\frac{p^2-1}{8}}$. Assim, $\left(\frac{2}{p}\right) \equiv \omega^{p-1} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p\,\mathbb{Z}[\zeta]}$. Como tanto $\left(\frac{2}{p}\right)$ quando $(-1)^{\frac{p^2-1}{8}}$ estão em $\{-1,1\}$ e $p > 2$, concluímos que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, como queríamos.

□

Observação 5.4. *O uso de raízes da unidade na prova acima parece totalmente "arbitrário", ou mesmo "mágico". Para justificar um pouco o surgimento desses elementos, podemos pensar na*

principal ideia da demonstração acima, que é simplesmente calcular $\left(\frac{p}{q}\right) \pmod q$ *utilizando o Critério de Euler. Em* $\mathbb{Z}[\sqrt{p}]$*, nós temos:*

$$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \equiv \sqrt{p}^{q-1} \pmod{q\,\mathbb{Z}[\sqrt{p}]}.$$

Com isso, basta calcularmos $\overline{\sqrt{p}}^{q-1} \in \mathbb{Z}[\sqrt{p}]/(q\,\mathbb{Z}[\sqrt{p}])$*. Para isso, buscamos uma expressão explícita para* $\overline{\sqrt{p}}$*, isto é, procuramos determinar uma raiz quadrada de* p *numa extensão de* $\mathbb{F}_q$*, e como vimos isso é possível através das somas de Gauss.*

Exemplo 5.5. *A partir da Lei de Reciprocidade Quadrática, podemos calcular símbolos de Legendre por meio da fatoração. Por exemplo, digamos que queremos determinar se* 2021 *é resíduo quadrático módulo o número primo* 5003*. Para isso, computamos* $\left(\frac{2021}{5003}\right)$ *da seguinte forma:*

$$\begin{aligned}
\left(\frac{2021}{5003}\right) = \left(\frac{43\cdot 47}{5003}\right) = \left(\frac{43}{5003}\right)\left(\frac{47}{5003}\right) &= \left(-\left(\frac{5003}{43}\right)\right)\left(-\left(\frac{5003}{47}\right)\right) \\
&= \left(\frac{15}{43}\right)\left(\frac{21}{47}\right) \\
&= \left(\frac{3}{43}\right)\left(\frac{5}{43}\right)\left(\frac{3}{47}\right)\left(\frac{7}{47}\right) \\
&= \left(-\left(\frac{43}{3}\right)\right)\left(\frac{43}{5}\right)\left(-\left(\frac{47}{3}\right)\right)\left(-\left(\frac{47}{7}\right)\right) \\
&= -\left(\frac{1}{3}\right)\left(\frac{3}{5}\right)\left(\frac{2}{3}\right)\left(\frac{5}{7}\right) \\
&= -\left(\frac{2}{3}\right)\left(\frac{5}{3}\right)\left(\frac{7}{5}\right) \\
&= -(-1)\left(\frac{2}{3}\right)\left(\frac{2}{5}\right) \\
&= (-1)(-1) = 1,
\end{aligned}$$

onde usamos repetidas vezes a Lei de Reciprocidade Quadrática e a multiplicatividade do símbolo de Legendre. Assim, 2021 *é resíduo quadrático módulo* 5003*.*

Podemos estender o símbolo de Legendre para todo inteiro positivo ímpar, por fatoração. Isso definirá o chamado **símbolo de Jacobi**:

Definição (Símbolo de Jacobi)**.** Seja n um inteiro positivo ímpar, e seja $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ a sua fatoração prima. Dado $a \in \mathbb{Z}$ qualquer, definimos o **símbolo de Jacobi** $\left(\frac{a}{n}\right)$ como sendo:

$$\left(\frac{a}{n}\right) \coloneqq \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k} = \prod_{j=1}^{k} \left(\frac{a}{p_j}\right)^{\alpha_j}.$$

Observe que com essa definição nós temos $\left(\frac{a}{1}\right) = 1$ para todo $a \in \mathbb{Z}$.

Note que para n primo os símbolos de Legendre e Jacobi coincidem. Assim, não temos problema em usar a mesma notação para os dois símbolos. Utilizando as propriedades que conhecemos do símbolo de Legendre, conseguimos deduzir propriedades similares do símbolo de Jacobi:

Teorema 5.6 (Propriedades do Símbolo de Jacobi)**.** *Sejam* m, n *inteiros positivos ímpares e* a, b *inteiros quaisquer. Então nós temos:*

(a) *Se* $a \equiv b \pmod{n}$, *então* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(b) $\left(\frac{a}{n}\right) = 0$ *se* $\mathrm{mdc}(a,n) > 1$ *e* $\left(\frac{a}{n}\right) = \pm 1$ *se* $\mathrm{mdc}(a,n) = 1$.

(c) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$. *Em particular,* $\left(\frac{a^2}{n}\right) \in \{0,1\}$.

(d) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$. *Em particular,* $\left(\frac{a}{n^2}\right) \in \{0,1\}$.

(e) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

(f) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right)$.

(g) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

As igualdades (c) *e* (d) *são chamadas de multiplicatividade do símbolo de Legendre, a igualdade* (e) *é chamada de Critério de Euler para o símbolo de Jacobi, e as igualdades* (f) *e* (g) *são chamadas de Lei de Reciprocidade Quadrática para o símbolo de Jacobi.*

Demonstração. Nos itens abaixo, denotaremos por $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ e por $m = q_1^{\beta_1}\cdots q_r^{\beta_r}$. Notemos ainda que todos os itens são fáceis de verificar caso $m = 1$ ou $n = 1$. Assim, suponhamos $m, n \neq 1$. Os itens (a), (b), (c) e (d) seguem facilmente da definição. Provemos (e), (f) e (g):

(e) Pela multiplicatividade e pelo Critério de Euler para o símbolo de Legendre:

$$\left(\frac{-1}{n}\right) = \prod_{j=1}^{k}\left(\frac{-1}{p_j}\right)^{\alpha_j} = \prod_{j=1}^{k}(-1)^{\alpha_j\cdot\frac{p_j-1}{2}} = (-1)^{\sum_{j=1}^{k}\alpha_j\cdot\frac{p_j-1}{2}}.$$

Assim, basta mostrarmos que $\sum_{j=1}^{k}\alpha_j\cdot\frac{p_j-1}{2} \equiv \frac{n-1}{2} \pmod 2$. Isso por sua vez segue facilmente por indução em $\alpha_1 + \cdots + \alpha_n$ do seguinte fato: dados u, v ímpares, temos $\frac{uv-1}{2} \equiv \frac{u-1}{2} + \frac{v-1}{2} \pmod 2$. Para verificar esse fato, basta notarmos que:

$$\begin{aligned}\frac{uv-1}{2} \equiv \frac{u-1}{2} + \frac{v-1}{2} \pmod 2 \quad &\iff \quad uv - 1 \equiv (u-1) + (v-1) \pmod 4\\ &\iff \quad uv - u - v + 1 \equiv 0 \pmod 4\\ &\iff \quad (u-1)(v-1) \equiv 0 \pmod 4,\end{aligned}$$

o que é verdade já que u e v são ímpares.

(f) Se $\mathrm{mdc}(m,n) > 1$, então pelo item (b) temos $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 0$, e temos a igualdade desejada. Suponhamos então $\mathrm{mdc}(m,n) = 1$. Assim, para $1 \leq i \leq k$ e $1 \leq j \leq r$ temos $p_i \neq q_j$.

Pela multiplicatividade e pela Lei de Reciprocidade Quadrática para o símbolo de Legendre:

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_{i=1}^{k}\left(\frac{m}{p_i}\right)^{\alpha_i}\prod_{j=1}^{r}\left(\frac{n}{q_j}\right)^{\beta_j}\\ &= \left(\prod_{i=1}^{k}\prod_{j=1}^{r}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}\right)\left(\prod_{j=1}^{r}\prod_{i=1}^{k}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}\right)\\ &= \prod_{i=1}^{k}\prod_{j=1}^{r}\left(\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)\right)^{\alpha_i\beta_j}\\ &= \prod_{i=1}^{k}\prod_{j=1}^{r}(-1)^{\alpha_i\beta_j\cdot\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\\ &= (-1)^{\sum_{i=1}^{k}\sum_{j=1}^{r}\alpha_i\beta_j\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.\end{aligned}$$

Assim, basta mostrarmos que $\sum_{i=1}^{k}\sum_{j=1}^{r}\alpha_i\beta_j\cdot\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}\equiv\frac{m-1}{2}\cdot\frac{n-1}{2}\pmod 2$. Mas nós temos:

$$\begin{aligned}\sum_{i=1}^{k}\sum_{j=1}^{r}\alpha_i\beta_j\cdot\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} &= \left(\sum_{i=1}^{k}\alpha_i\cdot\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{r}\beta_j\cdot\frac{q_j-1}{2}\right)\\ &\equiv \frac{n-1}{2}\cdot\frac{m-1}{2}\pmod 2,\end{aligned}$$

pelo fato que demonstramos no item (e).

(g) Pela multiplicatividade e pela Lei de Reciprocidade Quadrática para o símbolo de Legendre:

$$\left(\frac{2}{n}\right)=\prod_{j=1}^{k}\left(\frac{2}{p_j}\right)^{\alpha_j}=\prod_{j=1}^{k}(-1)^{\alpha_j\cdot\frac{p_j^2-1}{8}}=(-1)^{\sum_{j=1}^{k}\alpha_j\cdot\frac{p_j^2-1}{8}}.$$

Assim, basta provarmos que $\sum_{j=1}^{k}\alpha_j\cdot\frac{p_j^2-1}{8}\equiv\frac{n^2-1}{8}\pmod 2$. Isso por sua vez segue facilmente por indução em $\alpha_1+\cdots+\alpha_n$ do seguinte fato: dados u,v ímpares, temos $\frac{(uv)^2-1}{8}\equiv\frac{u^2-1}{8}+\frac{v^2-1}{8}\pmod 2$. Para verificar esse fato, basta notarmos que:

$$\begin{aligned}\frac{(uv)^2-1}{8}\equiv\frac{u^2-1}{8}+\frac{v^2-1}{8}\pmod 2 &\iff u^2v^2-1\equiv(u^2-1)+(v^2-1)\pmod{16}\\ &\iff u^2v^2-u^2-v^2+1\equiv 0\pmod{16}\\ &\iff (u^2-1)(v^2-1)\equiv 0\pmod{16},\end{aligned}$$

o que é verdade já que u e v são ímpares, e portanto $u^2-1,v^2-1\equiv 0\pmod 4$.

□

Também nos será útil estender a Lei de Reciprocidade Quadrática acima para inteiros negativos:

Proposição 5.7. *Sejam $m\in\mathbb{N}$ e $c\in\mathbb{Z}$ ímpares e primos entre si. Então:*

$$\left(\frac{c}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{c-1}{2}}\left(\frac{m}{|c|}\right).$$

Demonstração. Se c for positivo, a igualdade acima é simplesmente a Lei de Reciprocidade Quadrática para o símbolo de Jacobi. Suponhamos então $c < 0$. Assim, $|c| = -c$. Pelo Critério de Euler e pela Lei de Reciprocidade Quadrática para o símbolo de Jacobi:

$$\begin{aligned}\left(\frac{c}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{-c}{m}\right) &= (-1)^{\frac{m-1}{2}}(-1)^{\frac{m-1}{2}\cdot\frac{-c-1}{2}}\left(\frac{m}{-c}\right)\\ &= (-1)^{\frac{m-1}{2}\left(1+\frac{-c-1}{2}\right)}\left(\frac{m}{|c|}\right)\\ &= (-1)^{\frac{m-1}{2}\cdot\frac{1-c}{2}}\left(\frac{m}{|c|}\right)\\ &= (-1)^{\frac{m-1}{2}\cdot\frac{c-1}{2}}\left(\frac{m}{|c|}\right).\end{aligned}$$

□

Todo quadrado perfeito a^2 satisfaz $\left(\frac{a^2}{c}\right) \in \{0,1\}$, para todo c inteiro positivo ímpar. Mais interessante é que a recíproca também vale:

Proposição 5.8. *Seja n inteiro positivo tal que para todo c inteiro positivo ímpar tenhamos $\left(\frac{n}{c}\right) \in \{0,1\}$. Então n é um quadrado perfeito.*

Demonstração. Provaremos a contrapositiva. Isto é, se n não for um quadrado perfeito, acharemos um ímpar positivo c tal que $\left(\frac{n}{c}\right) = -1$. Seja $n = 2^{\alpha}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ a fatoração prima de n, onde $\alpha \geq 0$ e $\alpha_1, \ldots, \alpha_k > 0$. Podemos supor ser perda de generalidade que α_1 é ímpar. Pelo Teorema Chinês dos Restos, existe um inteiro positivo c que satisfaz o sistema de congruências:

$$\begin{cases} c \equiv 1 \pmod 8; \\ c \equiv r \pmod{p_1} \\ c \equiv 1 \pmod{p_j},\ 2 \leq j \leq k. \end{cases}$$

para um $r \in \mathbb{Z}$ que não seja resíduo quadrático módulo p_1. Note que as congruências acima já garantem c ímpar. Pela multiplicatividade do símbolo de Jacobi e pela Lei de Reciprocidade Quadrática, nós temos:

$$\left(\frac{n}{c}\right) = \left(\frac{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}}{c}\right) = \left(\frac{2}{c}\right)^{\alpha}\left(\frac{p_1}{c}\right)^{\alpha_1}\left(\frac{p_2}{c}\right)^{\alpha_2}\cdots\left(\frac{p_k}{c}\right)^{\alpha_k}.$$

Como $c \equiv 1 \pmod 8$, temos $\left(\frac{2}{c}\right) = 1$. Além disso, como $c \equiv 1 \pmod 4$, para $1 \leq j \leq k$ nós temos $\left(\frac{p_j}{c}\right) = \left(\frac{c}{p_j}\right)$. Assim:

$$\begin{aligned}\left(\frac{n}{c}\right) &= \left(\frac{2}{c}\right)^{\alpha}\left(\frac{p_1}{c}\right)^{\alpha_1}\left(\frac{p_2}{c}\right)^{\alpha_2}\cdots\left(\frac{p_k}{c}\right)^{\alpha_k}\\ &= \left(\frac{c}{p_1}\right)^{\alpha_1}\left(\frac{c}{p_2}\right)^{\alpha_2}\cdots\left(\frac{c}{p_k}\right)^{\alpha_k}\\ &= \left(\frac{c}{p_1}\right)\left(\frac{1}{p_2}\right)^{\alpha_2}\cdots\left(\frac{1}{p_k}\right)^{\alpha_k}\\ &= \left(\frac{r}{p_1}\right) = -1,\end{aligned}$$

Assim, achamos o c desejado, concluindo a demonstração. □

Observação 5.9. *Utilizando o Teorema de Dirichlet sobre progressões aritméticas, a mesma demonstração acima mostra um resultado mais forte: que se n é inteiro positivo tal que para todo p primo tenhamos n resíduo quadrático módulo p, então n é um quadrado perfeito. Isso ocorre porque podemos escolher c primo satisfazendo as congruências desejadas.*

5.2. Decomposição em Corpos Quadráticos

Seja $p \in \mathbb{N}$ primo, e consideremos um polinômio de segundo grau $ax^2+bx+c \in \mathbb{F}_p[x]$. Essa equação terá soluções em $\mathbb{F}_p$ se e só se b^2-4ac for um quadrado em $\mathbb{F}_p$, ou seja, se e só se $\left(\dfrac{b^2-4ac}{p}\right) \in \{0,1\}$. Sabendo calcular os símbolos de Legendre, conseguimos estudar a decomposição de ideais primos em um corpo quadrático $K=\mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$. Pelo Teorema 4.22, a fatoração de um ideal primo $p\mathbb{Z} \lhd \mathbb{Z}$ em $\mathcal{O}_K$ depende da fatoração do polinômio minimal de δ, onde $\delta=\sqrt{d}$ se $d \equiv 2,3 \pmod 4$ e $\delta=\frac{1+\sqrt{d}}{2}$ se $d \equiv 1 \pmod 4$.

Consideremos inicialmente $d \equiv 2,3 \pmod 4$. Nesse caso, o polinômio minimal a se considerar é $P(x) \coloneqq P_{\sqrt{d},\mathbb{Q}}(x)=x^2-d$. Seja $p \in \mathbb{N}$ um primo ímpar. Então $\overline{P}(x)=x^2-\overline{d}$ possui raiz em $\mathbb{F}_p$ se e só se d for resíduo quadrático módulo p.

- Se $\left(\dfrac{d}{p}\right)=-1$, então $\overline{P}(x)$ é irredutível, e nesse caso $p\mathcal{O}_K$ é um ideal primo de $\mathcal{O}_K$. Isto é, p é totalmente inerte.
- Se $\left(\dfrac{d}{p}\right)=1$, então $\overline{P}(x)$ possui duas raízes $\overline{r}$ e $-\overline{r}$ em $\mathbb{F}_p$. Desse modo, $\overline{P}$ se fatora como $\overline{P}(x)=(x-\overline{r})(x+\overline{r})$, e portanto a fatoração de $p\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ é:
$$p\mathcal{O}_K=(p\mathcal{O}_K+(\sqrt{d}-r)\mathcal{O}_K)\cdot(p\mathcal{O}_K+(\sqrt{d}+r)\mathcal{O}_K).$$
Nesse caso, p é totalmente decomposto.
- Se $\left(\dfrac{d}{p}\right)=0$, isto é, se $p \mid d$, então $\overline{P}(x)=x^2$. Desse modo, a fatoração de $p\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ é $p\mathcal{O}_K=(p\mathcal{O}_K+\sqrt{d}\mathcal{O}_K)^2$. Nesse caso, p é totalmente ramificado.

Falta analisarmos o que ocorre para $p=2$. Nesse caso, $\overline{P}(x)=\begin{cases}x^2, & \text{se } d \text{ for par;}\\ x^2-\overline{1}, & \text{se } d \text{ for ímpar.}\end{cases}$
Note que $x^2-\overline{1}=(x-\overline{1})^2$. Assim, se d for par a fatoração de $2\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ é $2\mathcal{O}_K=(2\mathcal{O}_K+\sqrt{d}\mathcal{O}_K)^2$, e se d for ímpar a fatoração de $2\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ é $2\mathcal{O}_K=(2\mathcal{O}_K+(\sqrt{d}-1)\mathcal{O}_K)^2$. Em qualquer caso, 2 é totalmente ramificado.

Consideremos agora $d \equiv 1 \pmod 4$. Nesse caso, o polinômio minimal a se considerar é $P(x) \coloneqq P_{(1+\sqrt{d})/2,\mathbb{Q}}(x)=x^2-x+\frac{1-d}{4}$, como é fácil verificar. Seja $p \in \mathbb{N}$ um primo ímpar. O discriminante dessa equação é $(-1)^2-4\cdot 1\cdot\left(\frac{1-d}{4}\right)=1+(d-1)=d$. Assim, como no caso anterior, basta analisarmos $\left(\dfrac{d}{p}\right)$. Comecemos observando que em $\mathbb{F}_p$ temos $1/2=(p+1)/2$.

- Se $\left(\dfrac{d}{p}\right)=-1$, então $\overline{P}(x)$ é irredutível, e nesse caso $p\mathcal{O}_K$ é um ideal primo de $\mathcal{O}_K$. Isto é, p é totalmente inerte.
- Se $\left(\dfrac{d}{p}\right)=1$, então $\overline{P}(x)$ possui duas raízes $\overline{\frac{1+r}{2}}$ e $\overline{\frac{1-r}{2}}$ em $\mathbb{F}_p$, onde $\overline{r}^2=\overline{d}$. Desse modo:
$$\overline{P}(x)=\left(x-\overline{\tfrac{1+r}{2}}\right)\left(x-\overline{\tfrac{1-r}{2}}\right)=\left(x-\overline{\tfrac{(1+r)(p+1)}{2}}\right)\left(x-\overline{\tfrac{(1-r)(p+1)}{2}}\right),$$
e a fatoração de $p\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ é:
$$p\mathcal{O}_K = \left(p\mathcal{O}_K+\left(\tfrac{1+\sqrt{d}}{2}-\tfrac{(1+r)(p+1)}{2}\right)\mathcal{O}_K\right)\cdot\left(p\mathcal{O}_K+\left(\tfrac{1+\sqrt{d}}{2}-\tfrac{(1-r)(p+1)}{2}\right)\mathcal{O}_K\right)$$
(note que é necessário substituir $1/2$ por $(p+1)/2$, pois $(1+r)/2$ não está necessariamente em $\mathbb{Z}$). Nesse caso, p é totalmente decomposto.

- Se $\left(\frac{d}{p}\right) = 0$, isto é, se $p \mid d$, então $\overline{P}(x)$ possui raiz dupla $1/2$. Desse modo:

$$\overline{P}(x) = \left(x - \overline{\tfrac{1}{2}}\right) = \left(x - \overline{\tfrac{p+1}{2}}\right),$$

e a fatoração de $p\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ é

$$p\mathcal{O}_K = \left(p\mathcal{O}_K + \left(\tfrac{1+\sqrt{d}}{2} - \tfrac{p+1}{2}\right)\mathcal{O}_K\right)^2 = \left(p\mathcal{O}_K + \tfrac{\sqrt{d}-p}{2}\mathcal{O}_K\right)^2.$$

Nesse caso, p é totalmente ramificado.

Falta analisarmos o que ocorre para $p = 2$. Nesse caso, $\overline{P}(x) = \begin{cases} x^2 - x, & \text{se } d \equiv 1 \pmod 8; \\ x^2 + x + \overline{1}, & \text{se } d \equiv 5 \pmod 8. \end{cases}$
Observemos que $x^2 - x = x(x - \overline{1})$ e $x^2 + x + \overline{1}$ é irredutível em $\mathbb{F}_2[x]$, pois não tem raízes em $\mathbb{F}_2$. Assim, se $d \equiv 1 \pmod 8$ a fatoração de $2\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ é

$$\begin{aligned} 2\mathcal{O}_K &= \left(2\mathcal{O}_K + \tfrac{1+\sqrt{d}}{2} \cdot \mathcal{O}_K\right) \cdot \left(2\mathcal{O}_K + \left(\tfrac{1+\sqrt{d}}{2} - 1\right) \cdot \mathcal{O}_K\right) \\ &= \left(2\mathcal{O}_K + \tfrac{\sqrt{d}+1}{2} \cdot \mathcal{O}_K\right) \cdot \left(2\mathcal{O}_K + \tfrac{\sqrt{d}-1}{2} \cdot \mathcal{O}_K\right), \end{aligned}$$

e se $d \equiv 5 \pmod 8$ o ideal $2\mathcal{O}_K$ é primo. Desse modo, se $d \equiv 1 \pmod 8$ o ideal $2\mathcal{O}_K$ é totalmente decomposto, e se $d \equiv 5 \pmod 8$ o ideal $2\mathcal{O}_K$ é totalmente inerte.

Observe que em ambos os casos o número de ideais ramificados (que nesse caso equivalem aos ideais totalmente ramificados) é finito, já que apenas um número finito de primos divide d. Isso é um caso particular do Corolário 4.26. Além disso, pelo Corolário 4.24, p ser ramificado em $\mathcal{O}_K$ equivale a p dividir d_K. Como $d_K = \begin{cases} 4d, & \text{se } d \equiv 2, 3 \pmod 4; \\ d, & \text{se } d \equiv 1 \pmod 4. \end{cases}$ isso equivale a dizer que $p \mid d$ ou $p = 2$ e $d \equiv 3 \pmod 4$. A análise que fizemos acima da decomposição dos ideais primos em $\mathcal{O}_K$ mostra que de fato esses são os únicos casos em que $p\mathcal{O}_K$ é ramificado. Essa análise, de fato, nos diz que o tipo de decomposição de um primo $p \in \mathbb{N}$ em $\mathcal{O}_K$ se dá da seguinte forma:

Proposição 5.10. *Sejam $d \in \mathcal{D}$, $K = \mathbb{Q}(\sqrt{d})$ e $p \in \mathbb{N}$ primo. Então:*

(a) p é totalmente ramificado em $\mathcal{O}_K$ se e somente se $p \mid d$ ou se $p = 2$ e $d \equiv 3 \pmod 4$.

(b) p é totalmente decomposto em $\mathcal{O}_K$ se e somente se p for ímpar e $\left(\frac{d}{p}\right) = 1$ ou se $p = 2$ e $d \equiv 1 \pmod 8$.

(c) p é totalmente inerte em $\mathcal{O}_K$ se e somente se p for ímpar e $\left(\frac{d}{p}\right) = -1$ ou se $p = 2$ e $d \equiv 5 \pmod 8$.

Exemplo 5.11. *O resultado acima aplicado para $d = -1$ nos permite reobter a caracterização dos tipos de decomposição em $\mathbb{Z}[i]$. Para isso notemos que pelo resultado acima, dado $p \in \mathbb{N}$ primo, temos:*

- *p é totalmente ramificado em $\mathbb{Z}[i]$ se e somente se $p = 2$.*
- *p é totalmente decomposto em $\mathbb{Z}[i]$ se e somente se p for ímpar e $\left(\frac{-1}{p}\right) = 1$.*
- *p é totalmente inerte em $\mathbb{Z}[i]$ se e somente se p for ímpar e $\left(\frac{-1}{p}\right) = -1$.*

Mas pelo Critério de Euler, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, e portanto -1 é resíduo quadrático módulo p se e somente se $p \equiv 1 \pmod 4$. Isso nos dá a caracterização que tínhamos anteriormente.

O exemplo acima nos mostra que para verificarmos se -1 é resíduo quadrático módulo p basta analisarmos o resto de p na divisão por 4. Com a Lei de Reciprocidade Quadrática em mãos, conseguimos mostrar que vale um mesmo tipo de critério em geral. Mais explicitamente, que o tipo de decomposição de um primo p em $\mathcal{O}_K$ depende unicamente do resto de p na divisão por $|d_K|$.

Para ver isso, escrevamos $d = 2^m d'$, com $m \in \{0, 1\}$ e d' ímpar (lembre que d é livre de quadrados). Seja $c \in \mathbb{Z}$ ímpar e primo com d_K. Então, pela Lei de Reciprocidade Quadrática, nós temos:

$$\left(\frac{d}{c}\right) = \left(\frac{2^m d'}{c}\right) = \left(\frac{2}{c}\right)^m \left(\frac{d'}{c}\right) = (-1)^{\frac{c^2-1}{8}m}(-1)^{\frac{c-1}{2}\cdot\frac{d'-1}{2}}\left(\frac{c}{|d'|}\right). \tag{5.1}$$

Essa equação nos garante que $\left(\frac{d}{c}\right)$ só depende do resto de c módulo $|d_K|$. De fato:

- Se $d \equiv 1 \pmod 4$, então $m = 0$ e $d' = d$. Assim, a equação (5.1) se torna simplesmente $\left(\frac{d}{c}\right) = \left(\frac{c}{|d|}\right)$, já que $(d-1)/2$ é par. Logo $\left(\frac{d}{c}\right) = \left(\frac{c}{|d|}\right)$ só depende do resto da divisão de c por $|d| = |d_K|$.
- Se $d \equiv 2 \pmod 4$, então $m = 1$. Assim, a equação (5.1) se torna

  $$\left(\frac{d}{c}\right) = (-1)^{\frac{c^2-1}{8}+\frac{c-1}{2}\cdot\frac{d'-1}{2}}\left(\frac{c}{|d'|}\right).$$

  Note que essa expressão depende apenas de $c \pmod 8$ e $c \pmod{|d'|}$. Ou seja, pelo Teorema Chinês dos Restos depende apenas de $c \pmod{8|d'|}$. Mas $8|d'| = |4d| = |d_K|$, como queríamos.
- Se $d \equiv 3 \pmod 4$, então $m = 0$ e $d' = d$. Assim, a equação (5.1) se torna simplesmente $\left(\frac{d}{c}\right) = (-1)^{\frac{c-1}{2}}\left(\frac{c}{|d|}\right)$, já que $(d-1)/2$ é ímpar. Note que essa expressão depende apenas de $c \pmod 4$ e $c \pmod{|d|}$. Assim, pelo Teorema Chinês dos Restos, depende apenas de $c \pmod{4|d|}$. Mas $4|d| = |4d| = |d_K|$, como queríamos.

Assim, mostramos que $\left(\frac{d}{c}\right)$ só depende do resto de c módulo $|d_K|$. Tomando c primo que não divide d nós obtemos a afirmação desejada de que o tipo de decomposição de um primo p em $\mathcal{O}_K$ depende unicamente do resto de p na divisão por $|d_K|$.

Na verdade, podemos obter um pouco mais do que isso. Baseado na conta acima, chamemos $S_K := \{c \in \mathbb{Z} \colon \operatorname{mdc}(d_K, c) = 1\}$, e consideremos $\chi_K \colon S_K \to \{-1, 1\}$ dado por

$$\chi_K(c) = \begin{cases} \left(\frac{c}{|d|}\right), & \text{se } d \equiv 1 \pmod 4; \\ (-1)^{\frac{c^2-1}{8}+\frac{c-1}{2}\cdot\frac{d'-1}{2}}\left(\frac{c}{|d'|}\right), & \text{se } d \equiv 2 \pmod 4; \\ (-1)^{\frac{c-1}{2}}\left(\frac{c}{|d|}\right), & \text{se } d \equiv 3 \pmod 4. \end{cases}$$

Observe que se c for ímpar, $\chi_K(c)$ nada mais é do que $\left(\frac{d}{c}\right)$, devido à conta que fizemos acima, e que c só pode ser par se $d \equiv 1 \pmod 4$, pois caso contrário $2 \mid d_K$. A função χ_K possui as seguinte propriedades:

Teorema 5.12. *(a) χ_K não depende da classe de c módulo $|d_K|$, ou seja, se $b, c \in S_K$ são tais que $b \equiv c \pmod{|d_K|}$ então $\chi_K(b) = \chi_K(c)$.*

(b) χ_K *é um homomorfismo sobrejetor de semigrupos multiplicativos.*

(c) Dado $p \in S_K$ *primo, temos que* $d \in \mathrm{RQ}(p) \iff \chi_K(p) = 1$*. Assim,* p *é decomposto se e só se* $\chi_K(p) = 1$*, e* p *é inerte se e só se* $\chi_K(p) = -1$*.*

Demonstração. (a) Segue diretamente pela análise que já fizemos acima. Note que o fato de c poder ser par não interfere nessa análise.

(b) Sejam $a, b \in S_K$. Se $d \equiv 2, 3 \pmod 4$, já sabemos que $\chi_K(a) = \left(\frac{d}{a}\right)$ e $\chi_K(b) = \left(\frac{d}{b}\right)$, e portanto $\chi_K(ab) = \left(\frac{d}{ab}\right) = \left(\frac{d}{a}\right)\left(\frac{d}{b}\right) = \chi_K(a)\chi_K(b)$. (poderíamos também ter feito a conta direta). Se $d \equiv 1 \pmod 4$, nós temos $\chi_K(ab) = \left(\frac{ab}{|d|}\right) = \left(\frac{a}{|d|}\right)\left(\frac{b}{|d|}\right) = \chi_K(a)\chi_K(b)$.

Falta mostrarmos que χ_K é sobrejetor. Em todos os casos, $\chi_K(1) = 1$, de modo que basta verificar que -1 está na imagem de χ_K. Se isso não ocorresse, então em particular para todo c inteiro positivo ímpar nós teríamos $\left(\frac{d}{c}\right) \in \{0, 1\}$. Mas como vimos na Proposição 5.8, isso implicaria que d é um quadrado perfeito, um absurdo já que $d \in \mathcal{D}$. Isso mostra que χ_K é sobrejetora.

(c) Para p ímpar, isso segue diretamente do fato de que $\chi_K(p) = \left(\frac{d}{p}\right)$ e da Proposição 5.10. Para o caso $p = 2$, devemos ter $d \equiv 1 \pmod 4$, e assim $\chi_K(2) = \left(\frac{2}{|d|}\right) = (-1)^{\frac{d^2-1}{8}}$. Assim, $\chi_K(2) = 1$ se $d \equiv 1 \pmod 8$ e $\chi_K(2) = -1$ se $d \equiv 5 \pmod 8$. O resultado desejado segue então da Proposição 5.10.

O homomorfismo χ_K é chamado de **caráter quadrático** de K. Podemos estender χ_K a um homomorfismo sobrejetor de semigrupos multiplicativos $\chi_K \colon \mathbb{Z} \to \{-1, 0, 1\}$ definindo $\chi_K(c) = 0$ se $c \in \mathbb{Z} \setminus S_K$. Com isso:

Corolário 5.13. *Para qualquer número primo* $p \in \mathbb{N}$*, nós temos:*

$$\chi_K(p) = \begin{cases} 1 \text{ se e somente se } p \text{ for decomposto em } K; \\ -1 \text{ se e somente se } p \text{ for inerte em } K; \\ 0 \text{ se e somente se } p \text{ for ramificado em } K. \end{cases}$$

Devido ao Teorema de Dirichlet sobre progressões aritméticas, sabemos que para todo corpo quadrático K temos um número infinito de primos decompostos e um número infinito de primos inertes, já que χ_K é sobrejetor.

Exemplo 5.14. *Seja* $K = \mathbb{Q}(\sqrt{-3})$*. Chamamos o anel de inteiros algébricos* $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ *de* ***anel dos inteiros de Eisenstein****. Com os resultados acima, conseguimos determinar rapidamente quais primos de* $\mathbb{N}$ *são decompostos, inertes e ramificados nesse anel. Nesse caso,* $d_K = d = -3$*, e dado* $c \in S_K$ *temos* $\chi_K(c) = \left(\frac{c}{3}\right)$*. Mas* $\left(\frac{0}{3}\right) = 0$*,* $\left(\frac{1}{3}\right) = 1$ *e* $\left(\frac{2}{3}\right) = -1$*, como é fácil verificar. Assim, os primos decompostos em* $\mathcal{O}_K$ *são os da forma* $3k + 1$*, os primos inertes são os da forma* $3k + 2$ *e os primos ramificados são aqueles da forma* $3k$ *(ou seja,* 3 *é o único primo ramificado nesse anel).*

□

5.3. Decomposição em Corpos Ciclotômicos

Sejam n um inteiro positivo, $\zeta \in \mathbb{C}$ uma raiz primitiva n-ésima da unidade e $K = \mathbb{Q}(\zeta)$. Nessa seção, estudaremos a decomposição de ideais primos de $\mathbb{Z}$ em K. De fato, obteremos um resultado parecido com o da seção passada. Mais especificamente, mostraremos que o tipo de decomposição de um primo em K depende unicamente de sua classe de congruência módulo n, assim como no caso de corpos quadráticos dependia de sua classe módulo $|d_K|$.

Primeiro, provaremos que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\,\zeta + \cdots + \mathbb{Z}\,\zeta^{\varphi(n)-1} = \mathbb{Z}[\zeta]$, como havíamos prometido no Capítulo 2. Assim, $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ será uma base integral de $\mathcal{O}_K$. Comecemos com o seguinte lema:

Lema 5.15. *Sejam p um número primo e r um inteiro positivo. Sejam ζ uma raiz primitiva p^r-ésima da unidade e $K = \mathbb{Q}(\zeta)$. Então o ideal principal $(1-\zeta)\mathcal{O}_K \lhd \mathcal{O}_K$ é primo, e a fatoração de $p\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ é $p\mathcal{O}_K = ((1-\zeta)\mathcal{O}_K)^{\varphi(p^r)}$. Em particular, p é totalmente ramificado em K, e portanto $\mathcal{O}_K/(1-\zeta)\mathcal{O}_K = \mathbb{F}_p$, com as devidas identificações.*

Demonstração. Como já vimos, o polinômio minimal de ζ sobre $\mathbb{Q}$ é[2]

$$\prod_{g \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (x - \zeta^g) = \Phi_{p^r}(x) = x^{(p-1)p^{r-1}} + \cdots + x^{2p^{r-1}} + x^{p^{r-1}} + 1.$$

Avaliando em 1, obtemos portanto $\prod_{g \in (\mathbb{Z}/p^r\mathbb{Z})^\times}(1-\zeta^g) = p$. Para cada $g \in (\mathbb{Z}/p^r\mathbb{Z})^\times$, definamos

$$\varepsilon_g \coloneqq \frac{1-\zeta^g}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{g-1}.$$

Então $\varepsilon_g \in \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$ é um inteiro algébrico. Temos $\varepsilon_g \in \mathcal{O}_K^\times$. De fato, sendo $g' \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ tal que $gg' \equiv 1 \pmod{p^r}$, nós temos:

$$\varepsilon_g^{-1} = \frac{1-\zeta}{1-\zeta^g} = \frac{1-(\zeta^g)^{g'}}{1-\zeta^g} = 1 + \zeta^g + \cdots + \zeta^{g(g'-1)} \in \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K,$$

como queríamos. Sendo assim:

$$p = \prod_{g \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (1-\zeta^g) = \prod_{g \in (\mathbb{Z}/p^r\mathbb{Z})^\times} [\varepsilon_g(1-\zeta)] = \varepsilon(1-\zeta)^{\varphi(p^r)},$$

onde $\varepsilon \coloneqq \prod_{g \in (\mathbb{Z}/p^r\mathbb{Z})^\times} \varepsilon_g \in \mathcal{O}_K^\times$. Isso mostra que $p\mathcal{O}_K = ((1-\zeta)\mathcal{O}_K)^{\varphi(p^r)}$. Mas uma vez que $[K : \mathbb{Q}] = \varphi(p^r)$, vemos pela identidade fundamental que $(1-\zeta)\mathcal{O}_K$ é ideal primo. Logo p é totalmente ramificado, de modo que $f_{(1-\zeta)\mathcal{O}_K} = 1$, isto é, $[\mathcal{O}_K/(1-\zeta)\mathcal{O}_K : \mathbb{F}_p] = 1$. Mas isso significa que $\mathcal{O}_K/(1-\zeta)\mathcal{O}_K = \mathbb{F}_p$. □

Com esse lema em mãos, conseguimos finalmente determinar $\mathcal{O}_K$:

Teorema 5.16. *Sejam n um inteiro positivo, $\zeta \in \mathbb{C}$ uma raiz primitiva n-ésima da unidade e $K = \mathbb{Q}(\zeta)$. Então $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\,\zeta + \cdots + \mathbb{Z}\,\zeta^{\varphi(n)-1} = \mathbb{Z}[\zeta]$. Assim, $\mathcal{O}_K$ possui base integral $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$. Além disso, se $n = p_1^{r_1} \cdots p_k^{r_k}$ for a fatoração prima de n em $\mathbb{Z}$, então:*

$$d_K = (-1)^{\frac{k\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{j=1}^k p_j^{\varphi(n)/(p_j-1)}}.$$

[2]Identificando $\mathbb{Z}/p^r\mathbb{Z}$ como seu conjunto de representantes $\{0, 1, \ldots, p^r - 1\} \subseteq \mathbb{Z}$ por simplicidade.

Demonstração. Comecemos provando esse resultado para $n = p^r$, onde p é um primo e r é um inteiro positivo ($r \geq 2$ se tivermos $p = 2$). Então, pela Proposição 2.29, temos:

$$\Delta(1, \zeta, \ldots, \zeta^{p^r} - 1) = (-1)^{\frac{\varphi(p^r)}{2}} p^s,$$

para $s := p^{r-1}(rp - r - 1)$. Pela Proposição 1.41, sabemos então que

$$p^s \mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K. \tag{5.2}$$

Pelo lema anterior, nós temos $\mathcal{O}_K/(1-\zeta)\mathcal{O}_K = \mathbb{F}_p$. Na identificação que fizemos, isso significa que toda classe de congruência módulo $(1-\zeta)\mathcal{O}_K$ possui um inteiro, ou seja, que $(1-\zeta)\mathcal{O}_K + \mathbb{Z} = \mathcal{O}_K$, e com maior razão $(1-\zeta)\mathcal{O}_K + \mathbb{Z}[\zeta] = \mathcal{O}_K$.

Multiplicando essa igualdade por $1-\zeta$, obtemos:

$$(1-\zeta)^2\mathcal{O}_K + (1-\zeta)\,\mathbb{Z}[\zeta] = (1-\zeta)\mathcal{O}_K.$$

Substituindo $(1-\zeta)\mathcal{O}_K$ pela expressão à esquerda na equação inicial, obtemos:

$$\mathcal{O}_K = (1-\zeta)\mathcal{O}_K + \mathbb{Z} = (1-\zeta)^2\mathcal{O}_K + (1-\zeta)\,\mathbb{Z}[\zeta] + \mathbb{Z},$$

e com maior razão $\mathcal{O}_K = (1-\zeta)^2\mathcal{O}_K + \mathbb{Z}[\zeta]$. Provemos por indução que para todo $t \geq 1$ temos $\mathcal{O}_K = (1-\zeta)^t\mathcal{O}_K + \mathbb{Z}[\zeta]$. Já fizemos os casos base. Suponhamos então que essa igualdade valha para certo $t \geq 1$. Multiplicando a igualdade $\mathcal{O}_K = (1-\zeta)\mathcal{O}_K + \mathbb{Z}[\zeta]$ por $(1-\zeta)^t$, obtemos:

$$(1-\zeta)^t\mathcal{O}_K = (1-\zeta)^{t+1}\mathcal{O}_K + (1-\zeta)^t\,\mathbb{Z}[\zeta].$$

Desse modo,

$$\mathcal{O}_K = (1-\zeta)^t\mathcal{O}_K + \mathbb{Z}[\zeta] = (1-\zeta)^{t+1}\mathcal{O}_K + (1-\zeta)^t\,\mathbb{Z}[\zeta] + \mathbb{Z}[\zeta],$$

e com maior razão $\mathcal{O}_K = (1-\zeta)^{t+1}\mathcal{O}_K + \mathbb{Z}[\zeta]$, concluindo a indução.

Façamos agora $t = s\varphi(p^r)$. Assim:

$$\mathcal{O}_K = (1-\zeta)^{s\varphi(p^r)}\mathcal{O}_K + \mathbb{Z}[\zeta] = [(1-\zeta)\mathcal{O}_K]^{s\varphi(p^r)} + \mathbb{Z}[\zeta] = (p\mathcal{O}_K)^s + \mathbb{Z}[\zeta] = p^s\mathcal{O}_K + \mathbb{Z}[\zeta],$$

pelo lema acima. Mas juntando (5.2) com a igualdade acima temos então:

$$\mathcal{O}_K = p^s\mathcal{O}_K + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta],$$

como desejado. Assim, provamos o teorema para as potências de primos.

Consideremos agora o caso geral, e seja $n = p_1^{r_1} \cdots p_k^{r_k}$ a fatoração prima de n. Então para $1 \leq j \leq k$ o número $\zeta_j := \zeta^{n/p_j^{r_j}}$ é uma raiz primitiva $p_j^{r_j}$-ésima da unidade. Pela Proposição 2.30, nós temos $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1)\cdots\mathbb{Q}(\zeta_k)$, e para $1 \leq i \leq k$ nós temos

$$(\mathbb{Q}(\zeta_1)\cdots\mathbb{Q}(\zeta_{i-1})) \cap \mathbb{Q}(\zeta_i) = \mathbb{Q}\,.$$

A ideia é aplicarmos o Teorema 2.9 várias vezes. Pelo que acabamos de provar, para $1 \leq i \leq k$ os elementos $1, \zeta_i, \ldots, \zeta_i^{\varphi(p_i^{r_i})-1}$ formam uma base integral de $\mathbb{Q}(\zeta_i)$. Além disso, a Proposição 2.29 nos diz que $\Delta(1, \zeta_i, \ldots, \zeta_i^{\varphi(p_i^{r_i})-1})$ é a menos de sinal uma potência de p_i. Desse modo, os k discriminantes obtidos são todos primos entre si. Logo estamos nas condições de aplicar 2.9 repetidamente, e obtemos que uma base integral de $\mathbb{Q}(\zeta)$ é dada por

$$\{\zeta_1^{j_1} \cdots \zeta_k^{j_r} : 0 \leq j_i \leq r_i - 1 \text{ para } 1 \leq i \leq k\}.$$

Mas cada um desses elementos é uma potência de ζ. Assim, concluímos que $\mathcal{O}_K \subseteq \mathbb{Z}[\zeta]$ e portanto $\mathcal{O}_K = \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\,\zeta + \cdots + \mathbb{Z}\,\zeta^{\varphi(n)-1}$, o que mostra que $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ é base integral de

$\mathcal{O}_K$. Determinemos agora d_K. Para isso, faremos indução no número k de fatores primos distintos na fatoração de n. Para $k=1$, $n=p_1^{r_1}$ é uma potência de primo, e temos:

$$\begin{aligned}
(-1)^{\frac{k\varphi(n)}{2}} \cdot \frac{n^{\varphi(n)}}{\prod_{j=1}^{k} p_j^{\varphi(n)/(p_j-1)}} &= (-1)^{\frac{\varphi(n)}{2}} \cdot \frac{n^{\varphi(n)}}{p_1^{\varphi(n)/(p_1-1)}} \\
&= (-1)^{\frac{\varphi(p_1^{r_1})}{2}} \cdot \frac{p_1^{r_1\varphi(p_1^{r_1})}}{p_1^{\varphi(p_1^{r_1})/(p_1-1)}} \\
&= (-1)^{\frac{\varphi(p_1^{r_1})}{2}} \cdot \frac{p_1^{r_1(p_1-1)p_1^{r_1-1}}}{p_1^{(p_1-1)p_1^{r_1-1}/(p_1-1)}} \\
&= (-1)^{\frac{\varphi(p_1^{r_1})}{2}} \cdot \frac{p_1^{r_1(p_1-1)p_1^{r_1-1}}}{p_1^{p_1^{r_1-1}}} \\
&= (-1)^{\frac{\varphi(p_1^{r_1})}{2}} \cdot p_1^{p_1^{r_1-1}(r_1p_1-r_1-1)} = d_K,
\end{aligned}$$

pela Proposição 2.29. Suponhamos agora que a igualdade desejada valha para produtos de até $k-1$ primos, e provemos que vale para $n=p_1^{r_1}\cdots p_k^{r_k}$. Sabemos que o resultado vale em particular para $a := p_1^{r_1}\cdots p_{k-1}^{r_{k-1}}$ e para $b=p_k^{r_k}$. Sejam α e β raízes primitivas a-ésima e b-ésima da unidade, respectivamente. Como a e b são primos entre si, a Proposição 2.30 nos garante que $\mathbb{Q}(\zeta)=\mathbb{Q}(\alpha\beta)=\mathbb{Q}(\alpha)\mathbb{Q}(\beta)$ e que $\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)=\mathbb{Q}$. Aplicando o Teorema 2.9 a esses dois corpos, temos então (lembremos que $\varphi(a)\varphi(b)=\varphi(ab)=\varphi(n)$):

$$\begin{aligned}
d_K &= d_{\mathbb{Q}(\alpha)}^{\varphi(b)} \cdot d_{\mathbb{Q}(\beta)}^{\varphi(a)} \\
&= \left((-1)^{\frac{(k-1)\varphi(a)}{2}} \cdot \frac{a^{\varphi(a)}}{\prod_{j=1}^{k-1} p_j^{\varphi(a)/(p_j-1)}}\right)^{\varphi(b)} \cdot \left((-1)^{\frac{\varphi(b)}{2}} \cdot \frac{b^{\varphi(b)}}{p_k^{\varphi(b)/(p_k-1)}}\right)^{\varphi(a)} \\
&= (-1)^{\frac{k\varphi(a)\varphi(b)}{2}} \cdot \frac{(ab)^{\varphi(a)\varphi(b)}}{\prod_{j=1}^{k} p_j^{\varphi(a)\varphi(b)/(p_j-1)}} \\
&= (-1)^{\frac{k\varphi(n)}{2}} \cdot \frac{n^{\varphi(n)}}{\prod_{j=1}^{k} p_j^{\varphi(n)/(p_j-1)}},
\end{aligned}$$

como desejado. □

O teorema acima mostra que o anel de inteiros algébricos de um corpo ciclotômico $K=\mathbb{Q}(\zeta)$ é monogêneo. Isso nos permite aplicar o Teorema 4.22 para estudarmos as decomposições dos primos de $\mathbb{N}$ em $\mathcal{O}_K=\mathbb{Z}[\zeta]$.

Teorema 5.17. *Sejam $n>1$ inteiro, $\zeta\in\mathbb{C}$ uma raiz primitiva n-ésima da unidade e $K=\mathbb{Q}(\zeta)$. Seja $n=\prod_p p^{\nu_p}$ a fatoração prima de n, onde p varia entre os primos positivos (note que $\nu_p=0$ para os primos que não dividem n, de forma que esse produtório na verdade é finito). Para cada primo $p\in\mathbb{N}$ definamos f_p como sendo a ordem de $\overline{p}$ no grupo multiplicativo $(\mathbb{Z}/(n/p^{\nu_p})\mathbb{Z})^\times$. Então em $\mathcal{O}_K$ o ideal $p\mathcal{O}_K$ tem fatoração da forma $p\mathcal{O}_K=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^{\varphi(p^{\nu_p})}$, onde $\mathfrak{P}_1,\ldots,\mathfrak{P}_g$ são ideais primos distintos de $\mathcal{O}_K$, todos com grau de inércia f_p. Note que sabendo f_p podemos determinar g pela identidade fundamental, uma vez que devemos ter $\varphi(p^{\nu_p})f_pg=\varphi(n)$.*

Demonstração. Pelo Teorema 4.22, basta mostrarmos que a fatoração prima do polinômio ciclotômico $\overline{\Phi_n}\in\mathbb{F}_p[x]$ é da forma $\overline{\Phi_n}=(\overline{P}_1\cdots\overline{P}_g)^{\varphi(p^{\nu_p})}$, com cada $\overline{P}_j\in\mathbb{F}_p[x]$ irredutível de grau f_p. Chamemos $m:=n/p^{\nu_p}$. Sejam $\xi_1,\ldots,\xi_{\varphi(m)}$ as raízes primitivas m-ésimas da unidade e

$\eta_1, \ldots, \eta_{\varphi(p^{\nu_p})}$ as raízes primitivas p^{ν_p}-ésimas da unidade. Então, pela Proposição 2.30, em $\mathcal{O}_K[x]$ vale a fatoração:

$$\Phi_n(x) = \prod_{i=1}^{\varphi(m)} \prod_{j=1}^{\varphi(p^{\nu_p})} (x - \xi_i \eta_j).$$

Notemos agora que em $\mathbb{F}_p[x]$ temos $x^{p^{\nu_p}} - 1 = (x-1)^{p^{\nu_p}}$. Se $\mathfrak{P} \lhd \mathcal{O}_K$ for um primo sobre p, em $(\mathcal{O}_K/\mathfrak{P})[x]$ temos a fatoração

$$x^{p^{\nu_p}} - 1 = (x-1) \prod_{j=1}^{\varphi(p^{\nu_p})} (x - \overline{\eta}_j).$$

Mas sendo $\mathcal{O}_K/\mathfrak{P}$ uma extensão de $\mathbb{F}_p$, a fatoração obtida anteriormente também vale. Por unicidade, concluímos que cada $\eta_j \equiv 1 \pmod{\mathfrak{P}}$. Mas então, em $(\mathcal{O}_K/\mathfrak{P})[x]$, nós temos:

$$\overline{\Phi}_n(x) = \prod_{i=1}^{\varphi(m)} \prod_{j=1}^{\varphi(p^{\nu_p})} (x - \overline{\xi_i} \cdot \overline{\eta_j}) = \prod_{i=1}^{\varphi(m)} \prod_{j=1}^{\varphi(p^{\nu_p})} (x - \overline{\xi_i}) = \overline{\Phi}_m(x)^{\varphi(p^{\nu_p})}.$$

Assim, basta mostrarmos que $\overline{\Phi}_m(x)$ se fatora em $\mathbb{F}_p[x]$ como $\overline{P}_1(x) \cdots \overline{P}_g(x)$, onde cada $\overline{P}_j$ possui grau f_p. Notemos que por definição f_p é o menor inteiro positivo tal que $p^{f_p} \equiv 1 \pmod{m}$. Como $p \nmid m$, o polinômio $x^m - \overline{1} \in \mathbb{F}_p[x]$ é separável, e portanto $\overline{\Phi}_m$ também o é. Assim, a fatoração de $\overline{\Phi}_m$ em $\mathbb{F}_p[x]$ é da forma $\overline{P}_1 \cdots \overline{P}_g$, onde os $\overline{P}_j$'s são irredutíveis dois a dois distintos.

Resta apenas mostrar que cada um desses polinômios tem grau f_p. Todas as raízes de $\overline{\Phi}_m$ são da forma $\overline{\xi}$, para $\xi \in K$ uma raiz primitiva m-ésima da unidade. Como $x^m - \overline{1} \in (\mathcal{O}_K/\mathfrak{P})[x]$ é separável, suas raízes $1, \overline{\xi}, \overline{\xi}^2, \ldots, \overline{\xi}^{m-1} \in \mathcal{O}_K/\mathfrak{P}$ são duas a duas distintas. Como $\overline{\xi}^m = \overline{\xi^m} = 1$, concluímos que $\overline{\xi}$ é uma raiz primitiva m-ésima da unidade em $\mathcal{O}_K/\mathfrak{P}$, e portanto pelo Teorema 2.31 temos $\mathbb{F}_p[\overline{\xi}] = \mathbb{F}_{p^{f_p}}$. Assim, o polinômio minimal de ξ sobre $\mathbb{F}_p[x]$ tem grau f_p. Isso conclui a demonstração, uma vez que cada $\overline{P}_j$ é o polinômio minimal de uma raiz de $\overline{\Phi}_m$. □

Para fins práticos, sempre podemos supor n ímpar ou múltiplo de 4. De fato, se $n = 2m$ para algum m ímpar, então os corpos ciclotômicos associados a n e a m coincidem. Isto é, $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^2)$. De fato, por um lado é claro que $\mathbb{Q}(\zeta^2) \subseteq \mathbb{Q}(\zeta)$. Mas

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = \varphi(2m) = \varphi(2)\varphi(m) = \varphi(m) = [\mathbb{Q}(\zeta^2) : \mathbb{Q}],$$

de forma que temos a igualdade desejada. Como consequência direta do teorema acima, obtemos:

Corolário 5.18. *Suponhamos que n seja ímpar ou múltiplo de 4, e seja $p \in \mathbb{N}$ primo.*

(a) p será ramificado em $\mathbb{Q}(\zeta)$ se e só se $p \mid n$.

(b) p será totalmente decomposto em $\mathbb{Q}(\zeta)$ se e só se $p \equiv 1 \pmod{n}$. Logo, todo corpo ciclotômico possui um número infinito de ideais primos totalmente decompostos.

(c) p será totalmente inerte em $\mathbb{Q}(\zeta)$ se e só se $\overline{p}$ for um gerador do grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^\times$.

(d) p será totalmente ramificado em $\mathbb{Q}(\zeta)$ se e só se $n = p^{\nu_p}$.

Demonstração. (a) p será ramificado em $\mathbb{Q}(\zeta)$ se e só se $\varphi(p^{\nu_p}) \geq 2$. Mas isso acontecerá se e só se $p^{\nu_p} \neq 1, p^{\nu_p} \neq 2$. Isto é, se e somente se $p \mid n$ e p for ímpar ou se $p = 2$ e $4 \mid n$. Como estamos supondo n ímpar ou múltiplo de 4, obtemos o resultado desejado.

(b) Um número primo $p \in \mathbb{Z}$ será totalmente decomposto em $\mathbb{Q}(\zeta)$ se e só se $g = \varphi(n)$. Pelo teorema acima, isso ocorre se e só se $f_p = \varphi(p^{\nu_p}) = 1 \iff p \nmid n$. Assim, f_p é a ordem de $\overline{p}$ em $(\mathbb{Z}/n\mathbb{Z})^\times$. Concluímos que p será totalmente decomposto se e só se $f_p = 1$, ou seja, se e só se $\overline{p} = \overline{1} \iff p \equiv 1 \pmod{n}$. A última observação segue do Teorema de Dirichlet sobre progressões aritméticas.

(c) Pelo teorema acima, um número primo $p \in \mathbb{Z}$ será totalmente inerte se e só se $f_p = \varphi(n)$. Nesse caso, $\varphi(p^{\nu_p}) = 1 \Rightarrow p \nmid n$. Sendo assim, f_p é a ordem de $\overline{p}$ em $(\mathbb{Z}/n\mathbb{Z})^\times$. Como esse grupo tem $\varphi(n)$ elementos, teremos $f_p = \varphi(n)$ se e só se $\overline{p}$ for um gerador desse grupo.

(d) Pelo teorema acima, um número primo $p \in \mathbb{Z}$ será totalmente ramificado se e só se tivermos $\varphi(p^{\nu_p}) = \varphi(n)$. Mas sendo $m := n/p^{\nu_p}$, temos $p \nmid m$, e portanto $\varphi(n) = \varphi(m)\varphi(p^{\nu_p})$. Assim, a igualdade $\varphi(p^{\nu_p}) = \varphi(n)$ é equivalente a $\varphi(m) = 1$, ou seja, a $m = 1$ ou $m = 2$. Como n é ímpar ou múltiplo de 4, concluímos que $n = p^{\nu_p}$.

□

Observação 5.19. *Podemos também encontrar os primos p ramificados em $Q(\zeta)$ diretamente a partir do Corolário 4.24. Além disso, os itens (c) e (d) nos dão exemplos de anéis de inteiros algébricos nos quais não existem primos de $\mathbb{Z}$ totalmente inertes ou totalmente ramificados. De fato, se $\mathbb{Z}/n\mathbb{Z}$ não for um grupo cíclico, então nenhum primo é totalmente inerte em $\mathbb{Q}(\zeta)$[3], e se n não for uma potência de primo então nenhum primo será totalmente ramificado em $\mathbb{Q}(\zeta)$.*

Suponhamos n ímpar ou múltiplo de 4. O corolário acima nos sugere que o tipo de decomposição de um primo p em $\mathbb{Q}(\zeta)$ depende apenas do resto deixado por p na divisão por n. Nos itens (b) e (c) por exemplo, vimos que o fato de p ser totalmente decomposto ou totalmente inerte dependem apenas da classe de congruência de p módulo n. Se $p \mid n$, então p é o único primo que deixa resto p na divisão por n. Mais interessante é analisar o que ocorre quando $p \nmid n$.

Observemos que pelo Teorema 5.17 o tipo de decomposição de um primo p depende somente de f_p e de $\varphi(p^{\nu_p})$. Mas $\varphi(p^{\nu_p}) = 1$, e portanto o tipo de decomposição de p depende somente de f_p, que é a ordem de $\overline{p}$ em $(\mathbb{Z}/n\mathbb{Z})^\times$. Assim, o tipo de decomposição de p depende somente do resto da divisão de p por n.

[3]E é um resultado conhecido de Teoria Elementar dos Números que $(\mathbb{Z}/n\mathbb{Z})^\times$ será cíclico se e só se $n = 1$, $n = 4$, $n = p^k$ ou $n = 2p^k$, para p primo ímpar. Veja por exemplo o Capítulo 4 de [12].

Capítulo 6

Extensões Galoisianas

No capítulo anterior, vimos como utilizar os resultados do Capítulo 4 para estudarmos os corpos quadráticos e ciclotômicos, cujos anéis de inteiros algébricos são extensões geradas por um único elemento. Mas as extensões quadráticas e ciclotômicas são particularmente especiais: todas elas são extensões galoisianas. Mais do que isso, abelianas. Neste capítulo iremos estudar extensões galoisianas de domínios de Dedekind.

6.1. Resultados Básicos e o Grupo de Decomposição

Sejam A um domínio de Dedekind, $K = Q(A)$ seu corpo de frações, L/K uma extensão galoisiana finita de grau n com grupo de Galois $G = \mathrm{Gal}(L/K)$ e $B = \overline{A}^L$. Começamos observando que para cada automorfismo $\sigma \in G$ nós temos $\sigma(B) = B$, pois se $\alpha \in B$ for raiz de um polinômio mônico em $A[x]$ então $\sigma(\alpha)$ será raiz desse mesmo polinômio. É fácil também observar que G age no conjunto dos ideais de B, e que essa ação se comporta bem com a multiplicação: dados $\mathfrak{A}, \mathfrak{B} \lhd B$ e $\sigma \in G$, temos $\sigma(\mathfrak{AB}) = \sigma(\mathfrak{A})\sigma(\mathfrak{B})$. Dado $\mathfrak{P} \lhd B$ primo, uma verificação direta nos mostra que $\sigma\mathfrak{P}$ também é um ideal primo de B, de modo que G também age no conjunto dos ideais primos de B. A proposição abaixo nos diz quais são as órbitas dessa ação:

Proposição 6.1. *Sejam $\mathfrak{p} \lhd A$ primo e $\mathfrak{P} \lhd B$ primo sobre $\mathfrak{p}$. Então, para todo $\sigma \in G$, o ideal primo $\sigma\mathfrak{P} \lhd B$ está sobre $\mathfrak{p}$. Além disso, dado $\mathfrak{Q} \lhd B$ primo sobre $\mathfrak{p}$, existe um automorfismo $\tau \in G$ tal que $\tau\mathfrak{P} = \mathfrak{Q}$. Dessa forma, as órbitas da ação de G sobre os ideais primos de B são exatamente os conjuntos da forma $\{\mathfrak{P} \lhd B \text{ primo} : \mathfrak{P} \mid \mathfrak{p}\}$, para $\mathfrak{p}$ variando entre os ideais primos de A.*

Demonstração. Dado $\sigma \in G$ qualquer, como σ fixa K nós temos $\sigma\mathfrak{P} \cap A = \mathfrak{P} \cap A = \mathfrak{p}$, mostrando que $\sigma\mathfrak{P}$ é um ideal primo sobre $\mathfrak{p}$. Seja agora $\mathfrak{Q} \lhd B$ sobre $\mathfrak{p}$. Suponhamos por absurdo que $\mathfrak{Q} \neq \sigma\mathfrak{P}$ para todo $\sigma \in G$. Então $\mathfrak{Q}$ e os $\sigma\mathfrak{P}$ são coprimos dois a dois, pela maximalidade desses ideais, e portanto podemos aplicar o Teorema Chinês dos Restos para encontrar $x \in B$ com $x \equiv 0 \pmod{\mathfrak{Q}}$ e $x \equiv 1 \pmod{\sigma\mathfrak{P}}$ para todo $\sigma \in G$.

Como A é integralmente fechado, temos $N(x) \in A$ pelo Corolário 1.30. Pelo mesmo corolário, x divide $N(x)$ em B, logo $x \in \mathfrak{Q} \Rightarrow N(x) \in \mathfrak{Q}$. Consequentemente, $N(x) \in A \cap \mathfrak{Q} = \mathfrak{p}$. Por outro lado, para todo $\sigma \in G$, $x \notin \sigma\mathfrak{P}$. Consequentemente, nenhum dos σx pertence a $\mathfrak{P}$ (se $\sigma x \in \mathfrak{P}$, teríamos $x \in \sigma^{-1}\mathfrak{P}$). Sendo $\mathfrak{P}$ primo, temos então $N(x) = \prod_{\sigma \in G} \sigma x \notin \mathfrak{P}$, um absurdo já que $N(x) \in \mathfrak{p}$. Dessa contradição concluímos que existe $\sigma \in G$ tal que $\mathfrak{Q} = \sigma\mathfrak{P}$. □

Para estudarmos melhor a extensão L/K, a "quebraremos" em extensões mais simples. Comecemos com as seguintes definições:

Definição (Grupo de Decomposição/Corpo de Decomposição)**.** Seja $\mathfrak{P} \lhd B$ um ideal primo. Definimos seu **grupo de decomposição** $G_{\mathfrak{P}} = G_{\mathfrak{P}}(L/K) \leq G$ como sendo o estabilizador de $\mathfrak{P}$ pela ação de G, isto é, $G_{\mathfrak{P}} \coloneqq \{\sigma \in G \colon \sigma\mathfrak{P} = \mathfrak{P}\}$. Definimos ainda o seu **corpo de decomposição** $Z_{\mathfrak{P}} = Z_{\mathfrak{P}}(L/K) \subseteq L$ como o corpo fixo por $G_{\mathfrak{P}}$.

Fixado $\mathfrak{P}$, denotaremos $B_Z \coloneqq \overline{A}^{Z_{\mathfrak{P}}} = B \cap Z_{\mathfrak{P}}$ e $\mathfrak{P}_Z \coloneqq \mathfrak{P} \cap B_Z \lhd B_Z$. Note que $\mathfrak{P}_Z$ é um ideal primo. Algumas consequências diretas da definição acima são:

Proposição 6.2. *Seja $\mathfrak{P} \lhd B$ um ideal primo. Então:*

(a) Dado $\sigma \in G$, temos $G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}$.

(b) Dado $\sigma \in G$, temos $Z_{\sigma\mathfrak{P}} = \sigma Z_{\mathfrak{P}}$.

(c) As seguintes condições são equivalentes:

(i) $G_{\mathfrak{P}}$ é um subgrupo normal de G.

(ii) $Z_{\mathfrak{P}}/K$ é uma extensão de Galois.

(iii) Todos os ideais primos sobre $\mathfrak{P} \cap A$ possuem o mesmo grupo de decomposição.

(iv) Todos os ideais primos sobre $\mathfrak{P} \cap A$ possuem o mesmo corpo de decomposição.

(d) Se $K \subseteq E \subseteq L$, então $G_{\mathfrak{P}}(L/E) = G_{\mathfrak{P}} \cap \mathrm{Gal}(L/E)$, e $Z_{\mathfrak{P}}(L/E) = Z_{\mathfrak{P}}(L/K) \cdot E$.

Demonstração. (a) Dado $\tau \in G$, nós temos;

$$\tau \in G_{\sigma\mathfrak{P}} \iff \tau\sigma\mathfrak{P} = \sigma\mathfrak{P} \iff \sigma^{-1}\tau\sigma\mathfrak{P} = \mathfrak{P} \iff \sigma^{-1}\tau\sigma \in G_{\mathfrak{P}} \iff \tau \in \sigma G_{\mathfrak{P}} \sigma^{-1}.$$

(b) Dado $x \in L$, pelo item (a) nós temos:

$$\begin{aligned} x \in Z_{\sigma\mathfrak{P}} \iff \forall\, \rho \in G_{\sigma\mathfrak{P}},\ \rho x = x &\iff \forall\, \tau \in G_{\mathfrak{P}},\ \sigma\tau\sigma^{-1}x = x \\ &\iff \forall\, \tau \in G_{\mathfrak{P}},\ \tau\sigma^{-1}x = \sigma^{-1}x \\ &\iff \sigma^{-1}x \in Z_{\mathfrak{P}} \\ &\iff x \in \sigma Z_{\mathfrak{P}}. \end{aligned}$$

(c) As equivalências $(i) \iff (ii)$ e $(iii) \iff (iv)$ seguem da teoria de Galois, enquanto $(i) \iff (iii)$ segue de (a) e da Proposição 6.1.

(d) Um elemento de $\mathrm{Gal}(L/E)$ pertence a $G_{\mathfrak{P}}(L/E)$ se e somente se ele fixa $\mathfrak{P}$, ou seja, se e só se está em $G_{\mathfrak{P}}$. Isso nos dá a igualdade desejada. A segunda igualdade segue então da teoria de Galois.

□

Notemos que, pelo Teorema da Órbita e do Estabilizador, a órbita de um primo $\mathfrak{P}$ tem $[G : G_{\mathfrak{P}}]$ elementos. Então, pela Proposição 6.1, o número de ideais primos de B sobre $\mathfrak{p}$ é igual a $[G : G_{\mathfrak{P}}]$. De fato nós temos:

Proposição 6.3. *Se $\mathfrak{p} \lhd A$ é um primo qualquer, e $\mathfrak{P} \lhd B$ é um primo sobre $\mathfrak{p}$, então:*

(a) O número de ideais primos de L sobre $\mathfrak{p}$ é igual a $[G : G_{\mathfrak{P}}]$.

(b) $\mathfrak{p}$ é totalmente decomposto em $L \iff G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L$.

(c) $\mathfrak{p}$ é não-decomposto em $L \iff G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K$.

Demonstração. (a) Feito acima.

(b) $\mathfrak{p}$ será totalmente decomposto em L se e só se o número de ideais primos de L sobre $\mathfrak{p}$ for igual a n. Mas por (a) isso ocorrerá se e só se $[G : G_{\mathfrak{P}}] = n \iff G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L$.

(c) $\mathfrak{p}$ será não-decomposto em L se e só se o número de ideais primos de L sobre $\mathfrak{p}$ for igual a 1. Mas por (a) isso ocorrerá se e só se $[G : G_{\mathfrak{P}}] = 1 \iff G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K$.

□

A análise que fizemos acima aplicada à extensão galoisiana $L/Z_{\mathfrak{P}}$ nos diz que o número de ideais primos de B sobre $\mathfrak{P}_Z$ é igual a $[\mathrm{Gal}(L/Z_{\mathfrak{P}}) : G_{\mathfrak{P}}] = [G_{\mathfrak{P}} : G_{\mathfrak{P}}] = 1$. Isto é, $\mathfrak{P}$ é o único ideal primo de B sobre $\mathfrak{P}_Z$. Esse é o menor corpo base para o qual isso ocorre:

Proposição 6.4. *O corpo $Z_{\mathfrak{P}}$ é o menor corpo intermediário E da extensão L/K para o qual $\mathfrak{P}$ é o único ideal primo de B sobre o primo $\mathfrak{P} \cap E \lhd \overline{A}^E$. Equivalentemente, $Z_{\mathfrak{P}}$ é o menor corpo intermediário E da extensão L/K para o qual $\mathfrak{P} \cap E$ é não-decomposto em L.*

Demonstração. Se $\mathfrak{P}$ for o único ideal primo de B sobre $\mathfrak{P} \cap E$, teremos $\sigma\mathfrak{P} = \mathfrak{P}$ para todo automorfismo $\sigma \in \mathrm{Gal}(L/E)$, pela Proposição 6.1. Então todo elemento de $\mathrm{Gal}(L/E)$ fixa $\mathfrak{P}$, ou seja, $\mathrm{Gal}(L/E) \subseteq G_{\mathfrak{P}}$. Aplicando a correspondência de Galois, vemos que isso é equivalente a termos $Z_{\mathfrak{P}} \subseteq E$, demonstrando o resultado desejado. □

Uma das características principais das extensões galoisianas é que todos os índices de ramificação e todos os graus de inércia dos primos sobre $\mathfrak{p}$ coincidem:

Proposição 6.5. *Seja $\mathfrak{p} \lhd A$ primo não-nulo.*

(a) A fatoração de $\mathfrak{p}B$ em primos de B é da forma $\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, onde $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ são primos distintos. Em particular, o índice de ramificação de todo primo $\mathfrak{P} \mid \mathfrak{p}$ é igual a e.

(b) Sejam $\mathfrak{P}, \mathfrak{Q} \lhd B$ primos sobre $\mathfrak{p}$. Então $B/\mathfrak{P} \cong B/\mathfrak{Q}$ por um isomorfismo de anéis que fixa $A/\mathfrak{p}$. Em particular, temos $f_{\mathfrak{P}} = f_{\mathfrak{Q}}$. Assim, os graus de inércia de todos os ideais primos $\mathfrak{P} \mid \mathfrak{p}$ coincidem e são iguais a um certo f.

Demonstração. (a) Seja $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ a fatoração prima de $\mathfrak{p}B$. Para $2 \leq j \leq g$, seja $\sigma_j \in G$ tal que $\sigma_j\mathfrak{P}_1 = \mathfrak{P}_j$ (tal σ_j existe pela Proposição 6.1). Desse modo:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \Rightarrow \sigma_j(\mathfrak{p}B) = (\sigma_j\mathfrak{P}_1)^{e_1} \cdots (\sigma_j\mathfrak{P}_g)^{e_g}.$$

Mas como $\sigma_j(\mathfrak{p}) = \mathfrak{p}$ e $\sigma_j(B) = B$, temos $\sigma_j(\mathfrak{p}B) = \mathfrak{p}B$. Assim, temos duas fatorações de $\mathfrak{p}B$ como produto de ideais primos distintos. Em $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, o primo $\mathfrak{P}_j$ aparece com expoente e_j, e em $(\sigma_j\mathfrak{P}_1)^{e_1} \cdots (\sigma_j\mathfrak{P}_g)^{e_g}$ o primo $\mathfrak{P}_j = \sigma_j\mathfrak{P}_1$ aparece com expoente e_1. Logo, pela unicidade da fatoração concluímos que $e_j = e_1$. Como $2 \leq j \leq g$ é qualquer, vale o resultado desejado.

(b) Por 6.1, existe $\sigma \in G$ tal que $\mathfrak{Q} = \sigma\mathfrak{P}$. Consideremos $\overline{\sigma}\colon B/\mathfrak{P} \to B/\mathfrak{Q}$ dada por $x + \mathfrak{P} \mapsto \sigma(x) + \mathfrak{Q}$. Essa é uma função bem-definida e injetora. De fato, dados $x, y \in B$ nós temos

$$\sigma(x) + \mathfrak{Q} = \sigma(y) + \mathfrak{Q} \iff \sigma(x - y) \in \mathfrak{Q} \iff x - y \in \sigma^{-1}(\mathfrak{Q}) = \mathfrak{P} \iff x + \mathfrak{P} = y + \mathfrak{P},$$

como desejado. Falta ver que $\overline{\sigma}$ é sobrejetora. Mas isso é claro, pois $\sigma\colon \mathfrak{P} \to \mathfrak{Q} = \sigma\mathfrak{P}$ é sobrejetora. Isso mostra que $\overline{\sigma}$ é uma bijeção. É fácil ver que essa função é um homomorfismo, e portanto um isomorfismo. Finalmente, como σ fixa A, $\overline{\sigma}$ fixa $A/\mathfrak{p}$. O que fizemos mostra que $B/\mathfrak{P} \cong B/\mathfrak{Q}$ são corpos isomorfos por um automorfismo que fixa $A/\mathfrak{p}$. Assim, é claro que $[B/\mathfrak{P} : A/\mathfrak{p}] = [B/\mathfrak{Q} : A/\mathfrak{p}]$. Mas isso é exatamente dizer que $f_{\mathfrak{P}} = f_{\mathfrak{Q}}$.

□

Com isso, nós conseguimos o seguinte importante resultado:

Teorema 6.6. *(Identidade Fundamental para Extensões Galoisianas) Seja $\mathfrak{p} \lhd A$ primo. Então os índices de ramificação e os graus de inércia de todos os primos de B sobre $\mathfrak{p}$ coincidem. Assim, existem inteiros positivos e, f tais que a fatoração de $\mathfrak{p}B$ é da forma $\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, onde cada $\mathfrak{P}_j$ tem grau de inércia f. Sendo assim, a identidade fundamental nesse caso se torna $n = efg$. Ademais, se $\mathfrak{P} \mid \mathfrak{p}$ então $\mathfrak{P}_Z$ é não-decomposto em L, e valem as igualdades*

$$e(\mathfrak{P} \mid \mathfrak{P}_Z) = e,\ f(\mathfrak{P} \mid \mathfrak{P}_Z) = f,\ g(\mathfrak{P} \mid \mathfrak{P}_Z) = 1,\ e(\mathfrak{P}_Z \mid \mathfrak{p}) = f(\mathfrak{P}_Z \mid \mathfrak{p}) = 1.$$

Sendo assim, $B_Z/\mathfrak{P}_Z = A/\mathfrak{p}$ e o primo $\mathfrak{P}_Z$ é não-decomposto na extensão $L/Z_\mathfrak{P}$. Além disso, se a extensão $Z_\mathfrak{P}/K$ for normal (e portanto galoisiana) vale $g(\mathfrak{P}_Z \mid \mathfrak{p}) = g$, de forma que $\mathfrak{p}$ será totalmente decomposto em $Z_\mathfrak{P}$.

Demonstração. Só falta verificarmos as últimas igualdades. Notemos que $g(\mathfrak{P} \mid \mathfrak{P}_Z) = 1$ segue direto da Proposição 6.4. Pela identidade fundamental, $efg = n$. Notemos que, pelas multiplicatividades do índice de ramificação e do grau de inércia (Proposição 4.15), nós temos $e = e(\mathfrak{P} \mid \mathfrak{P}_Z) \cdot e(\mathfrak{P}_Z \mid \mathfrak{p})$ e $f = f(\mathfrak{P} \mid \mathfrak{P}_Z) \cdot f(\mathfrak{P}_Z \mid \mathfrak{p})$. Assim, basta provarmos que $e(\mathfrak{P} \mid \mathfrak{P}_Z) = e$ e que $f(\mathfrak{P} \mid \mathfrak{P}_Z) = f$. Para isso, aplicamos a identidade fundamental à extensão galoisiana $L/Z_\mathfrak{P}$. Notemos que $|G_\mathfrak{P}| = |G|/[G : G_\mathfrak{P}] = n/g = ef$. Assim:

$$ef = |G_\mathfrak{P}| = [L : \mathbb{Z}_\mathfrak{P}] = e(\mathfrak{P} \mid \mathfrak{P}_Z) \cdot f(\mathfrak{P} \mid \mathfrak{P}_Z) \cdot g(\mathfrak{P} \mid \mathfrak{P}_Z) = e(\mathfrak{P} \mid \mathfrak{P}_Z) \cdot f(\mathfrak{P} \mid \mathfrak{P}_Z) \leq ef.$$

Como $e(\mathfrak{P} \mid \mathfrak{P}_Z) \leq e$ e $f(\mathfrak{P} \mid \mathfrak{P}_Z) \leq f$, devemos ter $e(\mathfrak{P} \mid \mathfrak{P}_Z) = e$ e $f(\mathfrak{P} \mid \mathfrak{P}_Z) = f$, como queríamos. Finalmente, se $Z_\mathfrak{P}/K$ for galoisiana, então a identidade fundamental da decomposição de $\mathfrak{p}$ em $Z_\mathfrak{P}$ se torna $g = [Z_\mathfrak{P} : K] = e(\mathfrak{P}_Z \mid \mathfrak{p}) \cdot f(\mathfrak{P}_Z \mid \mathfrak{p}) \cdot g(\mathfrak{P}_Z \mid \mathfrak{p}) = g(\mathfrak{P}_Z \mid \mathfrak{p})$. Assim, $g(\mathfrak{P}_Z \mid \mathfrak{p}) = g$, concluindo a demonstração. □

Observação 6.7. *Note que uma identidade fundamental da forma $n = efg$ ocorreu nas extensões quadráticas e ciclotômicas. Esses são casos particulares desse resultado. O seguinte diagrama, que sintetiza várias das informações obtidas acima, deve estar sempre em mente ao trabalharmos com extensões galoisianas de domínios de Dedekind:*

$$\begin{array}{ccccc}
\mathfrak{P} \lhd B & \hookrightarrow & L = Q(B) & \text{---------} & 1 \\
{\scriptstyle ef}\big| & & {\scriptstyle ef}\big| & & {\scriptstyle ef}\big| \\
\mathfrak{P}_Z \lhd B_Z & \hookrightarrow & Z_\mathfrak{P} = Q(B_Z) & \text{------} & G_\mathfrak{P} \\
{\scriptstyle g}\big| & & {\scriptstyle g}\big| & & {\scriptstyle g}\big| \\
\mathfrak{p} \lhd A & \hookrightarrow & K = Q(A) & \text{---------} & G
\end{array}$$

Quando L/K for uma extensão abeliana, o Teorema 6.6 nos garante que $\mathfrak{p}$ se decompõe totalmente em $Z_\mathfrak{P}$. Na verdade, vale o seguinte:

Proposição 6.8. *Suponhamos L/K abeliana. Sejam $\mathfrak{p}$ um primo de K e $\mathfrak{P} \mid \mathfrak{p}$ um primo de L. Então $Z_\mathfrak{P}$ é o maior subcorpo da extensão L/K no qual $\mathfrak{p}$ é totalmente decomposto.*

Demonstração. Seja F um subcorpo de L/K no qual $\mathfrak{p}$ é totalmente decomposto. Queremos mostrar que $F \subseteq Z_\mathfrak{P}$. Pela correspondência de Galois, isso equivale a provar que $G_\mathfrak{P} \subseteq \mathrm{Gal}(L/F)$. Seja então $\sigma \in G_\mathfrak{P}$. Como $\sigma\mathfrak{P} = \mathfrak{P}$, o primo $\mathfrak{P} \cap F$ de F fica fixo por σ, e assim temos $\sigma|_F \in G_{\mathfrak{P}\cap F}(F/K)$. Mas $\mathfrak{p}$ é totalmente decomposto em F, logo pela Proposição 6.3, nós temos $G_{\mathfrak{P}\cap F}(F/K) = 1$. Ou seja, $\sigma|_F = \mathrm{id}_F \Rightarrow \sigma \in \mathrm{Gal}(L/F)$. Sendo $\sigma \in G_\mathfrak{P}$ qualquer, concluímos que $G_\mathfrak{P} \subseteq \mathrm{Gal}(L/F)$, como desejávamos. □

Seja $\sigma \in G_{\mathfrak{P}}$. Consideremos a função $\overline{\sigma}\colon B/\mathfrak{P} \to B/\mathfrak{P}$ dada por $\overline{\sigma}(x+\mathfrak{P}) = \sigma(x)+\mathfrak{P}$. Então é fácil verificar que $\overline{\sigma}$ está bem-definida e é um automorfismo de $B/\mathfrak{P}$ que fixa $A/\mathfrak{p}$, de modo que[1] $\overline{\sigma} \in \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p}))$. Assim, temos um homomorfismo de grupos $G_{\mathfrak{P}} \to \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p}))$ dado por $\sigma \mapsto \overline{\sigma}$. Nós denotamos $\overline{G}_{\mathfrak{P}} \coloneqq \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p}))$.

6.2. O Grupo de Inércia

A partir de agora até o final deste capítulo, iremos assumir que a extensão $(B/\mathfrak{P})/(A/\mathfrak{p})$ é separável. Note que isso sempre ocorrerá numa extensão de corpos de números, pois nesse caso $A/\mathfrak{p}$ será um corpo finito, e portanto perfeito. Com isso, temos:

Proposição 6.9. *$B/\mathfrak{P}$ é uma extensão normal de $A/\mathfrak{p}$, logo galoisiana. Além disso, o mapa canônico $G_{\mathfrak{P}} \to \overline{G}_{\mathfrak{P}}$ dado por $\sigma \mapsto \overline{\sigma}$ é um homomorfismo sobrejetor.*

Demonstração. Comecemos mostrando que $B/\mathfrak{P}$ é uma extensão normal de $A/\mathfrak{p}$. Para isso, seja $\overline{\alpha} \in B/\mathfrak{P}$ qualquer. Provaremos que $\overline{P} \coloneqq \overline{P}_{\alpha,L/K} \in (A/\mathfrak{p})[x]$ se decompõe em fatores lineares em $(A/\mathfrak{p})[x]$. Como L/K é extensão de Galois, todas as raízes $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ estão em L. Mas sendo $P \in A[x]$ mônico, suas raízes são integrais sobre A, e portanto estão na verdade em B. Assim, P se escreve em B como $P(x) = (x-\alpha_1)\cdots(x-\alpha_m)$. Mas módulo $\mathfrak{P}$ isso significa que $\overline{P}(x) = (x-\overline{\alpha}_1)\cdots(x-\overline{\alpha}_m)$, como queríamos, e concluímos que $B/\mathfrak{P}$ é extensão normal de $A/\mathfrak{p}$.

Voltemo-nos agora para a segunda afirmação. Primeiramente, notemos que podemos nos reduzir ao caso em que $\mathfrak{P}$ é o único ideal de B sobre $\mathfrak{p}$. De fato, se esse não fosse o caso nós poderíamos "subir o corpo base" de K para $Z_{\mathfrak{P}}$, já que $G_{\mathfrak{P}}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$ e $B_Z/\mathfrak{P}_Z = A/\mathfrak{p}$. Assim, suponhamos que esse seja o caso. Então vale $G_{\mathfrak{P}} = G$.

Como L/K é uma extensão finita, $(B/\mathfrak{P})/(A/\mathfrak{p})$ também o é. Como essa extensão é separável, existe $\overline{\theta} \in B/\mathfrak{P}$ tal que $B/\mathfrak{P} = (A/\mathfrak{p})(\overline{\theta})$. Consideremos $\tau \in \overline{G}_{\mathfrak{P}}$ qualquer. O automorfismo τ é completamente determinado pela imagem de $\overline{\theta}$. Sendo $P \coloneqq P_{\theta,K}$, temos $\overline{P}(\overline{\theta}) = 0$, logo $\overline{P}(\tau(\overline{\theta})) = \tau(\overline{P}(\overline{\theta})) = 0$, e assim $\tau(\overline{\theta})$ deverá ser uma raiz de $\overline{P}$, e portanto da forma $\overline{\beta}$ para β raiz de P (lembre que P se fatora em fatores lineares de $B[x]$). Mas como P é irredutível, existe $\sigma \in G = G_{\mathfrak{P}}$ tal que $\sigma\theta = \beta$. Dessa forma, $\overline{\sigma}(\overline{\theta}) = \overline{\beta} = \tau(\overline{\theta})$. Isso mostra que $\tau = \overline{\sigma}$, concluindo a demonstração. □

Observação 6.10. *Mesmo que $(B/\mathfrak{P})/(A/\mathfrak{p})$ não seja separável, é possível concluir que essa extensão é normal e que o mapa $G_{\mathfrak{P}} \to \overline{G}_{\mathfrak{P}}$ é sobrejetor. Veja por exemplo a Proposição (9.4) de [2].*

Definição (Grupo de Inércia/Corpo de Inércia)**.** O núcleo $I_{\mathfrak{P}} = I_{\mathfrak{P}}(L/K) \lhd G_{\mathfrak{P}}$ do mapa canônico $G_{\mathfrak{P}} \to \overline{G}_{\mathfrak{P}}$ é chamado de **grupo de inércia** de $\mathfrak{P}$, e seu corpo fixo $T_{\mathfrak{P}} = T_{\mathfrak{P}}(L/K)$ é chamado de **corpo de inércia** de $\mathfrak{P}$.

Em geral, denotaremos $B_T \coloneqq \overline{A}^{T_{\mathfrak{P}}} = B \cap T_{\mathfrak{P}}$ e $\mathfrak{P}_T \coloneqq \mathfrak{P} \cap B_T \lhd B_T$. Note que $\mathfrak{P}_T$ é um ideal primo de $T_{\mathfrak{P}}$. Note que temos a cadeia de corpos $K \subseteq Z_{\mathfrak{P}} \subseteq T_{\mathfrak{P}} \subseteq L$ e a cadeia de grupos $1 \leq I_{\mathfrak{P}} \leq G_{\mathfrak{P}} \leq G$. Além disso, pela definição de $I_{\mathfrak{P}}$ e pelo fato do mapa canônico $G_{\mathfrak{P}} \to \overline{G}_{\mathfrak{P}}$ ser sobrejetor, nós temos a sequência exata $1 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \longrightarrow \overline{G}_{\mathfrak{P}} \longrightarrow 1$. Como consequência disso, $\overline{G}_{\mathfrak{P}} \cong G_{\mathfrak{P}}/I_{\mathfrak{P}}$. A seguinte proposição reúne as propriedades básicas envolvendo o grupo e o corpo de inércia:

Proposição 6.11. *(a) Seja $\sigma \in G$ qualquer. Então $I_{\sigma\mathfrak{P}} = \sigma I_{\mathfrak{P}} \sigma^{-1}$, e $T_{\sigma\mathfrak{P}} = \sigma T_{\mathfrak{P}}$.*

[1] A extensão $(B/\mathfrak{P})/(A/\mathfrak{p})$ não precisa ser galoisiana. Aqui entendemos o grupo de Galois no sentido estendido: dada uma extensão λ/κ, denotamos por $\mathrm{Gal}(\lambda/\kappa)$ o grupo dos automorfismos de λ que fixam κ.

(b) A extensão $L/T_{\mathfrak{P}}$ é galoisiana com grupo de Galois $I_{\mathfrak{P}}$ e a extensão $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ é galoisiana com $\mathrm{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \overline{G}_{\mathfrak{P}}$.

(c) $B/\mathfrak{P} = B_T/\mathfrak{P}_T$.

(d) Valem as igualdades:

$$\begin{aligned} e &= [L : T_{\mathfrak{P}}] = |I_{\mathfrak{P}}|; \\ f &= [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = (G_{\mathfrak{P}} : I_{\mathfrak{P}}) = |\overline{G}_{\mathfrak{P}}| = [B/\mathfrak{P} : A/\mathfrak{p}]; \\ e(\mathfrak{P} \mid \mathfrak{P}_T) &= e,\ f(\mathfrak{P} \mid \mathfrak{P}_T) = 1,\ g(\mathfrak{P} \mid \mathfrak{P}_T) = 1; \\ e(\mathfrak{P}_T \mid \mathfrak{P}_Z) &= 1,\ f(\mathfrak{P}_T \mid \mathfrak{P}_Z) = f,\ g(\mathfrak{P}_T \mid \mathfrak{P}_Z) = 1. \end{aligned}$$

Assim, $\mathfrak{P}_T$ é totalmente ramificado em L, $\mathfrak{P}_Z$ é totalmente inerte em $T_{\mathfrak{P}}$ e, se $Z_{\mathfrak{P}}/K$ for extensão normal, $\mathfrak{p}$ será totalmente decomposto em $Z_{\mathfrak{P}}$.

Demonstração. (a) Seja $\tau \in I_{\sigma\mathfrak{P}}$. Note que $\sigma^{-1}\tau\sigma \in \sigma^{-1}G_{\sigma\mathfrak{P}}\sigma = \sigma^{-1}(\sigma G_{\mathfrak{P}}\sigma^{-1})\sigma = G_{\mathfrak{P}}$, pela Proposição 6.2. Além disso, como $\tau \in I_{\sigma\mathfrak{P}}$, para todo $b \in B$ nós temos:

$$\tau(\sigma b) \equiv \sigma b \pmod{\sigma\mathfrak{P}} \Rightarrow (\sigma^{-1}\tau\sigma)b \equiv b \pmod{\mathfrak{P}}.$$

Dessa forma, $\sigma^{-1}\tau\sigma \in I_{\mathfrak{P}} \Rightarrow \tau \in \sigma I_{\mathfrak{P}}\sigma^{-1}$. Isso prova que $I_{\sigma\mathfrak{P}} \subseteq \sigma I_{\mathfrak{P}}\sigma^{-1}$.

Para a volta, basta observar que pelo que acabamos de provar, temos:

$$\sigma I_{\mathfrak{P}}\sigma^{-1} = \sigma I_{\sigma^{-1}(\sigma\mathfrak{P})}\sigma^{-1} \subseteq \sigma(\sigma^{-1}I_{\sigma\mathfrak{P}}\sigma)\sigma^{-1} = I_{\sigma\mathfrak{P}}.$$

A última afirmação se prova analogamente ao item (b) da Proposição 6.2.

(b) Segue da teoria de Galois e das observações acima da proposição.

(c) A extensão $(B/\mathfrak{P})/(B_T/\mathfrak{P}_T)$ é galoisiana. Assim, basta provar que todo automorfismo de $B/\mathfrak{P}$ que fixa $B_T/\mathfrak{P}_T$ é a identidade de $B/\mathfrak{P}$. Seja então τ um tal automorfismo. Aplicando a Proposição 6.9 à extensão $L/T_{\mathfrak{P}}$, que tem grupo de Galois $I_{\mathfrak{P}}$, garantimos a existência de um $\sigma \in I_{\mathfrak{P}}$ tal que $\tau = \overline{\sigma}$. Mas $\sigma \in I_{\mathfrak{P}} \Rightarrow \overline{\sigma} = \mathrm{id}_{B/\mathfrak{P}}$. Assim, provamos que $B/\mathfrak{P} = B_T/\mathfrak{P}_T$.

(d) Como $(B/\mathfrak{P})/(A/\mathfrak{p})$ é separável, temos:

$$f = [B/\mathfrak{P} : A/\mathfrak{p}] = |\overline{G}_{\mathfrak{P}}| = \frac{|G_{\mathfrak{P}}|}{|I_{\mathfrak{P}}|} = (G_{\mathfrak{P}} : I_{\mathfrak{P}}) = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}].$$

Assim:

$$e = \frac{n}{fg} = \frac{[L : K]}{[T_{\mathfrak{P}} : Z_{\mathfrak{P}}][Z_{\mathfrak{P}} : K]} = \frac{[L : K]}{[T_{\mathfrak{P}} : K]} = [L : T_{\mathfrak{P}}] = |I_{\mathfrak{P}}|.$$

Observemos agora que $g(\mathfrak{P} \mid \mathfrak{P}_T) = g(\mathfrak{P}_T \mid \mathfrak{P}_Z) = 1$, pois nós temos $g(\mathfrak{P} \mid \mathfrak{P}_Z) = 1$. Por (c), temos $f(\mathfrak{P} \mid \mathfrak{P}_T) = 1$. A identidade fundamental aplicada à decomposição de $\mathfrak{P}_T$ em L nos dá então:

$$e(\mathfrak{P} \mid \mathfrak{P}_T) = \frac{[L : T_{\mathfrak{P}}]}{f(\mathfrak{P} \mid \mathfrak{P}_T) \cdot g(\mathfrak{P} \mid \mathfrak{P}_T)} = \frac{[L : T_{\mathfrak{P}}]}{1 \cdot 1} = [L : T_{\mathfrak{P}}] = e.$$

Como $B/\mathfrak{P} = B_T/\mathfrak{P}_T$ e $B_Z/\mathfrak{P}_Z = A/\mathfrak{p}$:

$$f(\mathfrak{P}_T \mid \mathfrak{P}_Z) = [B_T/\mathfrak{P}_T : B_Z/\mathfrak{P}_Z] = [B/\mathfrak{P} : A/\mathfrak{p}] = f.$$

Finalmente, aplicando a identidade fundamental à decomposição de $\mathfrak{P}_Z$ em $T_\mathfrak{P}$:

$$e(\mathfrak{P}_T \mid \mathfrak{P}_Z) = \frac{[T_\mathfrak{P} : Z_\mathfrak{P}]}{f(\mathfrak{P}_T \mid \mathfrak{P}_Z) \cdot g(\mathfrak{P}_T \mid \mathfrak{P}_Z)} = \frac{f}{f \cdot 1} = 1,$$

enquanto o caso em que $Z_\mathfrak{P}/K$ é normal foi feito no Teorema 6.6.

□

Observação 6.12. *Os seguintes diagramas sintetizam os resultados dessa proposição:*

$$\begin{array}{ccccccc}
\mathfrak{P} \lhd B & \hookrightarrow & L = Q(B) & \text{---------} & 1 & & \\
{\scriptstyle e}\big| & & {\scriptstyle e}\big| & & {\scriptstyle e}\big| & & \\
\mathfrak{P}_T \lhd B_T & \hookrightarrow & T_\mathfrak{P} = Q(B_T) & \text{-------} & I_\mathfrak{P} & \qquad & B/\mathfrak{P} = B_T/\mathfrak{P}_T \\
{\scriptstyle f}\big| & & {\scriptstyle f}\big| & & {\scriptstyle f}\big| & & {\scriptstyle f}\big| \\
\mathfrak{P}_Z \lhd B_Z & \hookrightarrow & Z_\mathfrak{P} = Q(B_Z) & \text{------} & G_\mathfrak{P} & & A/\mathfrak{p} = B_Z/\mathfrak{P}_Z \\
{\scriptstyle g}\big| & & {\scriptstyle g}\big| & & {\scriptstyle g}\big| & & \\
\mathfrak{p} \lhd A & \hookrightarrow & K = Q(A) & \text{---------} & G & &
\end{array}$$

Assim, conseguimos "quebrar" a extensão L/K em extensões melhores. Dessa proposição ainda podemos obter:

Corolário 6.13. *(a) São equivalentes:*

(i) $I_\mathfrak{P} = 1$.

(ii) $T_\mathfrak{P} = L$.

(iii) $\mathfrak{p}$ *é não-ramificado em* L.

Nesse caso, $\overline{G}_\mathfrak{P} \cong G_\mathfrak{P}$.

(b) São equivalentes:

(i) $I_\mathfrak{P} = G$.

(ii) $T_\mathfrak{P} = K$.

(iii) $\mathfrak{p}$ *é totalmente ramificado em* L.

Nesse caso, $\overline{G}_\mathfrak{P} = 1$.

Demonstração. (a) A equivalência $(i) \iff (ii)$ segue da teoria de Galois. Como para todo primo $\mathfrak{Q} \mid \mathfrak{p}$ de B temos $B/\mathfrak{Q} \cong B/\mathfrak{P}$ por um isomorfismo que fixa $A/\mathfrak{p}$, vemos que a extensão $(B/\mathfrak{Q})/(A/\mathfrak{p})$ é separável. Assim, $\mathfrak{p}$ ser não-ramificado em L equivale a termos $e = 1$. Como $e = |I_\mathfrak{P}|$, obtemos a equivalência $(i) \iff (iii)$.

(b) A equivalência $(i) \iff (ii)$ segue da teoria de Galois, e $(i) \iff (iii)$ segue de $e = |I_\mathfrak{P}|$, já que $\mathfrak{p}$ ser totalmente ramificado em L equivale a $e = n$.

□

Lembremos que $Z_\mathfrak{P}$ é o menor corpo intermediário E de L/K com a propriedade de que $\mathfrak{P}$ é o único ideal primo de L sobre $\mathfrak{P} \cap E$. O corpo $T_\mathfrak{P}$ possui também uma caracterização minimal:

Proposição 6.14. *Seja* E *um corpo intermediário da extensão* $L/Z_\mathfrak{P}$. *Sejam* $B_E := \overline{A}^E = B \cap E$ *e* $\mathfrak{P}_E := \mathfrak{P} \cap B_E \lhd B_E$. *Então* $B/\mathfrak{P} = B_E/\mathfrak{P}_E$ *se e só se* $T_\mathfrak{P} \subseteq E$.

Demonstração. Notemos que $B_E/\mathfrak{P}_E = B/\mathfrak{P}$ equivale a $\mathrm{Gal}((B/\mathfrak{P})/(B_E/\mathfrak{P}_E)) = 1$. Chamemos $\varphi\colon G_\mathfrak{P} \to \overline{G}_\mathfrak{P}$ o mapa canônico. Aplicando a Proposição 6.9, isso é equivalente a termos $\varphi(\mathrm{Gal}(L/E)) = 1$. Ou seja, a $\mathrm{Gal}(L/E) \subseteq \ker\varphi = I_\mathfrak{P}$. Pela teoria de Galois, isso é equivalente a $E \supseteq T_\mathfrak{P}$, como queríamos. □

Esse corpo possui ainda uma caracterização maximal, que nos será útil mais adiante:

Proposição 6.15. *Seja E um corpo intermediário da extensão L/K. Então $e(\mathfrak{P}_E \mid \mathfrak{p}) = 1$ se e só se $E \subseteq T_\mathfrak{P}$.*

Demonstração. Notemos que $e(\mathfrak{P}_T \mid \mathfrak{p}) = e(\mathfrak{P}_T \mid \mathfrak{P}_Z)\cdot e(\mathfrak{P}_Z \mid \mathfrak{p}) = 1\cdot 1 = 1$, pelo Teorema 6.6 e pela Proposição 6.11. Se $E \subseteq T_\mathfrak{P}$, então $e(\mathfrak{P}_E \mid \mathfrak{p}) \leq e(\mathfrak{P}_T \mid \mathfrak{p}) = 1$, e portanto nós temos $e(\mathfrak{P}_E \mid \mathfrak{p}) = 1$.

Suponhamos então que $e(\mathfrak{P}_E \mid \mathfrak{p}) = 1$. Nesse caso, $e(\mathfrak{P} \mid \mathfrak{P}_E) = e$, o que significa que vale $[L : T_\mathfrak{P}(L/E)] = e$. Mas é fácil ver que $I_\mathfrak{P}(L/E) = \mathrm{Gal}(L/E)\cap I_\mathfrak{P}$, e portanto pela correspondência de Galois nós temos $T_\mathfrak{P}(L/E) = E\cdot T_\mathfrak{P}$. Ou seja, $[L : E\cdot T_\mathfrak{P}] = e = [L : T_\mathfrak{P}]$, de onde concluímos que $E\cdot T_\mathfrak{P} = T_\mathfrak{P}$. Isso mostra que $E \subseteq T_\mathfrak{P}$, como queríamos. □

6.3. Os Grupos de Ramificação

Na seção anterior, mostramos que podemos dividir a extensão L/K em três extensões especiais: $L/T_\mathfrak{P}$, $T_\mathfrak{P}/Z_\mathfrak{P}$ e $Z_\mathfrak{P}/K$. A extensão $L/T_\mathfrak{P}$ é a parte totalmente ramificada de L/K, isto é, $\mathfrak{P}_T \lhd B_T$ é totalmente ramificado em L. Nosso próximo objetivo é separar $L/T_\mathfrak{P}$ em extensões mais simples ainda. Comecemos notando que o grupo de inércia $I_\mathfrak{P}$ pode ser caracterizado como o conjunto:

$$\{\sigma \in G_\mathfrak{P}\colon \forall\, b \in B,\ \sigma b \equiv b \pmod{\mathfrak{P}}\}.$$

Definição (Grupos de Ramificação)**.** Para cada $i \in \mathbb{N}$, definimos o **i-ésimo grupo de ramificação** de $\mathfrak{P}$ sobre K como sendo o conjunto:

$$R^i_\mathfrak{P} = R^i_\mathfrak{P}(L/K) \coloneqq \{\sigma \in G_\mathfrak{P}\colon \forall\, b \in B,\ \sigma b \equiv b \pmod{\mathfrak{P}^{i+1}}\}.$$

Note que podemos representar ainda $R^i_\mathfrak{P}$ como

$$\{\sigma \in G\colon \forall\, b \in B, \sigma b \equiv b \pmod{\mathfrak{P}^{i+1}}\}.$$

De fato, para $\sigma \in G \setminus G_\mathfrak{P}$, existe $b \in \mathfrak{P}$ tal que $\sigma b \notin \mathfrak{P}$, e portanto $\sigma b - b \notin \mathfrak{P}$ nesse caso. A primeira coisa a se mostrar é que os grupos de ramificação são realmente grupos. De fato, temos o seguinte resultado, que nos dá as propriedades básicas dos grupos de ramificação:

Proposição 6.16. *(a) Nós temos $G_\mathfrak{P} \supseteq I_\mathfrak{P} = R^0_\mathfrak{P} \supseteq R^1_\mathfrak{P} \supseteq R^2_\mathfrak{P} \supseteq \cdots$. Além disso, existe $m \in \mathbb{N}$ tal que $R^m_\mathfrak{P}$ é o grupo trivial.*

(b) Para todo $i \in \mathbb{N}$, $R^i_\mathfrak{P}$ é um subgrupo normal de $G_\mathfrak{P}$.

(c) Seja E um corpo intermediário da extensão L/K. Então, para todo $i \in \mathbb{N}$, valem as igualdades:

$$R^i_\mathfrak{P}(L/E) = R^i_\mathfrak{P} \cap G_\mathfrak{P}(L/E) = R^i_\mathfrak{P} \cap \mathrm{Gal}(L/E).$$

Em particular, $I_\mathfrak{P}(L/E) = I_\mathfrak{P} \cap G_\mathfrak{P}(L/E) = I_\mathfrak{P} \cap \mathrm{Gal}(L/E)$.

(d) Para todo $i \in \mathbb{N}$, $R^i_\mathfrak{P}(L/T_\mathfrak{P}) = R^i_\mathfrak{P}$.

Demonstração. (a) A cadeia de inclusões é clara. Como $G_{\mathfrak{P}}$ é um conjunto finito, essa cadeia se estabiliza eventualmente. Assim, existe $m \in \mathbb{N}$ tal que $R^m_{\mathfrak{P}} = \cap_{i=0}^{\infty} R^i_{\mathfrak{P}}$. Ou seja, para todo automorfismo $\sigma \in R^m_{\mathfrak{P}}$ e todo $b \in B$, temos $\sigma b \equiv b \pmod{\mathfrak{P}^{i+1}}$ para todo $i \in \mathbb{N}$, de modo que $\sigma b - b \in \bigcap_{i=0}^{\infty} \mathfrak{P}^{i+1} = \{0\}$, e portanto $\sigma b = b$. Isso vale para todo $b \in B$, de forma que $\sigma|_B = \mathrm{id}_B \Rightarrow \sigma = \mathrm{id}_L$, já que $L = Q(B)$.

(b) Para ver que cada $R^i_{\mathfrak{P}}$ é um subgrupo normal de $G_{\mathfrak{P}}$, notemos que dado $\sigma \in G_{\mathfrak{P}}$ qualquer nós temos $\sigma\mathfrak{P}^{i+1} = (\sigma\mathfrak{P})^{i+1} = \mathfrak{P}^{i+1}$, de modo que podemos definir $\overline{\sigma} \in \mathrm{End}(B/\mathfrak{P}^{i+1})$ dado por $\overline{\sigma}(\overline{b}) = \overline{\sigma b}$. Essa função possui inversa $\overline{\sigma^{-1}}$, de modo que $\overline{\sigma} \in \mathrm{Aut}(B/\mathfrak{P}^{i+1})$. Assim, temos um homomorfismo de grupos $G_{\mathfrak{P}} \to \mathrm{Aut}(B/\mathfrak{P}^{i+1})$ dado por $\sigma \mapsto \overline{\sigma}$, e é claro que o núcleo desse homomorfismo é exatamente $R^i_{\mathfrak{P}}$, provando que esse conjunto é um subgrupo normal de $G_{\mathfrak{P}}$.

(c) Por definição, $R^i_{\mathfrak{P}}(L/E)$ é o conjunto dos $\sigma \in G_{\mathfrak{P}}(L/E)$ que satisfazem $\sigma b \equiv b \pmod{\mathfrak{P}^{i+1}}$ para todo $b \in B$, ou seja, o conjunto dos $\sigma \in G_{\mathfrak{P}}(L/E)$ tais que $\sigma \in R^i_{\mathfrak{P}}$. Isso mostra a primeira igualdade. A segunda igualdade segue da mesma forma.

(d) Basta aplicar os itens (a) e (c) juntamente com a Proposição 6.11:

$$R^i_{\mathfrak{P}}(L/T_{\mathfrak{P}}) = R^i_{\mathfrak{P}} \cap \mathrm{Gal}(L/T_{\mathfrak{P}}) = R^i_{\mathfrak{P}} \cap I_{\mathfrak{P}} = R^i_{\mathfrak{P}}.$$

□

O seguinte resultado nos diz como os grupos de decomposição, inércia e ramificação se comportam com localização. Na prática, ele nos diz que podemos trabalhar com a extensão de anéis $S^{-1}B/S^{-1}A$ e com os primos $S^{-1}\mathfrak{P} \mid S^{-1}\mathfrak{p}$ em vez de trabalharmos com B/A e com $\mathfrak{P} \mid \mathfrak{p}$.

Proposição 6.17. *Seja $S \subseteq A$ um conjunto multiplicativo. Então:*

(a) $G_{\mathfrak{P}} = G_{S^{-1}\mathfrak{P}}$.

(b) Para todo $i \in \mathbb{N}$, $R^i_{\mathfrak{P}} = R^i_{S^{-1}\mathfrak{P}}$. *Em particular,* $I_{\mathfrak{P}} = I_{S^{-1}\mathfrak{P}}$.

Demonstração. (a) ($\subseteq$): Seja $\sigma \in G_{\mathfrak{P}}$. Então $\sigma\mathfrak{P} = \mathfrak{P}$. Desse modo, como $S \subseteq K$ é fixo por σ, temos $\sigma(S^{-1}\mathfrak{P}) = S^{-1}\sigma\mathfrak{P} = S^{-1}\mathfrak{P}$, mostrando que $\sigma \in G_{S^{-1}\mathfrak{P}}$.

($\supseteq$): Seja $\sigma \in G_{S^{-1}\mathfrak{P}}$. Então $\sigma(S^{-1}\mathfrak{P}) = S^{-1}\mathfrak{P}$. Assim:

$$\sigma(\mathfrak{P}) = \sigma(S^{-1}\mathfrak{P} \cap B) = \sigma(S^{-1}\mathfrak{P}) \cap \sigma(B) = S^{-1}\mathfrak{P} \cap B = \mathfrak{P},$$

mostrando que $\sigma \in G_{\mathfrak{P}}$.

(b) Como $G_{\mathfrak{P}} = G_{S^{-1}\mathfrak{P}}$ basta provarmos que, dado $\sigma \in G_{\mathfrak{P}}$, a condição $\sigma b \equiv b \pmod{\mathfrak{P}^{i+1}}$ para todo $b \in B$ é equivalente à condição $\sigma b \equiv b \pmod{(S^{-1}\mathfrak{P})^{i+1}}$ para todo $b \in S^{-1}B$.

Suponhamos inicialmente que valha a primeira condição, e provemos a segunda. Tomemos $c \in S^{-1}B$ qualquer. Então $c = b/s$ para alguns $b \in B$ e $s \in S$, e nós temos:

$$\sigma c - c = \sigma\left(\frac{b}{s}\right) - \frac{b}{s} = \frac{\sigma b - b}{s} \in S^{-1}\mathfrak{P}^{i+1} = (S^{-1}\mathfrak{P})^{i+1},$$

como queríamos. Reciprocamente, suponhamos que valha a segunda condição, e seja $b \in B$ qualquer. Então sabemos que $\sigma b - b \in (S^{-1}\mathfrak{P})^{i+1} = S^{-1}\mathfrak{P}^{i+1}$. Assim, como $\sigma(B) = B$, nós obtemos $\sigma b - b \in B \cap S^{-1}\mathfrak{P}^{i+1} = \mathfrak{P}^{i+1}$, onde utilizamos o item (a) do Teorema 3.25.

□

Se $\mathfrak{p}$ for totalmente ramificado em L, temos uma forma mais simples de descrever os grupos de ramificação. Nesse caso, como vimos logo antes do Teorema 4.29, $B_\mathfrak{p}$ é um DVD com único ideal maximal $\mathfrak{P}_\mathfrak{p}$.

Proposição 6.18. *Suponhamos que $\mathfrak{p}$ seja totalmente ramificado em L. Então $G = G_\mathfrak{P} = I_\mathfrak{P}$ e, para todo $i \in \mathbb{N}$:*

$$R_\mathfrak{P}^i = \{\sigma \in G \colon \sigma\pi - \pi \in \mathfrak{P}_\mathfrak{p}^{i+1}\} = \{\sigma \in G \colon w(\sigma\pi - \pi) \geq i+1\},$$

onde π é um normalizador qualquer de $B_\mathfrak{p}$ e $w \colon L \to \mathbb{Z} \cup \{\infty\}$ é a valoração de $B_\mathfrak{p}$.

Demonstração. Por hipótese, $e = n$, $f = g = 1$. Desse modo, $(G : G_\mathfrak{P}) = (G_\mathfrak{P} : I_\mathfrak{P}) = 1$, de onde obtemos $G = G_\mathfrak{P} = I_\mathfrak{P}$. Vejamos então que valem as igualdades sobre os grupos de ramificação. Por um lado, se $\sigma \in R_\mathfrak{P}^i$, então pela proposição anterior vemos que $\sigma \in R_{\mathfrak{P}_\mathfrak{p}}^i$, e portanto $\sigma\pi - \pi \in \mathfrak{P}_\mathfrak{p}^{i+1}$. Assim, vale a inclusão $(\subseteq)$. Provemos $(\supseteq)$. Seja $\sigma \in G$ tal que $\sigma\pi - \pi \in \mathfrak{P}_\mathfrak{p}^{i+1}$. Como $R_\mathfrak{P}^i = R_{\mathfrak{P}_\mathfrak{p}}^i$, basta mostrarmos que $\sigma \in R_{\mathfrak{P}_\mathfrak{p}}^i$.

Seja $b \in B_\mathfrak{p}$ qualquer. Pelo item (c) do Teorema 4.29, podemos escrever $b = \sum_{j=0}^{n-1} b_j \pi^j$, para alguns $a_0, \ldots, a_{n-1} \in A_\mathfrak{p}$. Desse modo:

$$\sigma b - b = \sigma\left(\sum_{j=0}^{n-1} a_j\pi^j\right) - \sum_{j=0}^{n-1} a_j\pi^j = \sum_{j=0}^{n-1} a_j((\sigma\pi)^j - \pi^j).$$

Como $\sigma\pi - \pi \in \mathfrak{P}_\mathfrak{p}^{i+1}$ e para cada j temos $\sigma\pi - \pi \mid (\sigma\pi)^j - \pi^j$, vemos que $\sigma b - b \in \mathfrak{P}_\mathfrak{p}^{i+1}$, mostrando a inclusão inversa. □

Nós mostraremos a existência de certos homomorfismos ψ_i saindo de $R_\mathfrak{P}^i$ com núcleo $R_\mathfrak{P}^{i+1}$, que nos permitirão tirar informações importantes sobre os grupos de ramificação.

Teorema 6.19. *Suponhamos que $\mathfrak{p}$ seja totalmente ramificado em L. Seja π um normalizador de $B_\mathfrak{p}$, e sejam $U^{(0)}, U^{(1)}, \ldots$ os grupos de unidades de $B_\mathfrak{p}$. Então para todo $i \in \mathbb{N}$ a aplicação $\psi_i \colon R_\mathfrak{P}^i \to U^{(i)}/U^{(i+1)}$ dada por $\sigma \mapsto \frac{\sigma\pi}{\pi} \cdot U^{(i+1)}$ é um homomorfismo de grupos com núcleo $R_\mathfrak{P}^{i+1}$, que não depende da escolha de π. Assim, o homomorfismo induzido $\overline{\psi}_i \colon R_\mathfrak{P}^i/R_\mathfrak{P}^{i+1} \cong U^{(i)}/U^{(i+1)}$ é um isomorfismo de grupos.*

Demonstração. Fixemos $i \in \mathbb{N}$. Dado $\sigma \in R_\mathfrak{P}^i$, nós temos que $\sigma\pi - \pi \in \mathfrak{P}_\mathfrak{p}^{i+1}$, pela proposição acima. Em particular, $\sigma\pi \equiv \pi \equiv 0 \pmod{\mathfrak{P}_\mathfrak{p}}$. Assim, temos $\sigma\pi \in \mathfrak{P}_\mathfrak{p} = \pi B_\mathfrak{p}$, e faz sentido falarmos na divisão $\frac{\sigma\pi}{\pi}$. Chamando agora $y := \frac{\sigma\pi}{\pi}$, vemos que

$$y\pi = \sigma\pi \equiv \pi \pmod{\mathfrak{P}_\mathfrak{p}^{i+1}} \Rightarrow \pi(y-1) \equiv 0 \pmod{\mathfrak{P}_\mathfrak{p}^{i+1}}.$$

Assim, como $\pi B_\mathfrak{p} = \mathfrak{P}_\mathfrak{p}$, concluímos que $y - 1 \in \mathfrak{P}_\mathfrak{p}^i \Rightarrow y \in 1 + \mathfrak{P}_\mathfrak{p}^i = U^{(i)}$. Isso mostra que ψ_i está bem-definida. Observemos agora que, dado $\sigma \in R_\mathfrak{P}^i$, temos $\sigma u - u \in \mathfrak{P}_\mathfrak{p}^{i+1}$ para todo $u \in B_\mathfrak{p}$. Em particular, se $u \in B_\mathfrak{p}^\times$, multiplicando por u^{-1} nós obtemos que $\frac{\sigma u}{u} - 1 \in \mathfrak{P}_\mathfrak{p}^{i+1}$, e portanto $\frac{\sigma u}{u} \in U^{(i+1)}$. Para ver que ψ_i é um homomorfismo de grupos, sejam $\sigma, \tau \in R_\mathfrak{P}^i$ quaisquer. Então queremos mostrar que $\frac{\sigma\tau\pi}{\pi} \cdot U^{(i+1)} = \left(\frac{\sigma\pi}{\pi} \cdot U^{(i+1)}\right) \cdot \left(\frac{\tau\pi}{\pi} \cdot U^{(i+1)}\right) = \frac{(\sigma\pi)(\tau\pi)}{\pi^2} \cdot U^{(i+1)}$. Chamemos $u := \frac{\tau\pi}{\pi}$. Então $u \in U^{(i)} \subseteq B_\mathfrak{p}^\times$, e portanto $\frac{\sigma u}{u} \in U^{(i+1)}$. Agora:

$$\frac{(\sigma\pi)(\tau\pi)}{\pi^2} \cdot \frac{\sigma u}{u} = \frac{(\sigma\pi)(\tau\pi)}{\pi^2} \cdot \frac{\sigma\left(\frac{\tau\pi}{\pi}\right)}{\frac{\tau\pi}{\pi}} = \frac{(\sigma\pi)(\tau\pi)}{\pi^2} \frac{\pi \cdot \sigma\tau\pi}{(\sigma\pi)(\tau\pi)} = \frac{\sigma\tau\pi}{\pi}.$$

Logo ψ_i é homomorfismo de grupos. Calculemos agora seu núcleo. Nós temos

$$\begin{aligned} \psi_i(\sigma) = 0 \iff \frac{\sigma\pi}{\pi} \in U^{(i+1)} &\iff \frac{\sigma\pi}{\pi} \equiv 1 \pmod{\mathfrak{P}_\mathfrak{p}^{i+1}} \\ &\iff \frac{\sigma\pi - \pi}{\pi} \equiv 0 \pmod{\mathfrak{P}_\mathfrak{p}^{i+1}}. \end{aligned}$$

Como $\pi B_{\mathfrak{p}} = \mathfrak{P}_{\mathfrak{p}}$, é fácil ver que isso ocorre se e só se $\sigma\pi \equiv \pi \pmod{\mathfrak{P}_{\mathfrak{p}}^{i+2}} \iff \sigma \in R_{\mathfrak{P}}^{i+1}$, devido à Proposição 6.18. Assim, $\ker \psi_i = R_{\mathfrak{P}}^{i+1}$, como desejávamos. Finalmente, vejamos que ψ_i não depende do gerador π de $\mathfrak{P}_{\mathfrak{p}}$. Seja π' outro gerador desse ideal. Então temos $\pi' = u\pi$ para algum $u \in B_{\mathfrak{p}}^{\times}$. Assim, dado $\sigma \in R_{\mathfrak{P}}^{i}$ qualquer, temos:

$$\frac{\sigma\pi'}{\pi'} = \frac{\sigma(u\pi)}{u\pi} = \frac{(\sigma u)(\sigma\pi)}{u\pi} = \frac{\sigma\pi}{\pi} \cdot \frac{\sigma u}{u}.$$

Como $u \in B_{\mathfrak{p}}^{\times} \Rightarrow \frac{\sigma u}{u} \in U^{(i+1)}$, temos $\frac{\sigma\pi'}{\pi'} \cdot U^{(i+1)} = \frac{\sigma\pi}{\pi} \cdot U^{(i+1)}$, como queríamos. □

Localizando em relação ao primo $\mathfrak{P}_T \lhd B_T$ ao invés de $\mathfrak{p}$, podemos eliminar a hipótese de que $\mathfrak{p}$ é totalmente ramificado em L. Como sabemos que $\mathfrak{P}_T$ é totalmente ramificado em L, vemos que $B_{\mathfrak{P}_T}$ é um DVD com único ideal maximal $\mathfrak{P}\mathfrak{P}_T$. Assim, temos a seguinte versão mais geral do teorema acima:

Corolário 6.20. *Seja π um normalizador de $B_{\mathfrak{P}_T}$, e sejam $U^{(0)}, U^{(1)}, \ldots$ os grupos de unidades de $B_{\mathfrak{p}}$. Então para todo $i \in \mathbb{N}$ a aplicação $\psi_i \colon R_{\mathfrak{P}}^{i} \to U^{(i)}/U^{(i+1)}$ dada por $\sigma \mapsto \frac{\sigma\pi}{\pi} \cdot U^{(i+1)}$ é um homomorfismo de grupos com núcleo $R_{\mathfrak{P}}^{i+1}$, que não depende da escolha de π. Assim, o homomorfismo induzido $\overline{\psi}_i \colon R_{\mathfrak{P}}^{i}/R_{\mathfrak{P}}^{i+1} \cong U^{(i)}/U^{(i+1)}$.*

Demonstração. Aplicando o teorema acima para a extensão $L/T_{\mathfrak{P}}$, concluímos que a aplicação $\psi_i \colon R_{\mathfrak{P}}^{i}(L/T_{\mathfrak{P}}) \to U^{(i)}/U^{(i+1)}$ dada por $\sigma \mapsto \frac{\sigma\pi}{\pi} \cdot U^{(i+1)}$ é um homomorfismo de grupos com núcleo $R_{\mathfrak{P}}^{i+1}(L/T_{\mathfrak{P}})$, que não depende do gerador π. Mas pelo item (d) da Proposição 6.16, temos $R_{\mathfrak{P}}^{i}(L/T_{\mathfrak{P}}) = R_{\mathfrak{P}}^{i}$ e $R_{\mathfrak{P}}^{i+1}(L/T_{\mathfrak{P}}) = R_{\mathfrak{P}}^{i+1}$, concluindo a demonstração. □

Como consequência direta desse corolário, obtemos:

Corolário 6.21. *(a) O grupo $I_{\mathfrak{P}}/R_{\mathfrak{P}}^{1}$ é canonicamente isomorfo a um subgrupo do grupo multiplicativo $(B/\mathfrak{P})^{\times}$.*

(b) Para todo $i \geq 1$, o grupo $R_{\mathfrak{P}}^{i}/R_{\mathfrak{P}}^{i+1}$ é canonicamente isomorfo a um subgrupo do grupo aditivo de $B/\mathfrak{P}$.

Demonstração. Pelo corolário acima, nós temos um isomorfismo canônico $R_{\mathfrak{P}}^{i}/R_{\mathfrak{P}}^{i+1} \cong U^{(i)}/U^{(i+1)}$, para todo $i \geq 0$. Aplicando agora o Lema 3.29 ao DVD $B_{\mathfrak{P}_T}$, obtemos isomorfismos canônicos entre $U^{(0)}/U^{(1)}$ e $(B_{\mathfrak{P}_T}/\mathfrak{P}_{\mathfrak{P}_T})^{\times}$ e entre $U^{(i)}/U^{(i+1)}$ e o grupo aditivo $B_{\mathfrak{P}_T}/\mathfrak{P}_{\mathfrak{P}_T}$. Mas $B_{\mathfrak{P}_T}/\mathfrak{P}_{\mathfrak{P}_T}$ é canonicamente isomorfo a $B/\mathfrak{P}$, pelo Teorema 3.25, o que nos dá os resultados desejados. □

Isso nos permite obter informações interessantes sobre os grupos de ramificação. Lembremos que todo subgrupo finito do grupo multiplicativo de um corpo é cíclico, com ordem não divisível pela característica do corpo. Além disso, seja $\mathscr{L}$ um corpo qualquer. Se $\mathscr{L}$ tiver característica 0, então é claro que o seu único subgrupo aditivo finito é o trivial. Suponhamos então que a característica de $\mathscr{L}$ seja $p > 0$. Como todo elemento não-nulo de $\mathscr{L}$ tem ordem (aditiva) p nesse caso, vemos da caracterização dos grupos abelianos finitos que todo subgrupo aditivo finito de $\mathscr{L}$ deve ser um **p-grupo elementar**, isto é, um grupo da forma $\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$. Com essas observações, temos:

Corolário 6.22. *(a) Se $B/\mathfrak{P}$ tiver característica 0, então $I_{\mathfrak{P}}$ será um grupo cíclico e $R_{\mathfrak{P}}^{1}$ será o grupo trivial.*

(b) Se $B/\mathfrak{P}$ tiver característica $p > 0$, então $I_{\mathfrak{P}}/R_{\mathfrak{P}}^{1}$ será um grupo cíclico de ordem não divisível por p, e para todo $i \geq 1$, $R_{\mathfrak{P}}^{i}/R_{\mathfrak{P}}^{i+1}$ e $R_{\mathfrak{P}}^{i}$ serão p-grupos elementares. Além disso, $R_{\mathfrak{P}}^{1}$ será o único p-subgrupo de Sylow de $I_{\mathfrak{P}}$.

Demonstração. (a) Se $B/\mathfrak{P}$ tiver característica 0, então pelas observações acima vemos que $I_\mathfrak{P}/R^1_\mathfrak{P}$ será um grupo cíclico e que $R^i_\mathfrak{P}/R^{i+1}_\mathfrak{P} = 1$ para todo $i \geq 1$. Assim, $R^1_\mathfrak{P} = R^2_\mathfrak{P} = \cdots$. Como temos $R^m_\mathfrak{P} = 1$ para algum $m \in \mathbb{N}$, vemos então que $R^1_\mathfrak{P} = 1$. Desse modo, vemos que $I_\mathfrak{P} = I_\mathfrak{P}/R^1_\mathfrak{P}$ é cíclico.

(b) Se $B/\mathfrak{P}$ tiver característica $p > 0$, então pelas observações acima vemos que $I_\mathfrak{P}/R^1_\mathfrak{P}$ será um grupo cíclico de ordem não divisível por p e que, para todo $i \geq 1$, $R^i_\mathfrak{P}/R^{i+1}_\mathfrak{P}$ será um p-grupo elementar. Seja $m \in \mathbb{N}$ tal que $R^m_\mathfrak{P} = 1$. Então, para cada $1 \leq i \leq m$, temos:

$$|R^i_\mathfrak{P}| = \left|\frac{R^i_\mathfrak{P}}{R^{i+1}_\mathfrak{P}}\right| \cdot \left|\frac{R^{i+1}_\mathfrak{P}}{R^{i+2}_\mathfrak{P}}\right| \cdots \left|\frac{R^{m-1}_\mathfrak{P}}{R^m_\mathfrak{P}}\right|.$$

Assim, $|R^i_\mathfrak{P}|$ é uma potência de p, sendo portanto um p-grupo, como desejado. Finalmente, como $I_\mathfrak{P}/R^1_\mathfrak{P}$ possui ordem não divisível por p e $R^1_\mathfrak{P}$ é um p-grupo, vemos que $R^1_\mathfrak{P}$ é de fato um p-subgrupo de Sylow de $I_\mathfrak{P}$. Ele é o único p-subgrupo de Sylow de $I_\mathfrak{P}$, pois sabemos que $R^1_\mathfrak{P} \lhd I_\mathfrak{P}$ e que todos os p-subgrupos de Sylow de $I_\mathfrak{P}$ são conjugados, pelo Segundo Teorema de Sylow.

□

Vamos trabalhar agora com os corpos fixos pelos grupos de ramificação:

Definição (Corpos de Ramificação)**.** Para cada $i \in \mathbb{N}$, definimos o i-ésimo **corpo de ramificação** de $\mathfrak{P}$ sobre K como sendo o corpo $V^i_\mathfrak{P} \subseteq L$ fixo pelo grupo $R^i_\mathfrak{P}$.

Então, pela correspondência de Galois, é claro que $T_\mathfrak{P} = V^0_\mathfrak{P} \subseteq V^1_\mathfrak{P} \subseteq V^2_\mathfrak{P} \subseteq \cdots$, e que existe $m \in \mathbb{N}$ tal que $V^m_\mathfrak{P} = L$. Além disso, da teoria de Galois, da Proposição 6.16 e do Corolário 6.22, obtemos imediatamente:

Corolário 6.23. *(a) No caso em que $B/\mathfrak{P}$ tem característica 0, temos $V^1_\mathfrak{P} = V^2_\mathfrak{P} = \cdots = L$.*

(b) No caso em que $B/\mathfrak{P}$ tem característica $p > 0$, para todo $i \geq 1$ a extensão $L/V^i_\mathfrak{P}$ é finita galoisiana e $\mathrm{Gal}(L/V^i_\mathfrak{P}) = R^i_\mathfrak{P}$ é um p-grupo. Além disso, para todo $i \geq 1$, $V^{i+1}_\mathfrak{P}/V^i_\mathfrak{P}$ é finita galoisiana e $\mathrm{Gal}(V^{i+1}_\mathfrak{P}/V^i_\mathfrak{P}) \cong R^i_\mathfrak{P}/R^{i+1}_\mathfrak{P}$ é p-elementar. A extensão $V^1_\mathfrak{P}/T_\mathfrak{P}$ também é finita galoisiana, e $\mathrm{Gal}(V^1_\mathfrak{P}/T_\mathfrak{P}) \cong I_\mathfrak{P}/R^1_\mathfrak{P}$ é cíclico de ordem não divisível por p.

(c) Para todo $i \in \mathbb{N}$, $V^i_\mathfrak{P}/G_\mathfrak{P}$ é finita galoisiana.

Assim, como $Z_\mathfrak{P}$ e $T_\mathfrak{P}$, o corpo $V^1_\mathfrak{P}$ pode ser caracterizado por uma propriedade minimal, caso $B/\mathfrak{P}$ tenha característica positiva:

Teorema 6.24. *Suponhamos que $B/\mathfrak{P}$ tenha característica $p > 0$, e seja E um corpo com $T_\mathfrak{P} \subseteq E \subseteq L$. Então $V^1_\mathfrak{P} \subseteq E$ se e só se $e(\mathfrak{P} \mid \mathfrak{P}_E)$ for uma potência de p.*

Demonstração. Como $\mathfrak{P}_T$ é totalmente ramificado em L, $\mathfrak{P}_E$ também o é. Assim, nós temos $[L : E] = e(\mathfrak{P} \mid \mathfrak{P}_E)$, de modo que $e(\mathfrak{P} \mid \mathfrak{P}_E)$ será uma potência de p se e só se $\mathrm{Gal}(L/E)$ for um p-grupo. Mas isso ocorrerá se e só se $\mathrm{Gal}(L/E) \subseteq R^1_\mathfrak{P} = \mathrm{Gal}(L/V^1_\mathfrak{P})$, que é o único p-Sylow de $I_\mathfrak{P} = \mathrm{Gal}(L/T_\mathfrak{P})$. Finalmente, essa última continência equivale a $V^1_\mathfrak{P} \subseteq E$. □

Para tratarmos simultaneamente dos casos em que $B/\mathfrak{P}$ tem característica 0 ou positiva, convém introduzir a seguinte notação:

Definição (Expoente Característico)**.** Seja $\mathscr{L}$ um corpo. Então o **expoente característico** p de $\mathscr{L}$ é definido como 1, se $\mathscr{L}$ tiver característica 0, e como a característica de $\mathscr{L}$, se esta for positiva.

Seja p o expoente característico de $B/\mathfrak{P}$. Então $e = e(\mathfrak{P} \mid \mathfrak{p})$ se escreve de modo único como $e = p^t\tilde{e}$, onde $t \in \mathbb{N}$ e $\mathrm{mdc}(p, \tilde{e}) = 1$ (note que $\tilde{e} = e$ caso $p = 1$). Denotemos $B_V := \overline{A}^{V_{\mathfrak{P}}^1} = B \cap V_{\mathfrak{P}}^1$ e $\mathfrak{P}_V := \mathfrak{P} \cap B_V \lhd B_V$. Então:

Corolário 6.25. *(a)* $[L : V_{\mathfrak{P}}^1] = e(\mathfrak{P} \mid \mathfrak{P}_V) = p^t$.

(b) $[V_{\mathfrak{P}}^1 : T_{\mathfrak{P}}] = e(\mathfrak{P}_V \mid \mathfrak{P}_T) = \tilde{e}$, *e* $\mathrm{Gal}(V_{\mathfrak{P}}^1/T_{\mathfrak{P}})$ *é canonicamente isomorfo ao grupo* $W_{\tilde{e}}(B/\mathfrak{P})$.

Demonstração. Sabemos que $R_{\mathfrak{P}}^1 = \mathrm{Gal}(L/V_{\mathfrak{P}}^1)$ é o p-subgrupo de Sylow de $I_{\mathfrak{P}} = \mathrm{Gal}(L/T_{\mathfrak{P}})$, que tem cardinalidade $e = p^t\tilde{e}$. Assim, temos $|R_{\mathfrak{P}}^1| = p^t$, de onde $[L : V_{\mathfrak{P}}^1] = p^t$. Além disso, da mesma forma que na demonstração do teorema acima, vemos que $\mathfrak{P}_V$ é totalmente ramificado em L, e portanto $e(\mathfrak{P} \mid \mathfrak{P}_V) = [L : V_{\mathfrak{P}}^1] = p^t$. Disso, segue facilmente que $[V_{\mathfrak{P}}^1 : T_{\mathfrak{P}}] = e(\mathfrak{P}_V \mid \mathfrak{P}_T) = \tilde{e}$. Finalmente, sabemos que $\mathrm{Gal}(V_{\mathfrak{P}}^1/T_{\mathfrak{P}})$ tem cardinalidade $\tilde{e}$ e é canonicamente isomorfo a um subgrupo finito do grupo multiplicativo $(B/\mathfrak{P})^\times$. Assim, esse subgrupo deve ser $W_{\tilde{e}}(B/\mathfrak{P})$. □

Nós podemos refinar ainda mais o diagrama da Observação 6.12, para obter:

$$
\begin{array}{ccccccc}
\mathfrak{P} \lhd B & \hookrightarrow & L = Q(B) & \text{---------} & 1 & & \\
{\scriptstyle p^t}\big| & & {\scriptstyle p^t}\big| & & {\scriptstyle p^t}\big| & & \\
\mathfrak{P}_V \lhd B_V & \hookrightarrow & V_{\mathfrak{P}}^1 = Q(B_V) & \text{------} & R_{\mathfrak{P}}^1 & \quad \mathrm{Gal}(V_{\mathfrak{P}}^1/I_{\mathfrak{P}}) \cong I_{\mathfrak{P}}/R_{\mathfrak{P}}^1 \cong W_{\tilde{e}}(B/\mathfrak{P}) & \\
{\scriptstyle \tilde{e}}\big| & & {\scriptstyle \tilde{e}}\big| & & {\scriptstyle \tilde{e}}\big| & & \\
\mathfrak{P}_T \lhd B_T & \hookrightarrow & T_{\mathfrak{P}} = Q(B_T) & \text{-------} & I_{\mathfrak{P}} & \quad B/\mathfrak{P} = B_T/\mathfrak{P}_T & \\
{\scriptstyle f}\big| & & {\scriptstyle f}\big| & & {\scriptstyle f}\big| & \quad \big| & \\
\mathfrak{P}_Z \lhd B_Z & \hookrightarrow & Z_{\mathfrak{P}} = Q(B_Z) & \text{------} & G_{\mathfrak{P}} & \quad A/\mathfrak{p} = B_Z/P_Z & \\
{\scriptstyle g}\big| & & {\scriptstyle g}\big| & & {\scriptstyle g}\big| & & \\
\mathfrak{p} \lhd A & \hookrightarrow & K = Q(A) & \text{--------} & G & &
\end{array}
$$

Assim, dividimos a ramificação entre $T_{\mathfrak{P}}^1$ e L em duas etapas. De $T_{\mathfrak{P}}$ a $V_{\mathfrak{P}}^1$ ocorre a **ramificação mansa**, ou seja, com $\mathrm{mdc}(p, e(\mathfrak{P}_V \mid \mathfrak{P}_T)) = 1$, enquanto que de $V_{\mathfrak{P}}^1$ a L ocorre a **ramificação selvagem**, ou seja, com $e(\mathfrak{P} \mid \mathfrak{P}_V)$ igual a uma potência de p. Note que podemos ainda separar a ramificação selvagem no estudo dos p-grupos elementares $R_{\mathfrak{P}}^1/R_{\mathfrak{P}}^2$, $R_{\mathfrak{P}}^2/R_{\mathfrak{P}}^3, \ldots, R_{\mathfrak{P}}^{m-1}/R_{\mathfrak{P}}^m$, onde $m \in \mathbb{N}$ é o menor inteiro para o qual $R_{\mathfrak{P}}^m = 1$. É claro que se a característica de $\mathscr{L}$ for 0, não ocorrerá ramificação selvagem. Terminaremos estudando a solubilidade dos grupos $I_{\mathfrak{P}}$ e $G_{\mathfrak{P}}$:

Teorema 6.26. *(a)* $I_{\mathfrak{P}}$ *é um grupo solúvel.*

(b) Se $\overline{G}_{\mathfrak{P}}$ *for um grupo solúvel, então* $G_{\mathfrak{P}}$ *também o será.*

Demonstração. (a) Basta notar que temos a série normal $1 = R_{\mathfrak{P}}^m \lhd R_{\mathfrak{P}}^{m-1} \lhd \cdots \lhd R_{\mathfrak{P}}^1 \lhd I_{\mathfrak{P}}$, e que cada $R_{\mathfrak{P}}^i/R_{\mathfrak{P}}^{i+1}$ é abeliano. De fato, $I_{\mathfrak{P}}/R_{\mathfrak{P}}^1$ é cíclico, e para $i \geq 1$ temos $R_{\mathfrak{P}}^i/R_{\mathfrak{P}}^{i+1}$ igual a um produto finito de grupos cíclicos de ordem p.

(b) Nós temos $\overline{G}_{\mathfrak{P}} \cong G_{\mathfrak{P}}/I_{\mathfrak{P}}$. Assim, se $\overline{G}_{\mathfrak{P}}$ for um grupo solúvel, como $I_{\mathfrak{P}}$ também é solúvel por (a) vemos que $G_{\mathfrak{P}}$ será solúvel.

□

Como consequência imediata desse teorema, temos o seguinte interessante corolário:

Corolário 6.27. *(a) A extensão* $L/T_{\mathfrak{P}}$ *é solúvel por radicais.*

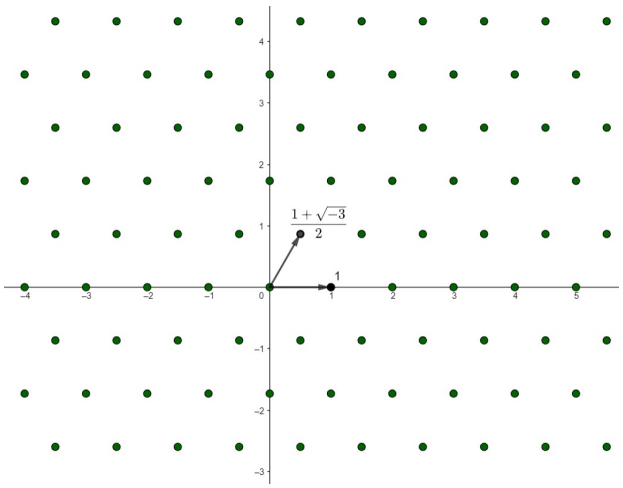
(b) Se $\overline{G}_{\mathfrak{P}}$ *for solúvel, então a extensão* $L/Z_{\mathfrak{P}}$ *será solúvel por radicais.*

Capítulo 7

O Método Geométrico e o Teorema das Unidades

Até agora, todos os resultados que obtivemos vieram de métodos puramente algébricos. Para conseguirmos mais resultados, precisaremos lançar mão de métodos geométricos, que estudaremos nesse capítulo. Além de conseguirmos uma cota melhor para o número de classes de um anel de inteiros algébricos, também obteremos resultados novos, como o Teorema das Unidades de Dirichlet. Esses resultados serão consequências do chamado Teorema de Minkowski sobre reticulados.

Como motivação, consideremos o corpo quadrático $K = \mathbb{Q}(\sqrt{-3})$. Então $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto 2, com base $\left\{1, \frac{1+\sqrt{-3}}{2}\right\}$. Desse modo, podemos identificar $\mathcal{O}_K$ com o conjunto dos pontos no plano cartesiano que são combinações inteiras dos vetores $(1, 0)$ e $(1/2, \sqrt{-3}/2)$, formando um **reticulado**:



Nós já utilizamos a ideia de reticulado implicitamente, no Teorema 2.19. De fato, o ponto "mais próximo" de $\mathcal{O}_K$ a um ponto de K nada mais é do que o ponto do reticulado mais próximo do ponto em questão. Isso já nos mostra um pouco de como a intuição geométrica pode nos ser útil.

7.1. Reticulados, Malhas e o Teorema de Minkowski

Seja V um $\mathbb{R}$-espaço vetorial de dimensão n, com uma base distinguida $\{e_1, \ldots, e_n\}$. Podemos então definir um produto interno e uma norma em V com relação a essa base: dados dois vetores $x = \xi_1 e_1 + \cdots + \xi_n e_n$ e $y = \eta_1 e_1 + \cdots + \eta_n e_n$, definimos:

$$\langle x, y\rangle \coloneqq \xi_1\eta_1 + \cdots + \xi_n\eta_n, \text{ e } \|x\| \coloneqq \sqrt{\langle x, x\rangle} = \sqrt{\xi_1^2 + \cdots + \xi_n^2}.$$

Com isso, V se torna um espaço normado. Dados $v \in V$ e $\rho > 0$ quaiquer, denotaremos por $B_\rho(v) \coloneqq \{x \in V \colon \|x - v\| \leq \rho\}$ a bola de centro v e raio ρ. Além disso, denotaremos a bola de centro 0 e raio ρ simplesmente por B_ρ. Note que a topologia induzida por essa norma é a topologia euclidiana, já que todas as normas em $\mathbb{R}^n$ são equivalentes.

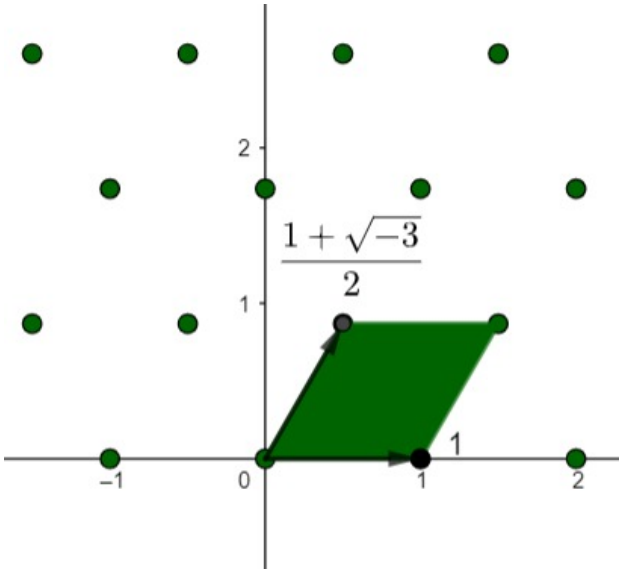
Dados $v_1, \ldots, v_m \in V$ quaisquer, consideramos os conjuntos

$$\begin{aligned}\Gamma &\coloneqq \mathbb{Z}\, v_1 + \cdots + \mathbb{Z}\, v_m = \left\{\sum_{i=1}^m a_i v_i \colon a_1, \ldots, a_m \in \mathbb{Z}\right\}, \text{ e}\\ \Phi &\coloneqq \left\{\sum_{i=1}^m \rho_i v_i \colon 0 \leq \rho_1, \ldots, \rho_m < 1\right\}.\end{aligned}$$

Definição (Reticulado)**.** Com as notações acima, dizemos que Φ é o **paralelepípedo** gerado pelos vetores $v_1, \ldots, v_m$. Além disso, dizemos que Γ é um **reticulado** de V se $v_1, \ldots, v_m$ forem linearmente independentes sobre $\mathbb{R}$. Nesse caso, chamamos $v_1, \ldots, v_m$ de uma **base de reticulado** associada a Γ, e de Φ a **malha fundamental** associada a essa base. Note que para isso ocorrer devemos ter $m \leq n$. Caso $m = n$, então Γ e $v_1, \ldots, v_m$ serão chamados de um **reticulado completo** e de uma **base de reticulado completa**, respectivamente. Chamamos ainda de **malha** de Γ associada à base $v_1, \ldots, v_m$ um conjunto da forma $\gamma + \Phi$, para $\gamma \in \Gamma$ qualquer.

Observação 7.1. *Se Γ for um reticulado com base $\{v_1, \ldots, v_m\}$ e malha fundamental com relação a essa base Φ, é fácil ver da decomposição de um $r \in \mathbb{R}$ como $r = \lfloor r\rfloor + (r - \lfloor r\rfloor)$ que nós temos $\Gamma + \Phi = \mathbb{R}\, v_1 + \cdots + \mathbb{R}\, v_m$. Em particular, Γ será completo se e só se $\Gamma + \Phi = V$.*

Exemplo 7.2. *A malha fundamental no reticulado de $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ é o paralelogramo verde indicado abaixo:*



O Teorema de Minkowski, que provaremos no final dessa seção, é um resultado que nos diz que todo subconjunto "suficientemente grande" de V que satisfaz determinadas condições contém um ponto não-nulo de um reticulado Γ, e pode ser pensado como uma espécie de "Princípio da Casa dos Pombos contínuo". Ele melhora (por muito) a cota encontrada para o número de classes de um corpo de números, que achamos utilizando o Princípio da Casa dos Pombos.

A princípio, a definição de um reticulado aparenta ser diretamente atrelada a uma base. O surpreendente é que temos uma caracterização para os reticulados de V que independe de acharmos uma base:

Proposição 7.3. *Um subconjunto $\Gamma \subseteq V$ será um reticulado de V se e somente se for um subgrupo aditivo discreto de V (na topologia euclidiana).*

Demonstração. ($\Rightarrow$): Suponhamos que Γ seja um reticulado de V, e que $v_1, \dots, v_m$ seja uma base para esse reticulado. Sendo $\Gamma = \mathbb{Z}\, v_1 + \cdots + \mathbb{Z}\, v_m$, é claro que Γ é um grupo aditivo. Para ver que Γ é discreto, estendemos o conjunto linearmente independente $\{v_1, \dots, v_m\}$ a uma base $\{v_1, \dots, v_n\}$ de V. Isso estende o reticulado Γ ao reticulado $\Gamma' \coloneqq \mathbb{Z}\, v_1 + \cdots + \mathbb{Z}\, v_n$. Então basta mostrar que Γ' é discreto. Seja $\gamma \in \Gamma'$ qualquer. Então temos $\gamma = a_1 v_1 + \cdots + a_n v_n$ para certos $a_1, \dots, a_n \in \mathbb{Z}$. Consideremos o conjunto

$$S \coloneqq \{x_1 v_1 + \cdots + x_n v_n \colon |x_i - a_i| < 1, \text{ para todo } 1 \leq i \leq n\}.$$

Então esse conjunto é aberto de V e claramente $S \cap \Gamma' = \{\gamma\}$, provando que Γ' é discreto.

($\Leftarrow$): Suponhamos que Γ seja um subgrupo aditivo discreto de V. Seja $\{u_1, \dots, u_m\}$ um sistema maximal de elementos de Γ linearmente independentes sobre $\mathbb{R}$. Eles formam a base do reticulado $\Gamma' \coloneqq \mathbb{Z}\, u_1 + \cdots + \mathbb{Z}\, u_m \subseteq \Gamma$. Seja Φ a malha fundamental de Γ' com respeito a essa base. Então temos $(\Gamma \cap \Phi) + \Gamma' = \Gamma$:

($\subseteq$): Segue do fato de que $\Gamma \cap \Phi, \Gamma' \subseteq \Gamma$ e que Γ é um grupo aditivo.

($\supseteq$): Seja $\gamma \in \Gamma$ qualquer. Então, pela maximalidade de $\{u_1, \dots, u_m\}$, existem $r_1, \dots, r_m \in \mathbb{R}$ tais que $\gamma = r_1 u_1 + \cdots + r_m u_m$. Note então que $\gamma = \sum_{i=1}^m \lfloor r_i \rfloor u_i + \sum_{i=1}^m (r_i - \lfloor r_i \rfloor) u_i$, e temos $\sum_{i=1}^m \lfloor r_i \rfloor u_i \in \Gamma' \subseteq \Gamma$ e $\sum_{i=1}^m (r_i - \lfloor r_i \rfloor) u_i = \gamma - \sum_{i=1}^m \lfloor r_i \rfloor u_i \in \Gamma \cap \Phi$, mostrando que $\gamma \in (\Gamma \cap \Phi) + \Gamma'$.

Essa igualdade nos diz que todo elemento do grupo aditivo Γ/Γ' está na classe de algum elemento de $\Gamma \cap \Phi$. Agora, como Γ é discreto e Φ é limitado na topologia euclidiana, temos $\Gamma \cap \Phi$ finito. Assim, Γ/Γ' é um grupo finito. Seja $q \coloneqq |\Gamma/\Gamma'|$. Então, por Lagrange, $q\Gamma \subseteq \Gamma'$, de forma que

$$\Gamma \subseteq q^{-1}\Gamma' = \mathbb{Z} \cdot \left(q^{-1} u_1\right) + \cdots + \mathbb{Z} \cdot \left(q^{-1} u_m\right).$$

Assim, Γ é um $\mathbb{Z}$-submódulo de um $\mathbb{Z}$-módulo livre de posto m, e pelo Teorema 1.38 concluímos que Γ é um $\mathbb{Z}$-módulo livre de posto menor ou igual a m. De fato, seu posto é exatamente m, como vemos pelas inclusões $\Gamma' \subseteq \Gamma \subseteq q^{-1}\Gamma'$. Segue ainda dessas inclusões que os $\mathbb{R}$-espaços gerados por Γ e por Γ' coincidem, e têm dimensão m já que $u_1, \dots, u_m$ são linearmente independentes sobre $\mathbb{R}$. Seja $v_1, \dots, v_m$ uma $\mathbb{Z}$-base de Γ. Então $\mathbb{R}\, v_1 + \cdots + \mathbb{R}\, v_m$ tem dimensão m, de onde tiramos que $\{v_1, \dots, v_m\}$ é um conjunto linearmente independente sobre $\mathbb{R}$. Assim, concluímos finalmente que Γ é um reticulado de V. □

No caso de um reticulado completo, vemos que intuitivamente a reunião de todas as suas malhas cobre todo V (veja, por exemplo, o reticulado de $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ mostrado acima). De fato, temos a seguinte importante caracterização dos reticulados completos:

Teorema 7.4. *Seja Γ um reticulado em V. As seguintes condições são equivalentes:*

(i) Γ *é um reticulado completo de* V.

(ii) Existe um subconjunto limitado C *de* V *tal que* $V = \bigcup_{\gamma\in\Gamma}(\gamma + C)$.

Nesse caso temos, em particular, que $V = \bigsqcup_{\gamma\in\Gamma}(\gamma + \Phi)$, *sendo* Φ *a malha fundamental associada a uma base qualquer de* Γ.

Demonstração. $(i) \Rightarrow (ii)$: Seja $\{v_1, \ldots, v_n\}$ uma base de Γ, e seja Φ a malha fundamental associada a essa base. Afirmamos que $V = \bigsqcup_{\gamma\in\Gamma}(\gamma + \Phi)$. Como Φ é limitado, isso provará (ii). Como V tem dimensão n, vemos que $\{v_1, \ldots, v_n\}$ é uma base de V. Seja $v \in V$ qualquer. Então $v = r_1v_1 + \cdots + r_nv_n$, para alguns $r_1, \ldots, r_n \in \mathbb{R}$. Assim:

$$v = \sum_{i=1}^{n} \lfloor r_i \rfloor v_i + \sum_{i=1}^{n} (r_i - \lfloor r_i \rfloor)v_i \in \bigcup_{\gamma\in\Gamma} (\gamma + \Phi).$$

Isso prova que $\bigcup_{\gamma\in\Gamma}(\gamma + \Phi) = V$. Falta mostrar que essa união é disjunta. Suponhamos que $\alpha, \beta \in \Gamma$ sejam tais que $(\alpha + \Phi) \cap (\beta + \Phi) \neq \emptyset$. Então existem elementos $z, w \in \Phi$ tais que $\alpha + z = \beta + w \Rightarrow \alpha - \beta = w - z$. Nós temos $w = r_1v_1 + \cdots + r_nv_n$ e $z = s_1v_1 + \cdots + s_nv_n$, para alguns $0 \leq r_i, s_i < 1$. Assim:

$$\alpha - \beta = w - z = (r_1 - s_1)v_1 + \cdots + (r_n - s_n)v_n.$$

Note que $-1 < r_i - s_i < 1$, para $1 \leq i \leq n$. Mas todas as coordenadas de $\alpha - \beta \in \Gamma$ na base $\{v_1, \ldots, v_n\}$ são inteiras, e portanto $r_i - s_i = 0$ para todo i. Isso prova que $\alpha - \beta = 0 \Rightarrow \alpha = \beta$. Desse modo, a união $V = \bigcup_{\gamma\in\Gamma}(\gamma + \Phi)$ é disjunta, como queríamos.

$(ii) \Rightarrow (i)$: Suponhamos que exista $C \subseteq V$ limitado tal que $V = \bigcup_{\gamma\in\Gamma}(\gamma + C)$. Seja V' o $\mathbb{R}$-subespaço de V gerado por Γ. Então queremos provar que $V' = V$. Seja $v \in V$ qualquer. Como $V = \bigcup_{\gamma\in\Gamma}(\gamma + C)$, para todo inteiro positivo n conseguimos encontrar $\gamma_n \in \Gamma$ e $c_n \in C$ tais que $nv = \gamma_n + c_n$. Para todo n inteiro positivo temos $v = (\gamma_n + c_n)/n$, logo

$$v = \lim_{n\to\infty} \frac{\gamma_n + c_n}{n} = \lim_{n\to\infty} \frac{\gamma_n}{n} + \lim_{n\to\infty} \frac{c_n}{n} = \lim_{n\to\infty} \frac{\gamma_n}{n},$$

uma vez que C é limitado e portanto $\lim_{n\to\infty} c_n/n = 0$. Finalmente, notemos que para todo n inteiro positivo temos $\gamma_n/n \in V'$, e que V' é fechado em V já que é um subespaço finitamente gerado de V. Assim, $v = \lim_{n\to\infty} \gamma_n/n \in V'$, como queríamos. Isso mostra que $V' = V$, e portanto Γ é reticulado completo. □

Sendo $V \cong \mathbb{R}^n$ com "base canônica" $\{e_1, \ldots, e_n\}$, podemos considerar uma medida de Lebesgue em V da mesma forma que fazemos em $\mathbb{R}^n$. Chamaremos a medida de Lebesgue de um conjunto $C \subseteq V$ de **volume** desse conjunto, e o denotaremos por $\mathrm{vol}(C)$.

Proposição 7.5. *Sejam* $v_1, \ldots, v_n \in V$, *e seja* Φ_v *o paralelepípedo gerado por esses vetores. Então:*

(a) $\mathrm{vol}(\Phi_v) = |\det(v_1, \ldots, v_n)|$.

(b) $\{v_1, \ldots, v_n\} \subseteq V$ *formará a base de um reticulado completo em* V *se e só se tivermos* $\det(v_1, \ldots, v_n) \neq 0$, *se e só se tivermos* $\mathrm{vol}(\Phi_v) \neq 0$.

(c) Seja $T\colon V^n \to V^n$ *um operador linear, e suponhamos* $T(v_1, \ldots, v_n) = (w_1, \ldots, w_n)$. *Então, sendo* Φ_w *o paralelepípedo gerado por* $w_1, \ldots, w_n$, *temos* $\mathrm{vol}(\Phi_w) = |\det T| \cdot \mathrm{vol}(\Phi_v)$.

(d) Para todas as bases de um reticulado completo Γ*, os volumes de suas malhas fundamentais associadas coincidem, e são iguais a um número real positivo.*

Demonstração. Os itens $(a), (b)$ e (c) seguem facilmente de álgebra linear e da teoria de integração. Provemos (d). Seja $\{v_1, \ldots, v_n\}$ uma base de Γ, com malha fundamental Φ_v, e tomemos $\{w_1, \ldots, w_n\} \subseteq V$ qualquer. Então existe um único operador linear $T\colon V^n \to V^n$ tal que $T(v_1, \ldots, v_n) = (w_1, \ldots, w_n)$. Sabemos que $\{w_1, \ldots, w_n\}$ será uma base do $\mathbb{Z}$-módulo Γ se e somente se $\det T \in \mathbb{Z}^\times = \{-1, 1\}$. Desse modo, para qualquer base $\{w_1, \ldots, w_n\}$ de Γ, temos $\mathrm{vol}(\Phi_w) = |\det T| \cdot \mathrm{vol}(\Phi_v) = \mathrm{vol}(\Phi_v)$. Finalmente, $\mathrm{vol}(\Phi_v) \neq 0$ pelo item (b), e $\mathrm{vol}(\Phi_v) < \infty$ já que esse é o determinante de uma matriz $n \times n$. □

Definição (Volume de um Reticulado)**.** Dado um reticulado Γ de V, definimos o seu **volume** $\mathrm{vol}(\Gamma)$ como sendo o volume de qualquer uma de suas malhas fundamentais.

Observação 7.6. *É claro que o volume de qualquer malha de* Γ *também será* $\mathrm{vol}(\Gamma)$*, já que toda malha de* Γ *é uma translação da malha fundamental de* Γ*.*

Já vimos que as malhas de um reticulado completo Γ são todas disjuntas. Mais geralmente, dado um subconjunto $C \subseteq V$, intuitivamente os conjuntos $\gamma + C$ só poderão ser disjuntos dois a dois se C for "suficientemente pequeno". Com a noção de volume, nós podemos formalizar essa intuição:

Teorema 7.7. *Seja* $C \subseteq V$ *tal que* $\mathrm{vol}(C)$ *esteja definido e seja* V *um reticulado completo. Se os conjuntos* $\gamma + C$*, para* $\gamma \in \Gamma$*, forem disjuntos dois a dois, então* $\mathrm{vol}(C) \leq \mathrm{vol}(\Gamma)$*.*

Demonstração. Seja Φ uma malha fundamental de Γ. Então, pelo Teorema 7.4, temos $V = \bigsqcup_{\gamma\in\Gamma}(\gamma + \Phi)$. Assim, $C = \bigsqcup_{\gamma\in\Gamma}(C \cap (\gamma + \Phi))$. Agora, é fácil ver que para todo $\gamma \in \Gamma$ nós temos:

$$C \cap (\gamma + \Phi) = ((-\gamma + C) \cap \Phi) + \gamma.$$

Pela hipótese do enunciado, temos os conjuntos $-\gamma + C$ disjuntos dois a dois para γ variando em Γ, de modo que temos a união disjunta $\bigsqcup_{\gamma\in\Gamma}(-\gamma + C) \cap \Phi$. Finalmente:

$$\begin{aligned} \mathrm{vol}(C) &= \sum_{\gamma\in\Gamma} \mathrm{vol}(C \cap (\gamma + \Phi)) = \sum_{\gamma\in\Gamma} \mathrm{vol}((-\gamma + C) \cap \Phi) \\ &= \mathrm{vol}\left(\bigsqcup_{\gamma\in\Gamma} (-\gamma + C) \cap \Phi\right) \leq \mathrm{vol}(\Phi) = \mathrm{vol}(\Gamma), \end{aligned}$$

como queríamos. □

Antes de enunciarmos o Teorema de Minkowski, precisamos de mais uma definição:

Definição (Conjunto Simétrico)**.** Um subconjunto $C \subseteq V$ é chamado de **simétrico (em relação à origem)** se $c \in C \Rightarrow -c \in C$.

Teorema 7.8 (Teorema de Minkowski)**.** *Seja* $C \subseteq V$ *simétrico e convexo tal que* $\mathrm{vol}(C)$ *esteja bem-definido, e seja* $\Gamma \subseteq V$ *um reticulado completo. Suponhamos ainda que* $\mathrm{vol}(C) > 2^n \mathrm{vol}(\Gamma)$*. Então* $C \cap (\Gamma \setminus \{0\}) \neq \emptyset$*.*

Demonstração. Aplicando o Teorema de Mudança de Variáveis, é fácil ver que temos a igualdade $\mathrm{vol}(C/2) = \mathrm{vol}(C)/2^n > \mathrm{vol}(\Gamma)$. Dessa forma, aplicando o teorema acima concluímos que existem $\gamma_1, \gamma_2 \in \Gamma$ distintos tais que $(\gamma_1 + C/2) \cap (\gamma_2 + C/2) \neq \emptyset$. Assim, existem $c_1, c_2 \in C$ tais que $\gamma_1 + c_1/2 = \gamma_2 + c_2/2$. Mas então:

$$\gamma_1 - \gamma_2 = \frac{c_2}{2} - \frac{c_1}{2} = \frac{c_2}{2} + \frac{-c_1}{2} \in C,$$

uma vez que $c_1 \in C \Rightarrow -c_1 \in C$ (pois C é simétrico) e que $c_2, -c_1 \in C \Rightarrow c_2/2 + (-c_1)/2 \in C$ (pois C é convexo). Assim, $\gamma_1 - \gamma_2 \in C \cap (\Gamma \setminus \{0\})$, provando o teorema. □

Observação 7.9. *A cota dada pelo Teorema de Minkowski é a melhor possível. De fato, seja* Γ *um reticulado completo com base* $\{v_1, \ldots, v_n\}$*, e seja* Φ *a malha fundamental associada a essa base. Consideremos o conjunto*

$$C \coloneqq \left\{ \sum_{i=1}^{n} \rho_i v_i \colon -1 < \rho_i < 1 \right\}.$$

Então é claro que $C \cap \Gamma = \{0\}$*. Também é fácil ver que* C *é simétrico, convexo e que nós temos* $\operatorname{vol}(C) = 2^n \operatorname{vol}(\Phi)$ *(a região* C *é a união de* 2^n *regiões congruentes a* Φ*, uma em cada semiespaço).*

7.2. Algumas Aplicações do Teorema de Minkowski

Nesta seção, mostraremos como algumas aplicações espertas do Teorema de Minkowski nos permitem resolver facilmente alguns problemas clássicos de Teoria dos Números. Lembremos que, no Capítulo 2, mostramos que todo primo em $\mathbb{N}$ congruente a 1 módulo 4 se escrevia como soma de dois quadrados. Também podemos chegar nesse resultado utilizando o Teorema de Minkowski:

Seja $p \in \mathbb{N}$ primo com $p \equiv 1 \pmod 4$. Então sabemos que -1 é resíduo quadrático módulo p, e portanto existe $r \in \mathbb{Z}$ tal que $p \mid r^2 + 1$. Consideremos $V = \mathbb{R}^2$ e $\Gamma = \mathbb{Z} \cdot (1, r) + \mathbb{Z} \cdot (0, p)$. Assim, Γ é um reticulado completo com base $\{(1, r), (0, p)\}$, e volume $\det \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix} = p$. Notemos agora que $B_{\sqrt{3p/2}} \subseteq \mathbb{R}^2$ é simétrico, convexo e tem volume $3p\pi/2 > 4p = 2^2 \operatorname{vol}(\Gamma)$. Portanto, podemos aplicar o Teorema de Minkowski para concluir que existe $(x, y) \in \Gamma \setminus \{0\}$ tal que $x^2 + y^2 \leq 3p/2$. Como $(x, y) \in \Gamma$, temos $y \equiv rx \pmod p$. Assim:

$$x^2 + y^2 \equiv x^2 + r^2 x^2 = x^2(1 + r^2) \equiv 0 \pmod p.$$

Como $0 < x^2 + y^2 \leq 3p/2$ e $x^2 + y^2 \equiv 0 \pmod p$, a única opção é termos $x^2 + y^2 = p$.

Outra aplicação interessante do Teorema de Minkowski é o conhecido Teorema dos Quatro Quadrados:

Teorema 7.10 (Teorema dos Quatro Quadrados)**.** *Todo número natural* n *pode ser escrito como a soma de quatro quadrados perfeitos. Isto é, existem* $a, b, c, d \in \mathbb{Z}$ *tais que* $n = a^2 + b^2 + c^2 + d^2$*.*

Demonstração. É claro que 0 e 1 podem ser escritos como somas de quatro quadrados. Comecemos notando que se $m, n \in \mathbb{N}$ puderem ser escritos como somas de quatro quadrados, então seu produto também será. De fato, se $m = a^2 + b^2 + c^2 + d^2$ e $n = x^2 + y^2 + z^2 + w^2$, então:

$$\begin{aligned} mn &= (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) \\ &= (ax - by - cz - dw)^2 + (ay + bx + cw - dz)^2 \\ &\quad + (az - bw + cx + dy)^2 + (aw + bz - cy + dx)^2, \end{aligned}$$

como se pode verificar diretamente[1]. Devido a essa observação, basta mostrarmos que todo número primo pode ser escrito como a soma de quatro quadrados. Como $2 = 1^2 + 1^2 + 0^2 + 0^2$ é soma de quatro quadrados, basta provar a afirmação para os primos ímpares. Assim, seja $p \in \mathbb{N}$

[1]Na verdade, essa identidade não é nada arbitrária: ela surge naturalmente do fato de que a norma dos quatérnios é multiplicativa.

um primo ímpar qualquer. Dados $0 \leq k < \ell \leq (p-1)/2$, é claro que $p \nmid (k-\ell)(k+\ell) = k^2 - \ell^2$. Assim, os conjuntos

$$\begin{aligned} A &:= \{r^2 + p\mathbb{Z} \colon 0 \leq r \leq (p-1)/2\} \text{ e} \\ B &:= \{(-s^2 - 1) + p\mathbb{Z} \colon 0 \leq s \leq (p-1)/2\} \end{aligned}$$

possuem ambos $(p+1)/2$ elementos. Como $\mathbb{F}_p$ possui p elementos, devemos ter $A \cap B \neq \emptyset$, de modo que existem $0 \leq u, v \leq (p-1)/2$ inteiros tais que $u^2 \equiv -v^2 - 1 \pmod{p}$, ou seja, $u^2 + v^2 + 1 \equiv 0 \pmod{p}$. Consideremos $V = \mathbb{R}^4$ e Γ o reticulado completo com base formada pelos vetores $(1, 0, u, v)$, $(0, 1, v, -u)$, $(0, 0, p, 0)$ e $(0, 0, 0, p)$. Note que o volume de Γ é igual a

$$\det \begin{pmatrix} 1 & 0 & u & v \\ 0 & 1 & v & -u \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix} = p^2.$$

Lembremos que, dado $r > 0$, temos $\operatorname{vol}(B_r) = \pi^2 r^4/2$. Procuramos achar r de modo que possamos aplicar o Teorema de Minkowski, isto é, tal que $\pi^2 r^4/2 > 2^4 \operatorname{vol}(\Gamma) = 16p^2$. Note que essa desigualdade equivale a $r^2 > \frac{4\sqrt{2}}{\pi} p \cong 1,8006p$. Assim, podemos escolher $r = \sqrt{19p/10}$. Aplicando o Teorema de Minkowski, encontramos um ponto $(a, b, c, d) \in \Gamma \setminus \{0\}$ tal que

$$0 < a^2 + b^2 + c^2 + d^2 \leq r^2 = 19p/10 < 2p.$$

Notemos agora que, como $(a, b, c, d) \in \Gamma$, temos $c \equiv au + bv \pmod{p}$ e $d \equiv av - bu \pmod{p}$, de forma que

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (au + bv)^2 + (av - bu)^2 \\ &= a^2 + b^2 + a^2u^2 + b^2v^2 + a^2v^2 + b^2u^2 \\ &= (a^2 + b^2)(u^2 + v^2 + 1) \equiv 0 \pmod{p}. \end{aligned}$$

Sendo assim, devemos ter $a^2 + b^2 + c^2 + d^2 = p$, concluindo a demonstração. □

7.3. Inteiros Algébricos e Reticulados

Nessa seção, veremos como enxergar um anel de inteiros algébricos como um reticulado dentro de um espaço vetorial chamado **espaço de Minkowski**. Com essa identificação, poderemos aplicar os resultados que obtivemos na Seção 7.1 para conseguir informações sobre o anel em questão. Seja K um corpo de números algébricos com $[K : \mathbb{Q}] = n$. Então sabemos que existem n imersões de K em $\mathbb{C}$. Podemos dividir estas entre aquelas cuja imagem está contida em $\mathbb{R}$ e aquelas cuja imagem não está contida em $\mathbb{R}$:

Definição (Imersões Reais/Complexas)**.** Seja $\tau \colon K \to \mathbb{C}$ uma imersão de K. Então dizemos que τ é uma **imersão real** de K se $\tau(K) \subseteq \mathbb{R}$ e que τ é uma **imersão complexa** de K se $\tau(K) \not\subseteq \mathbb{R}$.

A primeira coisa a se observar é que as imersões complexas de K estão pareadas. Chamemos de $F \colon \mathbb{C} \to \mathbb{C}$ o automorfismo dado por conjugação complexa. Note que $F^2 = \mathrm{id}$, e que o corpo fixo por F é $\mathbb{R}$ (de fato, F é o único automorfismo não-trivial de $\mathrm{Gal}(\mathbb{C} \,/\, \mathbb{R})$). Dada uma imersão $\tau \colon K \to \mathbb{C}$ tal que $\tau(K) \not\subseteq \mathbb{R}$, vemos que $\overline{\tau} := F\tau \colon K \to \mathbb{C}$ é uma imersão diferente de τ e tal que $\overline{\tau}(K) \not\subseteq \mathbb{R}$. Além disso, $\overline{\overline{\tau}} = \tau$. Isso mostra que podemos particionar o conjunto das imersões complexas de K em pares. Disso concluímos:

Proposição 7.11. *Seja K um corpo de números algébricos. Então o conjunto das imersões complexas de K se particiona em pares da forma $\{\tau, \overline{\tau}\}$, onde $\overline{\tau}$ é a composição de τ com a conjugação complexa. Em particular, existe um número par de imersões complexas de K.*

Assim, a cada corpo de números algébricos podemos associar a sua **assinatura**:

Definição (Assinatura)**.** Seja K um corpo de números algébricos. Seja r_1 o número de imersões reais e r_2 metade do número de imersões complexas de K. Então a **assinatura** de K é o par (r_1, r_2).

Observação 7.12. *Note que, devido à proposição acima, r_1 e r_2 são números inteiros, e que temos $n = r_1 + 2r_2$.*

A assinatura de K pode ser obtida analisando a fatoração em $\mathbb{R}[x]$ do polinômio minimal de um elemento primitivo $\alpha \in K$ da extensão $K/\mathbb{Q}$. De fato, suponhamos que

$$P_{\alpha,\mathbb{Q}}(x) = (x - \alpha_1) \cdots (x - \alpha_{r_1}) Q_1(x) \cdots Q_{r_2}(x)$$

seja essa fatoração, com $\alpha_1, \ldots, \alpha_{r_1} \in \mathbb{R}$ e $Q_1, \ldots, Q_{r_2} \in \mathbb{R}[x]$ polinômios irredutíveis de grau 2. Sejam, para $1 \leq i \leq r_2$, β_i e $\overline{\beta}_i \in \mathbb{C} \setminus \mathbb{R}$ as raízes de $Q_i(x)$. Como $\alpha \in K$ é elemento primitivo, todas as imersões de K são determinadas pela sua imagem, que deve ser uma raiz de seu polinômio minimal. Então as n imersões de K em $\mathbb{C}$ são $\sigma_1, \ldots, \sigma_{r_1}, \tau_1, \overline{\tau}_1, \ldots, \tau_{r_2}, \overline{\tau}_{r_2}$, onde para $1 \leq i \leq r_1$ temos $\sigma_i \colon K \to \mathbb{Q}(\alpha_i)$ dado por $\alpha \mapsto \alpha_i$ e para $1 \leq i \leq r_2$ temos $\tau_i \colon K \to \mathbb{Q}(\beta_i)$ dado por $\alpha \mapsto \beta_i$ e $\overline{\tau}_i \colon K \to \mathbb{Q}(\overline{\beta}_i)$ dado por $\alpha \mapsto \overline{\beta}_i$. Dessa forma, vemos que a assinatura de K é (r_1, r_2).

Definição (Espaço de Minkowski)**.** Seja K um corpo de números algébricos com assinatura (r_1, r_2). Então o **espaço de Minkowski** de K é o $\mathbb{R}$-espaço vetorial $K_{\mathbb{R}} \coloneqq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Nós representamos um ponto genérico de $K_{\mathbb{R}}$ por $(a_1, \ldots, a_{r_1}; z_1, \ldots, z_{r_2})$.

Observação 7.13. *A notação $K_{\mathbb{R}}$ não é arbitrária. De fato, pode-se mostrar que existe um isomorfismo natural $K_{\mathbb{R}} \cong K \otimes_{\mathbb{Q}} \mathbb{R}$.*

Note que o espaço de Minkowski de um corpo de números algébricos depende apenas de sua assinatura. Além disso, observe que $\dim_{\mathbb{Q}} K = n \Rightarrow \dim_{\mathbb{R}} K_{\mathbb{R}} = r_1 + 2r_2 = n$. Assim, podemos munir $K_{\mathbb{R}}$ com o produto interno usual de $\mathbb{R}^n$ (para isso identificamos cada número complexo z com o par ordenado $(\mathrm{Re}(z), \mathrm{Im}(z))$). Com isso, $K_{\mathbb{R}}$ se torna um espaço vetorial euclidiano, e podemos considerar uma norma e uma medida de Lebesgue nesse espaço.

Daqui até o fim deste capítulo, denotaremos as imersões reais de K por $\sigma_1, \ldots, \sigma_{r_1}$ e as imersões complexas de K por $\tau_1, \overline{\tau}_1, \ldots, \tau_{r_2}, \overline{\tau}_{r_2}$. Também denotaremos $\sigma_{r_1+2j-1} \coloneqq \tau_j$ e $\sigma_{r_1+2j} \coloneqq \overline{\tau}_j$ para $1 \leq j \leq r_2$, de modo que as n imersões de K sejam $\sigma_1, \ldots, \sigma_n$.

O mapa $\chi \colon K \to K_{\mathbb{R}}$ dado por $\chi(a) = (\sigma_1(a), \ldots, \sigma_{r_1}(a); \tau_1(a), \ldots, \tau_{r_2}(a))$ é um homomorfismo injetor de $\mathbb{Q}$-espaços. Em particular, um homomorfismo de $\mathbb{Z}$-módulos. Chamamos χ de **imersão canônica** de K. O fato que será fundamental para nós é que χ leva bases da extensão $K/\mathbb{Q}$ em bases de reticulados completos de $K_{\mathbb{R}}$, cujo volume sabemos calcular:

Teorema 7.14. *Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base da extensão $K/\mathbb{Q}$. Então o conjunto*

$$\Gamma_\alpha \coloneqq \chi(\mathbb{Z}\,\alpha_1 + \cdots + \mathbb{Z}\,\alpha_n)$$

é um reticulado completo de $K_{\mathbb{R}}$, com base $\{\chi\alpha_1, \ldots, \chi\alpha_n\}$ e volume

$$\mathrm{vol}(\Gamma_\alpha) = 2^{-r_2} \sqrt{|\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)|}.$$

Demonstração. Sendo χ um homomorfismo de $\mathbb{Z}$-módulos, temos

$$\Gamma_\alpha = \chi(\mathbb{Z}\,\alpha_1 + \cdots + \mathbb{Z}\,\alpha_n) = \mathbb{Z}\,\chi(\alpha_1) + \cdots + \mathbb{Z}\,\chi(\alpha_n).$$

Assim, pela Proposição 7.5 vemos que $\chi(\alpha_1), \ldots, \chi(\alpha_n)$ formarão a base de um reticulado completo se e só se $\det(\chi(\alpha_1), \ldots, \chi(\alpha_n)) \neq 0$, e que nesse caso o volume desse reticulado será igual ao módulo desse determinante. Desse modo, a demonstração estará completa se mostrarmos que

o determinante em questão é em módulo igual a $2^{-r_2}\sqrt{|\Delta_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)|}$, pois como $\alpha_1,\ldots,\alpha_n$ formam uma base da extensão $K/\mathbb{Q}$ temos $\Delta_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)\neq 0$.

Queremos calcular o determinante da seguinte matriz:

$$M := \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \mathrm{Re}(\tau_1(\alpha_1)) & \mathrm{Im}(\tau_1(\alpha_1)) & \cdots & \mathrm{Re}(\tau_{r_2}(\alpha_1)) & \mathrm{Im}(\tau_{r_2}(\alpha_1)) \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \mathrm{Re}(\tau_1(\alpha_2)) & \mathrm{Im}(\tau_1(\alpha_2)) & \cdots & \mathrm{Re}(\tau_{r_2}(\alpha_2)) & \mathrm{Im}(\tau_{r_2}(\alpha_2)) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \mathrm{Re}(\tau_1(\alpha_n)) & \mathrm{Im}(\tau_1(\alpha_n)) & \cdots & \mathrm{Re}(\tau_{r_2}(\alpha_n)) & \mathrm{Im}(\tau_{r_2}(\alpha_n)) \end{pmatrix}.$$

Denotemos as colunas de M, da esquerda para a direita, por $M_1,\ldots,M_n$. Para $1\leq k\leq r_2$, realizaremos uma sequência de operações elementares nas colunas M_{r_1+2k-1} e M_{r_1+2k}, como indicado abaixo:

1. $M_{r_1+2k}\mapsto i\cdot M_{r_1+2k}$;
2. $M_{r_1+2k-1}\mapsto M_{r_1+2k-1}+M_{r_1+2k}$;
3. $M_{r_1+2k}\mapsto 2\cdot M_{r_1+2k}$;
4. $M_{r_1+2k}\mapsto M_{r_1+2k}-M_{r_1+2k-1}$;
5. $M_{r_1+2k}\mapsto (-1)\cdot M_{r_1+2k}$.

Observe que os passos 2 e 4 não alteram o determinante da matriz, enquanto os passos $1,3$ e 5 multiplicam esse determinante por i, 2 e -1 respectivamente. Assim, após esses cinco passos o determinante da matriz é multiplicado por $-2i$. Como realizamos essa sequência de operações elementares r_2 vezes, o determinante da matriz N obtida ao final de todo o procedimento é $\det N=(-2i)^{r_2}\det M\Rightarrow|\det N|=2^{r_2}|\det M|$. Finalmente, é fácil ver que

$$N = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau}_1(\alpha_1) & \cdots & \tau_{r_2}(\alpha_1) & \overline{\tau}_{r_2}(\alpha_1) \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \tau_1(\alpha_2) & \overline{\tau}_1(\alpha_2) & \cdots & \tau_{r_2}(\alpha_2) & \overline{\tau}_{r_2}(\alpha_2) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau}_1(\alpha_n) & \cdots & \tau_{r_2}(\alpha_n) & \overline{\tau}_{r_2}(\alpha_n) \end{pmatrix}.$$

Pela Proposição 1.32, temos então que $(\det N)^2=\Delta_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)$, e portanto

$$|\det N|=\sqrt{|\Delta_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)|}\Rightarrow|\det M|=2^{-r_2}\det N=2^{-r_2}\sqrt{|\Delta_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)|},$$

como queríamos demonstrar. □

Corolário 7.15. *Seja $M\subseteq K$ um $\mathbb{Z}$-submódulo livre de posto n. Então χM é um reticulado completo de $K_{\mathbb{R}}$. Além disso, se $M\subseteq\mathcal{O}_K$ então $\mathrm{vol}(\chi M)=2^{-r_2}k_M\sqrt{|d_K|}$. Em particular, $\chi\mathcal{O}_K$ é um reticulado completo de $K_{\mathbb{R}}$ com volume $2^{-r_2}\sqrt{|d_K|}$, e dado $\mathfrak{a}\lhd\mathcal{O}_K$ não-nulo, $\chi\mathfrak{a}$ é um reticulado completo de $K_{\mathbb{R}}$ com volume $\mathrm{vol}(\chi\mathfrak{a})=2^{-r_2}\,\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|}$.*

Demonstração. Seja $\{\alpha_1,\ldots,\alpha_n\}$ uma base de M. Então, pelo teorema acima, χM é um reticulado completo de $K_{\mathbb{R}}$ com base $\{\chi\alpha_1,\ldots,\chi\alpha_n\}$ e volume

$$\mathrm{vol}(\chi M)=2^{-r_2}\sqrt{|\Delta_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)|}=2^{-r_2}\sqrt{|k_M^2d_K|}=2^{-r_2}k_M\sqrt{|d_K|}.$$

□

O corolário acima, juntamente com o Teorema de Minkowski, nos fornece um critério poderoso para encontrarmos elementos "pequenos" de ideais de $\mathcal{O}_K$:

Teorema 7.16. *Seja $\mathfrak{a} \lhd \mathcal{O}_K$ não-nulo, e sejam $a_1, \dots, a_{r_1}, b_1, \dots, b_{r_2} > 0$ tais que*

$$a_1 \cdots a_{r_1} b_1^2 \cdots b_{r_2}^2 > \left(\frac{2}{\pi}\right)^{r_2} \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|}.$$

Então existe $\alpha \in \mathfrak{a} \setminus \{0\}$ tal que $|\sigma_i \alpha| < a_i$ para todo $1 \leq i \leq r_1$ e $|\tau_i \alpha| = |\overline{\tau}_i \alpha| < b_i$, para todo $1 \leq i \leq r_2$.

Demonstração. Consideremos o conjunto

$$C \coloneqq \{(x_1, \dots, x_{r_1}; y_1, \dots, y_{r_2}) \in K_{\mathbb{R}} \colon |x_1| < a_1, \dots, |x_{r_1}| < a_{r_1}, |y_1| < b_1, \dots, |y_{r_2}| < b_{r_2}\}.$$

Essa região é claramente simétrica e convexa. Notemos que C é o produto dos r_1 segmentos $\{x_i \in \mathbb{R} \colon -a_i < x_i < a_i\}$ e dos r_2 discos $D_{b_i} \coloneqq \{y_i \in \mathbb{C} \colon |y_i| < b_i\}$. Desse modo, pelo Teorema de Fubini, o volume de C é dado por

$$\begin{aligned}
\operatorname{vol}(C) &= \int_{-a_1}^{a_1} \cdots \int_{-a_{r_1}}^{a_{r_1}} \int_{D_{b_1}} \cdots \int_{D_{b_{r_2}}} dx_1 \cdots dx_{r_1}\, dy_1 \cdots dy_{r_2} \\
&= \left(\int_{-a_1}^{a_1} dx_1\right) \cdots \left(\int_{-a_{r_1}}^{a_{r_1}} dx_{r_1}\right) \left(\int_{D_{b_1}} dy_1\right) \cdots \left(\int_{D_{b_{r_2}}} dy_{r_2}\right) \\
&= (2a_1) \cdots (2a_{r_1})(\pi b_1^2) \cdots (\pi b_{r_2}^2) \\
&= 2^{r_1} \pi^{r_2} a_1 \cdots a_{r_1} b_1^2 \cdots b_{r_2}^2 \\
&> 2^n \cdot \left(2^{-r_2}\, \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|}\right) = 2^n \operatorname{vol}(\chi \mathfrak{a}).
\end{aligned}$$

Desse modo, pelo Teorema de Minkowski, existe $v \in C \cap \chi\mathfrak{a}$ não-nulo. Seja $\alpha \in \mathfrak{a}$ tal que $v = \chi\alpha$. Então $\alpha \neq 0$ e, como $\chi\alpha = (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha); \tau_1(\alpha), \dots, \tau_{r_2}(\alpha)) \in C$, obtemos as desigualdades desejadas. □

Utilizando o teorema acima, conseguimos melhorar a cota do Lema 4.8. Lembremos que para cada ideal não-nulo $\mathfrak{a} \lhd \mathcal{O}_K$ nós definimos $t(\mathfrak{a}) \coloneqq \min\{\mathfrak{N}(\mathfrak{a})^{-1}\, \mathfrak{N}(\alpha \mathcal{O}_K) \colon \alpha \in \mathfrak{a} \setminus \{0\}\}$. Então queremos achar uma constante $M > 0$ tal que, para todo $\mathfrak{a} \lhd \mathcal{O}_K$ não-nulo, tenhamos $t(\mathfrak{a}) \leq M$. Notemos que $t(\mathfrak{a}) \leq M$ se e só se existir $\alpha \in \mathfrak{a}$ não-nulo tal que

$$\mathfrak{N}(\mathfrak{a})^{-1}\, \mathfrak{N}(\alpha \mathcal{O}_K) \leq M \iff |N(\alpha)| \leq M\, \mathfrak{N}(\mathfrak{a}).$$

Desejamos encontrar o menor M possível, para que o cálculo do número de classes h_K seja eficiente. Lembremos que $N(\alpha) = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \sigma(\alpha)$, de forma que o lema acima se mostra particularmente útil. Dado $t > 0$ tal que $t^n > \left(\frac{2}{\pi}\right)^{r_2} \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|}$, aplicando o teorema acima para $a_1 = \cdots = a_{r_1} = b_1 = \cdots = b_{r_2} = t$ nós encontramos $\alpha_t \in \mathfrak{a} \setminus \{0\}$ tal que $|\sigma(\alpha_t)| < t$ para toda imersão σ de K. Assim, $\alpha_t \in \mathfrak{a} \setminus \{0\}$ é tal que $|N(\alpha_t)| < t^n$. Como $t^n > \left(\frac{2}{\pi}\right)^{r_2} \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|}$ é qualquer, concluímos que para todo $\varepsilon > 0$ existe $\alpha_\varepsilon \in \mathfrak{a} \setminus \{0\}$ tal que

$$\begin{aligned}
|N(\alpha_\varepsilon)| < \left(\frac{2}{\pi}\right)^{r_2} \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|} + \varepsilon &= \left(\left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|} + \frac{\varepsilon}{\mathfrak{N}(\mathfrak{a})}\right) \mathfrak{N}(\mathfrak{a}) \\
&\Rightarrow \quad t(a) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|} + \frac{\varepsilon}{\mathfrak{N}(\mathfrak{a})}.
\end{aligned}$$

Como isso vale para todo $\varepsilon > 0$, concluímos que $t(a) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}$. Essa já é uma melhora significativa na constante do Lema 4.8. Podemos melhorá-la ainda mais, com uma utilização esperta do Teorema de Minkowski juntamente com a desigualdade das médias:

Teorema 7.17 (Cota de Minkowski)**.** *Para todo $\mathfrak{a} \lhd \mathcal{O}_K$ não-nulo, temos $t(\mathfrak{a}) \leq \mu_K$, onde*

$$\mu_K := \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|d_K|}.$$

Equivalentemente, para todo $\mathfrak{a} \lhd \mathcal{O}_K$ não-nulo, existe $\alpha \in \mathfrak{a}$ não-nulo tal que $|N(\alpha)| \leq \mu_K\, \mathfrak{N}(\mathfrak{a})$.

Note que, como $\frac{2^{n/2}n!}{n^n} \leq 1$ para todo $n \geq 2$, essa cota é de fato melhor do que a encontrada acima. A ideia para obtê-la é a seguinte: dado $\alpha \in K$, nós temos:

$$\begin{aligned} |N(\alpha)| &= \prod_{i=1}^{r_1}|\sigma_i(\alpha)| \prod_{j=1}^{r_2}|\tau_j(\alpha)||\overline{\tau}_j(\alpha)| = \prod_{i=1}^{r_1}|\sigma_i(\alpha)| \prod_{j=1}^{r_2}|\tau_j(\alpha)|^2 \\ &\leq \left(\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(\alpha)| + \frac{2}{n}\sum_{j=1}^{r_2}|\tau_j(\alpha)|\right)^n = \frac{\left(\sum_{i=1}^{r_1}|\sigma_i(\alpha)| + 2\sum_{j=1}^{r_2}|\tau_j(\alpha)|\right)^n}{n^n}, \end{aligned}$$

onde utilizamos a desigualdade entre as médias aritmética e geométrica. Assim, é interessante minimizarmos a expressão $\sum_{i=1}^{r_1}|\sigma_i(\alpha)| + 2\sum_{j=1}^{r_2}|\tau_j(\alpha)|$ para algum elemento não-nulo do ideal $\mathfrak{a}$. Então, devido ao Teorema de Minkowski, faz sentido considerarmos para cada $t > 0$ o conjunto:

$$C_t := \{(x_1, \ldots, x_{r_1}; y_1, \ldots, y_{r_2}) \in K_{\mathbb{R}} \colon |x_1| + \cdots + |x_{r_1}| + 2|y_1| + \cdots + 2|y_{r_2}| < t\}. \tag{7.1}$$

Essa região é claramente simétrica, e uma verificação direta nos mostra que ela também é convexa. Logo podemos aplicar o Teorema de Minkowski a C_t e ao reticulado $\chi\mathfrak{a}$. Para isso, precisamos calcular $\mathrm{vol}(C_t)$. Esse é o conteúdo do lema abaixo:

Lema 7.18. *Sejam $i, j \in \mathbb{N}$ e $t > 0$. Definimos*

$$C_t^{i,j} := \{(x_1, \ldots, x_i; y_1, \ldots, y_j) \in \mathbb{R}^i \times \mathbb{C}^j \colon |x_1| + \cdots + |x_i| + 2|y_1| + \cdots + 2|y_j| < t\}.$$

Então $\mathrm{vol}(C_t^{i,j}) = \frac{2^{i-j}\pi^j t^{i+2j}}{(i+2j)!}$.

Demonstração. A demonstração será por indução dupla em i e j. Note que temos

$$C_t^{1,0} = \{x \in \mathbb{R} \colon |x| < t\} = (-t, t),$$

e portanto $\mathrm{vol}(C_t^{1,0}) = 2t$. Observemos ainda que, para todo $i \in \mathbb{N}$, nós temos:

$$\begin{aligned} C_t^{i+1,0} &= \{(x_1, \ldots, x_{i+1}) \in \mathbb{R}^{i+1} \colon |x_1| + \cdots + |x_{i+1}| < t)\} \\ &= \{((x_1, \ldots, x_i), x_{i+1}) \in \mathbb{R}^i \times \mathbb{R} \colon x_{i+1} \in (-t, t),\ (x_1, \ldots, x_i) \in C_{t-|x_{i+1}|}^{i,0}\}. \end{aligned}$$

Desse modo, pelo Teorema de Fubini:

$$\begin{aligned} \mathrm{vol}(C_t^{i+1,0}) = \int_{C_t^{i+1,0}} d\mu = \int_{-t}^{t}\int_{C_{t-|x_{i+1}|}^{i,0}} d\mu\, dx_{i+1} &= \int_{-t}^{t} \mathrm{vol}(C_{t-|x_{i+1}|}^{i,0})\, dx_{i+1} \\ &= 2\int_0^t \mathrm{vol}(C_{t-x_{i+1}}^{i,0})\, dx_{i+1}, \end{aligned}$$

uma vez que $\mathrm{vol}(C_{t-|x_{i+1}|}^{i,0})$ é claramente uma função par de x_{i+1}. Com isso, mostraremos por indução em i que $\mathrm{vol}(C_t^{i,0}) = \frac{2^i t^i}{i!}$. Como $2^1 t^1/1! = 2t$, temos a base de indução. Finalmente, supondo a fórmula válida para i, nós temos:

$$\begin{aligned} \mathrm{vol}(C_t^{i+1,0}) &= 2\int_0^t \mathrm{vol}(C_{t-x_{i+1}}^{i,0})\, dx_{i+1} = 2\int_0^t \frac{2^i(t-x_{i+1})^i}{i!}\, dx_{i+1} \\ &= \frac{2^{i+1}}{i!}\int_0^t (t-x_{i+1})^i\, dx_{i+1} = \frac{2^{i+1}}{i!}\int_t^0 y^i\,(-dy) \\ &= \frac{2^{i+1}}{i!}\int_0^t y^i\, dy = \frac{2^{i+1}}{i!}\left[\frac{y^{i+1}}{i+1}\right]_0^t \\ &= \frac{2^{i+1}}{i!}\cdot\frac{t^{i+1}}{i+1} = \frac{2^{i+1}t^{i+1}}{(i+1)!}, \end{aligned}$$

mostrando a validade da fórmula para $i+1$. Fixemos agora $i \in \mathbb{N}$. Observemos que, para $j \in \mathbb{N}$ qualquer, o conjunto $C_t^{i,j+1}$ é igual a

$$\{(x_1,\dots,x_i;y_1,\dots,y_{j+1}) \in (\mathbb{R}^i \times \mathbb{C}^j) \times \mathbb{C} \colon y_{j+1} \in D_{t/2},\ (x_1,\dots,x_i;y_1,\dots,y_j) \in C^{i,j}_{t-2|y_{j+1}|}\},$$

onde $D_{t/2} \coloneqq \{z \in \mathbb{C} \colon |z| < t/2\}$. Desse modo, pelo Teorema de Fubini:

$$\begin{aligned}\operatorname{vol}(C_t^{i,j+1}) = \int_{C_t^{i,j+1}} d\mu &= \int_{D_{t/2}} \int_{C^{i,j}_{t-2|y_{j+1}|}} d\mu\, dy_{j+1} = \int_{D_{t/2}} \operatorname{vol}(C^{i,j}_{t-2|y_{j+1}|})\, dy_{j+1} \\ &= \int_0^{t/2}\int_0^{2\pi} \operatorname{vol}(C^{i,j}_{t-2r}) r\, d\theta\, dr = 2\pi \int_0^{t/2} \operatorname{vol}(C^{i,j}_{t-2r}) r\, dr,\end{aligned}$$

onde utilizamos mudança de coordenadas cartesianas para polares. Com isso, podemos mostrar por indução em j que $\operatorname{vol}(C_t^{i,j}) = \frac{2^{i-j}\pi^j t^{i+2j}}{(i+2j)!}$, o que concluirá a demonstração. Para $j=0$, essa fórmula se torna $\operatorname{vol}(C_t^{i,0}) = \frac{2^i t^i}{i!}$, que já mostramos ser verdadeira. Suponhamos então que a fórmula valha para j, e a provemos para $j+1$. Nós temos:

$$\begin{aligned}\operatorname{vol}(C_t^{i,j+1}) = 2\pi \int_0^{t/2} \operatorname{vol}(C^{i,j}_{t-2r}) r\, dr &= 2\pi \int_0^{t/2} \frac{2^{i-j}\pi^j (t-2r)^{i+2j}}{(i+2j)!} r\, dr \\ &= \frac{2^{i-j+1}\pi^{j+1}}{(i+2j)!} \int_0^{t/2} (t-2r)^{i+2j} r\, dr.\end{aligned}$$

Fazendo $u = t-2r$, temos $r = (t-u)/2$ e $dr = -du/2$. Assim:

$$\begin{aligned}\int_0^t (t-2r)^{i+2j} r\, dr &= \int_t^0 u^{i+2j} \frac{t-u}{2} \left(-\frac{1}{2}\right) du \\ &= \frac{1}{4}\int_0^t (tu^{i+2j} - u^{i+2j+1})\, du \\ &= \frac{1}{4}\left[\frac{tu^{i+2j+1}}{i+2j+1} - \frac{u^{i+2j+2}}{i+2j+2}\right]_0^t \\ &= \frac{1}{4}\left(\frac{t^{i+2j+2}}{i+2j+1} - \frac{t^{i+2j+2}}{i+2j+2}\right) \\ &= \left(\frac{1}{i+2j+1} - \frac{1}{1+2j+2}\right)\frac{t^{i+2(j+1)}}{4} \\ &= \frac{t^{i+2(j+1)}}{4(i+2j+1)(1+2j+2)}.\end{aligned}$$

Finalmente, obtemos:

$$\begin{aligned}\operatorname{vol}(C_t^{i,j+1}) = \frac{2^{i-j+1}\pi^{j+1}}{(i+2j)!}\int_0^{t/2} (t-2r)^{i+2j} r\, dr &= \frac{2^{i-j+1}\pi^{j+1}}{(i+2j)!} \cdot \frac{t^{i+2(j+1)}}{4(i+2j+1)(1+2j+2)} \\ &= \frac{2^{i-(j+1)}\pi^{j+1} t^{i+2(j+1)}}{(i+2(j+1))!},\end{aligned}$$

concluindo a indução. □

Demonstração (do Teorema 7.17): Fixemos $\mathfrak{a} \lhd \mathcal{O}_K$ não-nulo. Para cada $t > 0$, definimos C_t como em (7.1). Então C_t é simétrico, convexo e pelo lema acima seu volume é $\operatorname{vol}(C_t) = \frac{2^{r_1-r_2}\pi^{r_2}t^n}{n!}$. Para podermos aplicar o Teorema de Minkowski a C_t e ao reticulado completo $\chi\mathfrak{a}$,

devemos ter:

$$\begin{aligned}\operatorname{vol}(C_t) > 2^n \operatorname{vol}(\chi\mathfrak{a}) &\iff \frac{2^{r_1-r_2}\pi^{r_2}t^n}{n!} > 2^n 2^{-r_2}\,\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|} \\ &\iff t^n > 2^{n-r_1}\pi^{-r_2}n!\,\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|} \\ &\qquad = \left(\frac{4}{\pi}\right)^{r_2} n!\,\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|}.\end{aligned}$$

Para cada $t > 0$ satisfazendo essa condição, pelo Teorema de Minkowski existe um elemento não-nulo $v \in C_t \cap \chi\mathfrak{a}$. Sendo $\alpha_t \in \mathfrak{a}$ tal que $\chi\alpha_t = v$, temos $\alpha_t \neq 0$ e

$$\sum_{i=1}^{r_1}|\sigma_i(\alpha_t)| + 2\sum_{j=1}^{r_2}|\tau_j(\alpha_t)| < t.$$

Dessa forma, pela desigualdade que havíamos visto, $|N(\alpha_t)| < t^n/n^n$. Assim, $\alpha_t \in \mathfrak{a}\setminus\{0\}$ é tal que $|N(\alpha_t)| < t^n/n^n$. Como $t^n > \left(\frac{4}{\pi}\right)^{r_2} n!\,\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|}$ é qualquer, concluímos que para todo $\varepsilon > 0$ existe $\alpha_\varepsilon \in \mathfrak{a}\setminus\{0\}$ tal que

$$\begin{aligned}|N(\alpha_\varepsilon)| < \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\,\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|} + \frac{\varepsilon}{n^n} &= \left(\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|} + \frac{\varepsilon}{n^n\,\mathfrak{N}(\mathfrak{a})}\right)\mathfrak{N}(\mathfrak{a}) \\ &\Rightarrow\quad t(a) \le \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|} + \frac{\varepsilon}{n^n\,\mathfrak{N}(\mathfrak{a})}.\end{aligned}$$

Como isso vale para todo $\varepsilon > 0$, concluímos que $t(\mathfrak{a}) \le \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|}$, como queríamos. □

Como consequência da cota de Minkowski, também conseguimos estimativas sobre o discriminante d_K:

Teorema 7.19. *Para todo corpo de números algébricos K de grau $n \ge 2$, temos:*

$$|d_K| \ge \left(\frac{\pi}{4}\right)^n \cdot \frac{n^{2n}}{(n!)^2} \ge \frac{\pi}{3}\cdot\left(\frac{3\pi}{4}\right)^{n-1}.$$

Em particular, para todo corpo de números algébricos $K \neq \mathbb{Q}$ nós temos $|d_K| > 2$.

Demonstração. Seja $\mathfrak{a} \lhd K$ não-nulo. Então pelo Teorema 7.17 existe $\alpha \in \mathfrak{a}\setminus\{0\}$ tal que

$$|N(\alpha)| \le \mu_K\,\mathfrak{N}(\mathfrak{a}) \iff \mathfrak{N}(\alpha\mathcal{O}_K)\,\mathfrak{N}(\mathfrak{a})^{-1} \le \mu_K \iff \mathfrak{N}(\alpha\mathfrak{a}^{-1}) \le \mu_K.$$

Assim, $\mathfrak{b} := \alpha\mathfrak{a}^{-1} \lhd \mathcal{O}_K$ é tal que $\mathfrak{N}(\mathfrak{b}) \le \mu_K$, isto é:

$$\begin{aligned}\mathfrak{N}(\mathfrak{b}) \le \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|} &\le \left(\frac{4}{\pi}\right)^{n/2}\frac{n!}{n^n}\sqrt{|d_K|} \\ \Rightarrow\quad |d_K| \ge \left(\frac{\pi}{4}\right)^n\frac{n^{2n}}{(n!)^2}\,\mathfrak{N}(\mathfrak{b})^2 &\ge \left(\frac{\pi}{4}\right)^n\frac{n^{2n}}{(n!)^2},\end{aligned}$$

já que $\mathfrak{N}(\mathfrak{b}) \ge 1$. Para provarmos a segunda desigualdade, notemos que

$$\left(\frac{\pi}{4}\right)^n\cdot\frac{n^{2n}}{(n!)^2} \ge \frac{\pi}{3}\cdot\left(\frac{3\pi}{4}\right)^{n-1} \iff \frac{n^{2n}}{4(n!)^2} \ge 3^{n-2} \iff n^{2n} \ge 4\cdot 3^{n-2}(n!)^2.$$

Provaremos essa desigualdade por indução em n. Para $n = 2$, ela equivale à desigualdade

$$2^{2\cdot 2} \ge 4\cdot 3^{2-2}(2!)^2 \iff 16 \ge 16,$$

que é verdadeira. Supondo agora essa desigualdade válida para $n \geq 2$, temos:

$$4 \cdot 3^{n-1}((n+1)!)^2 = (4 \cdot 3^{n-2}(n!)^2) \cdot 3 \cdot (n+1)^2 \leq n^{2n} \cdot 3 \cdot (n+1)^2.$$

Queremos mostrar que

$$(n+1)^{2n+2} \geq n^{2n} \cdot 3 \cdot (n+1)^2 \iff \left(\frac{n+1}{n}\right)^{2n} \geq 3 \iff \left(1+\frac{1}{n}\right)^{2n} \geq 3.$$

Mas essa última desigualdade segue diretamente da desigualdade de Bernoulli, concluindo a indução. Finalmente, para ver que $|d_K| > 2$ para todo corpo de números algébricos $K \neq \mathbb{Q}$, basta notarmos que para $n \geq 2$ nós temos

$$|d_K| \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1} \geq \frac{\pi}{3} \cdot \frac{3\pi}{4} = \frac{\pi^2}{4} > 2.$$

□

Observação 7.20. *Note que o teorema acima também mostra que o número*

$$\min\{|d_K| \colon K \text{ é corpo de números algébricos com } [K:\mathbb{Q}] = n\}$$

cresce exponencialmente em função de n. Por exemplo, todo corpo de números algébricos de grau 3 tem o módulo de seu discriminante maior ou igual a

$$\left(\frac{\pi}{4}\right)^3 \cdot \frac{3^{2\cdot 3}}{(3!)^2} \cong 9,81,$$

e portanto maior ou igual a 10.

Utilizando o Teorema 7.19 juntamente com o Teorema 4.27, nós podemos concluir que toda extensão da forma $K/\mathbb{Q}$, onde $K \neq \mathbb{Q}$ é um corpo de números algébricos, é ramificada, isto é, existe algum primo $p \in \mathbb{N}$ que se ramifica em K. De fato, o Teorema 7.19 nos diz que $|d_K| > 2$. Assim, existe um primo $p \in \mathbb{N}$ tal que $p \mid d_K$, e concluímos pelo Teorema 4.27 que esse primo se ramifica em K. Desse modo, obtemos:

Teorema 7.21. *Para todo corpo de números algébricos $K \neq \mathbb{Q}$, a extensão $K/\mathbb{Q}$ é ramificada.*

7.4. O Teorema das Unidades de Dirichlet

Nessa seção, iremos utilizar métodos geométricos para deduzir o conhecido Teorema das Unidades de Dirichlet, que afirma que o grupo de unidades de um anel de inteiros algébricos $\mathcal{O}_K$ é o produto direto do grupo de torção de $\mathcal{O}_K$ por um número finito de grupos cíclicos infinitos.

Seja $K_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ como definido na seção anterior. Esse $\mathbb{R}$-espaço possui uma base canônica $e_1, \ldots, e_n$, sendo:

$$\begin{aligned} e_1 &= (1,0,\ldots,0;0,\ldots,0), \ldots, e_{r_1} = (0,\ldots,0,1;0,\ldots,0), \\ e_{r_1+1} &= (0,\ldots,0;1,0,\ldots,0), e_{r_1+2} = (0,\ldots,0;i,0,\ldots,0), \ldots \\ e_{n-1} &= (0,\ldots,0;0,\ldots,0,1), e_n = (0,\ldots,0;0,\ldots,0,i). \end{aligned}$$

Também denotaremos $f_j := e_{r_1+2j-1}$ e $g_j := e_{r_1+2j}$, para $1 \leq j \leq r_2$. Note que os f_j são os elementos em que aparece uma coordenada complexa 1, e que os g_j são os elementos em que aparece uma coordenada complexa i. Podemos definir uma norma $N \colon K_{\mathbb{R}} \to \mathbb{R}$ dada por

$$N(a_1,\ldots,a_{r_1};z_1,\ldots,z_{r_2}) = a_1 \cdots a_{r_1}|z_1|^2 \cdots |z_{r_2}|^2.$$

Proposição 7.22. *N é um homomorfismo multiplicativo e satisfaz $N \circ \chi = N_{K/\mathbb{Q}}$.*

Demonstração. Como a multiplicação em $K_{\mathbb{R}}$ é dada termo a termo, é claro que N é homomorfismo multiplicativo. Agora, basta notarmos que, dado $a \in K$, nós temos:

$$\begin{aligned}(N \circ \chi)(a) &= N(\sigma_1(a), \ldots, \sigma_{r_1}(a); \tau_1(a), \ldots, \tau_{r_2}(a)) = \prod_{i=1}^{r_1} \sigma_i(a) \prod_{j=1}^{r_2} |\tau_j(a)|^2 \\ &= \prod_{i=1}^{r_1} \sigma_i(a) \prod_{j=1}^{r_2} (\tau_j(a)\overline{\tau}_j(a)) = \prod_{\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \sigma(a) = N_{K/\mathbb{Q}}(a).\end{aligned}$$

□

Essa norma será útil para comparar os volumes de dois reticulados completos cujas bases distinguem por um fator de $c \in K_{\mathbb{R}}$. Mais especificamente:

Proposição 7.23. *Seja $c \in K_{\mathbb{R}}$, e sejam $\rho_{jk}, 1 \leq j, k \leq n$ tais que $ce_j = \sum_{k=1}^{n} \rho_{jk} e_k$, para todo $1 \leq j \leq n$.*

(a) Nós temos $N(c) = \det(\rho_{jk})$.

(b) Sejam $v_1, \ldots, v_n \in K_{\mathbb{R}}$ quaisquer, e sejam $w_1, \ldots, w_n$ os vetores obtidos dos v_j's por multiplicação por c, isto é, $w_j = cv_j$ para $1 \leq j \leq n$. Então, sendo Φ_v e Φ_w os paralelepípedos gerados por $v_1, \ldots, v_n$ e $w_1, \ldots, w_n$, respectivamente, temos:

$$\mathrm{vol}(\Phi_w) = |N(c)| \cdot \mathrm{vol}(\Phi_v).$$

Demonstração. (a) Escrevamos $c = (a_1, \ldots, a_{r_1}; b_1 + ic_1, \ldots, b_{r_2} + ic_{r_2})$, onde os a_j's, b_j's e c_j's são números reais. Então é fácil ver que para $1 \leq j \leq r_1$ nós temos $ce_j = a_j e_j$ e que para $1 \leq j \leq r_2$ nós temos $cf_j = b_j f_j + c_j g_j$ e $cg_j = -c_j f_j + b_j g_j$. Desse modo, a matriz (ρ_{jk}) é igual a

$$\begin{pmatrix} a_1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & a_{r_1} & 0 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & b_1 & c_1 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & -c_1 & b_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & b_{r_2} & c_{r_2} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & -c_{r_2} & b_{r_2} \end{pmatrix}.$$

Essa é uma matriz de blocos, com determinante

$$a_1 \cdots a_{r_1} (b_1^2 + c_1^2) \cdots (b_{r_2}^2 + c_{r_2}^2) = a_1 \cdots a_{r_1} |b_1 + ic_1|^2 \cdots |b_{r_2} + ic_{r_2}|^2 = N(c),$$

como queríamos.

(b) Escrevamos, para $1 \leq j \leq n$, $v_j = \sum_{h=1}^{n} \varepsilon_{jh} e_h$, onde cada $\varepsilon_{jh} \in \mathbb{R}$. Então nós temos, para $1 \leq j \leq n$:

$$w_j = cv_j = c \cdot \sum_{h=1}^{n} \varepsilon_{jh} e_h = \sum_{h=1}^{n} \varepsilon_{jh} ce_h = \sum_{h=1}^{n} \sum_{k=1}^{n} \varepsilon_{jh} \rho_{hk} e_k = \sum_{k=1}^{n} \left(\sum_{h=1}^{n} \varepsilon_{jh} \rho_{hk} \right) e_k.$$

Assim, pela Proposição 7.5 e pelo item (a), nós temos:

$$\mathrm{vol}(\Phi_w) = \left| \det \left(\sum_{h=1}^{n} \varepsilon_{jh} \rho_{hk} \right) \right| = |\det(\varepsilon_{jk})| \cdot |\det(\rho_{jk})| = \mathrm{vol}(\Phi_v) \cdot |N(c)|,$$

como desejávamos.

□

É claro que $K_{\mathbb{R}}^{\times} = (\mathbb{R}^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2}$ e que, dado $c \in K_{\mathbb{R}}$, $N(c) \neq 0 \iff c \in K_{\mathbb{R}}^{\times}$. Assim, como consequência direta da proposição acima, nós temos:

Corolário 7.24. *Seja $c \in K_{\mathbb{R}}$, e suponhamos que $v_1, \ldots, v_n \in K_{\mathbb{R}}$ formem a base de um reticulado completo Γ. Então $cv_1, \ldots, cv_n$ geram o $\mathbb{Z}$-módulo $c\Gamma \coloneqq \{cz \colon z \in \Gamma\}$. Além disso, $c\Gamma$ será um reticulado completo de $K_{\mathbb{R}}$ se e somente se $c \in K_{\mathbb{R}}^{\times}$, e nesse caso* $\mathrm{vol}(c\Gamma) = |N(c)| \cdot \mathrm{vol}(\Gamma)$.

Na demonstração do Teorema das Unidades de Dirichlet, utilizaremos a chamada teoria multiplicativa de Minkowski. Note que a restrição da imersão canônica a $K^{\times}$ nos dá um homomorfismo de grupos multiplicativos $\chi \colon K^{\times} \to K_{\mathbb{R}}^{\times}$. Para trabalharmos com reticulados, precisamos transformar esses grupos multiplicativos em grupos aditivos. Podemos fazer isso por meio do logaritmo! Mais especificamente, definimos homomorfismos de grupos $\mu_1, \ldots, \mu_{r_1}, \theta_1, \ldots, \theta_{r_2} \colon K_{\mathbb{R}}^{\times} \to \mathbb{R}$ do grupo multiplicativo $K_{\mathbb{R}}^{\times}$ para o grupo aditivo $\mathbb{R}$, dados por:

$$\mu_j(a_1, \ldots, a_{r_1}; z_1, \ldots, z_{r_2}) = \log|a_j|, \text{ para } 1 \leq j \leq r_1;$$
$$\theta_j(a_1, \ldots, a_{r_1}; z_1, \ldots, z_{r_2}) = \log|z_j|^2, \text{ para } 1 \leq j \leq r_2.$$

Nós ainda denotamos $\mu_{r_1+j} \coloneqq \theta_j$, para $1 \leq j \leq r_2$. É claro que os μ_j e os θ_j são todos sobrejetores. Nós definimos $\mu \colon K_{\mathbb{R}}^{\times} \to \mathbb{R}^{r_1+r_2}$ dado por

$$\mu c = (\mu_1 c, \ldots, \mu_{r_1+r_2} c) = (\mu_1 c, \ldots, \mu_{r_1} c, \theta_1 c, \ldots, \theta_{r_2} c).$$

Note que, escrevendo $c = (a_1, \ldots, a_{r_1}; z_1, \ldots, z_{r_2})$, nós temos:

$$\mu c = (\log|a_1|, \ldots, \log|a_{r_1}|, \log|z_1|^2, \ldots, \log|z_{r_2}|^2).$$

Segue da sobrejetividade dos μ_j e dos θ_j que μ também é sobrejetor. Definamos ainda o homomorfismo $\lambda \coloneqq \mu \circ \chi \colon K^{\times} \to \mathbb{R}^{r_1+r_2}$, e para $1 \leq j \leq r_1 + r_2$, os homomorfismos $\lambda_j \coloneqq \mu_j \circ \chi \colon K^{\times} \to \mathbb{R}$. O homomorfismo λ é chamado de **representação logarítmica** de $K^{\times}$, e dado $a \in K^{\times}$ é fácil ver que temos

$$\lambda a = (\lambda_1 a, \ldots, \lambda_{r_1+r_2} a) = (\log|\sigma_1(a)|, \ldots, \log|\sigma_{r_1}(a)|, \log|\tau_1(a)|^2, \ldots, \log|\tau_{r_2}(a)|^2).$$

Definamos $\mathrm{Tr} \colon \mathbb{R}^{r_1+r_2} \to \mathbb{R}$ dado pela soma das coordenadas:

$$\mathrm{Tr}(x_1, \ldots, x_{r_1+r_2}) = x_1 + \cdots + x_{r_1+r_2}.$$

É claro que essa é uma transformação $\mathbb{R}$-linear. O núcleo de Tr é o hiperplano

$$H \coloneqq \ker \mathrm{Tr} = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \colon x_1 + \cdots + x_{r_1+r_2} = 0\}.$$

Notemos que H é um $\mathbb{R}$-espaço de dimensão $r_1 + r_2 - 1$, que se torna um espaço vetorial euclidiano com a topologia induzida de $\mathbb{R}^{r_1+r_2}$.

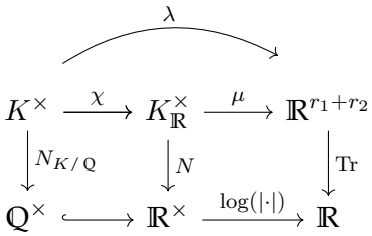
Proposição 7.25. *Nós temos* $\mathrm{Tr} \circ \mu = \log(|\cdot|) \circ N$.

Demonstração. Seja $c = (a_1, \ldots, a_{r_1}; z_1, \ldots, z_{r_2}) \in K_{\mathbb{R}}$ qualquer. Então

$$\begin{aligned}
(\mathrm{Tr} \circ \mu)(c) &= \mathrm{Tr}(\log|a_1|, \ldots, \log|a_{r_1}|, \log|z_1|^2, \ldots, \log|z_{r_2}|^2) \\
&= \log|a_1| + \cdots + \log|a_{r_1}| + \log|z_1|^2 + \cdots + \log|z_{r_2}|^2 \\
&= \log(|a_1| \cdots |a_{r_1}||z_1|^2 \cdots |z_{r_2}|^2) \\
&= \log(|a_1 \cdots a_{r_1}|z_1|^2 \cdots |z_{r_2}|^2|) \\
&= (\log(|\cdot|) \circ N)(c),
\end{aligned}$$

concluindo a demonstração. □

Devido às proposições 7.22 e 7.25, nós temos o seguinte diagrama comutativo:



Calculemos agora $\ker \mu$ e $\mu^{-1}(H)$:

Proposição 7.26. *(a) O núcleo de μ é dado por*

$$\ker \mu = \{(a_1, \dots, a_{r_1}; z_1, \dots, z_{r_2}) \in K_{\mathbb{R}}^{\times} : |a_1| = \cdots = |a_{r_1}| = |z_1| = \cdots = |z_{r_2}| = 1\}.$$

(b) $\mu^{-1}(H) = \{c \in K_{\mathbb{R}}^{\times} : N(c) = \pm 1\}$.

Demonstração. (a) Dado $c = (a_1, \dots, a_{r_1}; z_1, \dots, z_{r_2}) \in K_{\mathbb{R}}$, nós temos:

$$\begin{aligned} c \in \ker \mu &\iff 0 = \mu c = (\log|a_1|, \dots, \log|a_{r_1}|, \log|z_1|^2, \dots, \log|z_{r_2}|^2) \\ &\iff \log|a_1| = \cdots = \log|a_{r_1}| = \log|z_1| = \cdots = \log|z_{r_2}| = 0 \\ &\iff |a_1| = \cdots = |a_{r_1}| = |z_1| = \cdots = |z_{r_2}| = 1, \end{aligned}$$

provando a afirmação desejada.

(b) Dado $c \in K_{\mathbb{R}}$, nós temos:

$$\begin{aligned} c \in \mu^{-1}(H) &\iff \mu(c) \in H = \ker \operatorname{Tr} \iff \operatorname{Tr}(\mu(c)) = 0 \\ &\iff \log(|N(c)|) = 0 \iff |N(c)| = 1, \end{aligned}$$

onde utilizamos a proposição acima. Isso prova a afirmação desejada.

□

Mostraremos agora algumas propriedades sobre o subgrupo de torção de um corpo de números K. Lembremos que o subgrupo de torção de K é o subgrupo $W(K) \subseteq K^{\times}$ dos elementos de ordem finita de $K^{\times}$, que é o grupo das raízes da unidade de K. Como toda raiz da unidade de K é raiz de um polinômio da forma $x^m - 1$, vemos que $W(K) \subseteq \mathcal{O}_K$. Provaremos que $W(K)$ é finito e se caracteriza como o conjunto dos elementos de $\mathcal{O}_K$ tais que todas as suas imagens pelas imersões de K têm módulo 1. Começamos com o seguinte resultado:

Teorema 7.27. *Seja $k \geq 0$ qualquer. Então o conjunto $\{\alpha \in \mathcal{O}_K : |\sigma_1 \alpha| \leq k, \dots, |\sigma_n \alpha| \leq k\}$ é finito.*

Demonstração. Consideremos o conjunto

$$C \coloneqq \{(a_1, \dots, a_{r_1}; z_1, \dots, z_{r_2}) \in K_{\mathbb{R}} : |a_1| \leq k, \dots, |a_{r_1}| \leq k, |z_1| \leq k, \dots, |z_{r_2}| \leq k\}.$$

Então é claro que C é um subconjunto limitado de $K_{\mathbb{R}}$. Como $\chi \mathcal{O}_K$ é um reticulado de $K_{\mathbb{R}}$, esse é um subconjunto discreto de $K_{\mathbb{R}}$, e portanto $C \cap \chi \mathcal{O}_K$ é finito. Assim, existe um número finito de $\alpha \in \mathcal{O}_K$ tais que $|\sigma_1 \alpha| \leq k, \dots, |\sigma_{r_1} \alpha| \leq k, |\tau_1 \alpha| \leq k, \dots, |\tau_{r_2} \alpha| \leq k$. Finalmente, como para $1 \leq j \leq r_2$ temos $|\overline{\tau}_j \alpha| = |\tau_j \alpha|$, vemos que existe um número finito de $\alpha \in \mathcal{O}_K$ tais que $|\sigma_j \alpha| \leq k$ para todo $1 \leq j \leq n$, como queríamos. □

Lembremos que, dado m inteiro positivo, denotamos por $W_m(K)$ o conjunto das raízes m-ésimas da unidade em K. A partir do teorema acima, conseguimos o seguinte:

Teorema 7.28. *Nós temos* $W(K) = \{\alpha \in \mathcal{O}_K : |\sigma_1\alpha| = \cdots = |\sigma_n\alpha| = 1\}$. *Em particular,* $W(K)$ *é finito, e portanto temos* $W(K) = W_m(K)$ *para algum* m *inteiro positivo. Logo* $W(K)$ *é cíclico.*

Demonstração. Denotaremos o conjunto da direita por S. Mostremos que $W(K) = S$:

($\subseteq$): Dado $\alpha \in W(K)$, como já observamos acima temos $\alpha \in \mathcal{O}_K$. Sabemos que existe m inteiro positivo tal que $\alpha^m = 1$. Assim, para todo $1 \leq j \leq n$, nós temos $(\sigma_j\alpha)^m = 1$. Em particular, $|\sigma_j\alpha| = 1$. Isso prova que $\alpha \in S$.

($\supseteq$): Note que S é um conjunto finito pelo teorema acima. Seja $\alpha \in S$. Então $\alpha \in \mathcal{O}_K$ é tal que $|\sigma_1\alpha| = \cdots = |\sigma_n\alpha| = 1$. Vemos então que, para todo inteiro positivo k, nós temos $\alpha^k \in \mathcal{O}_K$ e $|\sigma_1\alpha^k| = \cdots = |\sigma_n\alpha^k| = 1$. Ou seja, $\alpha^k \in S$ para todo inteiro positivo k. Mas sendo S finito, vemos que existem $k_1 > k_2 > 0$ tais que $\alpha^{k_1} = \alpha^{k_2} \Rightarrow \alpha^{k_1-k_2} = 1$, mostrando que $\alpha \in W(K)$.

Assim, provamos que $W(K) = S$. Como observamos acima, S é finito, e portanto $W(K)$ também o é. Dessa forma, pela Proposição 2.23, vemos que existe um inteiro positivo m tal que $W(K) = W_m(K)$, que é cíclico. □

Com isso, conseguimos demonstrar:

Proposição 7.29. *(a)* $\ker\lambda = \{\alpha \in K^\times : |\sigma_1(\alpha)| = \cdots = |\sigma_n(\alpha)| = 1\}$. *Assim, nós temos* $\mathcal{O}_K \cap \ker\lambda = W(K)$.

(b) $\lambda^{-1}(H) = \{\alpha \in K^\times : N_{K/\mathbb{Q}}(\alpha) = \pm 1\}$. *Assim, nós temos* $\lambda^{-1}(H) \cap \mathcal{O}_K = \mathcal{O}_K^\times$.

Demonstração. (a) Dado $\alpha \in K^\times$ qualquer, nós temos:

$$\alpha \in \ker\lambda \iff 0 = \lambda\alpha = \mu\chi\alpha \iff \chi\alpha \in \ker\mu.$$

Pela Proposição 7.26, isso ocorre se e só se tivermos

$$\begin{aligned} & |\sigma_1(\alpha)| = \cdots = |\sigma_{r_1}(\alpha)| = |\tau_1(\alpha)| = \cdots = |\tau_{r_2}(\alpha)| = 1 \\ \iff \quad & |\sigma_1(\alpha)| = \cdots = |\sigma_n(\alpha)| = 1. \end{aligned}$$

Finalmente, se $\alpha \in \mathcal{O}_K$, então pelo Teorema 7.28 vemos que isso equivale a $\alpha \in W(K)$.

(b) Dado $\alpha \in K^\times$ qualquer, nós temos:

$$\alpha \in \lambda^{-1}(H) \iff \lambda\alpha \in H \iff \mu\chi\alpha \in H \iff \chi\alpha \in \mu^{-1}(H).$$

Pela Proposição 7.26, isso ocorre se e só se $N(\chi\alpha) = \pm 1$. Como $N \circ \chi = N_{K/\mathbb{Q}}$, isso equivale a $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Finalmente, a última afirmação segue de termos a igualdade $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K : N_{K/\mathbb{Q}}(\alpha) = \pm 1\}$, que é válida devido ao Corolário 2.3.

□

Uma consequência da proposição acima é que para qualquer subanel $A \subseteq \mathcal{O}_K$ nós temos $A^\times \subseteq \mathcal{O}_K^\times \subseteq \lambda^{-1}(H)$. Assim, $\lambda(A^\times) \subseteq H$. De fato, podemos mostrar o seguinte importante resultado:

Teorema 7.30. *Para qualquer subanel* $A \subseteq \mathcal{O}_K$, $\lambda(A^\times)$ *é um reticulado em* H.

Demonstração. Sendo λ homomorfismo de grupos, é claro que $\lambda(A^\times)$ é subgrupo aditivo de H. Basta então mostrar que $\lambda(A^\times)$ é um subconjunto discreto de H. É claro que isso equivale a mostrar que $\lambda(A^\times)$ é discreto em $\mathbb{R}^{r_1+r_2}$, o que por sua vez equivale a mostrar que a interseção de $\lambda(A^\times)$ com qualquer conjunto limitado de $\mathbb{R}^{r_1+r_2}$ é finita. Então é claro que é suficiente provar que para todo $t \geq 1$ a interseção $\lambda(A^\times) \cap C_t$ é finita, onde C_t é o paralelepípedo:

$$C_t \coloneqq \{(a_1, \dots, a_{r_1}, b_1, \dots, b_{r_2}) \in \mathbb{R}^{r_1+r_2} \colon |a_1| \leq t, \dots, |a_{r_1}| \leq t, |b_1| \leq 2t, \dots, |b_{r_2}| \leq 2t\},$$

uma vez que os conjuntos C_t para $t \geq 1$ cobrem $\mathbb{R}^{r_1+r_2}$. Notemos que, dado $\alpha \in A^\times$, nós temos:

$$\begin{aligned} \lambda(\alpha) \in C_t &\iff |\log|\sigma_1(\alpha)||, \dots, |\log|\sigma_{r_1}(\alpha)|| \leq t, |\log|\tau_1(\alpha)|^2|, \dots, |\log|\tau_{r_2}(\alpha)|^2| \leq 2t \\ &\iff e^{-t} \leq |\sigma_1(\alpha)|, \dots, |\sigma_{r_1}(\alpha)|, |\tau_1(\alpha)|, \dots, |\tau_{r_2}(\alpha)| \leq e^t \\ &\implies |\sigma_1(\alpha)|, \dots, |\sigma_n(\alpha)| \leq e^t. \end{aligned}$$

Aplicando o Teorema 7.27 para $k = e^t$, concluímos que existe apenas um número finito de elementos $\alpha \in A^\times \subseteq \mathcal{O}_K$ satisfazendo essas desigualdades. Isso prova que $\lambda(A^\times) \cap C_t$ é finito, concluindo a demonstração. □

Nós mostraremos agora que se $A \subseteq \mathcal{O}_K$ for uma ordem de K então $\lambda(A^\times)$ será de fato um reticulado completo em H. Para isso, precisaremos de dois lemas:

Lema 7.31. *Seja $C \subseteq \mu^{-1}(H)$ limitado em $K_\mathbb{R}$. Então o subconjunto $\mu C \subseteq H$ é limitado em $\mathbb{R}^{r_1+r_2}$ (e portanto em H).*

Demonstração. Como C é limitado em $K_\mathbb{R}$, existe algum $t \geq 1$ para o qual $C \subseteq S_t$, onde S_t é a região:

$$S_t \coloneqq \{(a_1, \dots, a_{r_1}; z_1, \dots, z_{r_2}) \in K_\mathbb{R} \colon |a_1| \leq t, \dots, |a_{r_1}| \leq t, |z_1|^2 \leq t, \dots, |z_{r_2}|^2 \leq t\}.$$

Dado $c = (a_1, \dots, a_{r_1}; z_1, \dots, z_{r_2}) \in C$, nós temos:

$$\mu c = (\mu_1 c, \dots, \mu_{r_1+r_2} c) = (\log|a_1|, \dots, \log|a_{r_1}|, \log|z_1|^2, \dots, \log|z_{r_2}|^2).$$

Assim, basta provarmos que existe $T > 0$ tal que, para todo $c \in C$ e para todo $1 \leq j \leq r_1 + r_2$, tenhamos $|\mu_j c| \leq T$. Notemos que, como $c \in S_t$, nós temos $\mu_j c \leq \log t$ para todo $1 \leq j \leq r_1 + r_2$. Agora, como $\mu c \in H$, nós temos $\operatorname{Tr}(\mu c) = 0$, ou seja, $\mu_1 c + \cdots + \mu_{r_1+r_2} c = 0$. Dessa forma, $\mu_j c$ também é limitado por baixo:

$$\mu_j c = -\mu_1 c - \cdots - \mu_{j-1} c - \mu_{j+1} c - \cdots - \mu_{r_1+r_2} c \geq -(r_1 + r_2 - 1) \log t.$$

Assim, para todo $1 \leq j \leq r_1 + r_2$, nós temos:

$$-(r_1 + r_2 - 1) \log t \leq \mu_j c \leq \log t \Rightarrow |\mu_j c| \leq (r_1 + r_2) \log t.$$

Dessa forma, basta tomarmos $T = (r_1 + r_2) \log t$. □

Lema 7.32. *Sejam $C \subseteq K_\mathbb{R}$ limitado e $v \in K_\mathbb{R}$ qualquer. Então $v \cdot C$ é um conjunto limitado.*

Demonstração. Como C é limitado, existe $t > 0$ tal que

$$C \subseteq \{(x_1, \dots, x_{r_1}; y_1, \dots, y_{r_2}) \in K_\mathbb{R} \colon |x_1| \leq t, \dots, |x_{r_1}| \leq t, |y_1| \leq t, \dots, |y_{r_2}| \leq t\}.$$

Escrevendo $v = (a_1, \dots, a_{r_1}; z_1, \dots, z_{r_2})$, vemos que para todo $c = (x_1, \dots, x_{r_1}; y_1, \dots, y_{r_2}) \in C$ nós temos $vc = (a_1 x_1, \dots, a_{r_1} x_{r_1}; z_1 y_1, \dots, z_{r_2} y_{r_2})$. Note que $|a_1 x_1| \leq |a_1| t, \dots, |a_{r_1} x_{r_1}| \leq |a_{r_1}| t$, $|z_1 y_1| \leq |z_1| t, \dots, |z_{r_2} y_{r_2}| \leq |z_{r_2}| t$. Assim, $v \cdot C$ está contido no conjunto

$$\{(v_1, \dots, v_{r_1}; w_1, \dots, w_{r_2}) \in K_\mathbb{R} \colon |v_1| \leq |a_1| t, \dots, |v_{r_1}| \leq |a_{r_1}| t, |w_1| \leq |z_1| t, \dots, |w_{r_2}| \leq |z_{r_2}| t\},$$

que é limitado. Logo $v \cdot C$ é limitado. □

Também precisaremos do seguinte resultado, que diz que para cada $k \in \mathbb{N}$ o número de classes de elementos associados que têm como norma absoluta k é finito:

Teorema 7.33. *Sejam A um subanel de K que é um $\mathbb{Z}$-módulo finitamente gerado e $k \in \mathbb{N}$. Então existem apenas finitas classes de elementos associados $A^\times \cdot \alpha_1, \ldots, A^\times \cdot \alpha_m$ em A tais que $|N_{K/\mathbb{Q}}(\alpha_j)| = k$, para todo $1 \leq j \leq m$.*

Demonstração. Afirmamos que se $\alpha, \beta \in A$ são tais que $|N(\alpha)| = |N(\beta)| = k$ e $\alpha \equiv \beta \pmod{kA}$, então α e β são associados. Sabemos que $\alpha \mid N(\alpha) = \pm k$ e $\beta \mid N(\beta) = \pm k$ em A. Assim, α e β dividem k em A, logo existem $x, y \in A$ tais que $\alpha x = \beta y = k$. Agora, como $\alpha \equiv \beta \pmod{kA}$, existe $a \in A$ tal que $\alpha - \beta = ka$. Desse modo:

$$\begin{aligned} \alpha &= \beta + ka = \beta + \beta ya = \beta(1 + ya), \text{ e} \\ \beta &= \alpha - ka = \alpha - \alpha xa = \alpha(1 - xa). \end{aligned}$$

Desse modo, concluímos que α e β são associados, justificando nossa afirmação. Com isso, basta mostrar que existe um número finito de classes de congruência módulo kA. Sejam $\gamma_1, \ldots, \gamma_r \in A$ tais que $A = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_r$. Então é fácil ver que todo $\alpha \in A$ está na classe de congruência módulo kA de algum elemento $d_1\gamma_1 + \cdots + d_r\gamma_r$ com $0 \leq d_j < k$ para todo $1 \leq j \leq r$. Como existem no máximo k^r de tais elementos, concluímos que o número de classes de congruência módulo kA é finito, terminando a demonstração. □

Teorema 7.34. *Seja A uma ordem de K. Então $\lambda(A^\times)$ é um reticulado completo em H.*

Demonstração. Pelo Teorema 7.30, $\lambda(A^\times)$ é um reticulado em H. Assim, resta mostrarmos que $\lambda(A^\times)$ é um reticulado completo. Pelo Teorema 7.4, basta provarmos que existe um subconjunto limitado $S \subseteq H$ tal que $H = \bigcup_{u \in A^\times} (\lambda(u) + S)$. É suficiente encontrarmos $B \subseteq \mu^{-1}(H)$ limitado em $\mathbb{R}^{r_1+r_2}$ tal que $\mu^{-1}(H) = \bigcup_{u \in A^\times} \chi(u) \cdot B$, pois como μ é sobrejetora nós teremos então:

$$H = \mu(\mu^{-1}(H)) = \mu\left(\bigcup_{u \in A^\times} \chi(u) \cdot B\right) = \bigcup_{u \in A^\times} \mu(\chi(u) \cdot B) = \bigcup_{u \in A^\times} (\lambda(u) + \mu B).$$

Como pelo Lema 7.31 μB é limitado em H, podemos tomar $S = \mu B$. Assim, encontremos um tal conjunto B. Pelo Corolário 7.15, sabemos que χA é um reticulado completo em $K_{\mathbb{R}}$. Tomemos $t > \sqrt[n]{\operatorname{vol}(\chi A)}$, e definamos $C \subseteq K_{\mathbb{R}}$ como sendo o cubo:

$$C \coloneqq \left\{ \sum_{j=1}^{n} \gamma_j e_j \colon -t \leq \gamma_j \leq t, \text{ para todo } 1 \leq j \leq n \right\}.$$

É claro que C é limitado, simétrico, convexo e que $\operatorname{vol}(C) = (2t)^n$. Para todo $c \in C$, nós temos $|N(c)| \leq 2^{r_2} t^n$. De fato, dado $c = \sum_{j=1}^{n} \gamma_j e_j \in C$:

$$\begin{aligned} |N(c)| &= |\gamma_1| \cdots |\gamma_{r_1}| |\gamma_{r_1+1} + i\gamma_{r_1+2}|^2 \cdots |\gamma_{n-1} + i\gamma_n|^2 \\ &= |\gamma_1| \cdots |\gamma_{r_1}| (\gamma_{r_1+1}^2 + \gamma_{r_1+2}^2) \cdots (\gamma_{n-1}^2 + \gamma_n^2) \\ &\leq \underbrace{t \cdots t}_{r_1 \text{ vezes}} \underbrace{(t^2 + t^2) \cdots (t^2 + t^2)}_{r_2 \text{ vezes}} \\ &= 2^{r_2} t^{r_1 + 2r_2} = 2^{r_2} t^n. \end{aligned}$$

Pelo Teorema 7.33, existem $\alpha_1, \ldots, \alpha_r \in A$ não-nulos tais que todo $\alpha \in A$ não-nulo satisfazendo $|N_{K/\mathbb{Q}}(\alpha)| \leq 2^{r_2} t^n$ seja associado a algum α_j para $1 \leq j \leq r$. Definamos

$$B \coloneqq \mu^{-1}(H) \cap \bigcup_{j=1}^{r} (\chi\alpha_j)^{-1} \cdot C.$$

Como C é limitado, cada $(\chi\alpha_j)^{-1}\cdot C$ é limitado pelo Lema 7.32. Assim, é claro que B é limitado. Desse modo, a prova estará completa se mostrarmos que $\bigcup_{u\in A^\times}\chi(u)\cdot B = \mu^{-1}(H)$:

($\subseteq$): Sejam $u\in A^\times$ e $b\in B$ quaisquer. Queremos mostrar que $\chi(u)b\in\mu^{-1}(H)$. Pela Proposição 7.26, nós temos $N(b)=\pm1$, e portanto $N(\chi(u)b)=N(\chi(u))N(b)=N_{K/\mathbb{Q}}(u)N(b)=\pm1$, logo também pela Proposição 7.26 nós concluímos que $\chi(u)b\in\mu^{-1}(H)$, como queríamos.

($\supseteq$): Seja $v\in\mu^{-1}(H)$ qualquer. Então pelas proposições 7.23 e 7.26 nós vemos que $v\cdot\chi A$ é um reticulado completo em $K_\mathbb{R}$ com volume $\operatorname{vol}(v\cdot\chi A)=|N(v)|\operatorname{vol}(\chi A)=\operatorname{vol}(\chi A)$. Assim, C é simétrico, convexo e

$$\operatorname{vol}(C)=2^nt^n>2^n\operatorname{vol}(\chi A)=2^n\operatorname{vol}(v\cdot\chi A).$$

Portanto, pelo Teorema de Minkowski, $C\cap(v\cdot\chi A)\setminus\{0\}\neq\emptyset$, e concluímos que existe um elemento $c=v\chi\alpha\in C$ para algum $\alpha\in A$ não-nulo. Notemos que

$$N(c)=N(v\chi\alpha)=N(v)N(\chi\alpha)=\pm N_{K/\mathbb{Q}}(\alpha).$$

Assim, como $c\in C$, temos $|N_{K/\mathbb{Q}}(\alpha)|=|N(c)|\leq 2^{r_2}t^n$. Com isso, sabemos que existem $1\leq j\leq r$ e $u\in A^\times$ tais que $\alpha_j=\alpha u$. Disso obtemos $\chi\alpha_j=\chi\alpha\cdot\chi u\Rightarrow(\chi\alpha)^{-1}=\chi u(\chi\alpha_j)^{-1}$. Assim, $v=(\chi\alpha)^{-1}\cdot c=\chi u(\chi\alpha_j)^{-1}c$. Além disso, nós temos:

$$\begin{aligned}\pm1=N(v)=N(\chi u(\chi\alpha_j)^{-1}c)=N(\chi u)N((\chi\alpha_j)^{-1}c) &= N_{K/\mathbb{Q}}(u)N((\chi\alpha_j)^{-1}c)\\ &= \pm N((\chi\alpha_j)^{-1}c),\end{aligned}$$

logo pela Proposição 7.26 nós concluímos que $(\chi\alpha_j)^{-1}c\in\mu^{-1}(H)$. Desse modo, $(\chi\alpha_j)^{-1}c\in B$, e portanto

$$v=\chi u(\chi\alpha_j)^{-1}c\in\bigcup_{\varepsilon\in A^\times}\chi(\varepsilon)\cdot B.$$

Concluímos que $\bigcup_{u\in A^\times}\chi(u)\cdot B=\mu^{-1}(H)$, e então $\lambda(A^\times)$ é um reticulado completo em H, como queríamos demonstrar. □

Como corolário desse resultado, nós obtemos o Teorema das Unidades de Dirichlet:

Teorema 7.35 (Teorema das Unidades de Dirichlet)**.** *Seja K um corpo de números algébricos com $[K:\mathbb{Q}]=n$ e assinatura (r_1,r_2), e seja A uma ordem de K. Então existem $\varepsilon_1,\dots,\varepsilon_{r_1+r_2-1}\in A^\times$ tais que $A^\times$ seja o produto direto $W(A)\odot\langle\varepsilon_1\rangle\odot\cdots\odot\langle\varepsilon_{r_1+r_2-1}\rangle$ do grupo cíclico finito $W(A)$ e dos grupos multiplicativos cíclicos infinitos gerados por $\varepsilon_1,\dots,\varepsilon_{r_1+r_2-1}$. Em resumo, $A^\times$ é um subgrupo finitamente gerado de $K^\times$, de posto r_1+r_2-1 e com grupo de torção cíclico.*

Demonstração. Denotemos $r:=r_1+r_2-1$. Pelo teorema acima, $\lambda(A^\times)$ é um reticulado completo em H, e portanto existem $\varepsilon_1,\dots,\varepsilon_r\in A^\times$ tais que $\lambda\varepsilon_1,\dots,\lambda\varepsilon_r$ formem uma base desse reticulado. Seja $u\in A^\times$ qualquer. Então existem únicos $k_1,\dots,k_r\in\mathbb{Z}$ tais que

$$\lambda u=k_1\lambda\varepsilon_1+\cdots+k_r\lambda\varepsilon_r=\lambda(\varepsilon_1^{k_1}\cdots\varepsilon_r^{k_r}),$$

já que λ é homomorfismo entre o grupo multiplicativo $K^\times$ e o grupo aditivo $\mathbb{R}^{r_1+r_2}$. Desse modo, $\lambda(u\varepsilon_1^{-k_1}\cdots\varepsilon_r^{-k_r})=0$, e assim $u\varepsilon_1^{-k_1}\cdots\varepsilon_r^{-k_r}\in\ker\lambda\cap A=W(K)\cap A=W(A)$, pela Proposição 7.29. Logo existe $w\in W(A)$ tal que $u\varepsilon_1^{-k_1}\cdots\varepsilon_r^{-k_r}=w\Rightarrow u=w\varepsilon_1^{k_1}\cdots\varepsilon_r^{k_r}$. Isso prova que $A^\times=W(A)\cdot\langle\varepsilon_1\rangle\cdots\langle\varepsilon_r\rangle$. Para vermos que esse produto é direto, basta mostrarmos que se $w\in W(A)$ e $k_1,\dots,k_r\in\mathbb{Z}$ são tais que $w\varepsilon_1^{k_1}\cdots\varepsilon_r^{k_r}=1$, então $w=1$ e $k_1=\cdots=k_r=0$. Aplicando λ de ambos os lados, nós obtemos:

$$\begin{aligned}\lambda(w\varepsilon_1^{k_1}\cdots\varepsilon_r^{k_r})=\lambda(1) &\Rightarrow \lambda(w)+k_1\lambda(\varepsilon_1)+\cdots+k_r\lambda(\varepsilon_r)=0\\ &\Rightarrow k_1\lambda(\varepsilon_1)+\cdots+k_r\lambda(\varepsilon_r)=0\\ &\Rightarrow k_1=\cdots=k_r=0,\end{aligned}$$

já que $1, w \in W(A) \subseteq \ker \lambda$ e $\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_r)$ são linearmente independentes. Assim, temos $1 = w\varepsilon_1^0 \cdots \varepsilon_r^0 = w$, e portanto esse produto é de fato direto. Note que isso nos diz em particular que $\varepsilon_1, \dots, \varepsilon_r \notin W(A)$, e portanto os grupos cíclicos $\langle \varepsilon_1 \rangle, \dots, \langle \varepsilon_r \rangle$ são de fato infinitos. Finalmente, como $W(K)$ é cíclico finito pelo Teorema 7.28, vemos que $W(A) \subseteq W(K)$ também o é, provando o teorema. □

Definição ((Sistema de) Unidades Fundamentais)**.** Nós dizemos que uma $r_1 + r_2 - 1$-upla de unidades $\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1}$ de uma ordem A de K é um **sistema de unidades fundamentais** de A se ela satisfizer a condição do teorema acima, e chamamos seus elementos de **unidades fundamentais** de A. Caso $A = \mathcal{O}_K$, chamaremos ainda esse sistema de **sistema de unidades fundamentais** de K, e seus elementos de **unidades fundamentais** de K.

Observemos que $r_1 + r_2 - 1 = 0$ só pode ocorrer se $(r_1, r_2) = (1, 0)$, caso em que $K = \mathbb{Q}$, ou se $(r_1, r_2) = (0, 1)$, caso em que $K = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático complexo, isto é, com $d < 0$. Esses são os únicos casos em que todas as unidades são raízes da unidade.

7.5. O Grupo das Unidades de um Corpo Quadrático

Nessa seção, estudaremos um exemplo particular do Teorema das Unidades de Dirichlet, o caso em que K é um corpo quadrático. Nós determinaremos a estrutura do grupo das unidades de suas ordens, e veremos como isso se relaciona com um tipo de equação diofantina: as chamadas **equações de Pell**.

Nós denotaremos, para $d \in \mathcal{D}$, $K_d := \mathbb{Q}(\sqrt{d})$. Seu anel de inteiros algébricos é $\mathbb{Z}[\delta_d]$, onde $\delta_d = \sqrt{d}$ se $d \equiv 2, 3 \pmod 4$ e $\delta_d = \frac{1+\sqrt{d}}{2}$ se $d \equiv 1 \pmod 4$. Para cada n inteiro positivo, definimos $A_{d,n} := \mathbb{Z}[n\delta_d]$. É claro que $A_{d,n} \subseteq \mathcal{O}_{K_d} = A_{d,1}$ é uma ordem de K_d, e que dados dois inteiros positivos n, n' nós temos $A_{d,n} \subseteq A_{d,n'} \iff n' \mid n$. Segue da Proposição 1.31 que $\Delta_{K/\mathbb{Q}}(1, n\delta_d) = n^2 \Delta_{K/\mathbb{Q}}(1, \delta_d) = n^2 d_{K_d}$. Desse modo, pelo Teorema 2.10, $(\mathcal{O}_{K_d} : A_{d,n}) = n$. Mostraremos agora que todo subanel de $\mathcal{O}_{K_d}$ diferente de $\mathbb{Z}$ é igual a algum dos anéis $A_{d,n}$:

Teorema 7.36. *O conjunto $\mathscr{A}_d$ dos subanéis A de $\mathcal{O}_{K_d}$ tais que $A \neq \mathbb{Z}$ está em correspondência biunívoca com o conjunto $\mathbb{N}^*$, por meio das aplicações $n \mapsto A_{d,n}$, $A \mapsto (\mathcal{O}_{K_d} : A)$.*

Demonstração. Nós sabemos que $(\mathcal{O}_{K_d} : A_{d,n}) = n$ e que a aplicação $n \mapsto A_{d,n}$ é injetora. Assim, basta mostrar que essa aplicação é também sobrejetora. Seja $A \neq \mathbb{Z}$ um subanel de $\mathcal{O}_{K_d}$. Então todo elemento de A é da forma $a + b\delta_d$, com $a, b \in \mathbb{Z}$. Seja $n \in \mathbb{N}^*$ minimal tal que $c + n\delta_d \in A$ para algum $c \in \mathbb{Z}$ (tal n existe já que $A \neq \mathbb{Z}$). Mostraremos que $A = A_{d,n}$, ou seja, que $A = \mathbb{Z}[n\delta_d]$. Como $c + n\delta_d \in A$, temos $n\delta_d \in A$, e assim é claro que $\mathbb{Z}[n\delta_d] \subseteq A$. Para mostrar a outra inclusão, seja $a + b\delta_d \in A$ qualquer, com $a, b \in \mathbb{Z}$. Então existem $q, r \in \mathbb{Z}$, $0 \leq r < n$, tais que $b = qn + r$. Assim:

$$A \ni (a + b\delta_d) - q(c + n\delta_d) = (a - qc) + (b - qn)\delta_d = (a - qc) + r\delta_d.$$

Pela minimalidade de n, concluímos que $r = 0$, e assim $a + b\delta_d = a + qn\delta_d \in \mathbb{Z}[n\delta_d]$, mostrando que $A \subseteq \mathbb{Z}[n\delta_d]$. Então provamos que $A = A_{d,n}$, concluindo a demonstração. □

Lembremos que $A_{d,n}^\times = \{x \in A_{d,n} \colon N_{K_d/\mathbb{Q}}(x) = \pm 1\} = \mathcal{O}_{K_d}^\times \cap A_{d,n}$. Será às vezes conveniente separarmos os elementos de norma 1 daqueles de norma -1. Assim, definimos:

$$U_0(A_{d,n}) := \{x \in A_{d,n} \colon N_{K_d/\mathbb{Q}}(x) = 1\},\ U_1(A_{d,n}) := \{x \in A_{d,n} \colon N_{K_d/\mathbb{Q}}(x) = -1\}.$$

Então é claro que $A_{d,n}^\times = U_0(A_{d,n}) \sqcup U_1(A_{d,n})$.

Proposição 7.37. *Sejam n um inteiro positivo, $d \in \mathcal{D}$ e $e \in \{0, 1\}$. Então:*

(a) *Dados $a, b \in \mathbb{Z}$, temos que $a + bn\sqrt{d} \in U_e(A_{d,n})$ se e só se (a, b) for solução da equação $x^2 - n^2dy^2 = (-1)^e$.*

(b) *Se $d \equiv 1 \pmod 4$, então $a + bn\delta_d \in U_e(A_{d,n})$ se e só se (a, b) for solução da equação $x^2 + nxy + n^2 \cdot \frac{1-d}{4}y^2 = (-1)^e$.*

Demonstração. (a) Nós temos $N(a + bn\sqrt{d}) = a^2 - n^2db^2$. Assim, é claro que nós teremos $a + bn\sqrt{d} \in U_e(A_{d,n}) \iff a^2 - n^2db^2 = (-1)^e$.

(b) Nós temos $N(a + bn\delta_d) = a^2 + nab + n^2 \cdot \frac{1-d}{4}b^2$, logo do mesmo modo que em (a) nós concluímos o resultado desejado.

□

Temos a seguinte generalização do Teorema 2.21 para os anéis $A_{d,n}$, que se prova facilmente:

Teorema 7.38. *(a) $A^\times_{-1,1} = \mathcal{O}^\times_{K_{-1}} = \{1, i, -i, -1\}$.*

(b) $A^\times_{-3,1} = \mathcal{O}^\times_{K_{-3}} = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$, onde $\zeta = \frac{1+\sqrt{-3}}{2}$ é uma raiz sexta da unidade.

(c) $A^\times_{d,n} = \{1, -1\}$ se $d < 0$ e $(d, n) \neq (-1, 1), (-3, 1)$.

Assim, o caso interessante ocorre quando $d > 0$. Nesse caso, as duas imersões de K_d são a identidade e a conjugação $\sqrt{d} \mapsto -\sqrt{d}$. Note que ambas são imersões reais. Assim, $r_1 = 2$ e $r_2 = 0$, de modo que $r_1 + r_2 - 1 = 1$. Pelo Teorema das Unidades, concluímos que para toda ordem A de K_d existe uma unidade $\varepsilon \in A^\times$ para a qual $A^\times = W(A) \odot \langle\varepsilon\rangle = \{1, -1\} \odot \langle\varepsilon\rangle$. Ou seja, $A^\times = \{\pm\varepsilon^j : j \in \mathbb{Z}\}$. Notemos que podemos trocar ε por qualquer um dos elementos $\pm\varepsilon$, $\pm\varepsilon^{-1}$, e que exatamente um deles é maior que 1. Assim, podemos supor sem perda de generalidade que $\varepsilon > 1$, e chamamos tal ε de **unidade fundamental** de A. Nós denotaremos $V(A) \coloneqq A^\times \cap [1, +\infty)$. Note que então $V(A) = \{\varepsilon^j : j \in \mathbb{N}^*\}$. Assim, ε é o menor elemento do conjunto $V(A)$.

Para fins práticos, é importante determinar ε. Começamos com o seguinte resultado, que nos diz que todo elemento de $V(A_{d,n})$, para $d > 0$, tem coeficientes positivos na base $\{1, n\delta_d\}$:

Proposição 7.39. *Sejam $d \in \mathcal{D}$ com $d > 0$ e $n \in \mathbb{N}^*$. Então nós temos:*

$$V(A_{d,n}) \subseteq \{a + bn\delta_d : a, b \in \mathbb{Z},\ a > 0,\ b > 0\},$$

exceto no caso $(d, n) = (5, 1)$, no qual a condição $a > 0$ deve ser substituída por $a \geq 0$.

Demonstração. Seja $\eta = a + bn\delta_d \in V(A_{d,n})$ qualquer, com $a, b \in \mathbb{Z}$. Então $a + bn\delta_d > 1$ e $|N(a + bn\delta_d)| = 1$. Seja $\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ dado por $\sqrt{d} \mapsto -\sqrt{d}$. Se $d \equiv 2, 3 \pmod 4$, temos $\delta_d = \sqrt{d} \mapsto -\sqrt{d}$, e se $d \equiv 1 \pmod 4$, temos $\delta_d = \frac{1+\sqrt{d}}{2} \mapsto \frac{1-\sqrt{d}}{2}$. Note que, em qualquer caso, $\delta_d - \sigma(\delta_d) > 0$ e $\sigma(\delta_d) < 0$. Além disso, para $d \neq 5$, temos $\sigma(\delta_d) < -1$.

Observemos agora que

$$1 = |N(\eta)| = |\eta \cdot \sigma\eta| \Rightarrow |\sigma\eta| = \frac{1}{\eta} < 1 \Rightarrow |a + bn\sigma(\delta_d)| < 1.$$

De $a + bn\delta_d > 1$ e $a + bn\sigma(\delta_d) < 1$ nós concluímos que

$$(a + bn\delta_d) - (a + bn\sigma(\delta_d)) > 0 \Rightarrow bn(\delta_d - \sigma(\delta_d)) > 0 \Rightarrow b > 0,$$

pois como já vimos $\delta_d - \sigma(\delta_d) > 0$. Agora, como $\sigma(\delta_d) < 0$ e $b \geq 1$, nós temos:

$$-1 < a + bn\sigma(\delta_d) \leq a - n|\sigma(\delta_d)| \Rightarrow a > n|\sigma(\delta_d)| - 1.$$

Para $d \neq 5$, temos então $a > n \cdot 1 - 1 = n - 1 \geq 0$, como queríamos. Suponhamos agora $d = 5$. Nesse caso, temos $\sigma(\delta_d) = \frac{1-\sqrt{5}}{2}$, e assim

$$a > n \cdot \frac{\sqrt{5}-1}{2} - 1 \geq \frac{\sqrt{5}-1}{2} - 1 = \frac{\sqrt{5}-3}{2} > -1 \Rightarrow a \geq 0,$$

e caso $n \geq 2$:

$$a > 2 \cdot \frac{\sqrt{5}-1}{2} - 1 = \sqrt{5} - 2 > 0,$$

como queríamos. □

Nós podemos ainda separar $V(A_{d,n})$ entre os elementos que têm norma 1 ou -1, definindo $V_0(A_{d,n}) := V(A_{d,n}) \cap U_0(A_{d,n})$ e $V_1(A_{d,n}) := V(A_{d,n}) \cap U_1(A_{d,n})$. É claro que nós temos $V(A_{d,n}) = V_0(A_{d,n}) \sqcup V_1(A_{d,n})$. Podemos caracterizar esses dois conjuntos da seguinte forma:

Teorema 7.40. *Sejam $d \in \mathcal{D}$ com $d > 0$, $n \in \mathbb{N}^*$ e $e \in \{0, 1\}$.*

(a) Se $d \equiv 2, 3 \pmod 4$, temos:

$$V_e(A_{d,n}) = \{a + bn\sqrt{d} \colon a, b \in \mathbb{N}^*,\ a^2 - n^2 d b^2 = (-1)^e\}.$$

(b) Se $d \equiv 1 \pmod 4$, temos:

$$\begin{aligned} V_e(A_{d,n}) &= \left\{a + bn\delta_d \colon a \in \mathbb{N},\ b \in \mathbb{N}^*,\ a^2 + nab + n^2 \cdot \frac{1-d}{4} \cdot b^2 = (-1)^e\right\} \\ &= \left\{\frac{a}{2} + \frac{b}{2} \cdot n\sqrt{d} \colon a, b \in \mathbb{N}^*,\ a^2 - n^2 d b^2 = 4(-1)^e\right\}. \end{aligned}$$

Demonstração. O item (a) e a primeira igualdade do item (b) seguem das proposições 7.37 e 7.39 e do fato de que, para $a \in \mathbb{N}$ e $b \in \mathbb{N}^*$, nós temos $a + bn\delta_d > 1$ (note que sempre temos $\delta_d > 1$). Mostremos a segunda igualdade de (b):

$(\subseteq)$: Sejam $a \in \mathbb{N}$, $b \in \mathbb{N}^*$ tais que $a^2 + nab + n^2 \cdot \frac{1-d}{4} \cdot b^2 = (-1)^e$. Notemos que

$$a + bn\delta_d = a + bn \cdot \frac{1+\sqrt{d}}{2} = \frac{2a + bn}{2} + \frac{b}{2} \cdot n\sqrt{d}.$$

Chamemos $\tilde{a} := 2a + bn \in \mathbb{N}^*$. Então $a + bn\delta_d = \frac{\tilde{a}}{2} + \frac{b}{2} \cdot n\sqrt{d}$. Notemos que $a = \frac{\tilde{a} - bn}{2}$. Assim:

$$\begin{aligned} (-1)^e = a^2 + nab + n^2 \cdot \frac{1-d}{4} \cdot b^2 &= \left(\frac{\tilde{a} - bn}{2}\right)^2 + n\left(\frac{\tilde{a} - bn}{2}\right) b + n^2 \cdot \frac{1-d}{4} \cdot b^2 \\ &= \frac{\tilde{a}^2 - 2\tilde{a}bn + n^2 b^2}{4} + \frac{\tilde{a}bn - n^2 b^2}{2} + n^2 \cdot \frac{1-d}{4} \cdot b^2 \\ &= \frac{\tilde{a}^2 - 2\tilde{a}bn + n^2 b^2 + 2\tilde{a}bn - 2n^2 b^2 + (1-d)n^2 b^2}{4} \\ &= \frac{\tilde{a}^2 - n^2 d b^2}{4}. \end{aligned}$$

Desse modo, $\tilde{a}^2 - n^2 d b^2 = 4(-1)^e$, provando esta inclusão.

$(\supseteq)$: Sejam $a, b \in \mathbb{N}^*$ tais que $a^2 - n^2 d b^2 = 4(-1)^e$. Avaliando essa equação módulo 4, obtemos $a^2 - (bn)^2 \equiv 0 \pmod 4$, de onde é fácil ver que devemos ter $2 \mid a - bn$. Além disso, notemos que

$$-4 \leq a^2 - n^2 d b^2 < a^2 - (bn)^2 = (a - bn)(a + bn) \Rightarrow a - bn > -\frac{4}{a + bn} \geq -\frac{4}{2} = -2,$$

e de $2 \mid a - bn$ concluímos que $a - bn \geq 0$. Definamos $\tilde{a} := \frac{a-bn}{2} \in \mathbb{N}$. Então nós temos $a = 2\tilde{a} + bn$, de modo que

$$\frac{a}{2} + \frac{b}{2} \cdot n\sqrt{d} = \frac{2\tilde{a} + bn}{2} + \frac{bn}{2} \cdot \sqrt{d} = \tilde{a} + bn \cdot \frac{1 + \sqrt{d}}{2} = \tilde{a} + bn\delta_d.$$

Além disso, obtemos que $\tilde{a}^2 + n\tilde{a}b + n^2 \cdot \frac{1-d}{4} \cdot b^2 = (-1)^e$ (é basicamente a mesma conta da inclusão ($\subseteq$), lida de trás para frente), o que prova essa inclusão. □

Com as caracterizações dadas acima para $V_e(A_{d,n})$, conseguimos o seguinte resultado, que será bastante útil para calcular ε:

Corolário 7.41. *Sejam $\eta_1, \eta_2 \in V(A_{d,n})$. Escrevamos, para $j = 1, 2$:*

$$\eta_j = \begin{cases} a_j + b_j n\sqrt{d}, & \text{se } d \equiv 2, 3 \pmod 4; \\ \frac{a_j}{2} + \frac{b_j}{2} \cdot n \cdot \sqrt{d}, & \text{se } d \equiv 1 \pmod 4. \end{cases}$$

onde $a_j, b_j \in \mathbb{N}^*$ (sabemos que essas representações para η_1 e η_2 existem pelo teorema acima). Então $\eta_1 \leq \eta_2 \Rightarrow b_1 \leq b_2$.

Demonstração. Nós provaremos a contrapositiva, ou seja, que $b_1 > b_2 \Rightarrow \eta_1 > \eta_2$. Suponhamos então $b_1 > b_2$. Denotemos $q = 1$, se $d \equiv 2, 3 \pmod 4$, e $q = 4$, se $d \equiv 1 \pmod 4$. Então nós sabemos pelo teorema acima que $a_j^2 - n^2 d b_j^2 = \pm q$, para $j = 1, 2$, e portanto

$$a_j^2 + q \geq n^2 d b_j^2 \geq a_j^2 - q, \text{ para } j = 1, 2.$$

Sendo $b_1 > b_2$, nós temos então:

$$a_1^2 + q \geq n^2 d b_1^2 \geq n^2 d (b_2 + 1)^2 > n^2 d b_2^2 + 2d \geq a_2^2 - q + 2d > a_2^2 + q,$$

já que $d > q$. Disso obtemos que $a_1 > a_2$. Assim, sendo $a_1 > a_2$ e $b_1 > b_2$, é claro que $\eta_1 > \eta_2$, como queríamos demonstrar. □

Como consequência disso, nós temos o seguinte critério com o qual podemos determinar a unidade fundamental de $A_{d,n}$ algoritmicamente:

Teorema 7.42. *Sejam $d \in \mathcal{D}$ com $d > 0$ e $n \in \mathbb{N}^*$. Então:*

(a) Se $d \equiv 2, 3 \pmod 4$, seja b_0 o menor inteiro positivo b para o qual $n^2 d b^2 + 1$ ou $n^2 d b^2 - 1$ seja um quadrado perfeito positivo. Então, sendo $a_0 \in \mathbb{N}^*$ a raiz quadrada desse quadrado perfeito, temos que a unidade fundamental ε de $A_{d,n}$ é $\varepsilon = a_0 + b_0 n\sqrt{d}$.

(b) Se $d \equiv 1 \pmod 4$, seja b_0 o menor inteiro positivo b para o qual $n^2 d b^2 + 4$ ou $n^2 d b^2 - 4$ seja um quadrado perfeito positivo. Então, sendo $a_0 \in \mathbb{N}^*$ a raiz quadrada desse quadrado perfeito, temos que a unidade fundamental ε de $A_{d,n}$ é $\varepsilon = \frac{a_0}{2} + \frac{b_0}{2} \cdot n\sqrt{d}$.

Demonstração. Nós provaremos o item (a). A prova de (b) é análoga.

Sejam $\tilde{a}, \tilde{b} \in \mathbb{Q}$ tais que $\varepsilon = \tilde{a} + \tilde{b} n\sqrt{d}$. Então pelo Teorema 7.40 nós vemos que $\tilde{a}, \tilde{b} \in \mathbb{N}^*$ e $\tilde{a}^2 - n^2 d \tilde{b}^2 = \pm 1$. Assim, $n^2 d \tilde{b}^2 + 1$ ou $n^2 d \tilde{b}^2 - 1$ é um quadrado perfeito positivo. Sendo assim, o conjunto dos inteiros positivos b para os quais $n^2 d b^2 + 1$ ou $n^2 d b^2 - 1$ é um quadrado perfeito positivo é não-vazio, e portanto b_0 está bem-definido. O inteiro positivo a_0 também está bem-definido, pois apenas um entre $n^2 d b_0^2 + 1$ e $n^2 d b_0^2 - 1$ é um quadrado perfeito.

Chamemos $\varepsilon_0 := a_0 + b_0 n\sqrt{d}$. Como $a_0, b_0 \in \mathbb{N}^*$ e $a_0^2 - n^2 d b_0^2 = \pm 1$, vemos pelo Teorema 7.40 que $\varepsilon_0 \in V(A_{d,n})$, e portanto $\varepsilon \leq \varepsilon_0$. Pelo corolário acima, concluímos então que $\tilde{b} \leq b_0$. Assim, pela minimalidade de b_0, vemos que $\tilde{b} = b_0$, e pela unicidade de a_0 concluímos que $\tilde{a} = a_0$. Logo $\varepsilon = \varepsilon_0 = a_0 + b_0 n\sqrt{d}$, como queríamos. □

Exemplo 7.43. *Vejamos como calcular as unidades fundamentais de* $A_{2,2} = \mathbb{Z}[2\sqrt{2}]$ *e de* $A_{17,1} = \mathbb{Z}\left[\frac{1+\sqrt{17}}{2}\right] = \mathcal{O}_{\mathbb{Q}(\sqrt{17})}$ *utilizando o teorema acima.*

Para $A_{2,2}$*, temos* $d = n = 2$*. Note que* $d \equiv 2 \pmod 4$*. Assim, devemos encontrar o menor inteiro positivo* b *para o qual* $2^2 \cdot 2 \cdot b^2 \pm 1 = 8b^2 \pm 1$ *seja um quadrado perfeito. Note que* $b = 1$ *já satisfaz, pois* $8 \cdot 1^2 + 1 = 9 = 3^2$*. Assim,* $b_0 = 1$ *e* $a_0 = 3$*. Concluímos que a unidade fundamental de* $A_{2,2}$ *é* $a_0 + b_0 \cdot 2\sqrt{2} = 3 + 2\sqrt{2}$*.*

Para $A_{17,1}$*, temos* $n = 1$ *e* $d = 17 \equiv 1 \pmod 4$*. Assim, devemos encontrar o menor inteiro positivo* b *para o qual* $1^2 \cdot 17 \cdot b^2 \pm 4 = 17b^2 \pm 4$ *seja um quadrado perfeito. Para* $b = 1$*, temos* $17 \cdot 1^2 \pm 4 = 13$ *ou* 21*, nenhum deles um quadrado perfeito. Já para* $b = 2$*, temos* $17 \cdot 2^2 \pm 4 = 64$ *ou* 72*. Como* $64 = 8^2$*, temos então* $b_0 = 2$ *e* $a_0 = 8$*. Concluímos que a unidade fundamental de* $A_{17,1}$ *é* $\frac{a_0}{2} + \frac{b_0}{2} \cdot \sqrt{17} = 4 + \sqrt{17}$*.*

É interessante ainda observar que a partir da unidade fundamental ε_d de $\mathcal{O}_{K_d} = A_{d,1}$ nós podemos encontrar a unidade fundamental $\varepsilon_{d,n}$ de $A_{d,n}$, para $n > 1$, como sendo a menor potência inteira positiva de ε_d que pertence a $A_{d,n}$, isto é, $\varepsilon_{d,n} = \varepsilon_d^{k_0}$ onde $k_0 \in \mathbb{N}^*$ é mínimo com $\varepsilon_d^{k_0} \in A_{d,n}$. Isso segue da igualdade $V(A_{d,n}) = V(\mathcal{O}_{K_d}) \cap A_{d,n}$.

Observação 7.44. *Existe um algoritmo ainda melhor que o descrito acima para calcular a unidade fundamental de* $A_{d,n}$*. Ele se baseia na determinação da* ***fração contínua*** *de* $n\sqrt{d}$*, um método da Teoria Analítica dos Números. Veja por exemplo o Capítulo 3 e a Seção 4.4 de [5].*

Dada uma ordem A de $\mathcal{O}_{K_d}$ com unidade fundamental ε, nós já vimos que $A^\times = \{\pm\varepsilon^j : j \in \mathbb{Z}\}$. Notemos que, pela multiplicatividade da norma, e pelo fato de que $N(1) = N(-1) = 1$ para extensões quadráticas, para todo $j \in \mathbb{Z}$ nós temos $N(\pm\varepsilon^j) = N(\varepsilon)^j$. Como $N(\varepsilon) = \pm 1$, nós obtemos o seguinte resultado:

Proposição 7.45. *Seja* A *uma ordem de* $\mathcal{O}_{K_d}$ *com unidade fundamental* ε*.*

(a) Se ε *tiver norma* 1*, então:*

$$\begin{aligned} V_0(A) &= \{\varepsilon^j : j \in \mathbb{N}^*\} = V(A),\ V_1(A) = \emptyset. \\ U_0(A) &= \{\pm\varepsilon^j : j \in \mathbb{Z}\} = A^\times,\ U_1(A) = \emptyset. \end{aligned}$$

(b) Se ε *tiver norma* -1*, então:*

$$\begin{aligned} V_0(A) &= \{\varepsilon^{2j} : j \in \mathbb{N}^*\},\ V_1(A) = \{\varepsilon^{2j+1} : j \in \mathbb{N}\}. \\ U_0(A) &= \{\pm\varepsilon^{2j} : j \in \mathbb{Z}\},\ U_1(A) = \{\pm\varepsilon^{2j+1} : j \in \mathbb{Z}\}. \end{aligned}$$

Observação 7.46. *Notemos que se a unidade fundamental* ε_d *de* $\mathcal{O}_{K_d}$ *tiver norma* 1*, então o mesmo ocorrerá com a unidade fundamental de qualquer ordem* A *de* K_d *(já que essa é uma potência de* ε_d*).*

Mostraremos agora como os resultados sobre as unidades dessas ordens servirão para resolver as chamadas **equações de Pell**:

Definição (Equação de Pell)**.** Dado $k \in \mathbb{N}$ que não é um quadrado perfeito, chamamos de **equação de Pell** para k a equação diofantina $x^2 - ky^2 = 1$. Chamaremos ainda de **equação de Pell generalizada** para k qualquer equação diofantina da forma $x^2 - ky^2 = c$, onde $c \in \mathbb{Z} \setminus \{0\}$.

Dado $k \in \mathbb{N}$ qualquer, podemos escrevê-lo de forma única como $k = n^2 d$, onde $d \in \mathbb{N}$ é livre de quadrados e $n \in \mathbb{N}$. Se $k = n^2$ for um quadrado perfeito, então a equação $x^2 - ky^2 = 1$ se torna $1 = x^2 - (ny)^2 = (x - ny)(x + ny)$, e é fácil ver que as únicas soluções dessa equação diofantina são $(x, y) = (\pm 1, 0)$. Assim, o caso interessante é quando k não é um quadrado perfeito, que é justamente o caso em que temos uma equação de Pell.

Supondo que k não seja um quadrado perfeito, temos $d \in \mathcal{D}$. Assim, observemos que a equação de Pell $x^2 - ky^2 = 1$ equivale a $(x - yn\sqrt{d})(x + yn\sqrt{d}) = 1$ na ordem $A_{d,n}$. Note que isso significa que $N(x + yn\sqrt{d}) = 1$, e portanto $x + yn\sqrt{d} \in U_0(A_{d,n})$.

Reciprocamente, suponhamos que $x, y \in \mathbb{Z}$ sejam tais que $x + yn\sqrt{d} \in U_0(A_{d,n})$. Então $x^2 - ky^2 = x^2 - n^2dy^2 = N(x + yn\sqrt{d}) = 1$. Ou seja, vemos que as soluções $(x, y) \in \mathbb{Z}^2$ da equação de Pell $x^2 - ky^2 = 1$ estão em bijeção com $U_0(A_{d,n})$, que sabemos determinar a partir de $\varepsilon_{d,n}$ pela Proposição 7.45. Em particular, sabemos que existem infinitas soluções para essa equação diofantina.

De fato, a mesma análise feita acima nos mostra que as soluções $(x, y) \in \mathbb{Z}^2$ da equação de Pell generalizada $x^2 - ky^2 = -1$ estão em bijeção com $U_1(A_{d,n})$. Note que, dependendo se a norma de ε for -1 ou 1, essa equação terá infinitas soluções ou então nenhuma. Desse modo, nós obtemos:

Teorema 7.47. *Seja $k \in \mathbb{N}$ que não é um quadrado perfeito, e sejam $n \in \mathbb{N}^*$, $d \in \mathcal{D}$ com $d > 0$ tais que $k = n^2d$. Então:*

(a) Os pares $(x, y) \in \mathbb{Z}^2$ que são soluções da equação de Pell $x^2 - ky^2 = 1$ são os pares para os quais $x + yn\sqrt{d} \in U_0(A_{d,n})$, isto é, para os quais:

- *Existe $j \in \mathbb{Z}$ tal que $x + yn\sqrt{d} = \varepsilon_{d,n}^j$, se $N(\varepsilon_{d,n}) = 1$.*
- *Existe $j \in \mathbb{Z}$ tal que $x + yn\sqrt{d} = \varepsilon_{d,n}^{2j}$, se $N(\varepsilon_{d,n}) = -1$.*

Em particular, a equação de Pell para k tem infinitas soluções.

(b) Os pares $(x, y) \in \mathbb{Z}^2$ que são soluções da equação de Pell generalizada $x^2 - ky^2 = -1$ são os pares para os quais $x + yn\sqrt{d} \in U_1(A_{d,n})$, isto é:

- *Se $N(\varepsilon_{d,n}) = -1$, então os (x, y) são os pares para os quais existe $j \in \mathbb{Z}$ tal que $x + yn\sqrt{d} = \varepsilon_{d,n}^{2j+1}$.*
- *Se $N(\varepsilon_{d,n}) = 1$, então essa equação não possui solução.*

Em particular, a equação de Pell generalizada para k e para $c = -1$ tem infinitas soluções se $N(\varepsilon_{d,n}) = -1$, e nenhuma solução se $N(\varepsilon_{d,n}) = 1$.

Consideremos agora a equação de Pell generalizada $x^2 - ky^2 = c$, para $c \in \mathbb{Z} \setminus \{0\}$ qualquer. Então nós temos:

$$x + y\sqrt{k} = c \iff (x + y\sqrt{k})(x - y\sqrt{k}) = c \iff N(x + y\sqrt{k}) = c,$$

onde N é a norma da extensão $\mathbb{Q}[\sqrt{k}]$. Assim, as soluções (x, y) dessa equação estão em bijeção com os elementos de $\mathbb{Z}[\sqrt{k}]$ de norma c. Pelo Teorema 7.33, existem $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}[\sqrt{k}]$ tais que todo elemento de $\mathbb{Z}[\sqrt{k}]$ de norma $\pm c$ é associado a um dos $\alpha_1, \ldots, \alpha_m$. Observemos ainda que $\mathbb{Z}[\sqrt{k}]$ é uma ordem de $\mathbb{Q}[\sqrt{k}]$, de modo que podemos aplicar os resultados dessa seção sobre $\mathbb{Z}[\sqrt{k}]^\times$. Em particular, vemos que esse grupo é infinito. Notemos que se $x + y\sqrt{k}$ tem norma c e $u \in \mathbb{Z}[\sqrt{k}]^\times$, então $u(x + y\sqrt{k})$ tem norma $\pm c$, sendo c se $N(u) = 1$ e $-c$ se $N(u) = -1$. Juntando tudo, nós temos:

Teorema 7.48. *As soluções $(x, y) \in \mathbb{Z}^2$ da equação de Pell generalizada $x^2 - ky^2 = c$ são os pares (x, y) para os quais $N(x + y\sqrt{k}) = c$. Essa equação possui ou nenhuma solução ou infinitas. Caso tenha infinitas soluções, existe apenas um número finito de soluções não-associadas duas a duas. Além disso, se a unidade fundamental de $\mathbb{Z}[\sqrt{k}]$ tiver norma -1, então a existência de soluções da equação $x^2 - ky^2 = c$ equivale à existência de soluções da equação $x^2 - ky^2 = -c$.*

Capítulo 8

Ordens

Seja K um corpo de números algébricos com $[K : \mathbb{Q}] = n$. Muito do que fizemos até aqui se baseou no estudo do anel de inteiros algébricos $\mathcal{O}_K$. Entretanto, existem outros subanéis de K que são de nosso interesse, como as ordens de K (que estão contidas em $\mathcal{O}_K$) e as localizações de $\mathcal{O}_K$ (que contêm $\mathcal{O}_K$).

Como vimos na Seção 7.5, o estudo das ordens de um corpo de números pode ser útil, como por exemplo para resolver equações diofantinas. Notemos porém que, para uma ordem $A \subsetneq \mathcal{O}_K$, nós não temos A integralmente fechada, já que $Q(A) = K$ e $\overline{A}^K = \mathcal{O}_K$. Assim, as ordens próprias de um corpo de números K não possuem propriedades tão boas como $\mathcal{O}_K$. Por exemplo, elas não são um DFU. Por outro lado, das três propriedades que caracterizam um domínio de Dedekind, as ordens próprias de $\mathcal{O}_K$ só perdem a propriedade de serem integralmente fechadas:

Proposição 8.1. *Seja A uma ordem de K. Então A é um domínio noetheriano e todo ideal primo não-nulo de A é maximal.*

Demonstração. Sendo A um $\mathbb{Z}$-módulo livre finitamente gerado, é claro que A é noetheriano. Seja agora $\mathfrak{p} \lhd A$ primo não-nulo. Como A contém uma base de $K/\mathbb{Q}$, é claro que $\mathfrak{p}$ também contém uma base dessa extensão, de modo que $\mathfrak{p}$ é um $\mathbb{Z}$-módulo de posto n. Esse módulo é livre, pelo Teorema 1.38. Também por esse teorema, dada uma base $\{\alpha_1, \ldots, \alpha_n\}$ de A nós conseguimos inteiros não-nulos $a_1, \ldots, a_n$ tais que o conjunto $\{a_1\alpha_1, \ldots, a_n\alpha_n\}$ seja uma base de $\mathfrak{p}$, e portanto:

$$A/\mathfrak{p} \cong (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z}).$$

Em particular, $A/\mathfrak{p}$ é finito. Como $\mathfrak{p}$ é primo, $A/\mathfrak{p}$ é um domínio finito, e portanto um corpo. Isso mostra que $\mathfrak{p}$ é maximal, como queríamos. □

Em geral, nós temos a seguinte definição:

Definição (Anel de Dimensão 1)**.** Dizemos que um anel A tem dimensão 1 se ele não for um corpo e se todo ideal primo não-nulo de A for maximal.

Assim, as ordens de um corpo de números são domínios noetherianos de dimensão 1. As localizações de $\mathcal{O}_K$ por um conjunto multiplicativo também são domínios noetherianos de dimensão 1. Enquanto as ordens de K não são mais integralmente fechadas, as localizações de $\mathcal{O}_K$ não são mais integrais sobre $\mathbb{Z}$. Desse modo, para estudarmos esses dois importantes tipos de subanéis de K, no que segue consideraremos A como sendo qualquer domínio noetheriano de dimensão 1 com $Q(A) = K$. Começamos mostrando a seguinte propriedade de finitude:

Lema 8.2. *Seja $\mathfrak{a} \lhd A$ não-nulo. Então existe apenas um número finito de ideais primos não-nulos $\mathfrak{p} \lhd A$ tais que $\mathfrak{p} \supseteq \mathfrak{a}$.*

Demonstração. Pelo Corolário 3.9, existem $\mathfrak{p}_1, \dots, \mathfrak{p}_m \lhd A$ primos não-nulos tais que $\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_m$. Assim, se $\mathfrak{p} \lhd A$ for primo não-nulo tal que $\mathfrak{p} \supseteq \mathfrak{a}$, temos $\mathfrak{p} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_m$, e portanto pela Proposição 3.7 nós concluímos que $\mathfrak{p} \supseteq \mathfrak{p}_j$ para $1 \leq j \leq m$. Mas sendo $\mathfrak{p}_j$ maximal, temos $\mathfrak{p} = \mathfrak{p}_j$. Assim, apenas os primos $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ podem conter $\mathfrak{a}$, concluindo a demonstração. □

Com isso, e utilizando um resultado sobre **decomposição primária** (veja por exemplo os capítulos 4 e 7 de [17]), conseguimos provar a seguinte versão do Teorema Chinês dos Restos:

Proposição 8.3. *Seja $\mathfrak{a} \lhd A$ não-nulo. Então nós temos*[1]*:*

$$A/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} = \bigoplus_{\mathfrak{p} \supseteq \mathfrak{a}} A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p},$$

com isomorfismo dado por $x + \mathfrak{a} \mapsto (x + \mathfrak{a}_\mathfrak{p})$. Assim, dados $x_\mathfrak{p} \in A_\mathfrak{p}$, para cada $\mathfrak{p}$, conseguimos achar $x \in A$ tal que $x \equiv x_\mathfrak{p} \pmod{\mathfrak{a}_\mathfrak{p}}$, para todo $\mathfrak{p}$ (note que apenas um número finito dessas congruências é não-trivial).

Demonstração. Se $\mathfrak{p} \not\supseteq \mathfrak{a}$, então $\mathfrak{a}_\mathfrak{p} = A_\mathfrak{p}$, e portanto $A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$ é o anel trivial. Desse modo, vale a última igualdade. Notemos ainda que existe apenas um número finito de primos tais que $\mathfrak{p} \supseteq \mathfrak{a}$, pelo lema acima. Assim, esse último produto é finito. Provemos então que $A/\mathfrak{a} \cong \bigoplus_{\mathfrak{p} \supseteq \mathfrak{a}} A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$. Pelo Teorema 3.31, nós temos $\mathfrak{a} = \bigcap_\mathfrak{p} \mathfrak{a}_\mathfrak{p}$. Assim:

$$\mathfrak{a} = A \cap \mathfrak{a} = \bigcap_{\mathfrak{p}} (A \cap \mathfrak{a}_\mathfrak{p}) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} (A \cap \mathfrak{a}_\mathfrak{p}),$$

pois como já vimos $\mathfrak{a}_\mathfrak{p} = A_\mathfrak{p}$ caso $\mathfrak{p} \not\supseteq \mathfrak{a}$. Suponhamos agora que $\mathfrak{p} \supseteq \mathfrak{a}$. Afirmamos que $\mathfrak{p}$ é o único ideal primo que contém $A \cap \mathfrak{a}_\mathfrak{p}$. De fato, seja $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ uma decomposição primária minimal de $\mathfrak{a}$, que sabemos existir já que A é noetheriano. Notemos que $\mathfrak{a}_\mathfrak{p} = (\mathfrak{q}_1)_\mathfrak{p} \cap \cdots \cap (\mathfrak{q}_m)_\mathfrak{p}$. Dado $\mathfrak{q} \neq 0$ ideal primário, se $\mathfrak{q} \subseteq \mathfrak{p}$ então $\sqrt{\mathfrak{q}} \subseteq \mathfrak{p}$. Como $\sqrt{\mathfrak{q}}$ é um primo não-nulo, e portanto maximal, de A, vemos que $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Com isso, vemos que $\mathfrak{q}_\mathfrak{p}$ será um ideal próprio de $A_\mathfrak{p}$ se e só se $\mathfrak{q}$ for $\mathfrak{p}$-primário. Como $\mathfrak{a}_\mathfrak{p}$ é um ideal próprio de $A_\mathfrak{p}$, pelo menos alguns dos $\mathfrak{q}_j$'s é $\mathfrak{p}$-primário, e como essa decomposição é minimal exatamente um dos $\mathfrak{q}_j$'s é $\mathfrak{p}$-primário. Suponhamos sem perda de generalidade que este seja $\mathfrak{q}_1$. Então vemos que $\mathfrak{a}_\mathfrak{p} = (\mathfrak{q}_1)_\mathfrak{p}$. Assim, $A \cap \mathfrak{a}_\mathfrak{p} = A \cap (\mathfrak{q}_1)_\mathfrak{p}$.

Mostremos que $A \cap (\mathfrak{q}_1)_\mathfrak{p} = \mathfrak{q}_1$. A inclusão ($\supseteq$) é óbvia. Seja então $x = q/s \in A \cap (\mathfrak{q}_1)_\mathfrak{p}$, com $q \in \mathfrak{q}_1$, $s \in A \setminus \mathfrak{p}$. Logo temos $sx = q \in \mathfrak{q}_1$. Como $s \notin \mathfrak{p} = \sqrt{\mathfrak{q}_1}$, devemos ter $x \in \mathfrak{q}_1$, como queríamos. Finalmente, justifiquemos nossa afirmação. Seja $\mathfrak{p}' \lhd A$ primo com $\mathfrak{p}' \supseteq A \cap \mathfrak{a}_\mathfrak{p} = \mathfrak{q}_1$. Então $\mathfrak{p}' \supseteq \sqrt{\mathfrak{q}_1} = \mathfrak{p}$, e pela maximalidade de $\mathfrak{p}$ concluímos que $\mathfrak{p}' = \mathfrak{p}$. Isso prova que $\mathfrak{p}$ é o único primo de A que contém $A \cap \mathfrak{a}_\mathfrak{p}$.

Assim, vemos que para $\mathfrak{p}, \mathfrak{q} \supseteq \mathfrak{a}$ primos com $\mathfrak{p} \neq \mathfrak{q}$, os ideais $A \cap \mathfrak{a}_\mathfrak{p}$ e $A \cap \mathfrak{a}_\mathfrak{q}$ são coprimos, e portanto estamos nas condições de aplicar o Teorema Chinês dos Restos para concluir que:

$$A/\mathfrak{a} = A/\bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} (A \cap \mathfrak{a}_\mathfrak{p}) \cong \bigoplus_{\mathfrak{p} \supseteq \mathfrak{a}} A/(A \cap \mathfrak{a}_\mathfrak{p}) \cong \bigoplus_{\mathfrak{p} \supseteq \mathfrak{a}} A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p},$$

onde a última congruência se demonstra de forma similar ao Corolário 1.49, observando que $(A \cap \mathfrak{a}_\mathfrak{p})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}$ e que $sA + (A \cap \mathfrak{a}_\mathfrak{p}) = A$ para todo $s \in A \setminus \mathfrak{p}$. Finalmente, notemos que os isomorfismos acima nos dão $x + \mathfrak{a} \mapsto (x + (A \cap \mathfrak{a}_\mathfrak{p})) \mapsto (x + \mathfrak{a}_\mathfrak{p})$. □

No caso em que A não é um domínio de Dedekind, o grupo dos ideais fracionários inversíveis $J(A)$ não é todo $I(A)$. Temos o seguinte critério para determinar os ideais fracionários inversíveis de A:

[1] Onde a soma direta abaixo indica que esse é um produto de anéis com apenas um número finito de anéis não-triviais, e $\mathfrak{p}$ varia entre os ideais primos não-nulos de A.

Proposição 8.4. *Seja $M \in I(A)$. Então M é inversível se e só se, para todo ideal primo $\mathfrak{p} \neq 0$ de A, o ideal fracionário $M_\mathfrak{p} \in I(A_\mathfrak{p})$ for principal.*

Demonstração. ($\Rightarrow$): Suponhamos que M seja inversível, e que $N \in I(A)$ seja tal que $MN = A$. Então existem $a_1, \dots, a_r \in M$, $b_1, \dots, b_r \in N$ tais que $a_1b_1 + \cdots + a_rb_r = 1$. Seja $\mathfrak{p} \lhd A$ primo não-nulo. Como $1 \notin \mathfrak{p}_\mathfrak{p}$, algum dos produtos $a_1b_1, \dots, a_rb_r$ não está em $\mathfrak{p}_\mathfrak{p}$.

Suponhamos sem perda de generalidade que $a_1b_1 \notin \mathfrak{p}_\mathfrak{p}$. Então $a_1b_1 \in A_\mathfrak{p} \setminus \mathfrak{p}_\mathfrak{p} = A_\mathfrak{p}^\times$. Afirmamos que $M_\mathfrak{p} = a_1A_\mathfrak{p}$. A inclusão ($\supseteq$) é óbvia. Para a outra inclusão, seja $x \in M_\mathfrak{p}$ qualquer. Notemos que $xb_1 \in M_\mathfrak{p}N_\mathfrak{p} = A_\mathfrak{p}$. Assim, nós temos $x = a_1xb_1(a_1b_1)^{-1} \in a_1A_\mathfrak{p}$, como queríamos.

($\Leftarrow$): Suponhamos que $M_\mathfrak{p}$ seja principal para todo ideal primo $\mathfrak{p} \neq 0$ de A. Assim, para cada $\mathfrak{p}$ existe $a_\mathfrak{p} \in K^\times$ tal que $M_\mathfrak{p} = a_\mathfrak{p}A_\mathfrak{p}$. Como $a_\mathfrak{p} \in M_\mathfrak{p}$, limpando os denominadores dos $a_\mathfrak{p}$'s se necessário nós podemos assumir que $a_\mathfrak{p} \in M$ para todo $\mathfrak{p}$. Afirmamos que o ideal quociente $(A : M) = \{x \in K \colon xM \subseteq A\}$ é o inverso de M. É claro que $(A : M)M \lhd A$. Suponhamos por absurdo que esse seja um ideal próprio de A. Então existiria $\mathfrak{p} \lhd A$ maximal tal que $(A : M)M \subseteq \mathfrak{p}$.

Mostremos que isso não é possível. Sabemos que M é finitamente gerado, e portanto existem $a_1, \dots, a_m \in M$ tais que $M = a_1A + \cdots + a_mA$. Como cada $a_j \in M \subseteq M_\mathfrak{p} = a_\mathfrak{p}A_\mathfrak{p}$, existem $b_j \in A$ e $s_j \in A \setminus \mathfrak{p}$ tais que $a_j = a_\mathfrak{p}b_j/s_j$. Assim, $s_ja_j = a_\mathfrak{p}b_j \in a_\mathfrak{p}A$. Chamando $s := s_1 \cdots s_m$, temos $s \in A \setminus \mathfrak{p}$ e $sa_j \in a_\mathfrak{p}A$ para todo $1 \leq j \leq m$. Assim, $sa_\mathfrak{p}^{-1}a_j \in A$ para todo $1 \leq j \leq m$. Como $a_1, \dots, a_m$ geram M, vemos então que $sa_\mathfrak{p}^{-1}M \subseteq A$, e portanto $sa_\mathfrak{p}^{-1} \in (A : M)$. Mas então nós teríamos $s = sa_\mathfrak{p}^{-1}a_\mathfrak{p} \in (A : M)M \subseteq \mathfrak{p}$, um absurdo! Isso mostra que $M(A : M) = A$, e assim M é inversível, como queríamos. □

Com os resultados acima, conseguimos uma interessante caracterização para o grupo de Picard de A. Lembre que $\mathrm{Pic}(A) = J(A)/P(A)$, onde $J(A)$ é o grupo dos ideais fracionários inversíveis de A e $P(A)$ é o grupo dos ideais fracionários principais de A.

Proposição 8.5. *A correspondência $M \mapsto (M_\mathfrak{p})$ nos dá um isomorfismo $J(A) \cong \bigoplus_\mathfrak{p} P(A_\mathfrak{p})$. Assim, identificando $P(A)$ com sua imagem na soma direta, $\mathrm{Pic}(A) \cong \left(\bigoplus_\mathfrak{p} P(A_\mathfrak{p})\right)/P(A)$.*

Demonstração. Dado $M \in J(A)$, pela proposição acima temos $M_\mathfrak{p} \in P(A_\mathfrak{p})$, para todo ideal primo $\mathfrak{p} \neq 0$ de A. Notemos que $M_\mathfrak{p} = A_\mathfrak{p}$ se e só se $M \cap (A \setminus \mathfrak{p}) \neq \emptyset$ e $M^{-1} \cap (A \setminus \mathfrak{p}) \neq \emptyset$ (a demonstração é igual ao que fizemos na Proposição 3.24). Assim, $M_\mathfrak{p} \neq A_\mathfrak{p}$ se e só se $\mathfrak{p} \supseteq M \cap A$ ou se $\mathfrak{p} \supseteq M^{-1} \cap A$. Mas $M \cap A$ e $M^{-1} \cap A$ são ideais não-nulos de A, e assim existe apenas um número finito de tais primos pelo Lema 8.2. Isso mostra que $M_\mathfrak{p} \neq A_\mathfrak{p}$ apenas para um número finito de $\mathfrak{p}$'s, de modo que $M \mapsto (M_\mathfrak{p})$ nos dá um homomorfismo de grupos $J(A) \to \bigoplus_\mathfrak{p} P(A_\mathfrak{p})$.

Esse homomorfismo é injetor. De fato, suponhamos que $M \in J(A)$ satisfaça $M_\mathfrak{p} = A_\mathfrak{p}$ para todo $\mathfrak{p}$. Então $M \subseteq M_\mathfrak{p} = A_\mathfrak{p}$ para todo $\mathfrak{p}$, e portanto $M \subseteq \bigcap_\mathfrak{p} A_\mathfrak{p} = A$, onde utilizamos o Teorema 3.31. Assim, $M \lhd A$. Devemos ter $M = A$. Caso contrário, haveria um ideal maximal $\mathfrak{p}$ com $M \subseteq \mathfrak{p}$, e nesse caso teríamos $M_\mathfrak{p} \neq A_\mathfrak{p}$, um absurdo! Isso prova a injetividade desse homomorfismo.

Provemos agora que essa função é sobrejetora. Sendo essa função um homomorfismo, basta mostrarmos que, fixados um primo não-nulo $\mathfrak{p} \lhd A$ e $\mathfrak{a}_\mathfrak{p} \lhd A_\mathfrak{p}$ um ideal principal não-nulo, o elemento $(M_\mathfrak{q}) \in \bigoplus_\mathfrak{p} P(A_\mathfrak{p})$ com $M_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}$ e $M_\mathfrak{q} = A_\mathfrak{q}$ para $\mathfrak{q} \neq \mathfrak{p}$ está na sua imagem. Mostraremos que $(M_\mathfrak{q})$ é a imagem de $A \cap \mathfrak{a}_\mathfrak{p} \lhd A$. É fácil ver que $(A \cap \mathfrak{a}_\mathfrak{p})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}$. Assim, basta mostrarmos que para $\mathfrak{q} \neq \mathfrak{p}$ nós temos $(A \cap \mathfrak{a}_\mathfrak{p})_\mathfrak{q} = A_\mathfrak{q}$. Mas isso segue do fato de que $\mathfrak{p}$ é o único ideal primo que contém $A \cap \mathfrak{a}_\mathfrak{p}$, que provamos durante a demonstração da Proposição 8.3. Assim, $A \cap \mathfrak{a}_\mathfrak{p} \mapsto (M_\mathfrak{q})$, como queríamos, mostrando a sobrejetividade. Logo temos de fato um isomorfismo. □

Consideremos agora a **normalização** de um domínio noetheriano de dimensão 1:

Definição (Normalização)**.** Seja A um domínio noetheriano de dimensão 1. Então nós definimos a sua **normalização** $\tilde{A}$ como sendo seu fecho integral em $K = Q(A)$, ou seja, $\tilde{A} := \overline{A}^K$.

A normalização de um domínio noetheriano de dimensão 1 sempre será um domínio de Dedekind, como veremos. Entretanto, isso não é óbvio, pois embora seja claro que $\tilde{A}$ seja integralmente fechado e de dimensão 1, nem sempre $\tilde{A}$ será um A-módulo finitamente gerado. Entretanto, vale a seguinte afirmação um pouco mais fraca, que nos será suficiente:

Lema 8.6. *Seja A um domínio noetheriano de dimensão 1 e seja $\tilde{A}$ sua normalização. Então, para cada ideal $\mathfrak{a} \lhd A$ não-nulo, o quociente $\tilde{A}/\mathfrak{a}\tilde{A}$ é um A-módulo finitamente gerado.*

Demonstração. Seja $\mathfrak{a} \lhd A$ não-nulo, e fixemos $a \in \mathfrak{a}$ não-nulo. Então nós temos $\tilde{A}/\mathfrak{a}\tilde{A} \cong \frac{\tilde{A}/a\tilde{A}}{\mathfrak{a}\tilde{A}/a\tilde{A}}$. Assim, $\tilde{A}/\mathfrak{a}\tilde{A}$ é um quociente de $\tilde{A}/a\tilde{A}$, e portanto basta provarmos que $\tilde{A}/a\tilde{A}$ é um A-módulo finitamente gerado. Comecemos observando que, como aA é um ideal não-nulo, o anel A/aA tem dimensão 0[2]. Sendo um anel noetheriano de dimensão 0, concluímos que A/aA é um anel artiniano. Com isso, vemos que a cadeia descendente de ideais de A,

$$a\tilde{A} \cap A + aA \supseteq a^2\tilde{A} \cap A + aA \supseteq \cdots \supseteq a^m\tilde{A} \cap A + aA \supseteq \cdots$$

se estabiliza. Assim, existe um inteiro positivo n tal que $a^m\tilde{A} \cap A + aA = a^n\tilde{A} \cap A + aA$, para todo $m \geq n$. Afirmamos que $\tilde{A} \subseteq a^{-n}A + a\tilde{A}$. Se provarmos isso, teremos então que $\frac{\tilde{A}}{a\tilde{A}} \subseteq \frac{a^{-n}A + a\tilde{A}}{a\tilde{A}}$. Esse último anel é um A-módulo gerado por $a^{-n} + a\tilde{A}$, e portanto é noetheriano, já que A o é. Em particular, seu submódulo $\tilde{A}/a\tilde{A}$ é finitamente gerado sobre A, como gostaríamos de demonstrar.

Mostremos então que $\tilde{A} \subseteq a^{-n}A + a\tilde{A}$. Seja $\beta \in \tilde{A}$ qualquer. Como $\tilde{A} \subseteq K = Q(A)$, existem $b, c \in A$, $c \neq 0$, tais que $\beta = b/c$. Pelo mesmo argumento acima, vemos que A/cA é artiniano. Assim, denotando $\overline{a} := a + cA$, vemos que a cadeia descendente de ideais de A/cA

$$\langle \overline{a} \rangle \supseteq \langle \overline{a}^2 \rangle \supseteq \cdots \supseteq \langle \overline{a}^m \rangle \supseteq \cdots$$

se estabiliza. Logo existe um inteiro positivo h tal que $\langle \overline{a}^h \rangle = \langle \overline{a}^{h+1} \rangle$. Consequentemente, existe $x \in A$ tal que $a^h \equiv xa^{h+1} \pmod{cA}$, isto é, $(1 - xa)a^h \in cA$. Desse modo, nós temos:

$$\beta = \frac{b}{c} = \frac{b}{c}(1 - xa) + \beta xa = \frac{b}{a^h}\frac{(1 - xa)a^h}{c} + \beta xa \in a^{-h}A + a\tilde{A}.$$

Portanto, existe um inteiro positivo k mínimo para o qual $\beta \in a^{-k}A + a\tilde{A}$. Assim, basta mostrarmos que $k \leq n$, pois então teremos $\beta \in a^{-k}A + a\tilde{A} \subseteq a^{-n}A + a\tilde{A}$, concluindo a demonstração. Suponhamos por absurdo que $k > n$. Como $\beta \in a^{-k}A + a\tilde{A}$, existem $u \in A$, $\tilde{u} \in \tilde{A}$ tais que $\beta = a^{-k}u + a\tilde{u}$. Logo:

$$u = a^k(\beta - a\tilde{u}) \in a^k\tilde{A} \cap A \subseteq a^k\tilde{A} \cap A + aA = a^{k+1}\tilde{A} \cap A + aA,$$

já que $k > n$. Então existem $u' \in A$ e $\tilde{u}' \in \tilde{A}$ tais que $u = a^{k+1}\tilde{u}' + au'$. Desse modo:

$$\beta = a^{-k}u + a\tilde{u} = a^{-k}(a^{k+1}\tilde{u}' + au') + a\tilde{u} = a^{-(k-1)}u' + a(\tilde{u} + \tilde{u}') \in a^{-(k-1)}A + a\tilde{A},$$

um absurdo pela minimalidade de k. Assim, $k \leq n$, concluindo a demonstração. □

Com esse lema, nós conseguimos provar uma generalização do Teorema 3.1, que vale para domínios não necessariamente de Dedekind e extensões de corpos não necessariamente separáveis:

Teorema 8.7 (Krull-Akizuki)**.** *Seja A um domínio noetheriano de dimensão 1 com corpo de frações $K = Q(A)$. Seja L uma extensão finita de K e seja $B = \overline{A}^L$. Então B é um domínio de Dedekind. Em particular, a normalização $\tilde{A} = \overline{A}^K$ de A é um domínio de Dedekind.*

[2]Isto é, todo ideal primo desse anel é maximal.

Demonstração. Provamos que B é integralmente fechado e tem dimensão 1 do mesmo modo que no Teorema 3.1. Assim, basta provarmos que B é noetheriano. Note que não podemos mais aplicar o Teorema 1.37, pois A não é necessariamente integralmente fechado. No lugar desse teorema, utilizaremos o lema acima.

Pelo Teorema 1.16, temos $Q(B) = L$. Assim, existem $\beta_1, \dots, \beta_n \in B$ que formam uma base da extensão L/K. O anel $B_0 \coloneqq A[\beta_1, \dots, \beta_n]$ é um A-módulo finitamente gerado, e portanto é noetheriano já que A o é. Como a extensão B_0/A é integral, podemos utilizar o Teorema 1.53 para concluir que B_0 tem dimensão 1. Notemos ainda que $\overline{B}_0^L = B$. Assim, B é a normalização de B_0, e podemos nos restringir ao caso em que $L = K$ e $B = \tilde{A}$ é a normalização de A.

Queremos mostrar que todo ideal $\mathfrak{A}$ de $\tilde{A}$ é finitamente gerado. Pelo Teorema 1.53, nós temos $\mathfrak{A} \cap A \neq 0$. Escolhamos $a \in \mathfrak{A} \cap A$ não-nulo. Pelo lema acima, vemos que $\tilde{A}/a\tilde{A}$ é um A-módulo finitamente gerado, logo noetheriano. Assim, seu submódulo $\mathfrak{A}/a\tilde{A}$ também é um A-módulo finitamente gerado. Desse modo, existem $\alpha_1, \dots, \alpha_m \in \mathfrak{A}$ tais que $\alpha_1 + a\tilde{A}, \dots, \alpha_m + a\tilde{A} \in \mathfrak{A}/a\tilde{A}$ geram $\mathfrak{A}/a\tilde{A}$ como A-módulo. Afirmamos que $\alpha_1, \dots, \alpha_m, a$ geram $\mathfrak{A}$ como $\tilde{A}$-módulo. De fato, seja $x \in \mathfrak{A}$ qualquer. Então existem $c_1, \dots, c_m \in A$ tais que

$$x + a\tilde{A} = c_1(\alpha_1 + a\tilde{A}) + \cdots + c_m(\alpha_m + a\tilde{A}) = (c_1\alpha_1 + \cdots + c_m\alpha_m) + a\tilde{A}.$$

Assim, existe $c \in \tilde{A}$ tal que $x = c_1\alpha_1 + \cdots + c_m\alpha_m + ca$, como queríamos. Isso mostra que $\tilde{A}$ é noetheriano, concluindo a demonstração. □

Observe que essa demonstração seria bastante simplificada se tivéssemos suposto que $\tilde{A}$ é um A-módulo finitamente gerado. Para o que se segue, de fato, nós assumiremos essa hipótese, que evitará casos patológicos. Note que, se A for uma ordem de um corpo de números K, isso ocorrerá. De fato, nesse caso $\tilde{A} = \mathcal{O}_K$, e qualquer base integral de $\mathcal{O}_K$ também é uma base de $\mathcal{O}_K$ como A-módulo. Com essa hipótese extra, nós conseguimos comparar os grupos de unidades e de Picard de A e de sua normalização:

Proposição 8.8. *Existe uma sequência exata canônica*

$$1 \to A^\times \to \tilde{A}^\times \to \bigoplus_{\mathfrak{p}} \tilde{A}_{\mathfrak{p}}^\times / A_{\mathfrak{p}}^\times \to \operatorname{Pic}(A) \to \operatorname{Pic}(\tilde{A}) \to 1,$$

onde $\tilde{A}_{\mathfrak{p}} = \overline{A}_{\mathfrak{p}}^K$ é a normalização de $A_{\mathfrak{p}}$, ou equivalentemente a localização de $\tilde{A}$ por $A \setminus \mathfrak{p}$ (lembre que localização comuta com fecho integral).

Demonstração. A ideia é usar as sequências exatas:

$$\begin{aligned} 1 &\to P(A) \to J(A) \to \operatorname{Pic}(A) \to 1, \text{ e} \\ 1 &\to P(\tilde{A}) \to J(\tilde{A}) \to \operatorname{Pic}(\tilde{A}) \to 1. \end{aligned}$$

Observemos que, dado R domínio qualquer com $K = Q(R)$, temos $P(R) \cong K^\times/R^\times$. Esse isomorfismo é induzido pelo homomorfismo $K^\times \to P(R)$ dado por $x \mapsto xR$. Desse modo, nós obtemos as sequências exatas:

$$\begin{aligned} 1 &\to K^\times/A^\times \to J(A) \to \operatorname{Pic}(A) \to 1, \text{ e} \\ 1 &\to K^\times/\tilde{A}^\times \to J(\tilde{A}) \to \operatorname{Pic}(\tilde{A}) \to 1. \end{aligned}$$

Notemos ainda que, pelas observações acima e pela Proposição 8.5, nós temos:

$$J(A) \cong \bigoplus_{\mathfrak{p}} P(A_{\mathfrak{p}}) \cong \bigoplus_{\mathfrak{p}} K^\times/A_{\mathfrak{p}}^\times.$$

Calculemos agora $J(\tilde{A})$. Pela Proposição 8.5, nós temos $J(\tilde{A}) \cong \bigoplus_{\tilde{\mathfrak{p}}} P(A_{\tilde{\mathfrak{p}}})$, onde $\tilde{\mathfrak{p}}$ varia entre os primos não-nulos de $\tilde{A}$. Dado um primo não-nulo $\mathfrak{p} \lhd A$ qualquer, como $\tilde{A}$ é domínio de Dedekind

vemos que existe um número finito de primos sobre $\mathfrak{p}$ (a saber, os fatores primos de $\mathfrak{p}\tilde{A}$). Da mesma forma, para cada $\mathfrak{p} \lhd A$ primo não-nulo, vemos que existe um número finito de primos de $\tilde{A}_\mathfrak{p}$ sobre cada ideal primo de $A_\mathfrak{p}$. Mas o único primo não-nulo de $A_\mathfrak{p}$ é $\mathfrak{p}_\mathfrak{p}$, de modo que $\tilde{A}_\mathfrak{p}$ possui um número finito de primos. Assim, pelo Teorema 3.23, $\tilde{A}_\mathfrak{p}$ é um DIP. Note que os ideais primos não-nulos de $\tilde{A}_\mathfrak{p}$ são os ideais da forma $\tilde{\mathfrak{p}}_\mathfrak{p}$, para $\tilde{p}$ ideal primo não-nulo de $\tilde{A}$ tal que $\tilde{\mathfrak{p}} \cap A \subseteq \mathfrak{p}$. Como $\tilde{\mathfrak{p}} \cap A$ é um primo não-nulo de A, e portanto um ideal maximal, devemos ter $\tilde{\mathfrak{p}} \cap A = \mathfrak{p}$. Ou seja, os ideais primos não-nulos de $\tilde{A}_\mathfrak{p}$ são os ideais da forma $\tilde{\mathfrak{p}}_\mathfrak{p}$ para $\tilde{\mathfrak{p}}$ sobre $\mathfrak{p}$.

Assim, pela Proposição 8.5, nós temos:

$$P(\tilde{A}_\mathfrak{p}) = J(\tilde{A}_\mathfrak{p}) \cong \bigoplus_{\tilde{\mathfrak{p}}|\mathfrak{p}} P((\tilde{A}_\mathfrak{p})_{\tilde{\mathfrak{p}}_\mathfrak{p}}) = \bigoplus_{\tilde{\mathfrak{p}}|\mathfrak{p}} P(\tilde{A}_{\tilde{\mathfrak{p}}}),$$

onde a última igualdade segue de $(\tilde{A}_\mathfrak{p})_{\tilde{\mathfrak{p}}_\mathfrak{p}} = \tilde{A}_{\tilde{\mathfrak{p}}}$, que é fácil de verificar. Observemos agora que cada primo $\tilde{\mathfrak{p}}$ de $\tilde{A}$ está sobre exatamente um primo $\mathfrak{p}$ de A. Desse modo:

$$J(\tilde{A}) \cong \bigoplus_{\tilde{\mathfrak{p}}} P(\tilde{A}_{\tilde{\mathfrak{p}}}) = \bigoplus_{\mathfrak{p}} \bigoplus_{\tilde{\mathfrak{p}}|\mathfrak{p}} P(\tilde{A}_{\tilde{\mathfrak{p}}}) \cong \bigoplus_{\mathfrak{p}} P(\tilde{A}_\mathfrak{p}) \cong \bigoplus_{\mathfrak{p}} K^\times / \tilde{A}_\mathfrak{p}^\times.$$

Com isso, nós temos sequências exatas

$$1 \to K^\times / A^\times \to \bigoplus_{\mathfrak{p}} K^\times / A_\mathfrak{p}^\times \to \operatorname{Pic}(A) \to 1, \text{ e}$$
$$1 \to K^\times / \tilde{A}^\times \to \bigoplus_{\mathfrak{p}} K^\times / \tilde{A}_\mathfrak{p}^\times \to \operatorname{Pic}(\tilde{A}) \to 1.$$

Consideremos o homomorfismo $\alpha\colon K^\times / A^\times \to K^\times / \tilde{A}^\times$ dado por $xA^\times \mapsto x\tilde{A}^\times$. É fácil ver que α está bem-definido, é sobrejetor e $\ker\alpha = \tilde{A}^\times / A^\times$. Da mesma forma, podemos definir $\beta\colon \bigoplus_\mathfrak{p} K^\times / A_\mathfrak{p}^\times \to \bigoplus_\mathfrak{p} K^\times / \tilde{A}_\mathfrak{p}^\times$ dado por $(x_\mathfrak{p} A_\mathfrak{p}^\times) \mapsto (x_\mathfrak{p} \tilde{A}_\mathfrak{p}^\times)$. Então β está bem-definido, é sobrejetor e $\ker\beta = \bigoplus_\mathfrak{p} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times$. Podemos ainda definir $\gamma\colon \operatorname{Pic}(A) \to \operatorname{Pic}(\tilde{A})$ por $[M] \mapsto [M\tilde{A}]$. Com isso, nós temos o seguinte diagrama comutativo:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K^\times / A^\times & \longrightarrow & \bigoplus_\mathfrak{p} K^\times / A_\mathfrak{p}^\times & \longrightarrow & \operatorname{Pic}(A) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
1 & \longrightarrow & K^\times / \tilde{A}^\times & \longrightarrow & \bigoplus_\mathfrak{p} K^\times / \tilde{A}_\mathfrak{p}^\times & \longrightarrow & \operatorname{Pic}(\tilde{A}) & \longrightarrow & 1
\end{array}$$

Aplicando o Lema da Serpente a esse diagrama, obtemos então uma sequência exata canônica

$$1 \to \ker\alpha \to \ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma \to 1.$$

Como α e β são sobrejetores, vemos que γ também deve ser sobrejetor, e assim nós temos a sequência exata:

$$1 \to \tilde{A}^\times / A^\times \to \bigoplus_{\mathfrak{p}} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times \to \ker\gamma \to 1.$$

Como o homomorfismo $\tilde{A}^\times / A^\times \to \bigoplus_\mathfrak{p} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times$ é induzido por um homomorfismo $\tilde{A}^\times \to \bigoplus_\mathfrak{p} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times$, podemos expandir essa sequência exata para a sequência exata:

$$1 \to A^\times \to \tilde{A}^\times \to \bigoplus_{\mathfrak{p}} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times \to \ker\gamma \to 1.$$

Consideremos agora a composição $\bigoplus_\mathfrak{p} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times \to \ker\gamma \hookrightarrow \operatorname{Pic}(A)$. Essa função possui o mesmo núcleo de $\bigoplus_\mathfrak{p} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times \to \ker\gamma$, e possui imagem $\ker\gamma$, que é igual ao núcleo da função sobrejetora $\operatorname{Pic}(A) \xrightarrow{\gamma} \operatorname{Pic}(\tilde{A})$. Desse modo, obtemos a sequência exata:

$$1 \to A^\times \to \tilde{A}^\times \to \bigoplus_{\mathfrak{p}} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times \to \operatorname{Pic}(A) \to \operatorname{Pic}(\tilde{A}) \to 1,$$

como queríamos. □

Definição (Ideal Primo Regular)**.** Um ideal primo $\mathfrak{p} \lhd A$ não-nulo é chamado de **regular** se $A_\mathfrak{p}$ for integralmente fechado, ou equivalentemente se $A_\mathfrak{p}$ for um DVD.

Observemos que, para os ideais primos regulares $\mathfrak{p}$, nós temos $\tilde{A}_\mathfrak{p} = A_\mathfrak{p}$, e assim os somandos $\tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times$ que aparecem na proposição acima são triviais para esses primos. Afirmamos que existe apenas um número finito de ideais primos não-regulares, e que eles são exatamente os divisores do condutor $\mathfrak{f} := \{a \in A \colon a\tilde{A} \subseteq A\}$ de A em $\tilde{A}$. Lembremos que $\mathfrak{f}$ é o maior ideal de $\tilde{A}$ contido em A. Como estamos supondo que $\tilde{A}$ é finitamente gerado como A-módulo, existem $\tilde{a}_1, \ldots, \tilde{a}_m \in \tilde{A}$ que geram $\tilde{A}$ como A-módulo. Uma vez que $K = Q(A)$, podemos escrever, para $1 \leq j \leq m$, $\tilde{a}_j = a_j/b_j$, para $a_j, b_j \in A$, $b_j \neq 0$. Chamando $b := b_1 \cdots b_m$, vemos então que $b\tilde{a}_j \in A$ para todo $1 \leq j \leq m$, e portanto $b\tilde{A} \subseteq A$. Assim, $b \in \mathfrak{f}$. Como $b \neq 0$, temos que $\mathfrak{f} \neq 0$.

Proposição 8.9. *Dado $\mathfrak{p} \lhd A$ primo não-nulo, nós temos $\mathfrak{p} \nmid \mathfrak{f}$ (isto é, $\mathfrak{p} \not\supseteq \mathfrak{f}$) se e só se $\mathfrak{p}$ for regular. Se esse for o caso, então $\tilde{\mathfrak{p}} := \mathfrak{p}\,\tilde{A}$ é um ideal primo de $\tilde{A}$ e $A_\mathfrak{p} = \tilde{A}_{\tilde{\mathfrak{p}}}$.*

Demonstração. ($\Rightarrow$): Suponhamos que $\mathfrak{p} \nmid \mathfrak{f}$, isto é, $\mathfrak{p} \not\supseteq \mathfrak{f}$. Então existe $t \in \mathfrak{f} \setminus \mathfrak{p}$. Assim, $t\tilde{A} \subseteq A \Rightarrow \tilde{A} \subseteq \frac{1}{t}A \subseteq A_\mathfrak{p}$. Com isso, podemos definir $\tilde{\mathfrak{p}} := \mathfrak{p}_\mathfrak{p} \cap \tilde{A}$. Então $\tilde{\mathfrak{p}}$ é um ideal primo de $\tilde{A}$ e $\tilde{\mathfrak{p}} \cap A = \mathfrak{p}_\mathfrak{p} \cap A \supseteq \mathfrak{p}$. Como $\mathfrak{p}$ é maximal, temos então $\mathfrak{p} = \tilde{\mathfrak{p}} \cap A$. Desse modo, $A_\mathfrak{p} \subseteq \tilde{A}_{\tilde{\mathfrak{p}}}$. Mostremos que vale também a inclusão reversa. Dado $a/s \in \tilde{A}_{\tilde{\mathfrak{p}}}$, com $a \in \tilde{A}$ e $s \in \tilde{A} \setminus \tilde{\mathfrak{p}}$, nós temos $ta \in A$ e $ts \in A \setminus \mathfrak{p}$, de modo que $a/s = ta/(ts) \in A_\mathfrak{p}$. Isso prova que $A_\mathfrak{p} = \tilde{A}_{\tilde{\mathfrak{p}}}$.

Como $\tilde{A}$ é domínio de Dedekind, vemos então que $A_\mathfrak{p} = \tilde{A}_{\tilde{\mathfrak{p}}}$ é um DVD, o que prova que $\mathfrak{p}$ é regular. Podemos ainda mostrar que $\tilde{\mathfrak{p}} = \mathfrak{p}\,\tilde{A}$. Se $\tilde{\mathfrak{q}} \lhd \tilde{A}$ for um ideal primo não-nulo sobre $\mathfrak{p}$, então $\tilde{A}_{\tilde{\mathfrak{p}}} = A_\mathfrak{p} \subseteq \tilde{A}_{\tilde{\mathfrak{q}}}$. Como o único primo não-nulo de $\tilde{A}_{\tilde{\mathfrak{p}}}$ é $\tilde{\mathfrak{p}}_{\tilde{\mathfrak{p}}}$, nós temos $\tilde{\mathfrak{p}}_{\tilde{\mathfrak{p}}} = \tilde{\mathfrak{q}}_{\tilde{\mathfrak{q}}} \cap \tilde{A}_{\tilde{\mathfrak{p}}}$. Assim:

$$\tilde{\mathfrak{q}} = \tilde{\mathfrak{q}}_{\tilde{\mathfrak{q}}} \cap \tilde{A} = \tilde{\mathfrak{p}}_{\tilde{\mathfrak{p}}} \cap \tilde{A} = \tilde{\mathfrak{p}}.$$

Isso mostra que o único primo na fatoração de $\mathfrak{p}\,\tilde{A}$ é $\tilde{\mathfrak{p}}$. Assim, existe e inteiro positivo tal que $\mathfrak{p}\,\tilde{A} = \tilde{\mathfrak{p}}^e$. Agora, observemos que no domínio de Dedekind $A_\mathfrak{p}$ nós temos:

$$\mathfrak{p}_\mathfrak{p} = \mathfrak{p}\,A_\mathfrak{p} = (\mathfrak{p}\,\tilde{A})A_\mathfrak{p} = \tilde{\mathfrak{p}}^e A_\mathfrak{p} = \tilde{\mathfrak{p}}_\mathfrak{p}^e = \mathfrak{p}_\mathfrak{p}^e,$$

onde a última igualdade segue de $\tilde{\mathfrak{p}}_\mathfrak{p} = (\mathfrak{p}_\mathfrak{p} \cap \tilde{A})_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$. Assim, pela fatoração única nós concluímos que $e = 1$, e portanto $p\tilde{A} = \tilde{\mathfrak{p}}$.

($\Leftarrow$): Suponhamos que $\mathfrak{p}$ seja um primo regular. Então $A_\mathfrak{p}$ é integralmente fechado. Como $A \subseteq A_\mathfrak{p}$, temos então $\tilde{A} = \overline{A}^K \subseteq A_\mathfrak{p}$. Sejam $\tilde{a}_1, \ldots, \tilde{a}_m$ geradores de $\tilde{A}$ como A-módulo. Como $\tilde{A} \subseteq A_\mathfrak{p}$, podemos escrever, para $1 \leq j \leq m$, $\tilde{a}_j = a_j/s_j$, para alguns $a_j \in A$, $s_j \in A \setminus \mathfrak{p}$. Chamemos $s := s_1 \cdots s_m \in A \setminus \mathfrak{p}$. Então $s\tilde{a}_j \in A$ para todo $1 \leq j \leq m$. Como os $\tilde{a}_j$'s geram $\tilde{A}$, vemos que $s\tilde{A} \subseteq A$, de modo que $s \in \mathfrak{f}$. Assim, $s \in \mathfrak{f} \setminus \mathfrak{p}$, o que prova que $\mathfrak{p} \not\supseteq \mathfrak{f}$, ou seja, $\mathfrak{p} \nmid \mathfrak{f}$. □

Podemos agora obter uma descrição mais simples para a soma direta $\bigoplus_\mathfrak{p} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times$ que aparece na Proposição 8.8:

Proposição 8.10. $\bigoplus_\mathfrak{p} \tilde{A}_\mathfrak{p}^\times / A_\mathfrak{p}^\times \cong (\tilde{A}/\mathfrak{f})^\times / (A/\mathfrak{f})^\times$.

Demonstração. A ideia é utilizar o Teorema Chinês dos Restos 8.3 e uma estratégia parecida com a que adotamos na Proposição 8.8. Por um lado, aplicando 8.3 ao ideal $\mathfrak{f} \lhd A$, nós obtemos:

$$A/\mathfrak{f} \cong \bigoplus_\mathfrak{p} A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p}. \tag{8.1}$$

Aplicando agora esse resultado ao ideal $\mathfrak{f} \lhd \tilde{A}$, nós obtemos:

$$\tilde{A}/\mathfrak{f} \cong \bigoplus_{\tilde{\mathfrak{p}}} \tilde{A}_{\tilde{\mathfrak{p}}}/\mathfrak{f}_{\tilde{\mathfrak{p}}} = \bigoplus_\mathfrak{p} \bigoplus_{\tilde{\mathfrak{p}} \mid \mathfrak{p}} \tilde{A}_{\tilde{\mathfrak{p}}}/\mathfrak{f}_{\tilde{\mathfrak{p}}}.$$

Dado agora $\mathfrak{p} \lhd A$ primo não-nulo qualquer, como já vimos na demonstração da Proposição 8.8 os ideais primos não-nulos de $\tilde{A}_\mathfrak{p}$ são os ideais da forma $\tilde{\mathfrak{p}}_\mathfrak{p}$ para $\tilde{\mathfrak{p}} \lhd \tilde{A}$ sobre $\mathfrak{p}$. Notemos ainda que, como $\mathfrak{f}$ é um ideal de $\tilde{A}$ contido em A, nós temos $\mathfrak{f}\tilde{A}_\mathfrak{p} = \mathfrak{f}_\mathfrak{p}$. Desse modo, aplicando 8.3 ao ideal $\mathfrak{f}_\mathfrak{p} = \mathfrak{f}\tilde{A}_\mathfrak{p} \lhd \tilde{A}_\mathfrak{p}$, nós obtemos:

$$\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p} \cong \bigoplus_{\tilde{\mathfrak{p}}|\mathfrak{p}} (\tilde{A}_\mathfrak{p})_{\tilde{\mathfrak{p}}_\mathfrak{p}}/(\mathfrak{f}_\mathfrak{p})_{\tilde{\mathfrak{p}}_\mathfrak{p}} = \bigoplus_{\tilde{\mathfrak{p}}|\mathfrak{p}} \tilde{A}_{\tilde{\mathfrak{p}}}/\mathfrak{f}_{\tilde{\mathfrak{p}}},$$

onde a última igualdade segue de $(\tilde{A}_\mathfrak{p})_{\tilde{\mathfrak{p}}_\mathfrak{p}} = \tilde{A}_{\tilde{\mathfrak{p}}}$ e $(\mathfrak{f}_\mathfrak{p})_{\tilde{\mathfrak{p}}_\mathfrak{p}} = \mathfrak{f}_{\tilde{\mathfrak{p}}}$, como é fácil verificar. Desse modo:

$$\tilde{A}/\mathfrak{f} \cong \bigoplus_{\mathfrak{p}} \bigoplus_{\tilde{\mathfrak{p}}|\mathfrak{p}} \tilde{A}_{\tilde{\mathfrak{p}}}/\mathfrak{f}_{\tilde{\mathfrak{p}}} \cong \bigoplus_{\mathfrak{p}} \tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p}. \tag{8.2}$$

Observando que o isomorfismo de (8.1) é dado pela restrição do isomorfismo de (8.2), restringindo esses isomorfismos aos grupos de unidades $(\tilde{A}/\mathfrak{f})^\times$ e $(A/\mathfrak{f})^\times$ e quocientando nós obtemos:

$$(\tilde{A}/\mathfrak{f})^\times/(A/\mathfrak{f})^\times \cong \bigoplus_{\mathfrak{p}} (\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times/(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times. \tag{8.3}$$

Para $\mathfrak{p}$ regular, nós temos $\tilde{A}_\mathfrak{p} = A_\mathfrak{p}$, e portanto $(\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times/(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times = 1$. Consideremos então o caso $\mathfrak{p}$ não-regular, isto é, $\mathfrak{p} \supseteq \mathfrak{f}$. Nós temos um homomorfismo $\varphi\colon \tilde{A}_\mathfrak{p}^\times \to (\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times/(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times$ dado por $x \mapsto (x + \mathfrak{f}_\mathfrak{p})(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times$. Esse homomorfismo é sobrejetor. De fato, seja

$$(\varepsilon + \mathfrak{f}_\mathfrak{p})(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times \in (\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times/(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times$$

qualquer, para $\varepsilon \in \tilde{A}_\mathfrak{p}$. Então $\varepsilon + \mathfrak{f}_\mathfrak{p}$ é uma unidade de $\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p}$, de modo que $\varepsilon + \mathfrak{f}_\mathfrak{p}$ não está em nenhum ideal maximal de $\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p}$. Um ideal maximal de $\tilde{A}_\mathfrak{p}$ é da forma $\tilde{\mathfrak{p}}_\mathfrak{p}$, para $\tilde{\mathfrak{p}} \lhd \tilde{A}$ maximal sobre $\mathfrak{p}$. Como $\mathfrak{f} \subseteq \mathfrak{p} \subseteq \tilde{\mathfrak{p}}$, temos $\mathfrak{f}_\mathfrak{p} \subseteq \tilde{\mathfrak{p}}_\mathfrak{p}$, e portanto $\tilde{\mathfrak{p}}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p}$ é um ideal maximal de $\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p}$. Isso significa que $\varepsilon + \mathfrak{p} \notin \tilde{\mathfrak{p}}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p}$, e portanto $\varepsilon \notin \tilde{\mathfrak{p}}_\mathfrak{p}$. Assim, ε é um elemento de $\tilde{A}_\mathfrak{p}$ que não está contido em nenhum ideal maximal de $\tilde{A}_\mathfrak{p}$, o que mostra que $\varepsilon \in \tilde{A}_\mathfrak{p}^\times$. Logo $(\varepsilon + \mathfrak{f}_\mathfrak{p})(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times = \varphi(\varepsilon)$, mostrando que φ é sobrejetor.

Notemos agora que, dado $x \in \tilde{A}_\mathfrak{p}$, temos $x \in \ker\varphi \iff x + \mathfrak{f}_\mathfrak{p} \in (A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times$. Como $\mathfrak{f}_\mathfrak{p} \subseteq \mathfrak{p}_\mathfrak{p}$ e $\mathfrak{p}_\mathfrak{p}$ é o único ideal maximal de $A_\mathfrak{p}$, vemos que $x + \mathfrak{f}_\mathfrak{p} \in (A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times \iff x \in A_\mathfrak{p}^\times$. Assim, $\ker\varphi = A_\mathfrak{p}^\times$. Desse modo, pelo Teorema do Isomorfismo:

$$(\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times/(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times = \operatorname{im}\varphi \cong \tilde{A}_\mathfrak{p}^\times/\ker\varphi = \tilde{A}_\mathfrak{p}^\times/A_\mathfrak{p}^\times.$$

É claro que esse isomorfismo vale também para os primos regulares, pois nesse caso ambos os lados do isomorfismo acima são os grupos triviais. Desse modo, a partir de (8.3) nós obtemos:

$$(\tilde{A}/\mathfrak{f})^\times/(A/\mathfrak{f})^\times \cong \bigoplus_{\mathfrak{p}} (\tilde{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times/(A_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times \cong \bigoplus_{\mathfrak{p}} \tilde{A}_\mathfrak{p}^\times/A_\mathfrak{p}^\times,$$

concluindo a demonstração. □

Como consequência direta das Proposições 8.8 e 8.10, nós obtemos:

Teorema 8.11. *Sejam A um domínio noetheriano de dimensão 1 e $\tilde{A}$ sua normalização. Então existe uma sequência exata canônica*

$$1 \to A^\times \to \tilde{A}^\times \to (\tilde{A}/\mathfrak{f})^\times/(A/\mathfrak{f})^\times \to \operatorname{Pic}(A) \to \operatorname{Pic}(\tilde{A}) \to 1,$$

onde $\mathfrak{f}$ é o condutor de A em $\tilde{A}$.

No caso em que A é uma ordem de um corpo de números K, o teorema acima nos dá a sequência exata

$$1 \to A^\times \to \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{f})^\times/(A/\mathfrak{f})^\times \to \operatorname{Pic}(A) \to \mathscr{C}\ell(\mathcal{O}_K) \to 1.$$

Isso nos dá:

Teorema 8.12. *Seja K um corpo de números, e seja A uma ordem de K. Então os grupos $\mathcal{O}_K^\times/A^\times$ e $\mathrm{Pic}(A)$ são finitos, e vale a relação*

$$|\mathrm{Pic}(A)| = \frac{h_K}{(\mathcal{O}_K^\times : A^\times)} \frac{|(\mathcal{O}_K/\mathfrak{f})^\times|}{|(A/\mathfrak{f})^\times|}.$$

Além disso, $A^\times$ é um $\mathbb{Z}$-módulo livre de mesmo posto[3] *de $\mathcal{O}_K^\times$.*

Demonstração. Como $\mathfrak{f} \lhd \mathcal{O}_K$, temos $|\mathcal{O}_K/\mathfrak{f}| = \mathfrak{N}(\mathfrak{f}) < \infty$. Assim, os grupos $(\mathcal{O}_K/\mathfrak{f})^\times$ e $(A/\mathfrak{f})^\times$ são finitos. Além disso, como o morfismo $\mathrm{Pic}(A) \to \mathscr{C}\ell(\mathcal{O}_K)$ é sobrejetor, $\mathscr{C}\ell(\mathcal{O}_K)$ é finito e o núcleo desse morfismo é a imagem do morfismo saindo do grupo finito $(\mathcal{O}_K/\mathfrak{f})^\times/(A/\mathfrak{f})^\times$, vemos que $\mathrm{Pic}(A)$ é finito. Desse modo, os únicos grupos possivelmente infinitos que aparecem na sequência exata acima são $A^\times$ e $\mathcal{O}_K^\times$, de onde obtemos que $A^\times$ e $\mathcal{O}_K^\times$ possuem o mesmo posto. A partir da sequência exata acima, nós podemos ainda obter uma sequência exata:

$$1 \to \mathcal{O}_K^\times/A^\times \xrightarrow{\alpha} (\mathcal{O}_K/\mathfrak{f})^\times/(A/\mathfrak{f})^\times \xrightarrow{\beta} \mathrm{Pic}(A) \xrightarrow{\gamma} \mathscr{C}\ell(\mathcal{O}_K) \to 1.$$

Disso obtemos também a finitude de $\mathcal{O}_K^\times/A^\times$. Finalmente, vamos encontrar uma relação entre os tamanhos desses grupos. Essa sequência exata nos dá

$$\mathscr{C}\ell(\mathcal{O}_K) = \operatorname{im}\gamma \cong \mathrm{Pic}(A)/\ker\gamma = \mathrm{Pic}(A)/\operatorname{im}\beta,$$

e também

$$\operatorname{im}\beta \cong \frac{(\mathcal{O}_K/\mathfrak{f})^\times/(A/\mathfrak{f})^\times}{\ker\beta} = \frac{(\mathcal{O}_K/\mathfrak{f})^\times/(A/\mathfrak{f})^\times}{\operatorname{im}\alpha}.$$

Assim:

$$|\mathrm{Pic}(A)| = |\mathscr{C}\ell(\mathcal{O}_K)||\operatorname{im}\beta| = h_K \frac{|(\mathcal{O}_K/\mathfrak{f})^\times/(A/\mathfrak{f})^\times|}{|\operatorname{im}\alpha|} = \frac{h_K}{(\mathcal{O}_K^\times : A^\times)} \frac{|(\mathcal{O}_K/\mathfrak{f})^\times|}{|(A/\mathfrak{f})^\times|}.$$

□

A definição do grupo de Picard $\mathrm{Pic}(A)$ de um domínio A qualquer nos restringe apenas ao estudo dos ideais fracionários inversíveis de A. No caso em que A é noetheriano mas não é um domínio de Dedekind, existe pelo menos um ideal primo não inversível de A, pois caso contrário mostraríamos que $I(A) = J(A)$ do mesmo modo que nos itens (b) e (c) do Teorema 3.11. Assim, quando nos restringimos a $\mathrm{Pic}(A) = J(A)/P(A)$, estamos ignorando alguns ideais primos de A. No caso em que A é um domínio noetheriano de dimensão 1, é possível construir outro grupo a partir de A, o chamado **grupo de classes de divisores**, ou **grupo de Chow** de A, que leva em conta todos os ideais primos de A, e tem sua construção baseada numa reintrodução artificial da fatoração única. Terminaremos este capítulo com a definição desse importante grupo.

Começamos definindo o **grupo dos divisores** de A como sendo o grupo abeliano livre $\mathrm{Div}(A) := \bigoplus_{\mathfrak{p}} \mathbb{Z}\,\mathfrak{p}$ que tem como base o conjunto dos ideais primos não-nulos de A. Assim, cada elemento de $\mathrm{Div}(A)$ é uma soma formal $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\,\mathfrak{p}$, onde apenas um número finito dos coeficientes $n_{\mathfrak{p}}$'s é não-nulo. Os elementos de $\mathrm{Div}(A)$ são chamados de **divisores**, ou **0-ciclos**, de A. Notemos que quando A é um domínio de Dedekind nós temos $I(A) \cong \mathrm{Div}(A)$, e a cada elemento $f \in K^\times$ nós podemos associar um elemento $\mathrm{div}(f) \in \mathrm{Div}(A)$ dado por $\mathrm{div}(f) := \sum_{\mathfrak{p}} v_{\mathfrak{p}}(f)\,\mathfrak{p}$. Note que os coeficientes de $\mathrm{div}(f)$ nada mais são do que os expoentes da fatoração prima de fA, pela Proposição 3.33. Desse modo, obtemos um homomorfismo $\mathrm{div}\colon K^\times \to \mathrm{Div}(A)$.

No caso geral em que A é um domínio noetheriano de dimensão 1, podem existir primos $\mathfrak{p} \lhd A$ não-nulos para os quais $A_{\mathfrak{p}}$ não é um DVD, de modo que não temos uma valoração associada a

[3] Note que já havíamos concluído essa parte a partir do Teorema das Unidades de Dirichlet, e que esse posto é de fato $r_1 + r_2 - 1$.

esses anéis. Mesmo assim, podemos definir um homomorfismo $\operatorname{ord}_{\mathfrak{p}}\colon K^\times \to \mathbb{Z}$ que generaliza uma valoração. Para definir esse homomorfismo, daremos uma outra interpretação para a valoração $v\colon K^\times \to \mathbb{Z}$ de um DVD B com único ideal maximal $\mathfrak{m}$. Sabemos que, dado $x \in B$ não-nulo, $v(x)$ é o inteiro positivo caracterizado pela expressão $xB = \mathfrak{m}^{v(x)}$. Como todo ideal de B é uma potência não-negativa de $\mathfrak{m}$, vemos que os únicos ideais de B que contêm xB são $B, \mathfrak{m}, \mathfrak{m}^2, \ldots, \mathfrak{m}^{v(x)} = xB$, e que temos a cadeia

$$B \supsetneq \mathfrak{m} \supsetneq \mathfrak{m}^2 \supseteq \cdots \supseteq \mathfrak{m}^{v(x)} = xB.$$

Isso significa que o comprimento do B-módulo B/xB é $\ell_B(B/xB) = v(x)$. Dado agora um elemento $a = x/y \in K^\times$ qualquer, com $x, y \in B$, $y \neq 0$, nós temos:

$$v(a) = v(x/y) = v(x) - v(y) = \ell_B(B/xB) - \ell_B(B/yB).$$

No caso em que B é apenas um domínio noetheriano de dimensão 1 nós podemos definir uma função $\operatorname{ord}\colon A \setminus \{0\} \to \mathbb{N}^*$ dada por $\operatorname{ord}(x) = \ell_B(B/xB)$. Note que essa função está bem-definida. De fato, B/xB é um anel noetheriano de dimensão 0, e portanto também artiniano. Isso nos diz que B/xB é noetheriano e artiniano também como B-módulo, sendo assim um B-módulo de comprimento finito.

Afirmamos que ord é homomorfismo de semigrupos, isto é, que $\operatorname{ord}(xy) = \operatorname{ord}(x) + \operatorname{ord}(y)$. Isso equivale a mostrar a igualdade

$$\ell_B(B/(xy)B) = \ell_B(B/xB) + \ell_B(B/yB).$$

Mas isso segue dos isomorfismos de B-módulos $B/xB \cong \frac{B/xyB}{xB/xyB}$ e $xB/xyB \cong B/yB$. Sendo ord um homomorfismo de semigrupos de $A \setminus \{0\}$ em $\mathbb{N}^*$, é fácil ver que essa função admite como extensão um homomorfismo de grupos bem-definido $\operatorname{ord}\colon K^\times \to \mathbb{Z}$ dado por

$$\operatorname{ord}(x/y) \coloneqq \operatorname{ord}(x) - \operatorname{ord}(y) = \ell_B(B/xB) - \ell_B(B/yB).$$

Para cada $\mathfrak{p} \lhd A$ primo não-nulo, podemos assim considerar um homomorfismo de grupos $\operatorname{ord}_{\mathfrak{p}}\colon K^\times \to \mathbb{Z}$, onde $\operatorname{ord}_{\mathfrak{p}}$ é o homomorfismo associado ao domínio $A_{\mathfrak{p}}$. Com isso, nós conseguimos definir $\operatorname{div}\colon K^\times \to \operatorname{Div}(A)$ dado por $\operatorname{div}(f) \coloneqq \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(f)\,\mathfrak{p}$. Como cada $\operatorname{ord}_{\mathfrak{p}}$ é um homomorfismo, vemos que div também é um homomorfismo.

Os elementos de $\operatorname{Div}(A)$ da forma $\operatorname{div}(f)$ para algum $f \in K^\times$ são chamados de **divisores principais**. O conjunto $\operatorname{im}\operatorname{div}$ formado por eles é um subgrupo $\mathcal{P}(A)$ de $\operatorname{Div}(A)$, chamado o **grupo dos divisores principais**. Dizemos que dois divisores $D, D' \in \operatorname{Div}(A)$ são **racionalmente equivalentes** se eles diferirem por um elemento de $\mathcal{P}(A)$, ou seja, se $D + \mathcal{P}(A) = D' + \mathcal{P}(A)$ em $\operatorname{Div}(A)/\mathcal{P}(A)$.

Definição (Grupo de Classes de Divisores/Grupo de Chow)**.** Definimos o **grupo de classes de divisores** de A, ou ainda o **grupo de Chow** de A, como $CH^1(A) \coloneqq \operatorname{Div}(A)/\mathcal{P}(A)$.

Nós temos um homomorfismo canônico $\operatorname{div}\colon \operatorname{Pic}(A) \to CH^1(A)$ que relaciona o grupo de Picard e o grupo de Chow de A. Dado $M \in J(A)$, pela Proposição 8.4 para todo primo não-nulo $\mathfrak{p} \lhd A$ existe $a_{\mathfrak{p}} \in K^\times$ tal que $M_{\mathfrak{p}} = a_{\mathfrak{p}} A_{\mathfrak{p}}$. Com isso, podemos definir $\operatorname{div}\colon J(A) \to \operatorname{Div}(A)$ dado por $\operatorname{div}(M) \coloneqq \sum_{\mathfrak{p}} (-\operatorname{ord}_{\mathfrak{p}}(a_{\mathfrak{p}}))\,\mathfrak{p}$. Essa função é um homomorfismo que leva ideais fracionários principais em divisores principais, e portanto induz um homomorfismo $\operatorname{div}\colon \operatorname{Pic}(A) \to CH^1(A)$. Por fim, é claro que nós temos:

Proposição 8.13. *Se A for um domínio de Dedekind,* $\operatorname{div}\colon \operatorname{Pic}(A) \to CH^1(A)$ *é um isomorfismo.*

Capítulo 9

Valores Absolutos e Completamentos

Neste capítulo, estudaremos corpos munidos de um **valor absoluto**. Mostraremos que, assim como na construção de $\mathbb{R}$ a partir de $\mathbb{Q}$, a partir de um corpo K com um valor absoluto $|\cdot|$ nós podemos construir o seu **completamento** $\hat{K}$. Como um caso particular, nós construiremos os corpos de **números p-ádicos**, que provêm das valorações p-ádicas, e que como veremos possuem um papel fundamental na resolução de equações diofantinas.

9.1. Valores Absolutos

Definição (Valor Absoluto)**.** Um **valor absoluto** ou **valoração multiplicativa** num corpo K é uma função $|\cdot|\colon K \to \mathbb{R}_+$ que satisfaz as propriedades:

(i) $|x| = 0 \iff x = 0$;

(ii) $|xy| = |x||y|$, para todos $x, y \in K$;

(iii) $|x + y| \leq |x| + |y|$. Essa propriedade é chamada de **desigualdade triangular**.

Além disso, chamaremos um valor absoluto de **não-arquimediano** se $|n|$ for limitado para todo $n \in \mathbb{N}$, isto é, se existir $C > 0$ tal que $|n| < C$ para todo $n \in \mathbb{N}$ (aqui, reconhecemos $\mathbb{N}$ com sua imagem pelo morfismo canônico $\mathbb{Z} \to K$). Caso contrário, ele será chamado de **valor absoluto arquimediano**.

Dado um valor absoluto $|\cdot|$ em K qualquer, observemos que $|1| = |1 \cdot 1| = |1|^2 \Rightarrow |1| = 1$. Do mesmo modo, é fácil ver que toda raiz da unidade em K tem valor absoluto 1. Notemos ainda que se K tiver característica positiva a imagem de $\mathbb{Z}$ pelo morfismo canônico $\mathbb{Z} \to K$ será finita, de modo que todo valor absoluto nesse corpo será não-arquimediano. Assim, a distinção entre os conceitos de valor absoluto arquimediano e não-arquimediano só é interessante no caso em que K tem característica 0.

Para todo corpo K, nós temos o **valor absoluto trivial** dado por $|0| = 0$ e $|x| = 1$ para todo $x \neq 0$. Na sequência, desconsideraremos esse valor absoluto. Assim, por valor absoluto entender-se-á valor absoluto não-trivial. A partir de um valor absoluto $|\cdot|\colon K \to \mathbb{R}_+$ nós conseguimos definir uma métrica em K com distância dada por $d(x, y) = |x - y|$. Em particular, esse valor absoluto define um topologia em K.

Definição (Valores Absolutos Equivalentes)**.** Dizemos que dois valores absolutos em K são **equivalentes** se eles definirem a mesma topologia em K.

Sendo $|\cdot|$ um valor absoluto em K e s um real positivo, suponhamos que a função $|\cdot|^s\colon K \to \mathbb{R}_+$ defina um valor absoluto em K (isso equivale a essa função satisfazer a desigualdade triangular).

Dados $x \in K$ e $r > 0$ quaisquer, denotando por $B_r(x)$ a bola de centro x e raio r na métrica definida por $|\cdot|$ e por $B'_r(x)$ a bola de centro x e raio r na métrica definida por $|\cdot|^s$, vemos que valem as igualdades $B'_r(x) = B_{r^{1/s}}(x)$ e $B_r(x) = B'_{r^s}(x)$, o que mostra que os valores absolutos $|\cdot|$ e $|\cdot|^s$ são equivalentes. Na verdade, dois valores absolutos em K serão equivalentes se e somente se um for uma potência real positiva do outro:

Proposição 9.1. *Sejam $|\cdot|_1$ e $|\cdot|_2$ valores absolutos em K. Então são equivalentes:*

(i) *$|\cdot|_1$ e $|\cdot|_2$ são equivalentes.*

(ii) *Para todo $x \in K$, nós temos $|x|_1 < 1 \Rightarrow |x|_2 < 1$.*

(iii) *Existe um número real $s > 0$ tal que $|\cdot|_1 = |\cdot|_2^s$.*

Demonstração. A implicação $(iii) \Rightarrow (i)$ foi demonstrada acima. Provemos $(i) \Rightarrow (ii) \Rightarrow (iii)$:

$(i) \Rightarrow (ii)$: Suponhamos que $|\cdot|_1$ e $|\cdot|_2$ sejam equivalentes. Comecemos observando que para um valor absoluto $|\cdot|\colon K \to \mathbb{R}_+$ qualquer vale que $|x| < 1 \iff \lim_{n\to\infty} x^n = 0$, onde o limite é tomado na métrica induzida por $|\cdot|$. Sendo $|\cdot|_1$ e $|\cdot|_2$ equivalentes, as sequências convergentes a 0 nas duas métricas induzidas coincidem, de modo que devemos ter $|x|_1 < 1 \iff |x|_2 < 1$, provando (ii).

$(ii) \Rightarrow (iii)$: Suponhamos (ii), e tomemos $y \in K$ tal que $|y|_1 > 1$. Esse valor sempre existe. De fato, como $|\cdot|_1$ não é o valor absoluto trivial, existe $\tilde{y} \neq 0$ com $|\tilde{y}|_1 \neq 1$. Se $|\tilde{y}|_1 > 1$, basta tomarmos $y = \tilde{y}$. Se por outro lado $|\tilde{y}|_1 < 1$, então basta tomarmos $y = \tilde{y}^{-1}$. Seja agora $x \in K$ não-nulo qualquer. Então existe algum $\alpha \in \mathbb{R}$ tal que $|x|_1 = |y|_1^\alpha$. Tomemos uma sequência decrescente de racionais (m_i/n_i), com $m_i, n_i \in \mathbb{Z}$, que converge a α. Então para todo $i \in \mathbb{N}$ nós temos:

$$|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i} \Rightarrow \left|\frac{x^{n_i}}{y^{m_i}}\right|_1 < 1 \Rightarrow \left|\frac{x^{n_i}}{y^{m_i}}\right|_2 < 1 \Rightarrow |x|_2 < |y|_2^{m_i/n_i}.$$

Como isso vale para todo i e $m_i/n_i \to \alpha$, nós concluímos que $|x|_2 \leq |y|_2^\alpha$. Tomando agora uma sequência crescente de racionais (c_i/d_i), com $c_i, d_i \in \mathbb{Z}$, que converge a α, nós obtemos de forma análoga que $|x|_2 > |y|_2^{c_i/d_i}$ para todo $i \in \mathbb{N}$, e portanto $|x|_2 \geq |y|_2^\alpha$. Assim, obtemos $|x|_2 = |y|_2^\alpha$. Seja $s \in \mathbb{R}$ tal que $|y|_1 = |y|_2^s$. Notemos que $s > 0$, pois $|y|_1 > 1 \Rightarrow |y|_2 > 1$ (para essa implicação, basta notarmos que $|y^{-1}|_1 < 1$). Desse modo, para todo $x \in K$ não-nulo, vale:

$$|x|_1 = |y|_1^\alpha = (|y|_2^s)^\alpha = (|y|_2^\alpha)^s = |x|_2^s.$$

Como essa igualdade claramente vale também para $x = 0$, concluímos que $|\cdot|_1 = |\cdot|_2^s$. □

A partir da proposição acima, nós podemos demonstrar o análogo ao Teorema Chinês dos Restos para valores absolutos:

Teorema 9.2 (Teorema da Aproximação)**.** *Sejam $|\cdot|_1, \ldots, |\cdot|_n$ valores absolutos em um corpo K dois a dois não-equivalentes, e sejam $a_1, \ldots, a_n \in K$. Então para todo $\varepsilon > 0$ existe $x \in K$ tal que $|x - a_i|_i < \varepsilon$, para todo $1 \leq i \leq n$.*

Demonstração. Se $a_1 = \cdots = a_n = 0$, basta tomarmos $x = 0$. Suponhamos então que pelo menos algum dos a_j's seja não-nulo. Nós provaremos por indução em n que existe $z \in K$ tal que $|z|_1 > 1$ e $|z|_j < 1$, para todo $2 \leq j \leq n$. Para $n = 2$, como $|\cdot|_1$ e $|\cdot|_2$ não são equivalentes nós conseguimos encontrar $\alpha \in K$ tal que $|\alpha|_1 < 1$ e $|\alpha|_2 \geq 1$ e $\beta \in K$ tal que $|\beta|_1 \geq 1$ e $|\beta|_2 < 1$. Notemos que $\alpha \neq 0$ já que $|\alpha|_2 \geq 1$. Tomando $z = \beta/\alpha$, nós vemos que $|z|_1 = |\beta|_1/|\alpha|_1 > 1$ e $|z|_2 = |\beta|_2/|\alpha|_2 < 1$, de modo que z satisfaz as condições desejadas.

Suponhamos agora por indução que exista $\tilde{z} \in K$ tal que $|\tilde{z}|_1 > 1$ e $|\tilde{z}|_j < 1$ para todo $2 \leq j \leq n-1$, e tomemos $y \in K$ tal que $|y|_1 > 1$ e $|y|_n < 1$. Se $|\tilde{z}|_n \leq 1$, então para todo $m \in \mathbb{N}$ nós temos $|\tilde{z}^m y|_1 > 1$ e $|\tilde{z}^m y|_n < 1$. Além disso, como $|\tilde{z}|_j < 1$ para $2 \leq j \leq n-1$, podemos tomar m suficientemente grande de modo que para todo $2 \leq j \leq n-1$ nós tenhamos $|\tilde{z}^m y|_j < 1$. Com isso, $z = \tilde{z}^m y$ satisfaz $|z|_1 > 1$ e $|z|_j < 1$ para todo $2 \leq j \leq n$.

Suponhamos então que $|\tilde{z}|_n > 1$. Nesse caso, notemos que a sequência $(\tilde{z}^m/(1+\tilde{z}^m))$ converge a 1 com respeito a $|\cdot|_1$ e $|\cdot|_n$ e converge a 0 com respeito a $|\cdot|_j$ para $2 \leq j \leq n-1$ (observe que essa sequência está bem-definida, pois como $|\tilde{z}|_1 > 1$ vemos que $\tilde{z}$ não é uma raiz da unidade). Desse modo, podemos tomar m suficientemente grande de modo que tenhamos $|\tilde{z}^m y/(1+\tilde{z}^m)|_1 > 1$ e $|\tilde{z}^m y/(1+\tilde{z}^m)|_j < 1$ para todo $2 \leq j \leq n$. Assim, basta tomarmos $z = \tilde{z}^m y/(1+\tilde{z}^m)$. Isso conclui a indução.

Seja então $z \in K$ tal que $|z|_1 > 1$ e $|z|_j < 1$ para todo $2 \leq j \leq n$. A sequência $(z^m/(1+z^m))$ converge a 1 com respeito a $|\cdot|_1$ e a 0 com respeito a $|\cdot|_j$ para $2 \leq j \leq n$. Desse modo, tomando m grande, vemos que para todo $\delta_1 > 0$ é possível encontrarmos um elemento $z_1 \in K$ tal que $|z_1 - 1|_1 < \delta$ e $|z_1|_j < \delta$ para todo $2 \leq j \leq n$.

De forma análoga, dado $\delta > 0$ qualquer nós podemos achar para todo $1 \leq i \leq n$ um elemento $z_i \in K$ tal que $|z_i - 1|_i < \delta$ e $|z_i|_j < \delta$ para todo $1 \leq j \leq n$ com $j \neq i$. Finalmente, tomemos $x = a_1 z_1 + \cdots + a_n z_n$. Então para todo $1 \leq i \leq n$ nós temos:

$$\begin{aligned} |x - a_i|_i &= |a_1 z_1 + \cdots + a_{i-1} z_{i-1} + a_i(z_i - 1) + a_{i+1} z_{i+1} + \cdots + a_n z_n|_i \\ &\leq |a_1|_i |z_1|_i + \cdots + |a_{i-1}|_i |z_{i-1}|_i + |a_i|_i |z_i - 1|_i + |a_{i+1}|_i |z_{i+1}|_i + \cdots + |a_n|_i |z_n|_i \\ &< |a_1|_i \delta + \cdots + |a_{i-1}|_i \delta + |a_i|_i \delta + |a_{i+1}|_i \delta + \cdots + |a_n|_i \delta \\ &= (|a_1|_i + \cdots + |a_n|_i)\delta. \end{aligned}$$

Dado $\varepsilon > 0$ qualquer, tomando $\delta > 0$ de modo que $\delta < (|a_1|_i + \cdots + |a_n|_i)^{-1}\varepsilon$ para todo $1 \leq i \leq n$, nós obtemos $|x - a_i|_i < \varepsilon$ para todo $1 \leq i \leq n$, como desejávamos. □

Mostraremos agora que um valor absoluto é não-arquimediano se e somente se satisfizer uma versão mais forte da desigualdade triangular:

Proposição 9.3. *Um valor absoluto $|\cdot|$ em K é não-arquimediano se e somente se ele satisfizer a **desigualdade ultramétrica**, isto é, se valer a desigualdade:*

$$|x + y| \leq \max\{|x|, |y|\}, \text{ para todos } x, y \in K.$$

Além disso, nesse caso temos $|n| \leq 1$ para todo $n \in \mathbb{N}$.

Demonstração. ($\Leftarrow$): Suponhamos que $|\cdot|$ satisfaça a desigualdade ultramétrica. Então é fácil ver por indução que vale $|x_1 + \cdots + x_n| \leq \max\{|x_1|, \ldots, |x_n|\}$, para todos $x_1, \ldots, x_n \in K$. Em particular, para todo $n \in \mathbb{N}$ nós temos $|n| = |1 + \cdots + 1| \leq \max\{|1|, \ldots, |1|\} = 1$, o que mostra que $|\cdot|$ é não-arquimediano.

($\Rightarrow$): Suponhamos que $|\cdot|$ seja um valor absoluto não-arquimediano. Então existe $C > 0$ tal que $|n| < C$ para todo $n \in \mathbb{N}$. Dado k inteiro positivo qualquer, nós temos $|n^k| = |n|^k$. Desse modo, devemos ter $|n| \leq 1$ para todo $n \in \mathbb{N}$. Sejam $x, y \in K$ quaisquer, e suponhamos sem perda de generalidade que $|x| \geq |y|$. Então queremos mostrar que $|x + y| \leq |x|$. Fixado n inteiro positivo, nós temos:

$$|x+y|^n = |(x+y)^n| = \left|\sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}\right| \leq \sum_{j=0}^{n} \left|\binom{n}{j}\right| |x|^j |y|^{n-j} \leq \sum_{j=0}^{n} |x|^n \leq (n+1)|x|^n.$$

Desse modo, para todo inteiro positivo n nós temos $|x + y| \leq (n+1)^{1/n}|x|$. Fazendo $n \to \infty$, concluímos que $|x + y| \leq |x|$, como desejado. Assim, $|\cdot|$ satisfaz a desigualdade ultramétrica. □

Observação 9.4. *Notemos que se $|\cdot|$ satisfizer a desigualdade ultramétrica, então nós temos $|x| \neq |y| \Rightarrow |x+y| = \max\{|x|, |y|\}$. De fato, suponhamos que $|x| > |y|$. Então, pela desigualdade ultramétrica, $|x+y| \leq |x|$. Por outro lado, $|-y| = |y|$, assim:*

$$|x| = |(x+y) - y| \leq \max\{|x+y|, |-y|\} = \max\{|x+y|, |y|\}.$$

Mas como $|x| > |y|$, devemos ter $|x| \leq |x+y|$, de forma que $|x+y| = |x|$, como desejado.

Dados um corpo K com um valor absoluto não-arquimediano $|\cdot|$ e $q > 1$ real, podemos definir $v\colon K \to \mathbb{R} \cup \{\infty\}$ dado por $v(x) = -\log_q |x|$, onde usamos a convenção $\log_q 0 = -\infty$. É fácil verificar que essa função satisfaz as seguintes propriedades ((iii) segue da desigualdade ultramétrica):

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) (Propriedade não-arquimediana) $v(x+y) \geq \min\{v(x), v(y)\}$.

Definição (Valoração (Exponencial)/Grupo de Valores)**.** Uma função $v\colon K \to \mathbb{R} \cup \{\infty\}$ é chamada de **valoração (exponencial)** se ela satisfizer as três propriedades acima. Além disso, chamamos $v(K^\times) \subseteq \mathbb{R}$ de **grupo de valores** de v. Notemos que $v(K^\times)$ é um subgrupo aditivo de $\mathbb{R}$.

Notemos que toda valoração discreta é uma valoração. Notemos ainda que toda valoração satisfaz as propriedades dadas pelo Lema 3.26 (de fato, na prova desse lema não utilizamos o fato da valoração ser discreta).

Assim, vemos que a cada valor absoluto não-arquimediano de K nós podemos associar uma valoração. É fácil ver que o caminho inverso também é possível. Isto é, dada uma valoração $v\colon K \to \mathbb{R} \cup \{\infty\}$, podemos definir um valor absoluto não-arquimediano $|\cdot|_v$ em K dado pela expressão $|x|_v = q^{-v(x)}$, onde $q > 1$ é um real fixado e definimos $q^{-\infty} = 0$. Com isso, conseguimos definir os **valores absolutos p-ádicos**:

Definição. [Valor Absoluto p-ádico/Métrica p-ádica] Seja $p \in \mathbb{N}$ um número primo. Definimos o **valor absoluto p-ádico** em $\mathbb{Q}$ como sendo a função $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}_+$ dada por $|x|_p = p^{-v_p(x)}$. Definimos ainda o **valor absoluto ∞-ádico** em $\mathbb{Q}$ como sendo o valor absoluto usual de $\mathbb{Q}$, e o denotamos $|\cdot|_\infty$. A partir do valor absoluto p-ádico, nós conseguimos definir uma **métrica p-ádica** em $\mathbb{Q}$, com distância dada por $d_p(x,y) = |x-y|_p$. Note que d_∞ é a distância euclidiana.

Para p primo, os valores absolutos p-ádicos são todos não-arquimedianos, já que todo número natural tem valor absoluto no máximo 1. Por outro lado, para $p = \infty$ nós obtemos um valor absoluto arquimediano, já que $\lim_{n\to\infty} |n|_\infty = \infty$.

A partir de agora, nós sempre excluiremos a **valoração trivial**, dada por $v(x) = 0$ para $x \neq 0$ e $v(0) = \infty$. Assim, por valoração se entenderá valoração não-trivial. Também temos uma noção de equivalência de valorações:

Definição (Valorações Equivalentes)**.** Duas valorações v_1 e v_2 em um corpo K se dizem **equivalentes** se existir um real $s > 0$ tal que $v_1 = sv_2$.

Note que todos os valores absolutos associados a uma valoração v serão equivalentes, e que duas valorações serão equivalentes se e somente se seus valores absolutos associados o forem, devido à Proposição 9.1. Como uma consequência direta do Teorema da Aproximação para valores absolutos, temos um Teorema da Aproximação para valorações:

Teorema 9.5 (Teorema da Aproximação)**.** *Sejam $v_1, \ldots, v_n$ valorações em um corpo K duas a duas não-equivalentes, e sejam $a_1, \ldots, a_n \in K$. Então para todo $C > 0$ existe $x \in K$ tal que $v_i(x - a_i) > C$, para todo $1 \leq i \leq n$.*

É fácil ver pela definição acima que as valorações p-ádicas, para $p \in \mathbb{N}$ primo, são duas a duas não-equivalentes. Assim, para p primo os valores absolutos p-ádicos são dois a dois não-equivalentes. Como $|\cdot|_\infty$ é arquimediano, vemos que o valor absoluto ∞-ádico também não é equivalentes aos demais. De fato, esses são os únicos valores absolutos de $\mathbb{Q}$ a menos de equivalência:

Proposição 9.6. *Todo valor absoluto de $\mathbb{Q}$ é equivalente a um único valor absoluto p-ádico, para $p \in \mathbb{N}$ primo ou $p = \infty$.*

Demonstração. Vimos acima que os valores absolutos p-ádicos são dois a dois não-equivalentes em $\mathbb{Q}$. Assim, basta mostrarmos que todo valor absoluto $|\cdot|\colon \mathbb{Q} \to \mathbb{R}_+$ é equivalente a algum valor absoluto p-ádico $|\cdot|_p$. Suponhamos inicialmente que $|\cdot|$ seja não-arquimediano. Então pela Proposição 9.3 temos $|n| \leq 1$ para todo $n \in \mathbb{Z}$. Assim, utilizando a desigualdade ultramétrica é fácil ver que o conjunto $\mathfrak{a} \coloneqq \{a \in \mathbb{Z}\colon |a| < 1\}$ é um ideal próprio de $\mathbb{Z}$. Como todo elemento de $\mathbb{Q}^\times$ se escreve como um produto finito de potências inteiras de números primos e $|\cdot|$ não é o valor absoluto trivial, concluímos que deve haver $p \in \mathbb{N}$ primo para o qual $|p| < 1$. Desse modo, $\mathfrak{a} \supseteq p\mathbb{Z}$. Mas $p\mathbb{Z}$ é maximal, e assim concluímos que $\mathfrak{a} = p\mathbb{Z}$. Isso prova que $|q| = 1$ para todo primo $q \neq p$. Em particular, $|u| = 1$ para todo $u \in \mathbb{Z}_{(p)}^\times$.

Chamemos $s \coloneqq -\log_p(|p|) > 0$. Assim, $|p| = p^{-s}$. Todo $x \in \mathbb{Q}^\times$ se escreve de modo único como $x = p^{v_p(x)}u$, para $u \in \mathbb{Z}_{(p)}^\times$. Então nós temos:

$$|x| = |p^{v_p(x)}u| = |p|^{v_p(x)} = (p^{-s})^{v_p(x)} = (p^{-v_p(x)})^s = |x|_p^s.$$

Como essa igualdade vale também para $x = 0$, concluímos que $|\cdot| = |\cdot|_p^s$, provando que $|\cdot|$ é equivalente a $|\cdot|_p$.

Suponhamos agora que $|\cdot|$ seja um valor absoluto arquimediano. Então existe um inteiro positivo $n > 1$ tal que $|n| > 1$. Sejam $m > 1$ e $k \geq 1$ inteiros. Escrevendo n^k na base m, nós obtemos $n^k = a_0 + a_1 m + \cdots + a_r m^r$, para alguns inteiros $0 \leq a_j \leq m - 1$. Notemos que $m^r \leq n^k \Rightarrow r \leq k \log n / \log m$. Além disso, para $0 \leq j \leq r$ nós temos pela desigualdade triangular que $|a_j| = |1 + \cdots + 1| \leq a_j|1| = a_j < m$. Assim:

$$\begin{aligned} |n|^k = |n^k| = \left|\sum_{j=0}^{r} a_j m^j\right| \leq \sum_{j=0}^{r} |a_r||m|^j &< \sum_{j=0}^{r} m|m|^j \\ &\leq m(r+1)\max\{1, |m|^r\} \\ &\leq m(1 + k\log n/\log m)\max\{1, |m|^{k\log n/\log m}\}. \end{aligned}$$

Tomando a raiz k-ésima dos dois lados, nós concluímos que para todo inteiro positivo k vale a desigualdade:

$$|n| \leq (m(1 + k\log n/\log m))^{1/k}\max\{1, |m|^{\log n/\log m}\}.$$

Fazendo $k \to \infty$, nós concluímos que $|n| \leq \max\{1, |m|^{\log n/\log m}\}$. Como $|n| > 1$, temos então que $|n| \leq |m|^{\log n/\log m} \Rightarrow |n|^{1/\log n} \leq |m|^{1/\log m}$. Notemos ainda que, como $\log n/\log m > 0$, temos:

$$1 < |n| \leq |m|^{\log n/\log m} \Rightarrow |m| > 1,$$

Assim, podemos repetir o argumento trocando as posições de m e de n, para concluirmos que $|m|^{1/\log m} \leq |n|^{1/\log n}$, e portanto vale a igualdade $|m|^{1/\log m} = |n|^{1/\log n}$, para todo inteiro positivo m. Definamos $s \coloneqq \log\left(|n|^{1/\log n}\right) > 0$, de modo que $e^s = |n|^{1/\log n}$. Afirmamos que $|x| = |x|_\infty^s$, para todo $x \in \mathbb{Q}$. Comecemos observando que isso vale para $x \in \mathbb{Z}$. De fato, para $x = 0$ ou $x = \pm 1$, isso é claro. Suponhamos então $x = \pm m$, onde $m > 1$ é um inteiro. Logo:

$$|x| = |m| = \left(|n|^{1/\log n}\right)^{\log m} = (e^s)^{\log m} = (e^{\log m})^s = m^s = |x|_\infty^s.$$

Mostremos agora que isso vale para todo $x \in \mathbb{Q}$. Podemos escrever $x = a/b$, para $a, b \in \mathbb{Z}$ e $b \neq 0$. Então $|x| = |a|/|b| = |a|_\infty^s / |b|_\infty^s = |a/b|_\infty^s = |x|_\infty^s$, concluindo a demonstração. □

Nós podemos definir valoração discreta de uma forma um pouco mais ampla, que dá sentido ao adjetivo **discreta**:

Definição (Valoração Discreta)**.** Uma valoração $v\colon K \to \mathbb{R} \cup \{\infty\}$ é chamada de **discreta** se seu grupo de valores $v(K^\times)$ for um subconjunto discreto de $\mathbb{R}$.

É fácil mostrar que todo subgrupo aditivo de $\mathbb{R}$ que também é discreto é da forma $s\mathbb{Z}$, onde $s > 0$ é o menor elemento positivo desse subgrupo. Desse modo, se v for uma valoração discreta, teremos $v(K^\times) = s\mathbb{Z}$ para algum $s > 0$. Assim, a valoração $\tilde{v} \coloneqq \frac{1}{s} v$ também será uma valoração discreta, equivalente a v, e tal que $\tilde{v}(K^\times) = \mathbb{Z}$. Então $\tilde{v}\colon K \to \mathbb{Z} \cup \{\infty\}$ é uma valoração discreta no sentido da Seção 3.3, e nesse contexto mais geral é chamada de **valoração discreta normalizada**.

Assim como nós associamos uma valoração discreta (normalizada) a um DVD, vemos que é possível associar uma valoração a um certo anel. De fato, as três condições que definem uma valoração implicam imediatamente no seguinte:

Proposição 9.7. *Seja $v\colon K \to \mathbb{R} \cup \{\infty\}$ uma valoração e seja $|\cdot|_v$ um valor absoluto relacionado a v. Então o conjunto*

$$A \coloneqq \{x \in K\colon v(x) \geq 0\} = \{x \in K\colon |x|_v \leq 1\}$$

é um subanel de K, que é local com grupo de unidades

$$A^\times \coloneqq \{x \in K\colon v(x) = 0\} = \{x \in K\colon |x|_v = 1\}$$

e único ideal maximal

$$\mathfrak{p} = \{x \in K\colon v(x) > 0\} = \{x \in K\colon |x|_v < 1\}.$$

O anel A é um domínio com corpo de frações K e com a propriedade de que para todo $x \in K^\times$ nós temos $x \in A$ ou $x^{-1} \in A$.

As últimas duas linhas da proposição acima nos dizem que o anel A é o que chamamos de um **domínio de valoração**:

Definição (Domínio de Valoração)**.** Um domínio A é chamado de **domínio de valoração**, ou ainda **anel de valoração**, se para todo elemento não-nulo x de seu corpo de frações nós tivermos $x \in A$ ou $x^{-1} \in A$.

O seguinte resultado nos diz um pouco sobre a estrutura dos domínios de valoração:

Proposição 9.8. *Seja A um domínio com corpo de frações $K = Q(A)$. Então são equivalentes:*

(i) A é um domínio de valoração.

(ii) Os ideais de A são totalmente ordenados por inclusão.

(iii) Os ideais principais de A são totalmente ordenados por inclusão.

Além disso, nesse caso A é local e integralmente fechado.

Demonstração. $(i) \Rightarrow (ii)$: Sejam $\mathfrak{a}, \mathfrak{b} \lhd A$ ideais quaisquer. Suponhamos por absurdo que $\mathfrak{a} \not\subseteq \mathfrak{b}$ e $\mathfrak{b} \not\subseteq \mathfrak{a}$. Tomemos $a \in \mathfrak{a} \setminus \mathfrak{b}$ e $b \in \mathfrak{b} \setminus \mathfrak{a}$. Então como A é domínio de valoração vemos que $a/b \in A$ ou $b/a \in A$. Mas se $x = a/b \in A$ então $a = xb \in \mathfrak{b}$, e se $y = b/a \in A$ então $b = ya \in \mathfrak{a}$, um absurdo! Concluímos que $\mathfrak{a} \subseteq \mathfrak{b}$ ou $\mathfrak{b} \subseteq \mathfrak{a}$, como desejávamos. Em particular, dados dois ideais maximais de A, um está contido no outro. Assim, A possui apenas um ideal maximal, logo é local.

$(ii) \Rightarrow (iii)$: É óbvio.

$(iii) \Rightarrow (i)$: Suponhamos que os ideais principais de A sejam totalmente ordenados por inclusão. Isso significa que os elementos de A são totalmente ordenados por divisibilidade. Isto é, dados $a, b \in A$ quaisquer temos $a \mid b$ ou $b \mid a$. Seja $x \in K$ qualquer. Então podemos escrever $x = a/b$, para alguns $a, b \in A$, $b \neq 0$. Então $a \mid b$ ou $b \mid a$. Se $b \mid a$, então $x = a/b \in A$. Se $a \mid b$, então $x^{-1} = b/a \in A$. Isso mostra que A é um domínio de valoração.

Mostremos agora que todo domínio de valoração A é integralmente fechado. Seja $x \in \overline{A}^K$. Então existem elementos $a_0, a_1, \ldots, a_{n-1} \in A$ tais que $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n = 0$. Suponhamos por absurdo que $x \notin A$. Então $x^{-1} \in A$, de modo que

$$x = -a_0(x^{-1})^{n-1} - a_1(x^{-1})^{n-2} - \cdots - a_{n-1} \in A,$$

um absurdo! Concluímos que $x \in A$, e portanto A é integralmente fechado. □

É interessante observar que a correspondência $v \mapsto K_v$ entre o conjunto das valorações de K e o conjunto dos domínios de valoração de K é injetora a menos de equivalências:

Proposição 9.9. *Sejam v e w valorações de K, com domínios de valoração A_v e A_w, respectivamente. Então $A_v = A_w$ se e somente se v for equivalente a w.*

Demonstração. Se v for equivalente a w, temos $v(x) \geq 0 \iff w(x) \geq 0$, o que mostra que $A_v = A_w$. Suponhamos, por outro lado, que $A_v = A_w$. Então em particular os ideais maximais desses dois anéis são iguais, de modo que $v(x) > 0 \iff w(x) > 0$. Em termos de valores absolutos, isso significa que $|x|_v < 1 \iff |x|_w < 1$, o que significa que esses dois valores absolutos são equivalentes pela Proposição 9.1. Isso mostra que v e w são equivalentes. □

Terminemos a seção com uma análise da topologia de um corpo K munido de uma valoração discreta normalizada v. Sejam $|\cdot|_v = q^{-v}$ um valor absoluto associado, A o DVD associado e $\mathfrak{p}$ o único ideal maximal desse DVD. Então todos os ideais fracionários não-nulos de A são da forma

$$\mathfrak{p}^n = \{x \in A \colon v(x) \geq n\} = \{x \in A \colon |x|_v \leq q^{-n}\},$$

para $n \in \mathbb{Z}$. A última caracterização acima nos mostra que os $\mathfrak{p}^n$'s são conjuntos fechados na topologia induzida. Mas sendo v uma valoração discreta, nós temos

$$\mathfrak{p}^n = \{x \in A \colon v(x) > n-1\} = \{x \in A \colon |x|_v < q^{-(n-1)}\}.$$

Assim, esses conjuntos também são abertos nessa topologia. Em particular, A é aberto e fechado em K. Na verdade, como a imagem de $|\cdot|_v$ é $\{0, \ldots, q^{-2}, q^{-1}, 1, q, q^2, \ldots\}$, vemos que os $\mathfrak{p}^n$ nos dão todas as bolas abertas (e fechadas) com centro em 0. É claro que, dado $a \in K$ qualquer, nós temos:

$$a + \mathfrak{p}^n = \{x \in A \colon |x - a|_v \leq q^{-n}\} = \{x \in A \colon |x - a|_v < q^{-(n-1)}\},$$

de modo que essas são as bolas abertas (e fechadas) com centro em a. Assim, para todo $a \in K$, o conjunto $\{a + \mathfrak{p}^n \colon n \in \mathbb{N}\}$ é um sistema fundamental de vizinhanças de a na topologia induzida por $|\cdot|_v$. Em particular, $\{\mathfrak{p}^n \colon n \in \mathbb{N}\}$ é um sistema fundamental de vizinhanças de 0, e $\{U^{(n)} \colon n \in \mathbb{N}\}$ é um sistema fundamental de vizinhanças de 1.

9.2. Completamentos

Para indicar que temos um corpo K munido de um valor absoluto $|\cdot|$, denotaremos $(K, |\cdot|)$. Similarmente, indicaremos um corpo munido de uma valoração v por (K, v). Finalmente, denotamos $(K, v, |\cdot|)$ quando quisermos indicar que um corpo está munido de um valor absoluto não-arquimediano $|\cdot|$ que induz uma valoração v. Começamos com a seguinte definição, análoga ao caso de espaços vetoriais normados:

Definição (Corpo Completo)**.** Um corpo $(K, |\cdot|)$ é dito **completo** se toda sequência de Cauchy em K convergir com relação a[1] $|\cdot|$.

Procedendo do mesmo modo que na construção dos reais, nós podemos construir, a partir de um corpo com valor absoluto $(K, |\cdot|)$, um corpo com valor absoluto completo $(\hat{K}, |\cdot|)$, chamado **completamento** de K com respeito a $|\cdot|$, de modo que K seja um subcorpo de $\hat{K}$, que o valor absoluto de $\hat{K}$ estenda o valor absoluto de K e que K seja denso em $\hat{K}$ com a topologia induzida por $|\cdot|$.

Começamos considerando o anel R das sequências de Cauchy em K, e o ideal $\mathfrak{m} \lhd R$ das sequências de Cauchy em K que convergem a 0. Esse ideal é maximal. De fato, tomemos $x = (x_n) \in R \setminus \mathfrak{m}$ qualquer. Queremos mostrar que $R = \mathfrak{m} + xR$. Como x é sequência de Cauchy que não converge a 0, nenhuma subsequência de x pode convergir a 0. Assim, existem $\delta > 0$ e $n_0 \in \mathbb{N}$ tais que $|x_n| > \delta$ para todo $n > n_0$.

Seja agora $y = (y_n) \in R$ qualquer. Definimos $z = (z_n) \in R$ por $z_n = 0$ para $n < n_0$ e $z_n = x_n^{-1} y_n$ para todo $n > n_0$. Como para $n > n_0$ temos $|x_n|$ limitado inferiormente, é fácil ver que z é uma sequência de Cauchy. Agora, vemos que $y - xz = (y_1, y_2, \dots, y_{n_0}, 0, 0, \dots) \in \mathfrak{m}$, e portanto $y \in \mathfrak{m} + xR$. Isso prova que $\mathfrak{m}$ é maximal.

Definimos $\hat{K} := R/\mathfrak{m}$. Então $\hat{K}$ é um corpo, e podemos ver K como um subcorpo de $\hat{K}$ por meio da inclusão $a \mapsto (a, a, a, \dots) + \mathfrak{m}$. Nós estendemos o valor absoluto $|\cdot|$ de K a um valor absoluto $|\cdot|$ de $\hat{K}$ definindo $|(x_n) + \mathfrak{m}| := \lim_{n\to\infty} |x_n|$. Para ver que essa função está bem-definida, comecemos observando que vale $||x_m| - |x_n|| \leq |x_m - x_n|$, o que mostra que $(|x_n|)$ é uma sequência de Cauchy de números reais, e portanto converge. Seja agora $(y_n) \in R$ tal que $(x_n) + \mathfrak{m} = (y_n) + \mathfrak{m}$. Então temos $(x_n - y_n) \in \mathfrak{m}$, de modo que $|x_n - y_n| \to 0 \Rightarrow ||x_n| - |y_n|| \to 0$, o que prova que $\lim_{n\to\infty} |y_n| = \lim_{n\to\infty} |x_n|$.

Estando bem-definido, é fácil verificar que $|\cdot|$ é de fato um valor absoluto em $\hat{K}$ que estende o valor absoluto de K. Essa extensão será arquimediana se e somente se o valor absoluto de K o for, já que a identificação de $\mathbb{N}$ dentro de K é a mesma que dentro de $\hat{K}$. Além disso, a completude de $\hat{K}$ se mostra da mesma forma que a completude de $\mathbb{R}$, e o fato de K ser denso em $\hat{K}$ se mostra da mesma forma que o fato de $\mathbb{Q}$ ser denso em $\mathbb{R}$.

Finalmente, o completamento $(\hat{K}, |\cdot|)$ é único a menos de isomorfismo. De fato, seja $(K', |\cdot|')$ um corpo com valor absoluto completo que possui $(K, |\cdot|)$ como subcorpo denso. Então pode-se mostrar que a função $\sigma\colon \hat{K} \to K'$, que para toda sequência (a_n) em K leva $\lim_{n\to\infty} a_n$ com respeito a $|\cdot|$ em $\lim_{n\to\infty} a_n$ com respeito a $|\cdot|'$, é um isomorfismo de corpos que preserva os valores absolutos, isto é, tal que para todo $x \in \hat{K}$ tenhamos $|x| = |\sigma x|'$.

Os exemplos mais conhecidos de corpos completos são $\mathbb{R}$ e $\mathbb{C}$. Ambos são completos em relação a um valor absoluto arquimediano. O interessante é que eles são os únicos corpos completos por um valor absoluto arquimediano, a menos de isomorfismo. De fato, denotando por $|\cdot|_\infty$ o valor absoluto de $\mathbb{R}$ ou $\mathbb{C}$, nós temos:

Teorema 9.10 (Teorema de Ostrowski)**.** *Seja K um corpo que é completo com respeito a um valor absoluto arquimediano $|\cdot|$. Então existe um isomorfismo σ de K em $\mathbb{R}$ ou $\mathbb{C}$, satisfazendo $|x| = |\sigma x|_\infty^s$, para todo $x \in K$, onde $s \in (0, 1]$ é fixado.*

[1] Isto é, na métrica induzida por $|\cdot|$.

Demonstração. Como já vimos, apenas corpos com característica 0 possuem valores absolutos arquimedianos. Assim, $\mathbb{Q}$ é um subcorpo de K. Desse modo, pela Proposição 9.6, a restrição do valor absoluto de K a $\mathbb{Q}$ é da forma $|\cdot|_\infty^s$, para algum $s > 0$. Logo $|\cdot|^{1/s} = |\cdot|_\infty$ em $\mathbb{Q}$. Sem perda de generalidade, troquemos $|\cdot|$ por $|\cdot|^{1/s}$. Então vale $|\cdot| = |\cdot|_\infty$ em $\mathbb{Q}$.

Seja $\hat{\mathbb{Q}}$ o fecho de $\mathbb{Q}$ em K com respeito a $|\cdot|$. Então $(\hat{\mathbb{Q}}, |\cdot|)$ é um completamento de $(\mathbb{Q}, |\cdot|) = (\mathbb{Q}, |\cdot|_\infty)$. Mas $(\mathbb{R}, |\cdot|_\infty)$ também é um completamento desse corpo, e portanto pela unicidade do completamento vemos que existe um isomorfismo de corpos $\sigma\colon \mathbb{R} \to \hat{\mathbb{Q}}$ que preserva valores absolutos. Assim, podemos supor sem perda de generalidade que $\mathbb{R}$ é subcorpo de K.

Nessas condições, iremos mostrar que $K = \mathbb{R}$ ou $K \cong \mathbb{C}$. Para isso, basta mostrar que a extensão $K / \mathbb{R}$ é algébrica. De fato, mostraremos que todo elemento $\xi \in K$ é raiz de um polinômio de segundo grau com coeficientes em $\mathbb{R}$. Para isso, consideremos a função contínua $f\colon \mathbb{C} \to \mathbb{R}$ dada por $f(z) = |\xi^2 - (z + \overline{z})\xi + z\overline{z}|$. Notemos que para todo $z \in \mathbb{C}$ temos $z + \overline{z}, z\overline{z} \in \mathbb{R} \subseteq K$, de modo que f está bem-definida. Desse modo:

$$f(z) = |\xi^2 - (z + \overline{z})\xi + z\overline{z}| \geq |z\overline{z}| - |(z + \overline{z})\xi| - |\xi^2| = |z\overline{z}|_\infty - |z + \overline{z}|_\infty |\xi| - |\xi|^2.$$

Escrevendo $z = a + bi$ para $a, b \in \mathbb{R}$, nós obtemos $|z\overline{z}|_\infty = a^2 + b^2$ e $|z + \overline{z}| = 2|a|_\infty$. Observando que $|z|_\infty = \sqrt{a^2 + b^2}$, vemos que quando $|z|_\infty \to \infty$ nós temos:

$$f(z) \geq (a^2 + b^2) - 2|a|_\infty |\xi| - |\xi|^2 \to \infty.$$

Isso mostra que f assume um valor mínimo m, e além disso que o conjunto $S \coloneqq f^{-1}(m) \subseteq \mathbb{C}$ é limitado. Sendo a pré-imagem de um ponto por uma função contínua, vemos que S também é fechado. Assim, S é compacto. Sendo S compacto, existe $z_0 \in S$ tal que $|z_0|_\infty \geq |z|_\infty$ para todo $z \in S$. Nós mostraremos que $m = 0$, pois então iremos concluir que $\xi^2 - (z_0 + \overline{z}_0)\xi + z_0\overline{z}_0 = 0$, de modo que ξ será a raiz de um polinômio de segundo grau com coeficientes em $\mathbb{R}$. Suponhamos por absurdo que $m > 0$. Fixemos $0 < \varepsilon < m$, e consideremos o polinômio

$$g(x) = x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0 + \varepsilon \in \mathbb{R}[x].$$

Como o polinômio $x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0 = (x - z_0)(x - \overline{z}_0)$ não possui raízes reais, nós temos $x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0 > 0$ para todo $x \in \mathbb{R}$. Assim, é claro que $g(x) > 0$ para todo $x \in \mathbb{R}$, de modo que $g(x)$ possui duas raízes não-reais z_1 e $\overline{z}_1$. Temos $z_1\overline{z}_1 = z_0\overline{z}_0 + \varepsilon$, logo $|z_1|_\infty > |z_0|_\infty$, e portanto $z_1 \notin S$. Assim, $f(z_1) > m$. Fixado n inteiro positivo, consideremos o polinômio

$$G(x) = (g(x) - \varepsilon)^n - (-\varepsilon)^n \in \mathbb{R}[x],$$

e sejam $\alpha_1, \ldots, \alpha_{2n} \in \mathbb{C}$ suas raízes, contadas com multiplicidade. É claro que $\overline{\alpha}_1, \ldots, \overline{\alpha}_{2n}$ também são as raízes de G, em alguma ordem. Portanto:

$$\begin{aligned} & G(x) = \prod_{i=1}^{2n} (x - \alpha_i) = \prod_{i=1}^{2n} (x - \overline{\alpha}_i) \\ \Rightarrow \quad & G(x)^2 = \prod_{i=1}^{2n} (x - \alpha_i) \cdot \prod_{i=1}^{2n} (x - \overline{\alpha}_i) = \prod_{i=1}^{2n} (x^2 - (\alpha_i + \overline{\alpha}_i)x + \alpha_i\overline{\alpha}_i). \end{aligned}$$

Como $g(z_1) = 0$, vemos que $G(z_1) = 0$. Suponhamos sem perda de generalidade que $z_1 = \alpha_1$. Assim:

$$|G(\xi)^2| = \prod_{i=1}^{2n} |\xi^2 - (\alpha_i + \overline{\alpha}_i)\xi + \alpha_i\overline{\alpha}_i)| = \prod_{i=1}^{2n} f(\alpha_i) \geq f(\alpha_1)m^{2n-1} = f(z_1)m^{2n-1}.$$

Por outro lado, como $g(x) - \varepsilon = x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0$, nós temos:

$$\begin{aligned} |G(\xi)| = |(g(\xi) - \varepsilon)^n - (-\varepsilon)^n| \quad &\leq \quad |\xi^2 - (z_0 + \overline{z}_0)\xi + z_0\overline{z}_0|^n + |\varepsilon^n| \\ &= \quad f(z_0)^n + \varepsilon^n = m^n + \varepsilon^n. \end{aligned}$$

Desse modo, obtemos:

$$f(z_1)m^{2n-1} \leq |G(\xi)^2| = |G(\xi)|^2 \leq (m^n + \varepsilon^n)^2 \Rightarrow \frac{f(z_1)}{m} \leq \frac{(m^n+\varepsilon^n)^2}{m^{2n}} = \left(1 + \left(\frac{\varepsilon}{m}\right)^n\right)^2.$$

Essa desigualdade vale para todo inteiro positivo n. Finalmente, fazendo $n \to \infty$, nós concluímos que $f(z_1)/m \leq 1 \Rightarrow f(z_1) \leq m$, um absurdo! Logo $m = 0$, e ξ é raiz de um polinômio de segundo grau com coeficientes em $\mathbb{R}$. Assim, $K = \mathbb{R}$ ou $K \cong \mathbb{C}$.

Traduzindo o que fizemos até aqui para o corpo com valor absoluto $(K, |\cdot|)$ inicial (lembre que identificamos K com um corpo que contém $\mathbb{R}$ e que consideramos $|\cdot|^{1/s}$ ao invés de $|\cdot|$), nós concluímos que existe um isomorfismo σ de K em $\mathbb{R}$ ou $\mathbb{C}$ satisfazendo $|x| = |\sigma x|_\infty^s$, onde $s > 0$. Falta apenas mostrar que $s \leq 1$. Para isso, mostraremos que para $s > 1$ a função $|\cdot|_\infty^s$ não satisfaz a desigualdade triangular em $\mathbb{R}$, e portanto também não em $\mathbb{C}$. Para isso, basta notarmos que $1^s + 1^s = 2 < 2^s = (1+1)^s$, o que conclui a demonstração. □

O teorema acima mostra que podemos restringir nosso estudo de completamentos aos valores absolutos não-arquimedianos. Na prática, muitas vezes é melhor trabalharmos com as valorações associadas a esses valores absolutos. Assim, seja $(K, v, |\cdot|)$ um corpo, e consideremos seu completamento $(\hat{K}, |\cdot|)$. Suponhamos que $q > 1$ seja tal que $|\cdot| = q^{-v}$. Nós podemos estender v a uma valoração $\hat{v}$ em $\hat{K}$ definindo, para cada $x \in \hat{K}$, $\hat{v}(x) = -\log_q|x|$. Assim, vale a relação $|\cdot| = q^{-\hat{v}}$ em $\hat{K}$. Note que pela definição que demos para $\hat{v}$ e pela definição da extensão $|\cdot|$, para todo $x \in \hat{K}$ e toda sequência (x_n) de elementos de K que converge a x nós temos $\hat{v}(x) = \lim_{n\to\infty} v(x_n)$. Como $(x_n) \to x$, temos $(x - x_n) \to 0 \Rightarrow |x - x_n| \to 0$. Assim, se $x \neq 0$ existe $n_0 \in \mathbb{N}$ tal que $n \geq n_0 \Rightarrow |x - x_n| < |x|$, o que mostra que $\hat{v}(x) < \hat{v}(x - x_n)$. Desse modo, como $\hat{v}$ é valoração que estende v, para todo $n \geq n_0$ nós temos:

$$v(x_n) = \hat{v}(x_n) = \hat{v}(x - (x - x_n)) = \min\{\hat{v}(x), \hat{v}(x - x_n)\} = \hat{v}(x).$$

Assim, vemos que a sequência $(v(x_n))$ é de fato eventualmente constante. Isso nos mostra que $\hat{v}(\hat{K}) = v(K)$. Assim, nós provamos:

Proposição 9.11. *Sejam $(K, v, |\cdot|)$ um corpo e $(\hat{K}, |\cdot|, \hat{v})$ seu completamento. Então os grupos de valores de v e de $\hat{v}$ são iguais, isto é, $v(K) = \hat{v}(\hat{K})$. Em particular, se v for discreta, $\hat{v}$ também será discreta, e se v for discreta normalizada, $\hat{v}$ também será discreta normalizada.*

A métrica induzida por uma valoração possui propriedades bem singulares:

Proposição 9.12. *Seja $(K, v, |\cdot|)$ um corpo. Então:*

(a) Uma sequência (x_n) em K converge a um $x \in K$ se e somente se $\lim_{n\to\infty} v(x - x_n) = \infty$, e é de Cauchy se e somente se $m, n \to \infty \Rightarrow v(x_m - x_n) \to \infty$.

(b) Uma sequência (x_n) em K é de Cauchy se e somente $\lim_{n\to\infty}(x_{n+1} - x_n) = 0$. Em particular, uma sequência de somas parciais $\left(\sum_{j=0}^{n-1} x_j\right)$ é de Cauchy se e somente se $\lim_{n\to\infty} x_n = 0$.

(c) Se K for completo, uma sequência (x_n) em K converge se e só se $\lim_{n\to\infty}(x_{n+1} - x_n) = 0$. Em particular, uma série $\sum_{n=0}^{\infty} x_n$ converge se e só se tivermos $\lim_{n\to\infty} x_n = 0$.

Demonstração. (a) Basta notar que $x_n \to x \iff |x - x_n| \to 0 \iff v(x - x_n) \to \infty$. A afirmação sobre sequências de Cauchy se prova do mesmo modo.

(b) É claro que se (x_n) for de Cauchy então $\lim_{n\to\infty}(x_{n+1} - x_n) = 0$. Reciprocamente, suponhamos que valha essa última condição. Então para todo $C > 0$ existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$ tenhamos $v(x_{n+1} - x_n) > C$. Mas então, para todos $m > n \geq n_0$:

$$\begin{aligned} v(x_m - x_n) &= v((x_m - x_{m-1}) + (x_{m-1} - x_{m-2}) + \cdots + (x_{n+1} - x_n)) \\ &\geq \min\{x_m - x_{m-1}, x_{m-1} - x_{m-2}, \ldots, x_{n+1} - x_n\} > C. \end{aligned}$$

Assim, $m, n \to \infty \Rightarrow v(x_m - x_n) \to \infty$, de modo que (x_n) é sequência de Cauchy.

(c) Segue imediatamente do item anterior.

□

Também temos uma relação entre os anéis de valoração de um corpo e de seu completamento. Para isso, usaremos a notação $(K, v, |\cdot|, A, \mathfrak{p}, \kappa)$ para indicar que K é um corpo com valoração v, valor absoluto associado $|\cdot|$ e domínio de valoração associado A, com único ideal maximal $\mathfrak{p}$ e corpo de resíduos $\kappa = A/\mathfrak{p}$. Eventualmente, omitiremos algumas dessas informações, por exemplo escrevendo $(K, v, |\cdot|)$ ou então $(K, v, A, \mathfrak{p}, \kappa)$.

Proposição 9.13. *Sejam $(K, v, |\cdot|, A, \mathfrak{p}, \kappa)$ um corpo e $(\hat{K}, |\cdot|, \hat{v}, \hat{A}, \hat{\mathfrak{p}}, \hat{\kappa})$ seu completamento. Então:*

(a) $A = \hat{A} \cap K$, e $\hat{A}$ é o fecho de A em $\hat{K}$ com relação a $|\cdot|$.

(b) $\mathfrak{p} = \hat{\mathfrak{p}} \cap K = \hat{\mathfrak{p}} \cap A$. Assim, $\hat{\mathfrak{p}} \mid \mathfrak{p}$. Além disso, $\hat{\mathfrak{p}}$ é o fecho de $\mathfrak{p}$ em $\hat{K}$ com relação a $|\cdot|$. Se v for discreta, teremos ainda $\mathfrak{p}^n = \hat{\mathfrak{p}}^n \cap K = \hat{\mathfrak{p}}^n \cap A$ para todo inteiro positivo n, de modo que $\hat{\mathfrak{p}}^n \mid \mathfrak{p}^n$ nesse caso, e além disso $\hat{\mathfrak{p}}^n$ será o fecho de $\mathfrak{p}^n$ em $\hat{K}$ com relação a $|\cdot|$.

(c) Nós temos um isomorfismo de corpos residuais $\kappa \cong \hat{\kappa}$, dado por $a + \mathfrak{p} \mapsto a + \hat{\mathfrak{p}}$. Além disso, se v for discreta, então para todo n inteiro positivo nós temos um isomorfismo de anéis $A/\mathfrak{p}^n \cong \hat{A}/\hat{\mathfrak{p}}^n$, dado por $a + \mathfrak{p}^n \mapsto a + \hat{\mathfrak{p}}^n$.

Demonstração. (a) Nós temos

$$A = \{x \in K \colon v(x) \geq 0\} = \{x \in K \colon \hat{v}(x) \geq 0\} = \hat{A} \cap K.$$

Mostremos agora que $\hat{A}$ é o fecho de A em $\hat{K}$. Denotemos por $\overline{A}$ esse fecho. Seja $x \in \overline{A}$. Então existe uma sequência de Cauchy (x_n) em A com $x = \lim_{n\to\infty} x_n$. Em particular, $\hat{v}(x) = \lim_{n\to\infty} v(x_n) \geq 0$. Isso mostra que $x \in \hat{A}$, e portanto $\overline{A} \subseteq \hat{A}$.

Reciprocamente, seja $x \in \hat{A}$. Se $x = 0$, é claro que $x \in \overline{A}$. Assim, suponhamos $x \neq 0$. Como K é denso em $\hat{K}$, existe uma sequência (x_n) em K com $x = \lim_{n\to\infty} x_n$. Sabemos que $\lim_{n\to\infty} v(x_n) = \hat{v}(x)$. Como já observamos, existe $n_0 \in \mathbb{N}$ tal que $v(x_n) = \hat{v}(x) \geq 0$ para todo $n \geq n_0$. Assim, para todo $n \geq n_0$, temos $x_n \in A$, de modo que x é limite de uma sequência de elementos de A. Isso prova que $\hat{A} \subseteq \overline{A}$, e portanto $\hat{A} = \overline{A}$, como queríamos.

(b) Nós temos

$$\mathfrak{p} = \{x \in K \colon v(x) > 0\} = \{x \in K \colon \hat{v}(x) > 0\} = \hat{\mathfrak{p}} \cap K = \hat{\mathfrak{p}} \cap A.$$

Suponhamos agora que v seja discreta, sem perda de generalidade normalizada. Nesse caso, $\hat{v}$ também será discreta normalizada, logo para todo n inteiro positivo nós temos:

$$\mathfrak{p}^n = \{x \in K \colon v(x) \geq n\} = \{x \in K \colon \hat{v}(x) \geq n\} = \hat{\mathfrak{p}}^n \cap K = \hat{\mathfrak{p}}^n \cap A.$$

As afirmações sobre os fechos se demonstram da mesma forma que no item (a).

(c) Como $A \subseteq \hat{A}$ e $\hat{p} \mid \mathfrak{p}$, a função $\kappa \to \hat{\kappa}$ dada por $a + \mathfrak{p} \mapsto a + \hat{\mathfrak{p}}$ é um homomorfismo injetor. Mostremos sua sobrejetividade. Seja $x \in \hat{A}$ qualquer. Como $\hat{A}$ é o fecho de A em $\hat{K}$, existe $a \in A$ tal que $|x - a| < 1$, o que equivale a $\hat{v}(x - a) > 0$. Isso significa que $x - a \in \hat{\mathfrak{p}}$, logo $x + \hat{\mathfrak{p}} = a + \hat{\mathfrak{p}}$. Isso mostra que o homomorfismo em questão é sobrejetor, e portanto um isomorfismo.

Suponhamos agora que v seja discreta, e seja n um inteiro positivo. Como $\hat{\mathfrak{p}}^n \mid \mathfrak{p}^n$, a função $A/\mathfrak{p}^n \to \hat{A}/\hat{\mathfrak{p}}^n$ dada por $a + \mathfrak{p}^n \mapsto a + \hat{\mathfrak{p}}^n$. é um homomorfismo injetor. Como $\hat{A}$ é o fecho de A em $\hat{K}$, existe $a \in A$ tal que $\hat{v}(x - a) \geq n$. Isso significa que $x - a \in \hat{\mathfrak{p}}^n$, logo $x + \hat{\mathfrak{p}}^n = a + \hat{\mathfrak{p}}^n$. Isso mostra que o homomorfismo em questão é sobrejetor, e portanto um isomorfismo.

□

O teorema acima nos diz que podemos identificar κ com $\hat{\kappa}$, e mais geralmente $A/\mathfrak{p}^n$ com $\hat{A}/\hat{\mathfrak{p}}^n$ caso v seja discreta. É o que faremos de agora em diante. Assim, dado $a \in \hat{A}$, denotaremos $a \pmod{\mathfrak{p}}$ para indicar $a \pmod{\hat{\mathfrak{p}}}$, e caso v for discreta denotaremos $a \pmod{\mathfrak{p}^n}$ para indicar $a \pmod{\hat{\mathfrak{p}}^n}$.

Mostraremos agora que, se v for discreta, nós conseguimos representar todo elemento de $\hat{K}$ de forma única como uma "série de Laurent" no normalizador de A, com coeficientes em certo conjunto:

Proposição 9.14. *Sejam $(K, v, A, \mathfrak{p})$ um corpo e $(\hat{K}, \hat{v}, \hat{A}, \hat{\mathfrak{p}})$ seu completamento. Suponhamos que v seja uma valoração discreta normalizada, e seja π um normalizador de A. Então:*

(a) π também é um normalizador de $\hat{A}$, e $\mathfrak{p}\hat{A} = \hat{\mathfrak{p}}$.

(b) Toda série da forma $\sum_{n=0}^{\infty} c_j \pi^j$, onde cada $c_j \in A$, converge em $\hat{A}$.

(c) Seja $S \subseteq A$ um sistema completo de representantes de $A/\mathfrak{p}$ tal que $0 \in S$. Então todo $x \in \hat{K}^\times$ admite representação única como uma série convergente $x = \pi^m \sum_{j=0}^{\infty} a_j \pi^j$, onde $a_j \in S$ para todo $j \in \mathbb{N}$, $a_0 \neq 0$ e $m \in \mathbb{Z}$. Além disso, $\hat{v}(x) = m$.

Demonstração. (a) Temos $v(\pi) = 1$, logo $\hat{v}(\pi) = v(\pi) = 1$, de onde vemos que π também é um normalizador de $\hat{A}$. Assim, $\mathfrak{p}\hat{A} = (\pi A)\hat{A} = \pi\hat{A} = \hat{\mathfrak{p}}$.

(b) A convergência dessa série em $\hat{K}$ equivale a termos $\lim_{n\to\infty} c_n\pi^n = 0$, pela Proposição 9.12. Mas $\hat{v}(c_n\pi^n) \geq \hat{v}(\pi^n) = n$, de modo que $\lim_{n\to\infty} c_n\pi^n = 0$ por essa mesma proposição. Assim, essa série converge. Finalmente, pela Proposição 9.13 essa série converge para um elemento de $\hat{A}$, já que é um limite de elementos de A.

(c) Seja $x \in \hat{K}$ qualquer. Como π é o normalizador de $\hat{A}$, podemos escrever de modo único $x = \pi^m u$, onde $m = \hat{v}(x)$ e $u \in \hat{A}^\times$. Como $\hat{A}/\hat{\mathfrak{p}} \cong A/\mathfrak{p}$, existe um único $a_0 \in S$ tal que $u \equiv a_0 \pmod{\hat{\mathfrak{p}}}$. Note que $a_0 \neq 0$, já que $u \notin \hat{\mathfrak{p}}$. Então podemos escrever $u = a_0 + b_1\pi$, para algum $b_1 \in \hat{A}$. Seja $a_1 \in S$ único tal que $b_1 \equiv a_1 \pmod{\hat{\mathfrak{p}}}$. Então existe $b_2 \in \hat{A}$ tal que $b_1 = a_1 + b_2\pi$, e portanto $u = a_0 + (a_1 + b_2\pi)\pi = a_0 + a_1\pi + b_2\pi^2$.

Continuando dessa forma, suponhamos que encontramos $a_0, a_1, \ldots, a_{n-1} \in \hat{A}$ e $b_n \in \hat{A}$ tais que $u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + b_n\pi^n$. Então existe um único $a_n \in S$ tal que $b_n \equiv a_n \pmod{\hat{\mathfrak{p}}}$. Sendo $b_{n+1} \in \hat{A}$ tal que $b_n = a_n + b_{n+1}\pi$, nós temos:

$$\begin{aligned} u &= a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + (a_n + b_{n+1}\pi)\pi^n \\ &= a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n + b_{n+1}\pi^{n+1}. \end{aligned}$$

Desse modo, obtemos uma sequência de somas parciais $(s_n) = \left(\sum_{j=0}^{n-1} a_j\pi^j\right)$. Como para cada $n \in \mathbb{N}$ temos $\hat{v}(u - s_n) = \hat{v}(b_n\pi^n) \geq n$, vemos que $\lim_{n\to\infty} \hat{v}(u - s_n) = \infty$, e portanto $\lim_{n\to\infty} s_n = u$. Concluímos que $u = \sum_{j=0}^{\infty} a_j\pi^j$. Assim, nós obtemos a representação $x = \pi^m \sum_{j=0}^{\infty} a_j\pi^j$, onde $a_j \in S$ para todo $j \in \mathbb{N}$, $a_0 \neq 0$ e $m = \hat{v}(x) \in \mathbb{Z}$.

Para mostrar a unicidade, suponhamos que $x = \pi^\ell \sum_{j=0}^{\infty} b_j\pi^j$, para $\ell \in \mathbb{Z}$, $b_j \in S$ para todo $j \in \mathbb{N}$ e $b_0 \neq 0$. Como para todo $n \geq 0$ temos $\hat{v}\left(\sum_{j=0}^{n-1} b_j\pi^j\right) = 0$ já que $b_0 \notin \hat{\mathfrak{p}}$, temos $\hat{v}\left(\sum_{j=0}^{\infty} b_j\pi^j\right) = \lim_{n\to\infty} \hat{v}\left(\sum_{j=0}^{n-1} b_j\pi^j\right) = 0$. Assim, vemos que $\hat{v}(x) = \ell$. Como $\hat{v}(x) = m$, vemos que $\ell = m$, e portanto nós temos $\sum_{j=0}^{\infty} a_j\pi^j = \sum_{j=0}^{\infty} b_j\pi^j \Rightarrow \sum_{j=0}^{\infty}(a_j - b_j)\pi^j = 0$. Então $\hat{v}\left(\sum_{j=0}^{\infty}(a_j - b_j)\pi^j\right) = \infty$. Se tivéssemos $a_j \neq b_j$ para algum $j \in \mathbb{N}$, é fácil ver que valeria $\hat{v}\left(\sum_{j=0}^{\infty}(a_j - b_j)\pi^j\right) = \min\{j \in \mathbb{N} \colon a_j \neq b_j\} < \infty$, um absurdo! Concluímos que $a_j = b_j$ para todo $j \in \mathbb{N}$, mostrando a unicidade.

□

Nós podemos ainda dar uma outra caracterização para $\hat{A}$, por meio de **limites projetivos**. Para isso, continuaremos na hipótese de v ser discreta normalizada. Consideremos o anel $\prod_{n=1}^{\infty} A/\mathfrak{p}^n$. Dizemos que uma sequência $(x_n \pmod{\mathfrak{p}^n})$ nesse anel é **coerente** se para todos $m < n$ nós tivermos $x_n \equiv x_m \pmod{\mathfrak{p}^m}$. Assim, podemos considerar o subanel definido por

$$\varprojlim_n A/\mathfrak{p}^n := \left\{ x \in \prod_{n=1}^{\infty} A/\mathfrak{p}^n : x \text{ é coerente} \right\}.$$

Ele é chamado de **limite projetivo** dos $A/\mathfrak{p}^n$. Com isso, nós temos o seguinte resultado:

Proposição 9.15. *O mapa canônico $\hat{A} \to \varprojlim_n A/\mathfrak{p}^n$ dado por $a \mapsto (a \pmod{\mathfrak{p}^n})$ é um isomorfismo de anéis.*

Demonstração. Essa mapa é claramente um homomorfismo de anéis, com núcleo $\bigcap_{n\geq 1} \hat{\mathfrak{p}}^n = 0$. Logo esse homomorfismo é injetor. Para mostrar que também é sobrejetor, sejam π um normalizador de A e $S \subseteq A$ um representante de classes de $A/\mathfrak{p}$ com $0 \in S$. Consideremos um elemento $x = (x_n \pmod{\mathfrak{p}^n}) \in \varprojlim_n A/\mathfrak{p}^n$ qualquer. É fácil mostrar por indução em n que existe uma única sequência (a_n) de elementos de S com $x = (x_n \pmod{\mathfrak{p}^n}) = \left(\sum_{j=0}^{n-1} a_j \pi^j \pmod{\mathfrak{p}^n}\right)$. Notemos agora que, pela proposição acima, $\left(\sum_{j=0}^{n-1} a_j \pi^j\right)$ converge a um elemento $a \in \hat{A}$. Finalmente, basta observar que $x = (x_n \pmod{\mathfrak{p}^n}) = (a \pmod{\mathfrak{p}^n})$ é a imagem de a pelo homomorfismo acima, que portanto é sobrejetor. Assim, esse mapa é um isomorfismo de anéis. □

9.3. Os números p-ádicos

Nessa seção, definiremos os **números p-ádicos** a partir do que fizemos nas seções anteriores. A Proposição 9.6 nos diz que todo valor absoluto de $\mathbb{Q}$ é da forma $|\cdot|_p$, para $p \in \mathbb{N}$ primo ou $p = \infty$. O completamento de $(\mathbb{Q}, |\cdot|_\infty)$ é $(\mathbb{R}, |\cdot|_\infty)$, e também podemos denotar $\mathbb{R} = \mathbb{Q}_\infty$. Os corpos p-ádicos surgem como o completamento de $\mathbb{Q}$ com relação aos seus outros valores absolutos:

Definição (Corpo dos Números p-ádicos/Anel dos Inteiros p-ádicos)**.** Seja $p \in \mathbb{N}$ um primo. Chamamos de **corpo dos números p-ádicos** o completamento do corpo $(\mathbb{Q}, v_p, |\cdot|_p, \mathbb{Z}_{(p)})$, e o denotamos por $(\mathbb{Q}_p, v_p, |\cdot|_p, \mathbb{Z}_p)$. Seu domínio de valoração discreta $\mathbb{Z}_p$ é chamado de **anel de inteiros p-ádicos**. Chamamos os elementos de $\mathbb{Q}_p$ de **números p-ádicos**, e os elementos de $\mathbb{Z}_p$ de **inteiros p-ádicos**.

Observe que de fato $\mathbb{Z}_p$ é um DVD, devido à Proposição 9.11. Nós também chamaremos as extensões de $|\cdot|_p$ e v_p a $\mathbb{Q}_p$ de **valor absoluto p-ádico** e **valoração p-ádica**, respectivamente. Do mesmo modo, a métrica induzida por essas extensões também será chamada de **métrica p-ádica**.

Teorema 9.16. *Seja $p \in \mathbb{N}$ um primo. Então:*

(a) O único ideal maximal de $\mathbb{Z}_p$ é $p\mathbb{Z}_p$. Equivalentemente, p é um normalizador de $\mathbb{Z}_p$.

(b) $\mathbb{Z}_p$ é o fecho de $\mathbb{Z}$ em $\mathbb{Q}_p$ com relação a $|\cdot|_p$.

(c) Nós temos um isomorfismo canônico de anéis $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ para todo inteiro positivo n, dado por $a \pmod{p^n} \mapsto a \pmod{p^n\mathbb{Z}_p}$. Em particular, $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Assim, dado $x \in \mathbb{Z}_p$ qualquer, podemos denotar $a \pmod{p^n}$ para indicar $a \pmod{p^n\mathbb{Z}_p}$.

(d) Toda série da forma $\sum_{n=0}^{\infty} c_j p^j$, onde cada $c_j \in \mathbb{Z}$, converge em $\mathbb{Z}_p$.

(e) *Todo* $x \in \mathbb{Q}_p^\times$ *admite representação única como uma série convergente* $x = p^m \sum_{j=0}^{\infty} a_j p^j$, *onde* $a_j \in \{0, 1, \ldots, p-1\}$ *para todo* $j \in \mathbb{N}$, $a_0 \neq 0$ *e* $m \in \mathbb{Z}$. *Além disso,* $v_p(x) = m$.

(f) *O mapa canônico* $\mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ *dado por* $a \mapsto (a \pmod{p^n})$ *é um isomorfismo de anéis.*

(g) *Seja* $\mathbb{Z}[\![x]\!] := \left\{\sum_{j=0}^{\infty} a_j x^j : a_j \in \mathbb{Z}\right\}$ *o anel das séries formais com coeficientes em* $\mathbb{Z}$. *Então* $\mathbb{Z}[\![x]\!]/\langle x-p\rangle \cong \mathbb{Z}_p$, *com isomorfismo dado por* $\sum_{j=0}^{\infty} a_j x^j + \langle x-p\rangle \mapsto \sum_{j=0}^{\infty} a_j p^j$.

Demonstração. (a) Segue diretamente de $v_p(p) = 1$.

(b) Chamemos o fecho de $\mathbb{Z}$ em $\mathbb{Q}_p$ de $\hat{\mathbb{Z}}$. Pela Proposição 9.13, sabemos que $\mathbb{Z}_p$ é o fecho de $\mathbb{Z}_{(p)}$ com relação a $|\cdot|$. Assim, basta mostrarmos que $\mathbb{Z}_{(p)} \subseteq \hat{\mathbb{Z}}$. Para isso, seja $x \in \mathbb{Z}_{(p)}$ qualquer. Pelo Teorema 3.25, para todo inteiro positivo n temos $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ por meio de $a \pmod{p^n} \mapsto a \pmod{p^n\mathbb{Z}_{(p)}}$. Assim, conseguimos encontrar $a \in \mathbb{Z}$ tal que $a \equiv x \pmod{p^n\mathbb{Z}_{(p)}}$, de modo que $v_p(a-x) \geq n$. Como n é um inteiro positivo qualquer, concluímos que podemos aproximar x tão bem quanto quisermos por inteiros, mostrando o resultado desejado.

(c) Basta compor os isomorfismos canônicos $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ e $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$, dados pelo Teorema 3.25 e pela Proposição 9.13, respectivamente.

(d) Segue do item (b) da Proposição 9.14

(e) Segue do item (c) da Proposição 9.14, juntamente com o fato de que $0, 1, \ldots, p-1$ formam um sistema completo de representantes módulo $\mathbb{Z}_p/p\mathbb{Z}_p$ devido a (c).

(f) Segue diretamente da Proposição 9.15 e do isomorfismo canônico $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ dado pelo Teorema 3.25

(g) Consideremos o homomorfismo $\mathbb{Z}[\![x]\!] \to \mathbb{Z}_p$ dado por $\sum_{j=0}^{\infty} a_j x^j \mapsto \sum_{j=0}^{\infty} a_j p^j$. Pelo item (e), esse homomorfismo é sobrejetor. Para concluir a demonstração, mostraremos que o núcleo desse homomorfismo é $\langle x-p\rangle$. Se $g(x) \in \mathbb{Z}[\![x]\!]$, então $(x-p)g(x)$ é levado em $(p-p)g(p) = 0$, de modo que $\langle x-p\rangle$ está contido no núcleo desse homomorfismo.

Seja agora $f(x) = \sum_{j=0}^{\infty} a_j x^j \in \mathbb{Z}[x]$ tal que $f(p) = \sum_{j=0}^{\infty} a_j p^j = 0$. Queremos mostrar que $f(x) \in \langle x-p\rangle$. Assim, queremos mostrar que existem $b_0, b_1, \ldots \in \mathbb{Z}$ para os quais tenhamos

$$f(x) = \sum_{j=0}^{\infty} a_j x^j = (x-p)\sum_{j=0}^{\infty} b_j x^j = \sum_{j=0}^{\infty} (b_{j-1} - pb_j)x^j,$$

onde definimos $b_{-1} = 0$. Desse modo, queremos encontrar inteiros b_j's tais que $a_j = b_{j-1} - pb_j$, para todo $j \in \mathbb{N}$. Note que essas equações nos permitem obter os b_j's por recorrência. Nós temos $b_0 = -a_0/p$, e $b_j = (b_{j-1} - a_j)/p$, para todo inteiro positivo j. Definindo os b_j's desse modo, valerá a igualdade $f(x) = (x-p)\sum_{j=0}^{\infty} b_j x^j$. Falta mostrar que temos $b_j \in \mathbb{Z}$, para todo $j \in \mathbb{N}$. Mas é fácil mostrar por indução que nós temos $b_n = -\frac{1}{p^n}\sum_{j=0}^{n-1} a_j p^j$. Analisando a igualdade $f(p) = 0$ módulo p^n para cada inteiro positivo n, obtemos $\sum_{j=0}^{n-1} a_j p^j \equiv 0 \pmod{p^n}$, de onde vemos que $b_j \in \mathbb{Z}$. Assim, provamos que $f(x) \in \langle x-p\rangle$, concluindo a demonstração.

□

Os itens (e) (f) e (g) do teorema acima nos dão outras caracterizações famosas dos inteiros p-ádicos. De fato, é possível definir o anel dos inteiros p-ádicos como o conjunto das séries formais $\sum_{j=0}^{\infty} a_j p^j$, onde cada $a_j \in \{0, 1, \ldots, p-1\}$, e então provar suas propriedades. Desse ponto de

vista, os inteiros p-ádicos generalizam a representação em base p. A partir dessa caracterização de $\mathbb{Z}_p$, é fácil calcularmos a sua cardinalidade: $|\mathbb{Z}_p| = |p^{\mathbb{N}}| = 2^{\aleph_0}$. Assim, $\mathbb{Z}_p$, e portanto também $\mathbb{Q}_p$, possuem a mesma cardinalidade dos reais.

Se $x \in \mathbb{Z}_p$ se escreve como $x = \sum_{j=0}^{\infty} a_j p^j$, com cada $a_j \in \{0, 1, \ldots, p-1\}$, nós chamamos essa série de **expansão p-ádica** de x. Note que a expansão p-ádica de um inteiro positivo é simplesmente sua representação em base p. Para calcularmos a expansão p-ádica de um $x \in \mathbb{Z}_p$ qualquer, notemos que para todo inteiro positivo n devemos ter $x \equiv \sum_{j=0}^{n-1} a_j p^j \pmod{p^n}$. Por outro lado, dado $a \in \mathbb{Z}$ qualquer, é fácil mostrar que existem únicos $a_0, \ldots, a_{n-1} \in \{0, 1, \ldots, p-1\}$ tais que $a \equiv \sum_{j=0}^{n-1} a_j p^j \pmod{p^n}$. Assim, para calcularmos a expansão p-ádica de um elemento de $\mathbb{Z}_p$ basta conhecermos seus restos módulo potências de p.

Exemplo 9.17. *Calculemos as expansões p-ádicas de -1 e de $1/(1-p)$:*

- *Nós temos, para todo inteiro positivo n, $p^n - 1 = (p-1) + (p-1)p + \cdots + (p-1)p^{n-1}$. Assim, $-1 \equiv (p-1) + (p-1)p + \cdots + (p-1)p^{n-1} \pmod{p^n}$. Isso mostra que a expansão p-ádica de -1 é $-1 = \sum_{j=0}^{\infty}(p-1)p^j$.*

- *Nós temos, para todo inteiro positivo n, $\frac{1-p^n}{1-p} = 1 + p + \cdots + p^{n-1}$. Sendo assim:*

$$\frac{1}{1-p} = \frac{1 + p + \cdots + p^{n-1}}{1 - p^n} \equiv 1 + p + \cdots + p^{n-1} \pmod{p^n}.$$

  Isso mostra que a expansão p-ádica de $1/(1-p)$ é $1/(1-p) = \sum_{j=0}^{\infty} p^j$. Note que isso se assemelha muito à igualdade $1/(1-x) = \sum_{j=0}^{\infty} x^j$, que vale nos anéis de séries formais, ou ainda à fórmula da soma de uma PG. De fato, essa é uma PG em $\mathbb{Z}_p$ já que $|p|_p = p^{-1} < 1$. Uma das vantagens de construirmos $\mathbb{Q}_p$ por meio de completamentos é justamente dar um sentido que não seja puramente formal a uma série dessa forma.

O que fizemos nos dá uma família de infinitos completamentos de $\mathbb{Q}$ (que são todos os completamentos possíveis): $\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \ldots, \mathbb{Q}_\infty = \mathbb{R}$. Esses corpos são dois a dois não-isomorfos, como veremos mais adiante. Os diferentes valores absolutos p-ádicos se relacionam do seguinte modo:

Proposição 9.18 (Fórmula do Produto)**.** *Para todo número racional $x \neq 0$, vale a relação $\prod_p |x|_p = 1$, onde p varia entre os números primos de $\mathbb{N}$ e ∞.*

Demonstração. Note que podemos escrever $x = \frac{x}{|x|_\infty} \cdot \prod_{p \text{ primo}} p^{v_p(x)}$ (observe que $x/|x|_\infty$ é o sinal de x). Desse modo:

$$1 = \frac{1}{|x|_\infty} \cdot \prod_{p \text{ primo}} p^{v_p(x)} = |x|_\infty^{-1} \prod_{p \text{ primo}} |x|_p^{-1} \Rightarrow \prod_p |x|_p = 1.$$

□

Terminaremos essa seção vendo a importância dos números p-ádicos para a resolução de equações diofantinas. Para isso, consideremos um polinômio $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. Estamos interessados em resolver a equação diofantina $F(x_1, \ldots, x_n) = 0$. Notemos que a existência de uma solução para essa equação implica na existência de uma solução para a equação $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}$, para todo primo $p \in \mathbb{N}$ e todo inteiro positivo ν. Com os inteiros p-ádicos, nós conseguimos "trocar" a existência de uma solução para todas as infinitas congruências $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}$ pela existência de solução de uma única equação nos inteiros p-ádicos:

Proposição 9.19. *Seja $F(x_1, \ldots, x_n)$ um polinômio com coeficientes inteiros, e seja $p \in \mathbb{N}$ um primo fixado. A congruência $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}$ possui solução para todo inteiro positivo ν se, e somente se, a equação $F(x_1, \ldots, x_n) = 0$ possuir solução nos inteiros p-ádicos.*

Demonstração. ($\Leftarrow$): Suponhamos que existam $f_1, \ldots, f_n \in \mathbb{Z}_p$ tais que $F(f_1, \ldots, f_n) = 0$. Avaliando módulo p^ν para cada inteiro positivo ν, nós obtemos:

$$F(f_1, \ldots, f_n) \equiv 0 \pmod{p^\nu} \Rightarrow F(f_1 \pmod{p^\nu}, \ldots, f_n \pmod{p^\nu}) \equiv 0 \pmod{p^\nu},$$

o que mostra que a equação $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}$ possui solução.

($\Rightarrow$): Aqui, identificaremos $\mathbb{Z}_p$ com o limite projetivo $\varprojlim_n \mathbb{Z}/p^\nu\mathbb{Z}$.

Suponhamos que para todo inteiro positivo ν a congruência $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}$ possua uma solução $(f_1^\nu \pmod{p^\nu}, \ldots, f_n^\nu \pmod{p^\nu})$. Se $(f_1^\nu \pmod{p^\nu}), \ldots, (f_n^\nu \pmod{p^\nu})$ fossem todas sequências coerentes, definindo $f_j := (f_j^\nu \pmod{p^\nu}) \in \mathbb{Z}_p$ para $1 \leq j \leq n$ nós concluiríamos que $F(f_1, \ldots, f_n) \equiv 0 \pmod{p^\nu}$ para todo inteiro positivo ν, o que implicaria que $F(f_1, \ldots, f_n) = 0$. Assim, obteríamos uma solução para $F(x_1, \ldots, x_n)$ em $\mathbb{Z}_p$, como desejado.

Porém, nem sempre as sequências indicadas são coerentes. O que faremos é extrair subsequências coerentes dessas sequências. Como $\mathbb{N}^*$ é infinito e $\mathbb{Z}/p\mathbb{Z}$ é finito, existem $g_1^1 \in \mathbb{Z}$ e um subconjunto infinito $A_1^1 \subseteq \mathbb{N}^*$ tal que $f_1^\nu \equiv g_1^1 \pmod{p}$ para todo $\nu \in A_1^1$. Da mesma forma, como A_1^1 é infinito e $\mathbb{Z}/p\mathbb{Z}$ é finito, existem $g_2^1 \in \mathbb{Z}$ e um subconjunto infinito $A_2^1 \subseteq A_1^1$ tais que $f_2^\nu \equiv g_2^1 \pmod{p}$ para todo $\nu \in A_2^1$. Continuando desse modo, nós obtemos um conjunto infinito

$$A^1 := A_n^1 \subseteq A_{n-1}^1 \subseteq \cdots \subseteq A_1^1 \subseteq \mathbb{N}^*$$

e inteiros $g_1^1, \ldots, g_n^1$ tais que para todo $\nu \in A^1$ tenhamos $f_1^\nu \equiv g_1^1 \pmod{p}, \ldots, f_n^\nu \equiv g_n^1 \pmod{p}$. Notemos que, fixado $\nu \in A^1$, nós temos $F(g_1^1, \ldots, g_n^1) \equiv F(f_1^\nu, \ldots, f_n^\nu) \pmod{p}$. Mas como $\nu \geq 1$ e $F(f_1^\nu, \ldots, f_n^\nu) \equiv 0 \pmod{p^\nu}$ por hipótese, concluímos que

$$F(g_1^1, \ldots, g_n^1) \equiv F(f_1^\nu, \ldots, f_n^\nu) \equiv 0 \pmod{p}.$$

Façamos agora um processo parecido. Como $\mathbb{Z}/p^2\mathbb{Z}$ é finito, nós podemos obter um conjunto infinito

$$A^2 := A_n^2 \subseteq A_{n-1}^2 \subseteq \cdots \subseteq A_1^2 \subseteq A^1$$

e inteiros $g_1^2, \ldots, g_n^2$ tais que para todo $\nu \in A^2$ tenhamos $f_1^\nu \equiv g_1^2 \pmod{p^2}, \ldots, f_n^\nu \equiv g_n^2 \pmod{p^2}$. Notemos que, fixado $\nu \in A^2$ com $\nu \geq 2$, nós temos $F(g_1^2, \ldots, g_n^2) \equiv F(f_1^\nu, \ldots, f_n^\nu) \equiv 0 \pmod{p^2}$, já que $\nu \geq 2$. Continuando esse processo, para cada inteiro positivo k nós podemos obter um conjunto infinito

$$A^k := A_n^k \subseteq A_{n-1}^k \subseteq \cdots \subseteq A_1^k \subseteq A^{k-1}$$

e inteiros $g_1^k, \ldots, g_n^k$ tais que para todo $\nu \in A^k$ tenhamos $f_1^\nu \equiv g_1^k \pmod{p^k}, \ldots, f_n^\nu \equiv g_n^k \pmod{p^k}$. Como A^k é infinito, fixando $\nu \geq k$ nesse conjunto nós obtemos

$$F(g_1^k, \ldots, g_n^k) \equiv F(f_1^\nu, \ldots, f_n^\nu) \equiv 0 \pmod{p^k}.$$

Com isso, nós obtemos sequências $(g_1^k), \ldots, (g_n^k)$ de inteiros de modo que $F(g_1^k, \ldots, g_n^k) \equiv 0 \pmod{p^k}$ para todo inteiro positivo k. Afirmamos que essas sequências induzem sequências coerentes $(g_1^k \pmod{p^k}), \ldots, (g_n^k \pmod{p^k})$. Fixemos $1 \leq j \leq n$, e sejam $k < \ell$ inteiros positivos. Escolhemos $\nu \in A^\ell$ qualquer. Então $f_j^\nu \equiv g_j^\ell \pmod{p^\ell}$, e como $\nu \in A^\ell \subseteq A^k$ temos também $f_j^\nu \equiv g_j^k \pmod{p^k}$. Desse modo, $g_j^\ell \equiv f_j^\nu \equiv g_j^k \pmod{p^k}$, como queríamos.

Com isso, podemos definir $g_1 := (g_1^k \pmod{p^k}) \in \mathbb{Z}_p, \ldots, g_n := (g_1^k \pmod{p^k}) \in \mathbb{Z}_p$. Afirmamos que $F(g_1, \ldots, g_n) = 0$. De fato, como soma e multiplicação em $\mathbb{Z}_p$ são dadas coordenada a coordenada, nós temos:

$$\begin{aligned} F(g_1, \ldots, g_n) &= (F(g_1^k \pmod{p^k}, \ldots, g_n^k \pmod{p^k})) \\ &= (F(g_1^k, \ldots, g_n^k) \pmod{p^k}) \\ &= (0 \pmod{p^k}) = 0. \end{aligned}$$

Isso prova que a equação $F(x_1, \ldots, x_n) = 0$ tem solução em $\mathbb{Z}_p$, como queríamos. □

Capítulo 10

Extensões de Valores Absolutos

Nosso objetivo neste capítulo é estudar as extensões algébricas L/K de um corpo com valor absoluto $(K, |\cdot|)$, e como podemos estender o valor absoluto de K para L.

10.1. O Lema de Hensel

O caso em que mais podemos tirar informações é quando $(K, |\cdot|)$ é completo. Se $|\cdot|$ for arquimediano, então o Teorema de Ostrowski nos garante que $K \cong \mathbb{R}$ ou $K \cong \mathbb{C}$. Suponhamos então que $|\cdot|$ seja não-arquimediano. Nesse caso, temos uma valoração v associada. Denotaremos $(K, v, |\cdot|, A, \mathfrak{p}, \kappa)$. Nesse contexto, aparece o **Lema de Hensel**. Como veremos, além de ser fundamental no estudo de extensões de valorações esse resultado é importante por si só, tendo aplicações diretas no estudo da estrutura de $\mathbb{Z}_p$ e na resolução de congruências módulo potências de primos.

Definição (Conteúdo/Polinômio Primitivo)**.** Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$. Definimos o **conteúdo** de f como sendo $|f| := \max\{|a_0|, \ldots, |a_n|\}$. O polinômio f é chamado de **primitivo** se $|f| = 1$. Note que isso é equivalente a dizer que algum dos coeficientes $a_0, \ldots, a_n$ não está em $\mathfrak{p}$. Denotaremos ainda $f \not\equiv 0 \pmod{\mathfrak{p}}$.

Com essa definição, conseguimos enunciar o Lema de Hensel:

Teorema 10.1 (Lema de Hensel)**.** *Seja $(K, v, |\cdot|, A, \mathfrak{p}, \kappa)$ um corpo completo. Suponhamos que um polinômio primitivo $f \in A[x]$ admita módulo $\mathfrak{p}$ uma fatoração $f \equiv \overline{g}\overline{h} \pmod{\mathfrak{p}}$, onde $\overline{g}, \overline{h} \in \kappa[x]$ são coprimos. Então f admite uma fatoração $f = gh$ em polinômios $g, h \in A[x]$ tais que $\partial\, g = \partial\, \overline{g}$, $g \equiv \overline{g} \pmod{\mathfrak{p}}$ e $h \equiv \overline{h} \pmod{\mathfrak{p}}$.*

Demonstração. Indiquemos por $\overline{f} \in \kappa[x]$ o polinômio induzido por f. Sendo f primitivo, vemos que $\overline{f} \neq 0$. Como $\overline{f} = \overline{g}\,\overline{h}$, vemos que $\partial\, \overline{f} = \partial\, \overline{g} + \partial\, \overline{h} \Rightarrow \partial\, \overline{h} = \partial\, \overline{f} - \partial\, \overline{g} \leq \partial\, f - \partial\, \overline{g}$. Chamemos $d := \partial\, f$ e $m := \partial\, \overline{g}$. Então $d - m \geq \partial\, \overline{h}$. Assim, conseguimos achar polinômios $g_0(x), h_0(x) \in A[x]$ com $\overline{g} = g_0 \pmod{\mathfrak{p}}$ e $\overline{h} = h_0 \pmod{\mathfrak{p}}$ tais que $\partial\, g_0 = \partial\, \overline{g} = m$ e $\partial\, h_0 = \partial\, \overline{h} \leq d - m$. Como $\overline{g}$ e $\overline{h}$ são coprimos em $\kappa[x]$, conseguimos ainda encontrar polinômios $a(x), b(x) \in A[x]$ tais que $ag_0 + bh_0 \equiv 1 \pmod{\mathfrak{p}}$.

Notemos que $f - g_0 h_0 \in \mathfrak{p}[x]$ e $ag_0 + bh_0 - 1 \in \mathfrak{p}[x]$. Entre todos os coeficientes desses dois polinômios, escolhemos π com maior valor absoluto possível, ou equivalentemente com menor valoração possível. Como $\pi \in \mathfrak{p}$, temos $v(\pi) > 0$. Sendo c qualquer outro coeficiente desses polinômios, vemos que $v(\pi) \leq v(c) \Rightarrow v(c/\pi) \geq 0$. Assim, $c/\pi \in A$. Isso mostra que π divide todos os coeficientes desses dois polinômios. Ou seja, $f \equiv g_0 h_0 \pmod{\pi}$ e $ag_0 + bh_0 \equiv 1 \pmod{\pi}$.

Nosso objetivo é definir sequências (p_n) e (q_n) de polinômios em $A[x]$ satisfazendo $\partial\, p_n < m$ e $\partial\, q_n \leq d - m$ para todo inteiro positivo n, de modo que, para todo inteiro positivo n, definindo os

polinômios $g_{n-1} := g_0 + p_1\pi + \cdots + p_{n-1}\pi^{n-1}$ e $h_{n-1} := h_0 + q_1\pi + \cdots + q_{n-1}\pi^{n-1}$, nós tenhamos $f \equiv g_{n-1}h_{n-1} \pmod{\pi^n}$. O caso $n = 1$ foi visto acima.

Suponhamos por indução que $p_1, \ldots, p_{n-1}$ e $q_1, \ldots, q_{n-1}$ já tenham sido determinados, de modo que $f \equiv g_{n-1}h_{n-1} \pmod{\pi^n}$. Notemos que, uma vez determinados p_n e q_n,nós teremos $g_n = g_{n-1} + p_n\pi^n$ e $h_n = h_{n-1} + q_n\pi^n$. Assim, queremos que valha a congruência

$$\begin{aligned} & f \equiv g_n h_n = (g_{n-1} + p_n\pi^n)(h_{n-1} + q_n\pi^n) \\ \equiv \quad & g_{n-1}h_{n-1} + \pi^n(g_{n-1}q_n + p_n h_{n-1}) \pmod{\pi^{n+1}} \\ \iff \quad & f - g_{n-1}h_{n-1} \equiv \pi^n(g_{n-1}q_n + p_n h_{n-1}) \pmod{\pi^{n+1}}. \end{aligned}$$

Seja $f_n := \pi^{-n}(f - g_{n-1}h_{n-1}) \in A[x]$. Então a última congruência acima equivale à congruência $g_{n-1}q_n + p_n h_{n-1} \equiv f_n \pmod{\pi}$. Como $g_{n-1} \equiv g_0 \pmod{\pi}$ e $h_{n-1} \equiv h_0 \pmod{\pi}$, isso por sua vez equivale a $g_0q_n + h_0p_n \equiv f_n \pmod{\pi}$. Como $ag_0 + bh_0 \equiv 1 \pmod{\pi}$, temos:

$$g_0(af_n) + h_0(bf_n) \equiv f_n \pmod{\pi}.$$

Nós gostaríamos de definir $q_n = af_n$ e $p_n = bf_n$, mas os graus desses polinômios podem ser grandes demais. Para resolver o problema, dividamos bf_n por g_0. Assim, encontramos $q, p_n \in K[x]$, com $\partial\, p_n < \partial\, g_0 = m$, tais que $bf_n = qg_0 + p_n$. Como $g_0 \equiv \overline{g} \pmod{\mathfrak{p}}$ e $\partial\, g_0 = \partial\, \overline{g}$, o coeficiente líder de g_0 não está em $\mathfrak{p}$, e portanto está em $A \setminus \mathfrak{p} = A^\times$. Sendo esse coeficiente líder inversível, vemos que $q(x), p_n(x) \in A[x]$. Assim, multiplicando a igualdade acima por $h_0(x)$ e somando g_0af_n de ambos os lados, nós obtemos:

$$g_0af_n + h_0bf_n = g_0af_n + h_0qg_0 + h_0p_n \Rightarrow f_n \equiv g_0(af_n + h_0q) + h_0p_n \pmod{\pi}.$$

Como $f_n = \pi^{-n}(f - g_{n-1}h_{n-1})$, $\partial\, f = d$ e $\partial(g_{n-1}h_{n-1}) = \partial(g_{n-1}) + \partial(h_{n-1}) \leq m + (d-m) = d$, temos $\partial\, f_n \leq d$. Além disso, $\partial\, g_0 = m$ e $\partial\, h_0p_n < (d-m) + m = d$. Desse modo, como nós temos a congruência $f_n \equiv g_0(af_n + h_0q) + h_0p_n \pmod{\pi}$, vemos que ignorando os coeficientes de $af_n + h_0q$ que são múltiplos de π nós obtemos um polinômio $q_n \in A[x]$ com $\partial\, q_n \leq d - m$. Com isso, nós temos $f_n \equiv g_0q_n + h_0p_n \pmod{\pi}$, e encontramos p_n e q_n que satisfazem as condições desejadas.

Então conseguimos as sequências (p_n) e (q_n), e a partir delas as sequências (g_n) e (h_n). Note que pelas definições de g_n e de h_n e pelas condições nos graus dos p_j's e q_j's nós temos $\partial\, g_n = m$ e $\partial\, h_n \leq d - m$, para todo $n \in \mathbb{N}$. Escrevamos agora g_0 e os p_j's por extenso, digamos:

$$\begin{aligned} g_0(x) &= \gamma_0^0 + \gamma_1^0 x + \cdots + \gamma_{m-1}^0 x^{m-1} + \gamma_m x^m, \text{ e} \\ p_j(x) &= \gamma_0^j + \gamma_1^j x + \cdots + \gamma_{m-1}^j x^{m-1}, \text{ para todo } j \geq 1. \end{aligned}$$

Assim, para todo $n \in \mathbb{N}$, nós temos:

$$g_n = g_0 + p_1\pi + \cdots + p_n\pi^n = \gamma_m x^m + \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n} \gamma_i^j \pi^j \right) x^i.$$

Para $0 \leq i \leq m-1$ os coeficientes de x^i nos g_n's formam uma série $\left(\sum_{j=0}^{n} \gamma_i^j \pi^j\right)$. Como $v(\pi) > 0$, temos $v(\pi^j) = jv(\pi)$ para todo $j \in \mathbb{N}$, logo $v(\pi^j) \to \infty \Rightarrow \pi^j \to 0$. Desse modo, é fácil ver que a série dos coeficientes de x^i converge para um $\gamma_i := \sum_{j=0}^{\infty} \gamma_i^j \pi^j \in A$. Obtemos então um polinômio $g(x) := \gamma_0 + \gamma_1 x + \cdots + \gamma_n x^n$ que é, em certo sentido, o limite dos polinômios $g_n(x)$.

Do mesmo modo, obtemos um polinômio $h(x) \in A[x]$, de grau no máximo $d - m$, que é o "limite" dos polinômios $h_n(x)$. Observemos que, para todo $n \in \mathbb{N}$, nós temos $g \equiv g_{n-1} \pmod{\pi^n}$ e $h \equiv h_{n-1} \pmod{\pi^n}$. Assim, para todo $n \geq 1$, nós temos $gh \equiv g_{n-1}h_{n-1} \equiv f \pmod{\pi^n}$. Ou seja, os coeficientes de gh e de f coincidem módulo π^n para todo inteiro positivo n.

Logo os coeficientes de $f - gh$ estão todos em $\bigcap_{n\geq 1} \pi^n A$. Afirmamos que essa interseção é 0. Seja $\alpha \in \bigcap_{n\geq 1} \pi^n A$ qualquer. Então, para todo $n \geq 1$, temos $\alpha \in \pi^n A \Rightarrow v(\alpha) \geq v(\pi^n) = nv(\pi)$.

Como $nv(\pi) \to \infty$, temos $v(\alpha) = \infty \Rightarrow \alpha = 0$, como queríamos. Assim, todos os coeficientes de $f - gh$ são 0, ou seja, $f = gh$. Finalmente, como $\pi \in \mathfrak{p}$, concluímos que $g \equiv g_0 \equiv \overline{g}_0 \pmod{\mathfrak{p}}$ e $h \equiv h_0 \equiv \overline{h}_0 \pmod{\mathfrak{p}}$, provando o resultado desejado. □

O Lema de Hensel, por vezes, também é conhecido como Lema do Levantamento de Hensel. Isso é devido a uma aplicação desse lema para "levantar" uma raiz em κ para uma raiz em A, ou ainda "levantar" uma solução de uma congruência módulo p para soluções dessa congruência módulo potências de p. De fato, nós temos os seguintes corolários, que também são conhecidos como Lema de Hensel:

Corolário 10.2 (Lema de Hensel)**.** *Seja $(K, A, \mathfrak{p}, \kappa)$ um corpo completo. Sejam $f \in A[x]$ um polinômio e $\overline{f} = f \pmod{\mathfrak{p}} \in \kappa[x]$. Suponhamos que $\overline{a} \in \kappa$ satisfaça $\overline{f}(\overline{a}) = 0$ e $\overline{f}'(\overline{a}) \neq 0$. Então existe um único $a \in A$ tal que $\overline{a} = a \pmod{\mathfrak{p}}$ e $f(a) = 0$.*

Demonstração. Como $\overline{f}(\overline{a}) = 0$ e $\overline{f}'(\overline{a}) \neq 0$, vemos que $\overline{a}$ é uma raiz simples de $\overline{f}$. Assim, $\overline{f}(x) = (x - \overline{a})\overline{h}(x)$, onde $\overline{h} \in \kappa[x]$ e $x - \overline{a} \nmid \overline{h}(x)$. Podemos então aplicar o Lema de Hensel para concluir que existem $a \in A$ e $h(x) \in A[x]$ tais que $f(x) = (x - a)h(x)$, $a \pmod{\mathfrak{p}} = \overline{a}$ e $h \pmod{\mathfrak{p}} = \overline{h}$. Assim, $f(a) = 0$ e vemos que a satisfaz todas as condições desejadas.

Finalmente, para mostrar a unicidade de a, suponhamos que exista $b \neq a$ em A com $f(b) = 0$ e $b \equiv a \pmod{\mathfrak{p}}$. Então devemos ter $h(b) = 0$, e portanto $h(a) \equiv h(b) \equiv 0 \pmod{\mathfrak{p}}$, um absurdo já que $x - \overline{a} \nmid \overline{h}(x)$. □

Corolário 10.3 (Lema de Hensel)**.** *Seja $p \in \mathbb{N}$ um primo.*

(a) Seja $f \in \mathbb{Z}_p[x]$, e suponhamos que $a \in \mathbb{Z}_p$ satisfaça $f(a) \equiv 0 \pmod{p}$ e $f'(a) \not\equiv 0 \pmod{p}$. Então existe um único $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$ e $\alpha \equiv a \pmod{p}$.

(b) Seja $f \in \mathbb{Z}[x]$, e suponhamos que $a \in \mathbb{Z}$ satisfaça $f(a) \equiv 0 \pmod{p}$ e $f'(a) \not\equiv 0 \pmod{p}$. Então, para todo inteiro positivo n, existe $\alpha_n \in \mathbb{Z}$ tal que $f(\alpha) \equiv 0 \pmod{p^n}$ e tenhamos $\alpha_n \equiv a \pmod{p}$.

Demonstração. (a) Segue facilmente do corolário acima.

(b) Seja $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$ em $\mathbb{Z}_p$ e $\alpha \equiv a \pmod{p}$, que existe pelo item (a). Para cada n inteiro positivo, seja $\alpha_n \in \mathbb{Z}$ tal que $\alpha_n \equiv \alpha \pmod{p^n}$. Então $f(\alpha_n) \equiv f(\alpha) = 0 \pmod{p^n}$ e $\alpha_n \equiv \alpha \equiv a \pmod{p}$, mostrando existência.

□

Exemplo 10.4. *Sejam $p \in \mathbb{N}$ um primo, n um inteiro positivo e $a \in \mathbb{Z}$. Procuramos determinar se existem raízes n-ésimas de a em $\mathbb{Q}_p$, ou seja, raízes do polinômio $x^n - a$ em $\mathbb{Q}_p$. Comecemos observando que, se $\alpha \in \mathbb{Q}_p$ for tal que $\alpha^n = a$, então $|\alpha|_p = \sqrt[n]{|a|_p} \leq 1$, e portanto $\alpha \in \mathbb{Z}_p$. Se existir uma raiz n-ésima $\alpha \in \mathbb{Z}_p$ de a, então $\alpha^n = a$, e analisando módulo p concluímos que $\overline{a}$ é potência n-ésima em $\mathbb{F}_p$. Supondo $p \nmid a, n$, a recíproca também vale. De fato, suponhamos que $x^n \equiv a \pmod{p}$ admita uma solução r. Em particular, $p \nmid r$. Notemos que $(x^n)' = nx^{n-1}$, e $nr^{n-1} \not\equiv 0 \pmod{p}$. Assim, estamos nas condições de aplicar o Lema de Hensel para concluir que existe um único $\alpha \in \mathbb{Z}_p$ tal que $\alpha^n = a$ e $\alpha \equiv r \pmod{p}$.*

Concluímos que, se $p \nmid a, n$ então as raízes n-ésimas de a em $\mathbb{Z}_p$ estão em bijeção com as raízes n-ésimas de $\overline{a}$ em $\mathbb{F}_p$. Em particular, a possuirá raiz n-ésima em $\mathbb{Z}_p$ se e somente se $\overline{a}$ possuir raiz n-ésima em $\mathbb{F}_p$.

Como um caso particular do exemplo acima, consideremos o problema de determinar todas as raízes da unidade em $\mathbb{Q}_p$. Pelo visto acima, basta encontrarmos as raízes em $\mathbb{Z}_p$ do polinômio $x^n - 1$, para n inteiro positivo. Comecemos considerando $n = p - 1$. Notemos que todos os elementos não-nulos de $\mathbb{F}_p$ são raízes de $x^{p-1} - 1$. Assim, pelo exemplo acima, concluímos que $\mathbb{Z}_p$

possui todas as $p-1$ raízes $(p-1)$-ésimas da unidade, e que estas juntamente com o 0 formam um sistema completo de representantes do corpo residual de $\mathbb{Z}_p$ que é fechado por multiplicação. Afirmamos que na verdade nós temos:

Proposição 10.5. *Seja $p \in \mathbb{N}$ primo. Então o corpo p-ádico $\mathbb{Q}_p$ possui todas as raízes $(p-1)$-ésimas da unidade, e estas são todas as raízes da unidade em $\mathbb{Q}_p$, exceto no caso $p = 2$ onde também temos a raiz da unidade -1.*

Demonstração. Seja n um inteiro positivo. Suponhamos inicialmente que $p \nmid n$. Então pelo Lema de Hensel vemos que as raízes n-ésimas da unidade estão em bijeção com as soluções de $x^n = 1$ em $\mathbb{F}_p$. Como $\mathbb{F}_p^\times$ é cíclico de ordem $p-1$, é fácil ver que o número de tais soluções é igual a $\mathrm{mdc}(n, p-1)$. Assim, existirá uma raiz primitiva n-ésima da unidade se e somente se $n = \mathrm{mdc}(n, p-1)$, ou seja, se e só se $n \mid p-1$. Note que caso $n \mid p-1$, toda raiz n-ésima da unidade também é uma raiz $(p-1)$-ésima, então não obtemos raízes novas além das $p-1$ que já tinhamos.

Falta considerar o caso $p \mid n$. Nesse caso, não podemos aplicar o Lema de Hensel, mas podemos aplicar um levantamento de raízes módulo potências de p também nesse caso. Comecemos considerando o caso $p > 2$. Mostraremos que não existem raízes p-ésimas primitivas da unidade em $\mathbb{Z}_p$, e portanto também não poderão existir raízes n-ésimas primitivas da unidade em $\mathbb{Z}_p$.

Para isso, suponhamos que $\alpha \in \mathbb{Z}_p$ seja tal que $\alpha^p = 1$. Pelo Pequeno Teorema de Fermat, $\alpha \equiv \alpha^p = 1 \pmod{p}$. Então podemos escrever $\alpha = p\beta + 1$, para $\beta \in \mathbb{Z}_p$. Mostraremos que $\beta = 0$. Para isso, notemos que para todo k inteiro positivo nós temos:

$$1 = \alpha^p = (p\beta+1)^p \equiv p^p\beta^p + 1 \pmod{p^k} \Rightarrow p^p\beta^p \equiv 0 \pmod{p^k} \Rightarrow \beta^p \equiv 0 \pmod{p^{k-p}}.$$

Como k é qualquer, vemos que $\beta^p \in \bigcap_{t\geq 0} p^t\mathbb{Z}_p = \{0\} \Rightarrow \beta = 0$. Assim, $\alpha = 1$ é a única raiz p-ésima da unidade em $\mathbb{Z}_p$, como queríamos.

Suponhamos agora $p = 2$. Então $x^2 - 1 = (x+1)(x-1)$ possui raízes 1 e -1 em $\mathbb{Q}_2$. Como $2 \mid n$, podemos escrever $n = 2^\nu m$, para $\nu = v_2(n)$ e m inteiro positivo ímpar. Então $\alpha^n = 1 \Rightarrow (\alpha^{2^\nu})^m = 1 \Rightarrow \alpha^{2^\nu} = 1$, já que a única raiz m-ésima da unidade em $\mathbb{Z}_2$ é 1. Isso mostra que não existem raízes primitivas n-ésimas da unidade para $m > 1$. Para concluirmos a demonstração, basta mostrarmos que não existe raiz primitiva quarta da unidade em $\mathbb{Z}_2$.

Suponhamos que α seja uma raiz primitiva quarta da unidade em $\mathbb{Z}_2$. Então $\alpha^4 = 1$, e assim $(\alpha^2-1)(\alpha^2+1) = 0$. Como α é raiz primitiva quarta, temos $\alpha^2 + 1 = 0$. Em particular, $\alpha^2 + 1 \equiv 0 \pmod{4}$, um absurdo já que -1 não é resíduo quadrático módulo 4.

Assim, só existem raízes primitivas n-ésimas da unidade em $\mathbb{Q}_p$ para $n \mid p-1$ e, caso $p = 2$, para $n = 2$, o que conclui a demonstração. □

Com o resultado acima, conseguimos ainda mostrar que os corpos p-ádicos são dois a dois não-isomorfos, como havíamos prometido:

Proposição 10.6. *Os corpos p-ádicos são dois a dois não-isomorfos. Isto é, dados $p \neq q$ primos ou ∞, temos $\mathbb{Q}_p \ncong \mathbb{Q}_q$.*

Demonstração. Pelo resultado acima, existem exatamente 2 raízes da unidade em $\mathbb{Q}_2$, $p-1$ raízes da unidade em $\mathbb{Q}_p$, para p primo ímpar, e 2 raízes da unidade em $\mathbb{Q}_\infty = \mathbb{R}$. Com isso, vemos que os únicos corpos p-ádicos que poderiam ser isomorfos entre si são $\mathbb{Q}_2$, $\mathbb{Q}_3$ e $\mathbb{Q}_\infty = \mathbb{R}$. Como 2 não é resíduo quadrático módulo 3, vemos que $x^2 - 2$ não possui raiz em $\mathbb{Q}_3$, e como 3 não é resíduo quadrático módulo 4, vemos que $x^2 - 3$ não possui raiz em $\mathbb{Q}_2$. Como esses polinômios claramente possuem soluções em $\mathbb{R}$, vemos que $\mathbb{R} \ncong \mathbb{Q}_2, \mathbb{Q}_3$. Finalmente, para ver que $\mathbb{Q}_2$ e $\mathbb{Q}_3$ não são isomorfos, consideremos o polinômio $x^2 - 10$. Como $10 \equiv 1 \pmod{3}$ é resíduo quadrático, pelo Lema de Hensel vemos que esse polinômio tem raiz em $\mathbb{Q}_3$. Por outro lado, como $10 \equiv 2 \pmod{4}$ não é resíduo quadrático, vemos que esse polinômio não tem raiz em $\mathbb{Q}_2$, mostrando portanto que $\mathbb{Q}_2 \ncong \mathbb{Q}_3$. □

Outra importante consequência do Lema de Hensel é a seguinte:

Corolário 10.7. *Seja $(K, |\cdot|, A, \kappa)$ um corpo com valor absoluto não-arquimediano completo. Então, para todo polinômio irredutível $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ tal que $a_0a_n \neq 0$, nós temos $|f| = \max\{|a_0|, |a_n|\}$. Em particular, se $a_n = 1$ e $a_0 \in A$ então $f \in A[x]$.*

Demonstração. É fácil ver que existe $c \in K$ tal que $|cf| = 1$. Em particular, $cf \in A[x]$. Desse modo, podemos supor sem perda de generalidade que $f \in A[x]$ é tal que $|f| = 1$. Seja $0 \leq r \leq n$ mínimo tal que $|a_r| = 1$, ou equivalentemente r mínimo tal que $a_r \notin \mathfrak{p}$. Então $f(x) \equiv x^r(a_r + a_{r+1}x + \cdots + a_nx^{n-r}) \pmod{\mathfrak{p}}$. Se tivéssemos $\max\{|a_0|, |a_n|\} < 1$, então teríamos $0 < r < n$, e $\overline{f}$ se fatoraria em $\kappa[x]$ em dois polinômios x^r e $\overline{a}_r + \overline{a}_{r+1}x + \cdots + \overline{a}_nx^{n-r}$ primos entre si. Portanto, pelo Lema de Hensel, f se fatoraria não-trivialmente em $A[x]$, um absurdo! Isso conclui a demonstração. □

10.2. Extensões de Corpos Completos

Nessa seção, mostraremos que toda extensão algébrica L de um corpo completo $(K, |\cdot|)$ admite uma única extensão de $|\cdot|$, e que se L/K for finita nós teremos uma fórmula para essa extensão e L também será completo. Comecemos definindo a noção de norma em um espaço vetorial sobre um corpo com valor absoluto, que generaliza a definição para espaços vetoriais normados sobre $\mathbb{R}$ e $\mathbb{C}$:

Definição (Norma/Espaço Normado/Normas Equivalentes)**.** Seja V um K-espaço vetorial. Uma **norma** em V é uma função $\|\cdot\| \colon V \to \mathbb{R}_+$ que satisfaz:

(i) Dado $v \in V$, $\|v\| = 0 \iff v = 0$;

(ii) Dados $a \in K$, $v \in V$, temos $\|av\| = |a|\|v\|$;

(iii) (Desigualdade Triangular) Dados $v, w \in V$, temos $\|v + w\| \leq \|v\| + \|w\|$.

Um K-espaço V munido de uma norma $\|\cdot\|$ é chamado de **espaço (vetorial) normado**, e denotado $(V, \|\cdot\|)$. Note que uma norma $\|\cdot\|$ em V induz uma métrica em V com distância dada por $d(x, y) \coloneqq \|x - y\|$, e portanto também induz uma topologia em V. Duas normas em V são ditas **equivalentes** se elas induzirem a mesma topologia em V.

Note que, dado n inteiro positivo, podemos definir no espaço vetorial K^n a **norma do máximo**, dada por $\|(a_1, \ldots, a_n)\| = \max\{|a_1|, \ldots, |a_n|\}$. Observe ainda que, dado um K-espaço V de dimensão n, fixada uma base $\{v_1, \ldots, v_n\}$ de V nós temos um isomorfismo $\varphi \colon K^n \to V$ dado por $(a_1, \ldots, a_n) \mapsto a_1v_1 + \cdots + a_nv_n$. Por meio desse isomorfismo, nós podemos transferir a norma do máximo de K^n para V, definindo a norma do máximo em V associada a $v_1, \ldots, v_n$ de modo que valha a relação $\|\varphi(\cdot)\| = \varphi(\|\cdot\|)$, isto é, $\|a_1v_1 + \cdots + a_nv_n\| \coloneqq \max\{|a_1|, \ldots, |a_n|\}$. É claro que $\varphi \colon (K^n, \|\cdot\|) \to (V, \|\cdot\|)$ é um homeomorfismo.

A seguinte proposição generaliza resultados clássicos sobre espaços vetoriais normados de dimensão finita sobre $\mathbb{R}$ ou $\mathbb{C}$:

Proposição 10.8. *Seja $(K, |\cdot|)$ um corpo completo.*

(a) Seja n um inteiro positivo. Então $(K^n, \|\cdot\|)$ é completo, onde $\|\cdot\|$ é a norma do máximo.

(b) Seja $(V, |\cdot|)$ um K-espaço vetorial normado de dimensão finita n. Então, para toda base $\{v_1, \ldots, v_n\} \in V$, a norma do máximo $\|\cdot\|$ associada a $v_1, \ldots, v_n$ é equivalente à norma $|\cdot|$ de V.

Assim, o isomorfismo $(K^n, \|\cdot\|) \to (V, |\cdot|)$ dado por $(a_1, \ldots, a_n) \mapsto a_1v_1 + \cdots + a_nv_n$ é um homeomorfismo e $(V, |\cdot|)$ é completo.

Demonstração. (a) Seja $((a_1^k, \ldots, a_n^k))$ uma sequência de Cauchy em $(K^n, \|\cdot\|)$. Como a norma em K^n é a do máximo, isso significa que (a_j^k) é uma sequência de Cauchy em $(K, |\cdot|)$ para todo $1 \leq j \leq k$. Como $(K, |\cdot|)$ é completo, vemos que para $1 \leq j \leq n$ temos $a_j^k \to a_j \in K$. Assim, é fácil ver que $(a_1^k, \ldots, a_n^k) \to (a_1, \ldots, a_n) \in K^n$. Isso prova que K^n é completo.

(b) Comecemos observando que, se mostrarmos que $|\cdot|$ é equivalente a $\|\cdot\|$, então podemos concluir que o mapa $(K^n, |\cdot|) \to (V, |\cdot|)$ dado por $(a_1, \ldots, a_n) \mapsto a_1v_1 + \cdots + a_nv_n$ é um homeomorfismo, pois ele é a composição do homeomorfismo $(K^n, \|\cdot\|) \to (V, \|\cdot\|)$ dado por $(a_1, \ldots, a_n) \mapsto a_1v_1 + \cdots + a_nv_n$ com a identidade $\mathrm{id}\colon (V, \|\cdot\|) \to (V, |\cdot|)$, que é um homeomorfismo já que $\|\cdot\|$ e $|\cdot|$ são equivalentes. Note que isso mostra que $(V, |\cdot|)$ é completo, pelo item (a).

Provaremos a equivalência dessas normas por indução em n. Comecemos considerando o caso $n = 1$. Seja $v \in V$ não-nulo e $\|\cdot\|$ a norma do máximo correspondente à base $\{v\}$. Seja $|\cdot|$ uma norma qualquer em V. Dado $x \in V$ qualquer, podemos escrever x de modo único como $x = av$, para $a \in K$. Então $|x| = |a||v| = \|x\||v|$. Assim, $\|\cdot\|$ e $|\cdot|$ diferem por uma constante multiplicativa, de modo que induzem a mesma topologia, e portanto são equivalentes.

Suponhamos por indução que valham as afirmações do enunciado para $n-1$, e seja $(V, |\cdot|)$ um espaço vetorial sobre K de dimensão finita n. Sejam $v_1, \ldots, v_n \in V$ elementos que formam uma base e $\|\cdot\|$ a norma do máximo correspondente. Para provarmos que $|\cdot|$ é equivalente a $\|\cdot\|$, basta mostrarmos que existem constantes $\rho, \rho' > 0$ tais que:

$$\rho\|x\| \leq |x| \leq \rho'\|x\|, \text{ para todo } x \in V.$$

Dado $x \in V$ qualquer, podemos escrever $x = a_1v_1 + \cdots + a_nv_n$ para $a_1, \ldots, a_n \in K$. Assim:

$$|x| = |a_1v_1 + \cdots + a_nv_n| \leq |a_1||v_1| + \cdots + |a_n||v_n| \leq (|v_1| + \cdots + |v_n|)|x|.$$

Logo podemos tomar $\rho' = |v_1| + \cdots + |v_n|$. Para cada $1 \leq i \leq n$, seja $V_i \subseteq V$ o subespaço $(n-1)$-dimensional $V_i \coloneqq Kv_1 + \cdots + Kv_{i-1} + Kv_{i+1} + \cdots + Kv_n$. Pela hipótese de indução, cada V_i é completo com respeito à restrição de $|\cdot|$. Assim, V_i é um subconjunto fechado de V com relação a $|\cdot|$, e portanto $v_i + V_i$ também o é. Como $0 \notin \bigcup_{i=1}^n (v_i + V_i)$ e $\{0\}$ é compacto, existe uma vizinhança de 0 disjunta de $\bigcup_{i=1}^n (v_i + V_i)$. Dessa forma, existe $\rho > 0$ tal que $|w_i| \geq \rho$, para todos $1 \leq i \leq n$ e $w_i \in v_i + V_i$.

Afirmamos que ρ satisfaz a condição desejada. Para isso, seja $x \in V$ qualquer. Podemos escrever $x = a_1v_1 + \cdots + a_nv_n$, para $a_1, \ldots, a_n \in K$. Suponhamos que $1 \leq r \leq n$ seja tal que $|a_r| = \max\{|a_1|, \ldots, |a_n|\} = \|x\|$. Então $a_r^{-1}x = a_r^{-1}a_1v_1 + \cdots + v_r + \cdots + a_r^{-1}v_n \in v_r + V_r$, de modo que $|a_r^{-1}x| \geq \rho$. Logo $|x| \geq \rho|a_r| = \rho\|x\|$, como queríamos. Assim, $\|\cdot\|$ e $|\cdot|$ são equivalentes, concluindo a demonstração.

□

Finalmente, nós conseguimos obter o seguinte resultado sobre extensões de valores absolutos:

Teorema 10.9. *Seja $(K, |\cdot|)$ um corpo com valor absoluto completo, e seja L uma extensão algébrica de K. Então $|\cdot|$ admite uma única extensão a um valor absoluto de L. Além disso, se $[L : K] = n < \infty$, então essa extensão é dada por $|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$ e L é completo com relação a esse valor absoluto.*

No caso de $|\cdot|$ ser não-arquimediano, temos ainda que o anel de valoração associado a $|\cdot|$ em L é igual ao fecho integral em L do anel de valoração de K (mesmo no caso de uma extensão algébrica infinita).

Demonstração. Se $|\cdot|$ for um valor absoluto arquimediano, então pelo Teorema de Ostrowski temos $K = \mathbb{R}$ ou $\mathbb{C}$. Como a única extensão algébrica não-trivial de $\mathbb{R}$ é $\mathbb{C}$ e $\mathbb{C}$ é algebricamente fechado, basta considerar o caso em que $K = \mathbb{R}$ e queremos estender seu valor absoluto usual $|\cdot|_\infty$ para $\mathbb{C}$. Como todos os valores absolutos de $\mathbb{C}$ são da forma $|\cdot|_\infty^s$ para $s \in (0, 1]$, o único valor absoluto de $\mathbb{C}$ que estende $|\cdot|_\infty$ é o valor absoluto usual $|\cdot|_\infty$ de $\mathbb{C}$. Finalmente, notemos que dado $z \in \mathbb{C}$, temos $N_{\mathbb{C}\,/\,\mathbb{R}}(z) = z\overline{z} = |z|_\infty^2$, de modo que vale a fórmula indicada.

Consideremos agora o caso $|\cdot|$ não-arquimediano. Suponhamos inicialmente $[L : K] = n < \infty$. Comecemos mostrando a existência de uma extensão de $|\cdot|$ a L. Para isso, mostraremos que vale:

$$B = \{\alpha \in L \colon N_{L/K}(\alpha) \in A\}, \tag{10.1}$$

onde A é o anel de valoração de K e $B := \overline{A}^L$. Como A é integralmente fechado pela Proposição 9.8, a continência ($\supseteq$) segue do Corolário 1.30. Para a outra continência, seja $\alpha \in L^\times$ tal que $N_{L/K}(\alpha) \in A$. Seja

$$P_{\alpha,K}(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d \in K[x]$$

o polinômio minimal de α sobre K. Então temos $N_{L/K}(\alpha) = \pm a_0^m$, para $m = [L : K(\alpha)]$. Como $|N_{L/K}(\alpha)| \leq 1$, temos $|a_0| \leq 1$, e portanto pelo Corolário 10.7 nós concluímos que $P_{\alpha,K}(x) \in A[x]$, e portanto $\alpha \in B$. Consideremos então a função $|\cdot| \colon L \to \mathbb{R}_+$ dada por $|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$. Para $a \in K$, temos $N_{L/K}(a) = a^n$, de modo que $|\cdot|$ é uma função que estende nosso valor absoluto original. Mostremos que esse é um valor absoluto em L:

- $|\alpha| = 0 \iff N_{L/K}(\alpha) = 0 \iff \alpha = 0$;
- Dados $\alpha, \beta \in L$ quaisquer, $|\alpha\beta| = \sqrt[n]{|N_{L/K}(\alpha\beta)|} = \sqrt[n]{|N_{L/K}(\alpha)|}\sqrt[n]{|N_{L/K}(\beta)|} = |\alpha||\beta|$;
- Mostraremos que a desigualdade ultramétrica segue da implicação $|x| \leq 1 \Rightarrow |x + 1| \leq 1$, para todo $x \in L$. Suponhamos que valha essa implicação, e sejam $\alpha, \beta \in L$ quaisquer. Suponhamos sem perda de generalidade que $|\alpha| \leq |\beta|$, e que $\beta \neq 0$. Queremos mostrar que $|\alpha + \beta| \leq |\beta|$. Dividindo por $|\beta|$, isso equivale a $\left|\frac{\alpha}{\beta} + 1\right| \leq 1$. Como $|\alpha/\beta| \leq 1$, a desigualdade ultramétrica segue então da nossa implicação tomando $x = \alpha/\beta$.

  Provemos então que vale $|x| \leq 1 \Rightarrow |x + 1| \leq 1$, para todo $x \in L$. Mas dado $y \in L$, temos $|y| \leq 1 \iff |N_{L/K}(y)| \leq 1 \iff N_{L/K}(y) \in A \iff y \in B$, onde a última equivalência segue de (10.1). Assim, a implicação $|x| \leq 1 \Rightarrow |x + 1| \leq 1$ equivale a $x \in B \Rightarrow x + 1 \in B$, que é claramente verdadeira.

Assim, $|\cdot|$ como definido acima é de fato um valor absoluto em L que estende o valor absoluto inicial de K. Notemos ainda que B é o anel de valoração associado. De fato:

$$\begin{aligned} B = \{\alpha \in L \colon N_{L/K}(\alpha) \in A\} = \{\alpha \in L \colon |N_{L/K}(\alpha)| \leq 1\} &= \left\{\alpha \in L \colon \sqrt[n]{|N_{L/K}(\alpha)|} \leq 1\right\} \\ &= \{\alpha \in L \colon |\alpha| \leq 1\}. \end{aligned}$$

Mostraremos agora unicidade. Seja $|\cdot|'$ outra extensão de $|\cdot|$, e seja B' seu anel de valoração. Chamaremos o único ideal maximal de B de $\mathfrak{P}$ e o único ideal maximal de B' de $\mathfrak{P}'$. Provaremos que $B \subseteq B'$. Suponhamos por absurdo que exista $\alpha \in B \setminus B'$. Então nós temos $|\alpha|' > 1 \Rightarrow |\alpha^{-1}|' < 1 \Rightarrow \alpha^{-1} \in \mathfrak{P}'$. Seja $P_{\alpha,K}(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d \in A[x]$. Logo:

$$a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} + \alpha^d = 0 \Rightarrow 1 = -a_0(\alpha^{-1})^d - a_1(\alpha^{-1})^{d-1} - \cdots - a_{d-1}\alpha^{-1} \in \mathfrak{P}',$$

um absurdo! Assim, $B \subseteq B'$. Com isso, obtemos que $|\alpha| \leq 1 \Rightarrow |\alpha|' \leq 1$ para todo $\alpha \in L$. Isso significa que os valores absolutos $|\cdot|$ e $|\cdot|'$ são equivalentes, pois caso contrário pela demonstração do Teorema da Aproximação nós conseguiríamos encontrar $\alpha \in L$ tal que $|\alpha| < 1$ e $|\alpha|' > 1$.

Sendo equivalentes, $|\cdot|' = |\cdot|^s$ para algum $s > 0$. Mas como ambos os valores absolutos coincidem em K, vemos que $|\cdot|' = |\cdot|$, como queríamos. A completude de L segue então imediatamente da Proposição 10.8, já que L é um K-espaço vetorial de dimensão n e $|\cdot|\colon L \to \mathbb{R}_+$ é uma norma.

Consideremos agora o caso em que L é uma extensão algébrica qualquer de K. Para não confundir a notação, denotaremos o valor absoluto de K por $|\cdot|_K$, e para cada extensão finita M de K denotaremos por $|\cdot|_M$ o único valor absoluto em M que estende $|\cdot|_K$.

Nesse caso nós definimos, para $\alpha \in L$ qualquer, $|\alpha| = \sqrt[[K(\alpha):K]]{|N_{K(\alpha):K}(\alpha)|} = |\alpha|_{K(\alpha)}$. É claro que $|\alpha| = 0 \iff \alpha = 0$. Mostremos agora as outras duas propriedades de um valor absoluto. Sejam $\alpha, \beta \in L$ quaisquer. Notemos que a restrição de $|\cdot|_{K(\alpha,\beta)}$ a $K(\alpha)$ coincide com $|\cdot|_{K(\alpha)}$, pela unicidade que já provamos. Assim, $|\alpha| = |\alpha|_{K(\alpha)} = |\alpha|_{K(\alpha,\beta)}$. Da mesma forma, vemos que $|\beta| = |\beta|_{K(\alpha,\beta)}$, $|\alpha+\beta| = |\alpha+\beta|_{K(\alpha,\beta)}$ e $|\alpha\beta| = |\alpha\beta|_{K(\alpha,\beta)}$. Finalmente, como $|\cdot|_{K(\alpha,\beta)}$ é valor absoluto, nós temos:

$$\begin{aligned} |\alpha\beta| &= |\alpha\beta|_{K(\alpha,\beta)} = |\alpha|_{K(\alpha,\beta)}|\beta|_{K(\alpha,\beta)} = |\alpha||\beta|, \text{ e} \\ |\alpha+\beta| &= |\alpha+\beta|_{K(\alpha,\beta)} \leq |\alpha|_{K(\alpha,\beta)} + |\beta|_{K(\alpha,\beta)} = |\alpha| + |\beta|, \end{aligned}$$

provando que $|\cdot|$ é valor absoluto em L, que claramente estende $|\cdot|_K$. Sua unicidade segue imediatamente das unicidades para as extensões finitas. Falta apenas mostrar que o anel de valoração B associado a $|\cdot|$ é igual a $\overline{A}^L$:

($\subseteq$): Seja $\alpha \in B$. Então $|\alpha|_{K(\alpha)} = |\alpha| \leq 1$, o que mostra que α está no anel de valoração associado a $|\cdot|_{K(\alpha)}$, que é $\overline{A}^{K(\alpha)}$ pelo que vimos. Assim, $\alpha \in \overline{A}^{K(\alpha)} \subseteq \overline{A}^L$.

($\supseteq$): Seja $\alpha \in \overline{A}^L$. Então $\alpha \in \overline{A}^{K(\alpha)}$. Como $\overline{A}^{K(\alpha)}$ é o anel de valoração associado a $|\cdot|_{K(\alpha)}$, temos $|\alpha|_{K(\alpha)} \leq 1$. Mas então $|\alpha| = |\alpha|_{K(\alpha)} \leq 1 \Rightarrow \alpha \in B$. □

Como consequência direta desse resultado, nós temos também um resultado sobre extensões de valorações:

Corolário 10.10. *Seja (K, v) um corpo completo, e seja L uma extensão algébrica de K. Então v admite uma única extensão a uma valoração w em L. Além disso, se tivermos $[L:K] = n < \infty$, então L será completo com relação a essa extensão, que é dada explicitamente pela expressão $w(\alpha) = \frac{1}{n} v(N_{L/K}(\alpha))$. Em particular, nesse caso w será discreta se e somente se v o for.*

Terminaremos essa seção estudando um pouco do que ocorre no caso em que (K, v) não é necessariamente completo (veremos mais sobre isso nas próximas seções). Consideremos o caso em que L/K é uma extensão finita de grau n e w é uma valoração de L que estende v. Sejam κ e λ os corpos residuais de L e K, respectivamente. Então $v(K^\times) \subseteq w(L^\times)$ são grupos aditivos de $\mathbb{R}$, e $\kappa \subseteq \lambda$ com a inclusão canônica.

Definição (Índice de Ramificação/Grau de Inércia)**.** Nas condições acima, nós definimos o **índice de ramificação** da extensão $(L, w)/(K, v)$ como sendo $e(L \mid K) = e(w \mid v) \coloneqq (w(L^\times) : v(K^\times))$, e o **grau de inércia** da extensão $(L, w)/(K, v)$ como sendo $f(L \mid K) = f(w \mid v) \coloneqq [\lambda : \kappa]$.

No caso de w, e portanto também v, serem discretas, essa noção de índice de ramificação se relaciona com a outra definição de índice de ramificação. Para ver isso, sejam A o DVD de K, $\mathfrak{p}$ seu único ideal maximal e π seu normalizador. Sejam ainda B o DVD de L, $\mathfrak{P}$ seu único ideal maximal e Π seu normalizador. Então $v(K^\times) = v(\pi)\,\mathbb{Z}$ e $w(L^\times) = w(\Pi)\,\mathbb{Z}$, de modo que $e(w \mid v) = (w(\Pi)\,\mathbb{Z} : v(\pi)\,\mathbb{Z})$. Assim, $v(\pi) = e(w \mid v) w(\Pi)$. Sejam $e \in \mathbb{Z}$ e $u \in B^\times$ tais que $\pi = u\Pi^e$. Então nós temos $v(\pi) = ew(\Pi)$, de onde concluímos que $e = e(w \mid v)$. Agora, como $\mathfrak{p} = \pi A$ e $\mathfrak{P} = \Pi B$, nós temos:

$$\mathfrak{p}\,B = \pi B = \Pi^e B = (\Pi B)^e = \mathfrak{P}^e.$$

Ou seja, o índice de ramificação $e(w \mid v)$ coincide com o índice de ramificação $e(\mathfrak{P} \mid \mathfrak{p})$.

A princípio, não sabemos se o índice de ramificação e e o grau de inércia f de $(L,w)/(K,v)$ são cardinais finitos no caso geral. Mostraremos que isso é verdade e, mais do que isso, que temos $ef \leq n = [L:K]$. Comecemos mostrando a finitude do grau de inércia:

Proposição 10.11. *Seja $(L,w)/(K,v)$ uma extensão finita de corpos com valoração de dimensão n. Então o grau de inércia de $(L,w)/(K,v)$ é menor ou igual a $[L:K]$, isto é, $f(w \mid v) \leq n$.*

Demonstração. Denotemos $(K,v,|\cdot|,A,\mathfrak{p},\kappa)$ e $(L,w,|\cdot|,B,\mathfrak{P},\lambda)$. Nós mostraremos que dados $\overline{x}_1,\dots,\overline{x}_n \in \lambda$ linearmente independentes sobre κ, teremos $x_1,\dots,x_n \in B$ linearmente independentes sobre K, de modo que devemos ter $[\lambda:\kappa] \leq [L:K] = n$. Para isso, suponhamos que $\lambda_1,\dots,\lambda_n \in K$ sejam tais que $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$. Suponhamos por absurdo que algum $\lambda_j \neq 0$. Assim, podemos supor sem perda de generalidade que $\lambda_1 \neq 0$ possui valor absoluto máximo entre os λ_j's. Dividindo por λ_1, obtemos a relação

$$x_1 + \mu_2 x_2 + \cdots + \mu_n x_n = 0,$$

onde $\mu_j \coloneqq \lambda_j/\lambda_1$ para $2 \leq j \leq n$. Notemos que $|\mu_j| \leq 1$ para todo $2 \leq j \leq n$, de modo que cada $\mu_j \in A$. Analisando módulo $\mathfrak{P}$, obtemos $\overline{x}_1 + \overline{\mu}_2\overline{x}_2 + \cdots + \overline{\mu}_n\overline{x}_n = 0$, de onde obtemos uma relação não-trivial entre $\overline{x}_1,\dots,\overline{x}_n \in \lambda$ com coeficientes em κ, um absurdo! Isso conclui a demonstração. □

Com isso, conseguimos mostrar também a finitude do índice de ramificação de $(L,w)/(K,v)$ e a relação entre $e(w \mid v)$ e $f(w \mid v)$:

Proposição 10.12. *Seja $(L,w)/(K,v)$ uma extensão finita de corpos com valoração de dimensão n. Denotemos $e = e(w \mid v)$ e $f = f(w \mid v)$. Então temos $ef \leq n = [L:K]$. Em particular, e é finito.*

Demonstração. Denotemos $(K,v,A,\mathfrak{p},\kappa)$ e $(L,w,B,\mathfrak{P},\lambda)$. Pela Proposição 10.11, f é finito. Sejam $\omega_1,\dots,\omega_f \in B$ representantes de uma base da extensão λ/κ. Seja $\{\pi_j : 0 \leq j < e\} \subseteq L^\times$ tal que $\{w(\pi_j) : 0 \leq j < e\} \subseteq \mathbb{R}$ forme um conjunto de representantes das classes laterais de $w(L^\times)/v(K^\times)$. Nós mostraremos que os elementos da forma $\omega_j\pi_i$, para $1 \leq j \leq f$ e $0 \leq i < e$, são linearmente independentes sobre K, o que nos dará a desigualdade desejada. Fixemos para isso $0 \leq r < e$ inteiro positivo, e mostremos que $\{\omega_j\pi_i : 1 \leq j \leq f,\ 0 \leq i \leq r\}$ é LI sobre K.

Sejam $a_{ij} \in K$ tais que $\sum_{i=0}^{r}\sum_{j=1}^{f} a_{ij}\omega_j\pi_i = 0$, e suponhamos por absurdo que nem todos os a_{ij}'s sejam nulos. Consideremos, para $0 \leq i \leq r$, $s_i \coloneqq \sum_{j=1}^{f} a_{ij}\omega_j$. Como nem todos os a_{ij}'s são nulos e $\omega_1,\dots,\omega_f$ são linearmente independentes sobre K pela demonstração da Proposição 10.11, vemos que nem todos os s_i's são nulos.

Afirmamos que quando $s_i \neq 0$ temos $w(s_i) \in v(K^\times)$. De fato, suponhamos que valha $s_i = \sum_{j=1}^{f} a_{ij}\omega_j \neq 0$, e seja a_{it} o coeficiente de menor valoração entre $a_{i1},\dots,a_{if}$. Então chamando $b_{ij} \coloneqq a_{ij}/a_{it}$, nós temos $s_i/a_{it} = \sum_{j=1}^{f} b_{ij}\omega_j$, temos cada $b_{ij} \in A$ e $b_{it} = 1$. Notemos que $s_i/a_{it} \notin \mathfrak{P}$, pois caso contrário teríamos $\sum_{j=1}^{f} \overline{b}_{ij}\overline{\omega}_j = 0$, um absurdo pela independência linear de $\overline{\omega}_1,\dots,\overline{\omega}_n$. Assim, $s_i/a_{it} \in B \setminus \mathfrak{P}$, de modo que

$$w(s_i/a_{it}) = 0 \Rightarrow w(s_i) = w(a_{it}) = v(a_{it}) \in v(K^\times).$$

Observemos agora que $\sum_{i=0}^{r} s_i\pi_i = 0$, logo pelo Lema 3.26 vemos que existem $0 \leq i < j \leq r$ tais que $w(s_i\pi_i) = w(s_j\pi_j)$. Desse modo:

$$w(s_i) + w(\pi_i) = w(s_j) + w(\pi_j) \Rightarrow w(\pi_i) = w(\pi_j) + w(s_j) - w(s_i) \in w(\pi_j) + v(K^\times).$$

Assim, $w(\pi_i) + v(K^\times) = w(\pi_j) + v(K^\times)$, um absurdo, pois $w(\pi_i)$ e $w(\pi_j)$ por hipótese representam classes diferentes de $w(L^\times)/v(K^\times)$. Assim, para todo $0 \leq r < e$ inteiro positivo o conjunto indicado é linearmente independente sobre K, de modo que $(r+1)f \leq [L:K] = n$. Disso concluímos que e é finito e $ef \leq n$, como queríamos. □

No caso em K é completo e v é uma valoração discreta, vale de fato a **identidade fundamental**:

Proposição 10.13. *Seja $(L,w)/(K,v)$ uma extensão finita de corpos com valoração de dimensão n. Denotemos $e = e(w \mid v)$ e $f = f(w \mid v)$. Suponhamos que K seja completo e que v seja uma valoração discreta. Então vale a* ***identidade fundamental*** $ef = n = [L:K]$.

Demonstração. Notemos que v discreta implica em w discreta, devido ao Corolário 10.10. Utilizemos as mesmas notações da demonstração da proposição acima. Nesse caso, como v é discreta, podemos tomar $\pi_i = \Pi^i$, para $0 \leq i \leq e-1$, onde Π é o normalizador do DVD B. Então nós temos o A-módulo livre

$$M \coloneqq \sum_{i=0}^{e-1} \sum_{j=1}^{f} A\omega_j \Pi^i \subseteq B.$$

Pelo Teorema 10.9, temos $B = \overline{A}^L$, e como A é um DVD vemos que B é um A-módulo livre de posto $n = [L:K]$. Assim, a demonstração estará completa se mostrarmos que $B = M$ é um A-módulo livre de posto ef, e de quebra ainda mostraremos como achar uma base de B como A-módulo. Para isso, seja $N \coloneqq \sum_{j=1}^{f} A\omega_j$. Então $M = \sum_{i=0}^{e-1} \Pi^i N$. Como as classes de $\omega_1, \ldots, \omega_f$ geram $B/\mathfrak{P} = B/(\Pi B)$ como um $A/\mathfrak{p}$-módulo, vemos que $B = N + \Pi B$. Assim:

$$\begin{aligned} B = N + \Pi B &= N + \Pi(N + \Pi B) = N + \Pi N + \Pi^2 B \\ &= N + \Pi N + \Pi^2(N + \Pi B) = N + \Pi N + \Pi^2 N + \Pi^3 B \\ &= \cdots \\ &= N + \Pi N + \cdots + \Pi^{e-1} N + \Pi^e B \\ &= M + \Pi^e B = M + (\Pi B)^e = M + \mathfrak{p}\, B. \end{aligned}$$

Então $B = M + \mathfrak{p}\, B$, e queremos concluir que $M = B$. Para isso, notemos que

$$\begin{aligned} B = M + \mathfrak{p}\, B &= M + \mathfrak{p}(M + \mathfrak{p}\, B) = M + \mathfrak{p}\, M + \mathfrak{p}^2\, B = M + \mathfrak{p}^2\, B \\ &= M + \mathfrak{p}(M + \mathfrak{p}^2\, B) = M + \mathfrak{p}\, M + \mathfrak{p}^3\, B = M + \mathfrak{p}^3\, B \\ &= \cdots \\ &= M + \mathfrak{p}^k\, B, \end{aligned}$$

para todo inteiro positivo k. Como $\{\mathfrak{p}^k\, B \colon k \in \mathbb{N}^*\}$ é um sistema fundamental de vizinhanças de 0 em B, concluímos que M é um subconjunto denso de B. Consideremos agora

$$M' \coloneqq \sum_{i=0}^{e-1} \sum_{j=1}^{f} K\omega_j \Pi^i.$$

Então $M \subseteq M' \subseteq L$ e M' é um K-espaço de dimensão ef, de onde concluímos da Proposição 10.8 que M' é completo, e portanto fechado em L (é aqui que utilizamos a hipótese de K ser completo). Como A é fechado em K, é fácil ver que M é fechado em M', e portanto M é fechado em L, logo também é fechado em B. Sendo M denso em B, concluímos que $M = B$, como queríamos. □

10.3. Extensões Finitas

Nessa seção, mudaremos por praticidade a notação que utilizamos até então. Denotaremos por v tanto uma valoração não-arquimediana, que é o tipo de valoração que consideramos até então, quanto uma valoração arquimediana, que é obtida como $v = -\log_q |\cdot|$ para algum valor absoluto

$|\cdot|$ arquimediano. Note que isso significa que v poderá não satisfazer mais a propriedade não-arquimediana $v(x+y) \geq \min\{v(x), v(y)\}$.

Indicaremos ainda por $|\cdot|_v$ o valor absoluto associado a v, e sendo (K, v) um corpo com valoração, indicaremos por (K_v, v) o seu completamento. Fixado um fecho algébrico $\overline{K}_v$ de K_v, como (K_v, v) é completo sabemos pelo Teorema 10.9 que v se estende a uma única valoração $\overline{v}$ de $\overline{K}_v$, com a qual $(\overline{K}_v, \overline{v})$ se torna um corpo com valoração. Notemos que $\overline{K}_v$ é um corpo algebricamente fechado que contém K.

Seja L/K uma extensão algébrica qualquer. Então existe uma imersão $\tau\colon L \hookrightarrow \overline{K}_v$ que fixa K. Notemos que τL se torna um corpo com valoração com a restrição de $\overline{v}$, e essa valoração estende v. Assim, $(L, \overline{v} \circ \tau)$ é um corpo com valoração e $w := \overline{v} \circ \tau$ estende v. Em termos de valores absolutos, temos $|x|_w = |\tau x|_{\overline{v}}$ para todo $x \in L$. Assim, $(L, |\cdot|_w)$ é um corpo com valor absoluto e $|\cdot|_w$ estende $|\cdot|_v$.

Com isso, é fácil ver que $\tau\colon (L, |\cdot|_w) \to (\overline{K}_v, |\cdot|_{\overline{v}})$ é uma função contínua que fixa $(K, |\cdot|_v)$. Suponhamos agora que L/K seja finita. Consideremos o completamento L_w de L. Então podemos estender τ para uma imersão $\tau\colon L_w \to \overline{K}_v$ dada por $\lim_{n\to\infty} x_n \mapsto \lim_{n\to\infty} \tau x_n$, onde (x_n) é uma sequência de Cauchy em L com respeito a $|\cdot|_w$, o limite da esquerda é tomado com respeito a $|\cdot|_w$ e o limite da direita é tomado com respeito a $|\cdot|_{\overline{v}}$ (note que τ preserva sequências de Cauchy, já que é uma função contínua). Observemos que $\tau\colon L_w \to \overline{K}_v$ também é contínua, e que τ fixa K_v, onde vemos $K_v \subseteq L_w$ da forma canônica.

Como vimos, cada imersão $\tau\colon L \to \overline{K}_v$ que fixa K nos dá uma extensão $w := \overline{v} \circ \tau$ de v a L. Para cada automorfismo[1] $\sigma \in \mathrm{Gal}(\overline{K}_v/K_v)$, podemos considerar $\tau'\colon L \to \overline{K}_v$ dado por $\tau' := \sigma \circ \tau$. Então τ' também é uma imersão de L em $\overline{K}_v$ que fixa K, e dizemos que τ' e τ são **imersões conjugadas** sobre K_v.

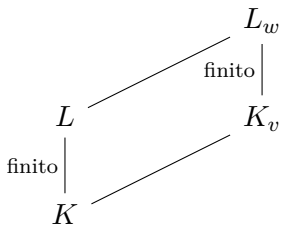
Nosso objetivo é mostrar que toda valoração w de L que estende v é da forma $w = \overline{v} \circ \tau$, para alguma imersão $\tau\colon L \hookrightarrow \overline{K}_v$. Para mostrarmos isso, seja w uma valoração qualquer de L que estende v. Então podemos ver L_w como extensão de K_v de forma canônica. Essa extensão é finita:

Proposição 10.14. *Com as condições acima, suponhamos que $L = K\alpha_1 + \cdots + K\alpha_n$, com $\alpha_1, \ldots, \alpha_n \in L$ linearmente independentes sobre K. Então $L_w = K_v\alpha_1 + \cdots + K_v\alpha_n$. Assim, $[L_w : K_v] \leq [L : K]$. Além disso, $L_w = LK_v$.*

Demonstração. Como $K_v \subseteq L_w$ e $L \subseteq L_w$, a inclusão $K_v\alpha_1 + \cdots + K_v\alpha_n \subseteq L_w$ é clara. Para mostrar a inclusão contrária, notemos que $L = K\alpha_1 + \cdots + K\alpha_n \subseteq K_v\alpha_1 + \cdots + K_v\alpha_n$. Observemos agora que $K_v\alpha_1 + \cdots + K_v\alpha_n$ é completo pela Proposição 10.8, já que é um espaço vetorial de dimensão finita sobre K_v. Sendo esse um espaço completo que contém L, vemos que $L_w \subseteq K_v\alpha_1 + \cdots + K_v\alpha_n$, e portanto vale a igualdade $L_w = K_v\alpha_1 + \cdots + K_v\alpha_n$, como queríamos.

Mostremos agora que $L_w = LK_v$. É claro que $LK_v \subseteq L_w$. Para a inclusão contrária, notemos que LK_v é um K_v-espaço de dimensão finita, logo é completo pela Proposição 10.8, e como $L \subseteq LK_v$ nós concluímos que $L_w \subseteq LK_v$. □

Assim, temos o seguinte diagrama:



Note que (L_w, w) é uma extensão de (K_v, v). Na verdade, sendo L_w/K_v finita, vemos pelo Teorema 10.9 que w é a única extensão de v a L_w. Mais do que isso, sendo $n = [L : K]$, esse

[1] Aqui, $\mathrm{Gal}(\overline{K}_v/K_v)$ denota o grupo dos automorfismos de $\overline{K}_v$ que fixam K_v.

teorema nos dá a fórmula $|x|_w = \sqrt[n]{|N_{L_w/K_v}(x)|_v}$. O diagrama acima nos mostra a passagem de uma extensão finita L/K para uma extensão finita L_w/K_v, e representa o importante **Princípio Local-Global**, que busca relacionar informações sobre objetos e seus completamentos. O motivo para esta nomenclatura vem do fato de que a localização de um **corpo global** é um **corpo local**. Esses são dois conceitos importantes da Teoria dos Corpos de Classes, como veremos brevemente no Capítulo 12. O que fizemos acima nos permite demonstrar o seguinte resultado:

Teorema 10.15. *(Teorema da Extensão) Seja L/K uma extensão finita de corpos e seja v uma valoração de K. Então:*

(a) Toda extensão w da valoração v a L é da forma $w = \overline{v} \circ \tau$ para alguma imersão $\tau\colon L \to \overline{K}_v$ que fixa K. Em particular, toda extensão de uma valoração discreta é discreta.

(b) Duas extensões $\overline{v} \circ \tau$ e $\overline{v} \circ \tau'$ serão iguais se e só se τ e τ' forem conjugadas sobre K_v.

Demonstração. (a) Seja w uma valoração de L que estende v, e consideremos sua extensão canônica w a L_w. Seja $\tau\colon L \to \overline{K}_v$ uma imersão que fixa K qualquer. Então, como vimos, essa imersão se estende a uma imersão $\tau\colon L_w \to \overline{K}_v$ que fixa K_v. Agora, $\overline{v} \circ \tau$ é uma extensão de v a L_w. Como w também é uma extensão de v a L_w, vemos pela unicidade do Teorema 10.9 que $w = \overline{v} \circ \tau$ em L_w. Restringindo essas valorações a L, obtemos o resultado desejado.

(b) Suponhamos que τ e τ' sejam conjugadas, isto é, $\tau' = \sigma \circ \tau$ para um certo $\sigma \in \mathrm{Gal}(\overline{K}_v/K_v)$. Notemos que $\overline{v} \circ \sigma$ é uma valoração de $\overline{K}_v$ que estende a valoração v de K_v. Mas, pela unicidade do Teorema 10.9, $\overline{v}$ é a única tal valoração, de modo que $\overline{v} = \overline{v} \circ \sigma$. Isso mostra que $\overline{v} \circ \tau' = \overline{v} \circ \sigma \circ \tau = \overline{v} \circ \tau$, como queríamos.

Reciprocamente, suponhamos que $\tau, \tau'\colon L \to \overline{K}_v$ sejam imersões que fixam K tais que $\overline{v} \circ \tau = \overline{v} \circ \tau'$. Então $\sigma\colon \tau L \to \tau' L$ dado por $\sigma := \tau' \circ \tau^{-1}$ é um isomorfismo de corpos que fixa K. Como $\overline{v} \circ \sigma = \overline{v} \circ \tau' \circ \tau^{-1} = \overline{v} \circ \tau \circ \tau^{-1} = \overline{v}$, é fácil ver que σ é uma função contínua.

Afirmamos que conseguimos estender σ a um isomorfismo $\sigma\colon \tau L \cdot K_v \to \tau' L \cdot K_v$ que fixa K_v. Para ver isso, comecemos observando que τL é denso em $\tau L \cdot K_v \subseteq \overline{K}_v$, uma vez que $K \subseteq \tau L$ é denso em K_v. Assim, todo elemento $x \in \tau L \cdot K_v$ pode ser escrito como $x = \lim_{n\to\infty} \tau x_n$, onde cada $x_n \in L$. Notemos agora que a sequência $(\tau' x_n) = (\sigma \tau x_n)$ converge a um elemento $\sigma x := \lim_{n\to\infty} \sigma\tau x_n = \lim_{n\to\infty} \tau' x_n \in \tau' L \cdot K_v$, uma vez que σ é contínua e $\tau' L \cdot K_v$ é completo já que é extensão finita de K_v.

É fácil ver que $\sigma\colon \tau L \cdot K_v \to \tau' L \cdot K_v$ está bem-definida (isto é, não depende da sequência (x_n) escolhida) e é um isomorfismo de corpos que fixa K_v. Assim, podemos estender σ a um automorfismo $\sigma\colon \overline{K}_v \to \overline{K}_v$ que fixa K_v, isto é, a $\sigma \in \mathrm{Gal}(\overline{K}_v/K_v)$. Desse modo, obtemos que $\tau' = \sigma \circ \tau$ é conjugada a τ, como queríamos.

□

Como um caso concreto desse teorema, consideremos $L = K(\alpha)$, onde $\alpha \in L$ é raiz de um polinômio irredutível $f(x) \in K[x]$. Nesse caso, as imersões de L em $\overline{K}_v$ são da forma $\tau\colon L \to \overline{K}_v$ dadas por $\tau(\alpha) = \beta$, onde $\beta \in \overline{K}_v$ é uma raiz de $f(x)$. Suponhamos que a decomposição de $f(x)$ em fatores irredutíveis de $K_v[x]$ seja $f(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r}$. Então duas imersões τ e τ' de L em $\overline{K}_v$ serão conjugadas sobre K_v se e só se as raízes $\tau(\alpha)$ e $\tau'(\alpha)$ de $f(x)$ forem conjugadas sobre K_v, isto é, se forem raízes do mesmo polinômio irredutível $f_j(x)$. Assim, como consequência do Teorema da Extensão, nós obtemos:

Proposição 10.16. *Suponhamos que $L = K(\alpha)$, onde $\alpha \in L$ é raiz de um polinômio irredutível $f(x) \in K[x]$, e seja v uma valoração de K. Então as valorações $w_1, \ldots, w_r$ de L que estendem w estão em bijeção com os fatores irredutíveis $f_1, \ldots, f_r$ da decomposição $f(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r}$ de $f(x)$ em polinômios irredutíveis de $K_v[x]$. Para obter w_j explicitamente, para $1 \leq j \leq r$,*

fixamos $\alpha_j \in \overline{K}_v$ raiz de $f_j(x)$, e tomamos $\tau\colon L \to \overline{K}_v$ dada por $\tau(\alpha) = \alpha_j$. Então $w_j = \overline{v} \circ \tau_j$. Além disso, $\tau_j\colon L \to \overline{K}_v$ se estende a um isomorfismo $\tau_j\colon L_{w_j} \to K_v(\alpha_j)$.

Dada uma extensão finita L/K, usaremos a notação $w \mid v$ para indicar que w é uma extensão de v a L. Note que para cada $w \mid v$ nós temos um homomorfismo de K_v-álgebras $\varphi_w\colon L \otimes_K K_v \to L_w$ dado por $a \otimes b \mapsto ab$. Assim, obtemos um homomorfismo de K_v-álgebras $\varphi\colon L \otimes_K K_v \to \prod_{w|v} L_w$ dado por $a \otimes b \mapsto (ab)$. Se L/K for separável, esse homomorfismo será de fato um isomorfismo:

Proposição 10.17. *Com as condições acima, se L/K for separável então $L \otimes_K K_v \cong \prod_{w|v} L_w$ como K_v-álgebras étale, com isomorfismo dado por φ.*

Demonstração. Seja $\alpha \in L$ tal que $L = K(\alpha)$, e seja $f(x) \in K[x]$ o polinômio minimal de α. Pela proposição acima, os fatores primos de $f(x)$ em $K_v[x]$ estão em correspondência com as valorações $w \mid v$. Como essa extensão é separável, temos $f(x) = \prod_{w|v} f_w(x)$, onde cada $f_w(x) \in K_v[x]$ é irredutível. Desse modo, temos $L \otimes_K K_v \cong \prod_{w|v} \frac{K_v[x]}{\langle f_w(x)\rangle}$, pelo Corolário 1.21, com isomorfismo dado por $g(\alpha) \otimes b \mapsto (g(x)b \pmod{f_w})$.

Fixemos $w \mid v$. Notemos que $\frac{K_v[x]}{\langle f_w(x)\rangle}$ é o corpo de decomposição de f_w sobre K_v, de modo que também pela proposição acima podemos concluir que $\frac{K_v[x]}{\langle f_w(x)\rangle} \cong L_w$, com isomorfismo dado por $h(x) \pmod{f_w} \mapsto h(\alpha_w)$, onde $\alpha_w \in \overline{K}_v$ é uma raiz de f_w.

Desse modo, temos um isomorfismo de K_v-álgebras $L \otimes_K K_v \cong \prod_{w|v} L_w$, que é dado por $g(\alpha) \otimes b \mapsto (g(\alpha_w)b)$. Finalmente, basta notarmos que estamos identificando todos os α_w's com α, de modo que nosso isomorfismo é $g(\alpha) \otimes b \mapsto (g(\alpha)b)$. Mas isso é exatamente o que queríamos! □

Como corolário, nós obtemos várias relações entre a extensão L/K e as extensões L_w/K_v:

Corolário 10.18. *Com as condições acima, se L/K for separável então nós temos a igualdade $[L : K] = \sum_{w|v} [L_w : K_v]$. Além disso, para todo $\alpha \in L$ nós temos:*

$$N_{L/K}(\alpha) = \prod_{w|v} N_{L_w/K_v}(\alpha) \text{ e } \operatorname{Tr}_{L/K}(\alpha) = \sum_{w|v} \operatorname{Tr}_{L_w/K_v}(\alpha).$$

Demonstração. Segue imediatamente do resultado acima, juntamente com as Proposições 1.20 e 1.24 □

Seja κ o corpo de resíduos de K. Para cada $w \mid v$, denotaremos por λ_w o corpo de resíduos de L_w, por $e_w = (w(L^\times) : v(K^\times))$ o índice de ramificação de $(L, w)/(K, v)$ e por $f_w = [\lambda_w : \kappa]$ o grau de inércia de $(L, w)/(K, v)$. Então nós obtemos a **identidade fundamental da teoria de valorações**:

Proposição 10.19. *Com as condições acima:*

(a) Dado $w \mid v$, o índice de ramificação de L_w/K_v é e_w, e o grau de inércia de L_w/K_v é f_w. Assim, $[L_w : K_v] = e_w f_w$.

(b) (Identidade Fundamental) Se v for discreta e L/K for separável, então nós temos a igualdade $\sum_{w|v} e_w f_w = [L : K]$.

Demonstração. (a) Sabemos que $v(K^\times) = v(K_v^\times)$ e que o corpo de resíduos de $K_v^\times$ é isomorfo a κ. Além disso, para cada $w \mid v$ temos $w(L^\times) = w(L_w^\times)$ e o corpo de resíduos de $L_w^\times$ é isomorfo a λ_w. Com isso, o índice de ramificação e o grau de inércia da extensão L_w/K_v são iguais a e_w e f_w, e a identidade fundamental para corpos completos nos dá $[L_w : K_v] = e_w f_w$.

(b) Pelo corolário acima, temos $[L:K] = \sum_{w|v}[L_w : K_v]$, de onde pelo item (a) nós obtemos $[L:K] = \sum_{w|v} e_w f_w$, como queríamos.

□

Suponhamos agora que A seja um domínio de Dedekind com corpo de frações $K = Q(A)$, L seja uma extensão finita e separável de grau n de K e $B = \overline{A}^L$. Dado $x \in K^\times$ qualquer, temos $xA = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(x)}$, e assim:

$$xB = (xA)B = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(x)} B = \prod_{\mathfrak{p}} (\mathfrak{p}\, B)^{v_\mathfrak{p}(x)} = \prod_{\mathfrak{p}} \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P} v_\mathfrak{p}(x)}.$$

Isso mostra que, dado $\mathfrak{p} \lhd A$ primo não-nulo e $\mathfrak{P} \mid \mathfrak{p}$, nós temos $v_\mathfrak{P}(x) = e_\mathfrak{P} v_\mathfrak{p}(x)$. Assim, $\frac{1}{e_\mathfrak{P}} v_\mathfrak{P}$ é uma valoração de L que estende $v_\mathfrak{p}$. De fato, o teorema abaixo nos diz que as valorações dessa forma nos dão todas as extensões de $v_\mathfrak{p}$ a L. Denotemos por $K_\mathfrak{p}$ o completamento de $(K, v_\mathfrak{p})$ e por $L_\mathfrak{P}$ o completamento de $(L, v_\mathfrak{P})$.

Teorema 10.20. *Seja $\mathfrak{p} \lhd A$ primo não-nulo. Então o mapa $\mathfrak{P} \mapsto \frac{1}{e_\mathfrak{P}} v_\mathfrak{P}$ nos dá uma bijeção entre o conjunto dos primos de B sobre $\mathfrak{p}$ e o conjunto das valorações de L que estendem $v_\mathfrak{p}$. Em particular, nós temos $L \otimes_K K_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$, e portanto valem as fórmulas:*

$$[L:K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P}, \;\; N_{L/K}(\alpha) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha) \;\; e \;\; \mathrm{Tr}_{L/K}(\alpha) = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha)$$

Demonstração. É claro que, para $\mathfrak{P} \mid \mathfrak{p}$ e $\mathfrak{Q} \mid \mathfrak{p}$ distintos, nós temos $v_\mathfrak{P}$ e $v_\mathfrak{Q}$ não-equivalentes. Assim, basta provarmos que toda valoração de L que estende $v_\mathfrak{p}$ é da forma $\frac{1}{e_\mathfrak{P}} v_\mathfrak{P}$ para algum $\mathfrak{P} \mid \mathfrak{p}$. Seja $w \mid v$. Então w é discreta, pelo Teorema da Extensão. Chamemos de W o seu DVD correspondente, e de $\mathfrak{m}$ o único ideal maximal de W.

Como $w|_K = v_\mathfrak{p}$, nós temos $A \subseteq W$ e $\mathfrak{m} \cap A = \mathfrak{p}$. Como W é um DVD, ele é integralmente fechado em L, e portanto $B = \overline{A}^L \subseteq \overline{W}^L = W$. Chamemos $\mathfrak{P} \coloneqq \mathfrak{m} \cap B \lhd B$. Como $\mathfrak{m} \mid \mathfrak{p}$, vemos que $\mathfrak{P} \mid \mathfrak{p}$. Como $B \setminus \mathfrak{P} \subseteq W \setminus \mathfrak{m} = W^\times$, vemos que $B_\mathfrak{P} \subseteq W$. Assim, $B_\mathfrak{P} \subseteq W \subseteq L = Q(B_\mathfrak{P})$. Como não existem anéis intermediários entre um DVD e seu corpo de frações, vemos que $W = B_\mathfrak{P}$, e portanto w e $v_\mathfrak{P}$ são equivalentes, pela Proposição 9.9. Como $w|_K = v$, é claro que $w = \frac{1}{e_\mathfrak{P}} v_\mathfrak{P}$, como queríamos. □

Observação 10.21. *Note que a fórmula $[L:K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P}$ é exatamente a identidade fundamental clássica. Assim, nós a reobtemos no contexto de valorações.*

Pela Proposição 9.6, todas as valorações não-arquimedianas de $\mathbb{Q}$ são, a menos de equivalência, as p-ádicas, para p primo. Desse modo, devido ao teorema acima, nós temos:

Teorema 10.22. *Seja K um corpo de números algébricos. Então toda valoração não-arquimediana de K é, a menos de equivalência, da forma $v_\mathfrak{p}$, onde $\mathfrak{p} \lhd \mathcal{O}_K$ é um primo não-nulo.*

Demonstração. Seja v uma valoração não-arquimediana de K. Então ela é a extensão da valoração $v|_\mathbb{Q}$ de $\mathbb{Q}$, que deve ser equivalente a v_p para algum $p \in \mathbb{N}$ primo. Assim, pelo teorema acima, v deve ser equivalente a $v_\mathfrak{p}$ para $\mathfrak{p} \lhd \mathcal{O}_K$ sobre p, o que conclui a demonstração. □

10.4. Extensões Galoisianas

Suponhamos que L/K seja uma extensão finita galoisiana, com grupo de Galois $G = \mathrm{Gal}(L/K)$, e que v seja uma valoração de K. Dados $w \mid v$ e $\sigma \in G$ quaisquer, vemos que $w \circ \sigma \mid v$. Assim, G age nas valorações de L que estendem v. Todas as valorações $w \mid v$ são de fato conjugadas por essa ação. Note que esse resultado é do mesmo estilo da Proposição 6.1. Na demonstração dela, utilizamos o Teorema Chinês dos Restos. Desse modo, não é surpresa que utilizaremos o Teorema da Aproximação para demonstrar esse resultado:

Proposição 10.23. *O grupo G age transitivamente no conjunto W_v das extensões $w \mid v$, isto é, quaisquer duas extensões de v a L são conjugadas por essa ação.*

Demonstração. Sejam $w \mid v$ e $w' \mid v$. Suponhamos por absurdo que w e w' estejam em órbitas diferentes por essa ação. Então as órbitas $\{w \circ \sigma \colon \sigma \in G\}$ e $\{w' \circ \sigma \colon \sigma \in G\}$ de w e de w' por essa ação são disjuntas. Isso significa que os conjuntos $\{|\sigma(\cdot)|_w\}$ e $\{|\sigma(\cdot)|_{w'}\}$ são disjuntos, e portanto os valores absolutos de um conjunto e de outro são não-equivalentes, já que todos estendem $|\cdot|_v$.

Desse modo, pelo Teorema da Aproximação existe $x \in L$ tal que $|\sigma x|_w < 1$ e $|\sigma x|_{w'} > 1$, para todo $\sigma \in G$. Então por um lado obteríamos $|N_{L/K}(x)|_v = \prod_{\sigma \in G} |\sigma(x)|_w < 1$, e por outro lado obteríamos $|N_{L/K}(x)|_v = \prod_{\sigma \in G} |\sigma(x)|_{w'} > 1$, um absurdo! □

Da mesma forma que o resultado acima lembra a Proposição 6.1, como veremos ao longo desta seção nós traçaremos um paralelo com o Capítulo 6. No caso de v ser não-arquimediana, denotaremos $(K, v, |\cdot|_v, A, \mathfrak{p}, \kappa)$, e para cada $w \mid v$, $(L, w, |\cdot|_w, B_w, \mathfrak{P}_w, \lambda_w)$.

É fácil ver que $B_{w\circ\sigma} = \sigma^{-1} B_w$ e $\mathfrak{P}_{w\circ\sigma} = \sigma^{-1}\mathfrak{P}_w$, para todo $\sigma \in G$. Com isso, vemos que $\sigma \colon B_{w\circ\sigma} \to B_w$ induz um isomorfismo $\lambda_{w\circ\sigma} \cong \lambda_w$ que fixa κ. Assim, $[\lambda_{w\circ\sigma} : \kappa] = [\lambda_w : \kappa]$, ou seja, $f_{w\circ\sigma} = f_w$. Temos também $(w \circ \sigma)(L^\times) = w(L^\times)$, o que mostra que $e_{w\circ\sigma} = e_w$. Logo pela proposição acima e pela identidade fundamental nós concluímos:

Proposição 10.24. *Se L/K for uma extensão finita galoisiana e v for não-arquimediana, todo $w \mid v$ possui o mesmo índice de ramificação e o mesmo grau de inércia. Chamemos esse índice de ramificação comum de e, esse grau de inércia comum de f e de $g := |W_v|$ o número de valorações de L que estendem v. Então caso v for discreta temos a* ***identidade fundamental*** *$efg = [L : K]$.*

A notação e, f, g definida acima será padrão.

Definição (Grupo de Decomposição/Corpo de Decomposição)**.** O **grupo de decomposição** de $w \mid v$ é definido por $G_w = G_w(L/K) := \{\sigma \in G \colon w \circ \sigma = w\}$. Assim, G_w é o estabilizador de w pela ação de G. Seu corpo fixo é chamado de **corpo de decomposição** de w sobre K, e é denotado por $Z_w = Z_w(L/K) := \{x \in L \colon \sigma x = x \text{ para todo } \sigma \in G_w\}$.

Como G age transitivamente em W_v, vemos que $g = (G : G_w)$, para todo $w \in W_v$. O grupo de decomposição de w consiste precisamente dos automorfismos de L que fixam K e que são contínuos em relação a w:

Proposição 10.25. *G_w é o conjunto dos $\sigma \in G$ tais que σ é contínuo com relação a w (isto é, com relação a $|\cdot|_w$).*

Demonstração. Se $\sigma \in G_w$, então $w \circ \sigma = w$, e portanto $|\sigma(x)|_w = |x|_w$ para todo $x \in L$. Com isso, como σ é automorfismo é fácil ver que σ é contínuo com relação a w nesse caso. Reciprocamente, suponhamos que $\sigma \in G$ seja contínuo com relação a w. Dado $x \in L$ qualquer tal que $|x|_w < 1$, temos que $(x^n) \to 0$, e pela continuidade de σ temos $(\sigma(x)^n) \to 0$. Isso equivale a $|\sigma(x)|_w < 1$. Ou seja, $|x|_w < 1 \Rightarrow |\sigma x|_w < 1$. Isso significa que $|\cdot|_w$ e $|\sigma(\cdot)|_w$ são valores absolutos equivalentes. Assim, $w \circ \sigma$ e w são valorações equivalentes, e portanto iguais já que ambas são extensões de v. Isso prova que $w \circ \sigma = w$, e portanto $\sigma \in G_w$, como queríamos. □

No caso em que v é uma valoração não-arquimediana, nós conseguimos ainda definir seu grupo de inércia e seu grupo de ramificação:

Definição (Grupos/Corpos de Inércia/Ramificação)**.** O **grupo de inércia** de $w \mid v$ é definido por:

$$\begin{aligned} I_w = I_w(L/K) &:= \{\sigma \in G_w \colon \sigma x \equiv x \pmod{\mathfrak{P}_w}, \text{ para todo } x \in B_w\} \\ &= \{\sigma \in G_w \colon w(\sigma x - x) > 0, \text{ para todo } x \in B_w\}. \end{aligned}$$

Seu corpo fixo é chamado de **corpo de inércia** de w sobre K, e é denotado:

$$T_w = T_w(L/K) \coloneqq \{x \in L \colon \sigma x = x, \text{ para todo } \sigma \in I_w\}.$$

O **grupo de ramificação** de $w \mid v$ é definido por:

$$\begin{aligned} R_w = R_w(L/K) &\coloneqq \left\{\sigma \in G_w \colon \frac{\sigma x}{x} \equiv 1 \pmod{\mathfrak{P}_w}, \text{ para todo } x \in L^\times\right\} \\ &= \left\{\sigma \in G_w \colon w\left(\frac{\sigma x}{x} - 1\right) > 0, \text{ para todo } x \in L^\times\right\}. \end{aligned}$$

Seu corpo fixo é chamado de **corpo de ramificação** de w sobre K, e é denotado:

$$V_w = V_w(L/K) = \{x \in L \colon \sigma x = x, \text{ para todo } x \in R_w\}.$$

Observação 10.26. *Notemos que se $\sigma \in G_w$, então de $w \circ \sigma = w$ nós conseguimos obter que $\sigma B_w = B_w$ e que $\sigma x/x \in B_w$ para todo $x \in L^\times$, de modo que as definições acima fazem sentido.*

Nós temos então as continências $G \supseteq G_w \supseteq I_w \supseteq R_w$, e portanto $K \subseteq Z_w \subseteq T_w \subseteq V_w$. Suponhamos agora que L/K e L'/K' sejam extensões de Galois finitas, e que tenhamos um diagrama comutativo:

$$\begin{array}{ccc} L & \xrightarrow{\tau} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\tau} & K' \end{array}$$

Esse diagrama induz um homomorfismo $\tau^* \colon \mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$ dado por $\tau^*(\sigma') = \tau^{-1}\sigma'\tau$. Para ver que essa função está bem-definida, devemos verificar que $\sigma'\tau L \subseteq \tau L$, para podermos aplicar τ^{-1}. Mas isso é verdade porque $\tau L/\tau K$ é extensão normal, uma vez que L/K o é.

Suponhamos agora que w' seja uma valoração de L', e denotemos $v' \coloneqq w'|_{K'}$, $w \coloneqq w' \circ \tau$ e $v \coloneqq w|_K$. Então é claro que v', w e v são valorações de K', L e K, respectivamente, e que temos $w' \mid v'$ e $w \mid v$.

Proposição 10.27. *Com as notações acima, $\tau^* \colon \mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$ induz um homomorfismo $G_{w'}(L'/K') \to G_w(L/K)$. Além disso, se v for não-arquimediana, τ^* induz também homomorfismos $I_{w'}(L'/K') \to I_w(L/K)$ e $R_{w'}(L'/K') \to R_w(L/K)$.*

Demonstração. Suponhamos que $\sigma' \in G_{w'}(L'/K')$. Então $w' \circ \sigma' = w'$. Como $w = w' \circ \tau$, temos $w' = w \circ \tau^{-1}$ em τL. Seja $x \in L$ qualquer. Então como já vimos $\sigma'\tau(x) \in \tau L$, e portanto:

$$w \circ \tau^*(\sigma') = w \circ \tau^{-1}\sigma'\tau(x) = w' \circ \sigma'\tau(x) = w' \circ \tau(x) = w(x).$$

Isso mostra que $\tau^*(\sigma') \in G_w(L/K)$, como queríamos. Consideremos agora v (e portanto v', w e w') não-arquimediana. Suponhamos que $\sigma' \in I_{w'}(L'/K')$. Sendo B o anel de valoração de L, queremos mostrar que para todo $x \in B$ temos $w(\tau^*(\sigma')x - x) > 0$. Como $w = w' \circ \tau$, é fácil ver que τx pertence ao DVD de L'. Desse modo:

$$w(\tau^*(\sigma')x - x) = w(\tau^{-1}\sigma'\tau x - x) = w(\tau^{-1}(\sigma'\tau x - \tau x)) = w'(\sigma'\tau x - \tau x) > 0,$$

onde na última desigualdade utilizamos que $\sigma' \in I_{w'}(L'/K')$. Isso prova que $\tau^*(\sigma') \in I_w(L/K)$. Suponhamos agora que $\sigma' \in R_{w'}(L'/K')$. Dado $x \in L^\times$ qualquer, temos $\tau x \in L'^\times$, e portanto:

$$w\left(\frac{\tau^*(\sigma')x}{x} - 1\right) = w\left(\frac{\tau^{-1}\sigma'\tau x}{x} - 1\right) = w\left(\tau^{-1}\left(\frac{\sigma'\tau x}{\tau x} - 1\right)\right) = w'\left(\frac{\sigma'\tau x}{\tau x} - 1\right) > 0,$$

onde na última desigualdade utilizamos que $\sigma' \in R_{w'}(L'/K')$. Isso prova que $\tau^*(\sigma') \in R_w(L/K)$. □

É claro que se τ for um isomorfismo então os homomorfismos τ^* dados acima também serão isomorfismos, com inversa dada por $(\tau^{-1})^*$. Como casos particulares disso, nós obtemos:

Proposição 10.28. *(a) Seja L/K uma extensão finita galoisiana com grupo de Galois G, e sejam $w \mid v$ valorações. Então para todo $\tau \in G$ nós temos:*

$$\begin{aligned} G_{w\circ\tau} &= \tau^{-1}G_w\tau,\ I_{w\circ\tau} = \tau^{-1}I_w\tau,\ \text{e}\ R_{w\circ\tau} = \tau^{-1}R_w\tau, \\ Z_{w\circ\tau} &= \tau^{-1}Z_w,\ I_{w\circ\tau} = \tau^{-1}I_w,\ \text{e}\ V_{w\circ\tau} = \tau^{-1}V_w. \end{aligned}$$

(b) Seja L/K uma extensão galoisiana e sejam $w \mid v$ valorações. Então para todo corpo intermediário $K \subseteq M \subseteq L$, nós temos:

$$\begin{aligned} G_w(L/M) &= G_w(L/K) \cap \mathrm{Gal}(L/M); \\ I_w(L/M) &= I_w(L/K) \cap \mathrm{Gal}(L/M); \\ R_w(L/M) &= R_w(L/K) \cap \mathrm{Gal}(L/M). \end{aligned}$$

Demonstração. (a) Consideremos o diagrama

$$\begin{array}{ccc} L & \xrightarrow{\tau} & L \\ \uparrow & & \uparrow \\ K & \xrightarrow{\tau} & K \end{array}$$

Então $\tau^*\colon G \to G$ é um automorfismo, e pela proposição acima ele induz isomorfismos $G_w \to G_{w\circ\tau}$, $I_w \to I_{w\circ\tau}$ e $R_w \to R_{w\circ\tau}$, dados por $\sigma \mapsto \tau^{-1}\sigma\tau$. Mas isso justifica as igualdades desejadas entre os grupos, e as igualdades entre os corpos saem facilmente destas.

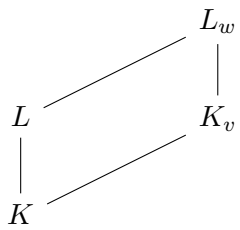
(b) Consideremos o diagrama

$$\begin{array}{ccc} L & \hookrightarrow & L \\ \uparrow & & \uparrow \\ K & \hookrightarrow & M \end{array}$$

Nesse caso, τ^* é a inclusão $\mathrm{Gal}(L/M) \hookrightarrow \mathrm{Gal}(L/K)$. Com isso, a proposição acima nos dá as igualdades desejadas.

□

Suponhamos agora L/K finita galoisiana com grupo de Galois G e $w \mid v$. Consideremos o seguinte diagrama:



Pela Proposição 10.14, $L_w = LK_v$, e assim é claro que L_w/K_v também é uma extensão galoisiana. Dado $\sigma \in G_w(L/K)$, pela Proposição 10.25 temos σ contínuo com respeito a w. Sendo assim, vemos que σ se estende a um único automorfismo contínuo $\hat{\sigma} \in \mathrm{Gal}(L_w/K_v)$, que é dado por $\hat{\sigma}x := \lim_{k\to\infty}\sigma(x_k)$, onde (x_k) é uma sequência em L com $\lim_{k\to\infty} x_k = x$ (aqui usamos de fato que σ é uniformemente contínuo).

Assim, temos um homomorfismo de grupos $\varphi\colon G_w(L/K) \to \mathrm{Gal}(L_w/K_v)$ dado por $\varphi(\sigma) = \hat{\sigma}$. Se $\hat{\sigma} = \mathrm{id}_{L_w}$, então $\sigma = \hat{\sigma}|_L = \mathrm{id}_L$, de modo que φ é injetor. Por outro lado, seja $\tau \in \mathrm{Gal}(L_w/K_v)$

qualquer. Note que $\mathrm{Gal}(L_w/K_v) = G_w(L_w/K_v)$, já que w é a única extensão de v a L_w. Então $w \circ \tau = w$ em L_w, de modo que $\sigma := \tau|_L \in G_w(L/K)$. Sendo τ contínuo com respeito a w e L denso em L_w, vemos que $\tau = \hat{\sigma}$. Isso prova que φ é de fato um isomorfismo, cuja inversa é a restrição.

Com a hipótese de v ser não-arquimediana, é fácil ainda mostrar que valem as igualdades $\varphi(I_w(L/K)) = I_w(L_w/K_v)$ e $\varphi(R_w(L/K)) = R_w(L_w/K_v)$, de modo que temos os isomorfismos $I_w(L/K) \cong I_w(L_w/K_v)$ e $R_w(L/K) \cong R_w(L_w/K_v)$ nesse caso. Juntando tudo, obtemos:

Proposição 10.29. *Sejam L/K uma extensão finita galoisiana e $w \mid v$. Então L_w/K_v também é uma extensão finita galoisiana, e temos $\mathrm{Gal}(L_w/K_v) = G_w(L_w/K_v) \cong G_w(L/K)$, onde esse isomorfismo é induzido pela extensão $\varphi\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_w/K_v)$ descrita acima, cuja inversa é a restrição $\tau \mapsto \tau|_L$. Além disso, se v for não-arquimediana, φ também induzirá os isomorfismos $I_w(L_w/K_v) \cong I_w(L/K)$ e $R_w(L_w/K_v) \cong R_w(L/K)$.*

O corpo de decomposição Z_w possui as seguintes propriedades:

Proposição 10.30. *Sejam L/K uma extensão finita galoisiana e $w \mid v$.*

(a) A restrição w_Z de w ao corpo de decomposição Z_w admite extensão única a L.

(b) Se v for não-arquimediana discreta, $Z_w = L \cap K_v$, onde essa interseção é tomada dentro de L_w.

(c) Se v for não-arquimediana discreta, w_Z terá o mesmo corpo de resíduos e o mesmo grupo de valores que v.

Demonstração. (a) O grupo de Galois de L/Z_w é G_w, pela correspondência de Galois. Assim, pela Proposição 10.23, toda extensão de w_Z é da forma $w \circ \sigma$, para $\sigma \in G_w$. Mas como $\sigma \in G_w$, temos $w \circ \sigma = w$, o que mostra que w é a única extensão de w_Z a L.

(b) ($\subseteq$): Seja $x \in Z_w$ qualquer. Então é claro que $x \in L$. Como $\sigma x = x$ para todo $\sigma \in G_w$, identificando G_w com $\mathrm{Gal}(L_w/K_v)$ vemos que $x \in K_v$. Assim, temos $x \in L \cap K_v$.

($\supseteq$): Seja $x \in L \cap K_v$. Consideremos $\sigma \in G_w$ qualquer, e seja $\hat{\sigma}$ sua extensão a L_w. Então, como $\hat{\sigma} \in \mathrm{Gal}(L_w/K_v)$, temos $\hat{\sigma}x = x$, e portanto $\sigma x = x$. Isso prova que $x \in Z_w$.

(c) Segue do fato de que a extensão de v a K_v tem mesmo corpo de resíduos e grupo de valores de v, e de $K \subseteq Z_w \subseteq K_v$.

□

Se supusermos que K é completo[2] e que v é discreta, w será a única extensão de v a L e teremos $B_w = A^L$. Nesse caso, podemos aplicar vários resultados do Capítulo 6, já que temos a extensão de DVD's B_w/A. Sendo $w \mid v$ único, por simplicidade denotemos $B_w = B$, $\mathfrak{P}_w = \mathfrak{P}$ e $\lambda_w = \lambda$. Então é fácil ver que temos $G_w = G_{\mathfrak{P}} = G$, $I_w = I_{\mathfrak{P}}$ e $R_w = R^1_{\mathfrak{P}}$. Desse modo, obtemos o familiar diagrama:

$$\begin{array}{ccccc}
\mathfrak{P} \lhd B & \hookrightarrow & L = Q(B) & \text{---------} & 1 \\
{\scriptstyle p^t}\big| & & {\scriptstyle p^t}\big| & & {\scriptstyle p^t}\big| \\
\mathfrak{P}_V \lhd B_V & \hookrightarrow & V_w = Q(B_V) & \text{------} & R_w \\
{\scriptstyle \tilde{e}}\big| & & {\scriptstyle \tilde{e}}\big| & & {\scriptstyle \tilde{e}}\big| \\
\mathfrak{P}_T \lhd B_T & \hookrightarrow & T_w = Q(B_T) & \text{-------} & I_w \\
{\scriptstyle f}\big| & & {\scriptstyle f}\big| & & {\scriptstyle f}\big| \\
\mathfrak{p} \lhd A & \hookrightarrow & K = Q(A) & \text{--------} & G
\end{array}
\qquad \mathrm{Gal}(V_w/T_w) \cong I_w/R_w \cong W_{\tilde{e}}(\lambda)$$

$$\lambda = B_T/\mathfrak{P}_T$$
$$\big|$$
$$\kappa$$

[2] A mesma argumentação a seguir funciona para corpos henselianos. Veja mais sobre isso na próxima seção.

onde p é o expoente característico de λ, $e = p^t\tilde{e}$ e $p \nmid \tilde{e}$. Assim, podemos aplicar todos os resultados que obtivemos no Capítulo 6 a essa configuração.

10.5. Corpos Henselianos

Nessa seção, voltaremos a considerar como valorações apenas as valorações não-arquimedianas. Seja K um corpo qualquer, munido com um valor absoluto $|\cdot|$, e seja L uma extensão algébrica de K. Queremos estudar quais são as extensões do valor absoluto de K para um valor absoluto de L. No caso de K ser completo com respeito a $|\cdot|$, o Teorema 10.9 nos garante que uma tal extensão existe, é única e sabemos a sua expressão. Analisando atentamente a demonstração do caso $|\cdot|$ não-arquimediano, vemos que para mostrar existência e unicidade dessa extensão utilizamos a hipótese de K ser completo apenas uma vez: precisamos dessa hipótese para podermos aplicar o Corolário 10.7, que por sua vez segue do Lema de Hensel (10.1). Isso nos sugere definir:

Definição (Corpo Henseliano)**.** Um **corpo henseliano** é um corpo K, munido de uma valoração v, cujo anel de valoração A satisfaz o Lema de Hensel (10.1). Dizemos ainda que v é uma **valoração henseliana** e que A é um **anel de valoração henseliano**.

É claro que todo corpo com valoração completo é henseliano, e que em todo corpo henseliano vale o Corolário 10.7. Com isso, valerão também o Teorema 10.9 e o Corolário 10.10, na seguinte versão:

Teorema 10.31. *Seja $(K, v, |\cdot|, A)$ um corpo henseliano, e seja L uma extensão algébrica de K. Então $|\cdot|$ admite uma única extensão a um valor absoluto $|\cdot|$ de L, v admite uma única extensão a uma valoração $\hat{v}$ de L e o anel de valoração associado a $\hat{v}$ é $\overline{A}^L$.*

Além disso, se $[L : K] = n < \infty$, então essas extensões são dadas por $|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$ e $\hat{v}(\alpha) = \frac{1}{n}v(N_{L/K}(\alpha))$. Em particular, a valoração estendida será discreta se e somente se a valoração de K o for.

Para construir um exemplo de um corpo henseliano que não é completo, comecemos considerando $(K, v, A, \mathfrak{p})$ um corpo com valoração qualquer, e $(\hat{K}, \hat{v}, \hat{A}, \hat{\mathfrak{p}})$ o seu completamento. Consideremos K^v o fecho separável de K em $\hat{K}$. Então K^v é um corpo com valoração dada pela restrição de $\hat{v}$.

Definição (Henselianização)**.** O corpo $(K^v, \hat{v}, A^v, \mathfrak{p}^v)$ é chamado de **henselianização** do corpo $(K, v, A, \mathfrak{p})$.

Como o nome sugere, a henselianização K^v de um corpo (K, v) qualquer é um corpo henseliano. Nós provaremos isso no caso particular em que K^v é algebricamente fechado em K. Começaremos mostrando uma versão do Lema de Gauss para um corpo com valor absoluto não-arquimediano:

Lema 10.32 (Lema de Gauss não-arquimediano)**.** *Seja $(K, |\cdot|)$ um corpo com valor absoluto não-arquimediano, e seja A seu anel de valoração.*

(a) O conteúdo é multiplicativo, isto é, dados $f, g \in A[x]$ quaisquer nós temos $|fg| = |f||g|$.

(b) Seja $f \in A[x]$ primitivo, e suponhamos que $f = gh$ com $g, h \in K[x]$. Então existe $c \in K^\times$ tal que $cg, c^{-1}h \in A[x]$, de modo que $f = (cg)(c^{-1}h)$ é uma fatoração de f em polinômios primitivos de $A[x]$.

Demonstração. (a) Escrevamos $f(x) = a_0 + a_1x + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + \cdots + b_nx^n$. Suponhamos que $0 \leq i \leq m$ e $0 \leq j \leq n$ sejam mínimos de modo que $|a_i| = |f|$ e $|b_j| = |g|$. Então o coeficiente de x^{i+j} em fg é a soma de elementos da forma a_rb_s com $r + s = i + j$. Uma dessas parcelas é a_ib_j, que satisfaz $|a_ib_j| = |a_i||b_j| = |f||g|$, e as demais parcelas possuem $r < i$ ou $s < j$, de modo que pela maximalidade de $|a_i|$ e $|b_j|$ e pelas minimalidades de i e j nós temos $|a_rb_s| = |a_r||b_s| < |a_i||b_j| = |f||g|$. Assim, pela desigualdade ultramétrica vemos que o coeficiente de x^{i+j} em fg tem valor absoluto $|f||g|$, de onde $|fg| \geq |f||g|$.

Por outro lado, todos os coeficientes de fg são somas de parcelas da forma a_rb_s, que satisfazem $|a_rb_s| = |a_r||b_s| \leq |f||g|$. Assim, pela desigualdade ultramétrica, os coeficientes de fg possuem valor absoluto no máximo $|f||g|$, de onde obtemos $|fg| \leq |f||g|$. Desse modo, temos $|fg| = |f||g|$, como queríamos.

(b) Como f é primitivo, temos $1 = |f| = |gh| = |g||h|$, onde utilizamos o item (a). Seja $c \in K^\times$ tal que $|c| = |h|$ (podemos tomar c como sendo um dos coeficientes de maior valor absoluto de h, por exemplo). Então $|c^{-1}h| = |c|^{-1}|h| = 1$, e $|cg| = |c||g| = |c||h|^{-1} = 1$. Assim, $c^{-1}h$ e cg são primitivos. Em particular, $cg, c^{-1}h \in A[x]$.

□

Proposição 10.33. *Com as notações acima, suponhamos que K^v seja algebricamente fechado em $\hat{K}$. Então K^v é um corpo henseliano. Em particular, isso ocorrerá se K tiver característica 0, já que nesse caso K^v será o fecho algébrico de K em $\hat{K}$.*

Demonstração. Seja $f(x) \in A^v[x]$ primitivo, e seja $\overline{f}(x) \in (A^v/\,\mathfrak{p}^v)[x]$ seu polinômio induzido. Suponhamos que existam $\overline{g}(x), \overline{h}(x) \in (A^v/\,\mathfrak{p}^v)[x]$ primos entre si tais que $\overline{f} = \overline{g}\overline{h}$. É claro que $\hat{K}$ também é o completamento de K^v. Assim, pela Proposição 9.13 nós temos $A^v/\,\mathfrak{p}^v \cong \hat{A}/\hat{\mathfrak{p}}$ com as inclusões canônicas. Desse modo, podemos ver a fatoração $\overline{f} = \overline{g}\overline{h}$ em $(\hat{A}/\hat{\mathfrak{p}})[x]$. Com isso, como $\hat{K}$ é henseliano, existem $g(x), h(x) \in \hat{A}[x]$ tais que $f = gh$, os polinômios induzidos por g e h no corpo residual são $\overline{g}$ e $\overline{h}$ respectivamente e $\partial\, g = \partial\, \overline{g}$.

Como $gh = f \in A[x]$, vemos pelo Teorema 1.18 que $g, h \in \overline{A}^{\hat{K}}[x]$. Como estamos supondo que K^v é algebricamente fechado em $\hat{K}$, nós temos $g, h \in K^v[x]$. Multiplicando g e h por constantes adequadas, podemos pelo Lema de Gauss não-arquimediano supor que $g, h \in A^v[x]$ e satisfazem as mesmas condições (multiplicando também $\overline{g}$ e $\overline{h}$ por constantes se necessário). Assim, vemos que o Lema de Hensel se aplica para K^v, mostrando que K^v é henseliano, como queríamos. □

Vale observar que K^v é "muito menor" que o completamento $\hat{K}$: a extensão K^v/K é sempre algébrica, enquanto que se pode mostrar que $\hat{K}/K$ nunca será algébrica se K não for completo, isto é, se $K \neq \hat{K}$. Pela unicidade da extensão de uma valoração dada pelo Teorema 10.31 e pela Proposição 10.19, vemos que a identidade fundamental para extensões finitas de corpos henselianos se torna:

Proposição 10.34. *Seja (K, v) um corpo henseliano, e seja (L, w) uma extensão finita de (K, v) de grau n. Suponhamos que v seja discreta e que L/K seja separável. Denotemos $e = e(w \mid v)$ e $f = f(w \mid v)$. Então vale a **identidade fundamental** $ef = n = [L : K]$.*

É interessante que vale a volta do Teorema 10.31: um corpo com valor absoluto (K, v) será henseliano se e somente se toda extensão algébrica de K admitir única extensão de v. Para isso, estudaremos o chamado **polígono de Newton**, um método que nos permite relacionar as valorações das raízes de um polinômio com as valorações dos coeficientes desse polinômio.

Definição (Envoltória Convexa Inferior)**.** Seja $S = \{p_1 = (x_1, y_1), \ldots, p_n = (x_n, y_n)\}$ um conjunto finito de pontos de $\mathbb{R}^2$, com $x_1 < \cdots < x_n$. Nós definimos a **envoltória convexa inferior** de S como sendo "a menor poligonal convexa que está abaixo de todos os pontos de S". Formalmente, a envoltória convexa é a poligonal definida da seguinte forma:

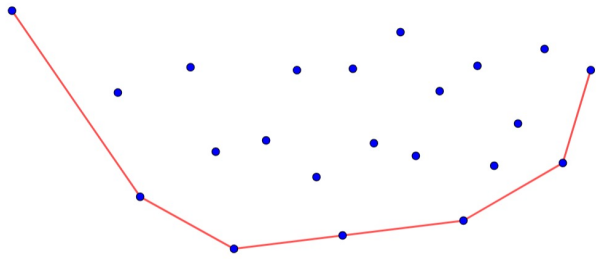
- Seu primeiro segmento liga p_1 a p_{i_2}, onde i_2 é o maior $1 < i \leq n$ tal que todos os pontos de S estão no semiplano superior fechado determinado pela reta que liga p_1 a p_i.
- Seu segundo segmento liga p_{i_2} a p_{i_3}, onde i_3 é o maior $i_2 < i \leq n$ tal que todos os pontos de S estão no semiplano superior fechado determinado pela reta que liga p_{i_1} a p_{i_2}.

  $\vdots$

- Seu último segmento liga p_{i_r} a p_n.

Assim, a envoltória convexa inferior de S é dada por $p_1 p_{i_2} p_{i_3} \cdots p_{i_r} p_n$.

Exemplo 10.35. *Na figura abaixo, a poligonal em vermelho é a envoltória convexa inferior do conjunto de pontos azuis. Ela é formada por* 5 *segmentos (note que há um ponto sobre a poligonal que não é um vértice).*



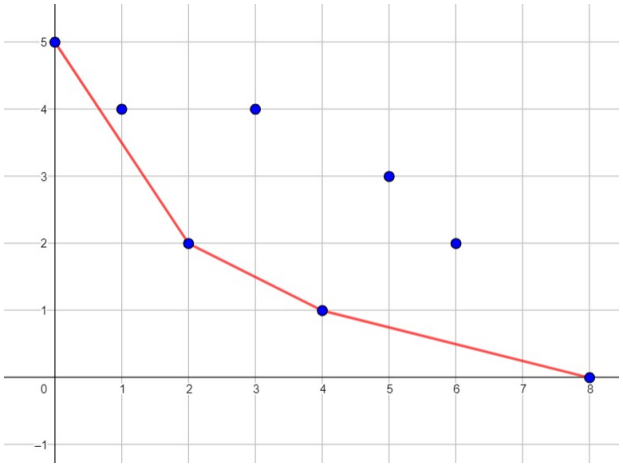
Note que a envoltória convexa inferior de um conjunto de pontos é formada por segmentos com inclinação estritamente crescente, da esquerda para a direita.

Definição (Polígono de Newton)**.** Seja (K, v) um corpo com valoração, e consideremos um polinômio $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ com $a_0, a_n \neq 0$. A cada monômio $a_i x^i$ com $a_i \neq 0$ nós associamos o ponto $(i, v(a_i)) \in \mathbb{R}^2$. Assim, nós temos um conjunto de pontos $S_f \coloneqq \{(i, v(a_i)) \colon 0 \leq i \leq n,\ a_i \neq 0\}$. O **polígono de Newton** do polinômio $f(x)$ é definido como sendo a envoltória convexa inferior do conjunto de pontos S_f.

Exemplo 10.36. *Consideremos o polinômio:*

$$f(x) = x^8 - 18x^6 + 54x^5 + 3x^4 - 81x^3 - 36x^2 + 162x - 1215 \in \mathbb{Q}_3[x].$$

O polígono de Newton de f é a poligonal vermelha da figura abaixo:



Proposição 10.37. *Seja (K, v) um corpo, e seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ um polinômio com $a_0, a_n \neq 0$. Seja L o corpo de decomposição de f, e suponhamos que v se estenda a uma valoração w de L. Suponhamos que $(r, v(a_r))$ e $(s, v(a_s))$, com $r < s$, sejam dois pontos consecutivos do polígono de Newton de f, e seja $-m$ a inclinação do segmento que os liga. Então f possui exatamente $s - r$ raízes (contadas com multiplicidade) com valoração m.*

Demonstração. Comecemos observando que dividir por a_n apenas faz o polígono de Newton de f se deslocar verticalmente, uma vez que $v(a_i/a_n) = v(a_i) - v(a_n)$ para todo $0 \leq i \leq n$. Assim, podemos assumir sem perda de generalidade que $a_n = 1$. Sejam $m_1 < m_2 < \cdots < m_{t+1}$ as valorações assumidas pelas raízes de f em L. Numeraremos as raízes de L por $\alpha_1, \ldots, \alpha_n$ (com multiplicidade), de modo que tenhamos:

$$\begin{aligned} w(\alpha_1) &= \cdots = w(\alpha_{s_1}) = m_1; \\ w(\alpha_{s_1+1}) &= \cdots = w(\alpha_{s_2}) = m_2; \\ &\vdots \\ w(\alpha_{s_t+1}) &= \cdots = w(\alpha_n) = m_{t+1}. \end{aligned}$$

Vendo os coeficientes de f como funções simétricas nas raízes $\alpha_1, \ldots, \alpha_n$ e utilizando a propriedade não-arquimediana, nós obtemos:

$$\begin{aligned} v(a_n) &= v(1) = 0; \\ v(a_{n-1}) &\geq \min\{w(\alpha_i) \colon 1 \leq i \leq n\} = m_1; \\ v(a_{n-2}) &\geq \min\{w(\alpha_i\alpha_j) \colon 1 \leq i < j \leq n\} = 2m_1; \\ &\vdots \\ v(a_{n-s_1}) &= \min\{w(\alpha_{i_1} \cdots \alpha_{i_{s_1}}) \colon i_1 < \cdots < i_{s_1}\} = s_1m_1, \end{aligned}$$

onde a primeira igualdade da última linha segue do fato de que $\alpha_{i_1} \cdots \alpha_{i_{s_1}}$ é o único termo na expressão de a_{n-s_1} que tem valoração s_1m_1 (em todos os outros termos aparece uma raiz com valoração maior que m_1).

Notemos que as expressões acima implicam que, para todo $n - s_1 \leq i \leq n$, o ponto $(i, v(a_i))$ está acima da reta que liga $(n - s_1, v(a_{n-s_1})) = (n - s_1, s_1m_1)$ e $(n, v(a_n)) = (n, 0)$, cuja inclinação é $\frac{0-s_1m_1}{n-(n-s_1)} = \frac{-s_1m_1}{s_1} = -m_1$. Procedendo analogamente, nós obtemos:

$$\begin{aligned} v(a_{n-s_1-1}) &\geq \min\{w(\alpha_{i_1} \cdots \alpha_{i_{s_1+1}}) \colon i_1 < \cdots < i_{s_1+1}\} = s_1m_1 + m_2; \\ v(a_{n-s_1-2}) &\geq \min\{w(\alpha_{i_1} \cdots \alpha_{i_{s_1+2}}) \colon i_1 < \cdots < i_{s_1+2}\} = s_1m_1 + 2m_2; \\ &\vdots \\ v(a_{n-s_2}) &= \min\{w(\alpha_{i_1} \cdots \alpha_{i_{s_2}}) \colon i_1 < \cdots < i_{s_2}\} = s_1m_1 + (s_2 - s_1)m_2, \end{aligned}$$

e assim por diante. Como $v(a_{n-s_1-1}) \geq s_1m_1 + m_2 > (s_1 + 1)m_1$, é fácil ver que $(n - s_1, s_1m_1)$ está abaixo da reta que liga $(n - s_1 - 1, v(a_{n-s_1-1}))$ a $(n, 0)$. Com isso, concluímos que o último segmento do polígono de Newton de f é o segmento ligando $(n - s_1, s_1m_1)$ a $(n, 0)$. Pelas expressões acima, para todo $n - s_2 \leq i \leq n - s_1$, o ponto $(i, v(a_i))$ está acima da reta que liga $(n - s_2, v(a_{n-s_2})) = (n - s_2, s_1m_1 + (s_2 - s_1)m_2)$ e $(n - s_1, s_1m_1)$, cuja inclinação é

$$\frac{s_1m_1 - (s_1m_1 + (s_2 - s_1)m_2)}{(n - s_1) - (n - s_2)} = \frac{-(s_2 - s_1)m_2}{s_2 - s_1} = -m_2.$$

Continuando do mesmo modo, nós concluímos que os vértices do polígono de Newton são, da

direita para a esquerda:

$$\begin{aligned}
&(n, 0);\\
&(n - s_1, s_1 m_1);\\
&(n - s_2, s_1 m_1 + (s_2 - s_1)m_2);\\
&\quad\vdots\\
&(n - s_j, s_1 m_1 + (s_2 - s_1)m_2 + \cdots + (s_j - s_{j-1})m_j);\\
&\quad\vdots\\
&(0, s_1 m_1 + (s_2 - s_1)m_2 + \cdots + (n - s_t)m_{t+1}),
\end{aligned}$$

e a inclinação de um segmento genérico dessa poligonal é:

$$\frac{(s_1 m_1 + \cdots + (s_j - s_{j-1})m_j) - (s_1 m_1 + \cdots + (s_{j+1} - s_j)m_{j+1})}{(n - s_j) - (n - s_{j+1})} = \frac{(s_j - s_{j+1})m_{j+1}}{s_{j+1} - s_j} = -m_{j+1}.$$

Ou seja, da direita para a esquerda os segmentos do polígono de Newton têm inclinações iguais a $-m_1, -m_2, \ldots, -m_{t+1}$, e as distâncias horizontais entre seus vértices, também da direita para a esquerda, são iguais a $s_1, s_2 - s_1, \ldots, s_t - s_{t-1}, n - s_t$. Note que isso é exatamente o que queríamos mostrar! □

Exemplo 10.38. *Consideremos o polinômio $f(x)$ do Exemplo 10.36. Pela proposição acima, no corpo de decomposição de f esse polinômio possui duas raízes com valoração $3/2$, duas raízes com valoração $1/2$ e quatro raízes com valoração $1/4$.*

Notemos que, pela proposição acima, um polinômio $f(x) \in K[x]$ se fatora em $L[x]$ como $f(x) = a_n \prod_{j=1}^{r} f_j(x)$, onde para $1 \leq j \leq r$ temos:

$$f_j(x) := \prod_{\substack{\alpha \text{ raiz de } f(x)\\ w(\alpha) = m_j}} (x - \alpha),$$

onde $m_1 < \cdots < m_r$ são as valorações das raízes de f em L e o produto acima considera multiplicidades. Observemos que cada $f_j(x)$ corresponde ao $(r - j + 1)$-ésimo segmento do polígono de Newton, da esquerda para a direita. Em particular, o polígono de Newton de f será formado por um único segmento se e somente se todas as raízes de f tiverem a mesma valoração em L. O curioso é que, se a extensão de v a L for única, a fatoração para f dada acima será na verdade uma fatoração em $K[x]$:

Proposição 10.39. *Com as notações acima, se w for a única extensão de v a uma valoração no corpo de decomposição L de f, então a fatoração $f(x) = a_n \prod_{j=1}^{r} f_j(x)$ é uma fatoração em $K[x]$, ou seja, $f_1(x), \ldots, f_r(x) \in K[x]$.*

Demonstração. Nós podemos assumir sem perda de generalidade que $a_n = 1$. Assim, nós temos a fatoração $f(x) = \prod_{j=1}^{r} f_j(x)$. Consideremos primeiramente o caso f irredutível sobre $K[x]$. Nesse caso, dadas duas raízes $\alpha, \beta \in L$ de f, sabemos que existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\beta = \sigma\alpha$. Notemos que $w \circ \sigma$ também é uma valoração de L que estende v. Logo, por unicidade, temos que $w \circ \sigma = w$. Portanto $w(\beta) = w(\sigma\alpha) = w(\alpha)$. Desse modo, mostramos que todas as raízes de f possuem mesma valoração, e portanto $r = 1$ e nós temos simplesmente a igualdade $f_1(x) = f(x) \in K[x]$.

A demonstração do caso geral será por indução em $\partial f = n$. Para $n = 1$, não temos nada a provar. Seja então $n \geq 2$, e suponhamos que o resultado seja válido para todos os polinômios de grau menor que n. Fixemos uma raiz $\alpha \in L$ de f, e seja $p := P_{\alpha,K} \in K[x]$ seu polinômio minimal

sobre K. Definamos $g(x) := f(x)/p(x) \in K[x]$. Como p é irredutível em $K[x]$, vemos que todas as raízes de p possuem a mesma valoração, sem perda de generalidade m_1. Então p divide f_1 em $L[x]$. Chamemos $g_1(x) := f_1(x)/p(x) \in L[x]$. Então nós temos:

$$g(x) = \frac{f(x)}{p(x)} = \frac{\prod_{j=1}^{r} f_j(x)}{p(x)} = g_1(x) \prod_{j=2}^{r} f_j(x).$$

Notemos que essa fatoração de $g(x)$ é exatamente a dada pelo polígono de Newton, uma vez que as raízes de $g_1, f_2, \ldots, f_r$ possuem valorações $m_1, m_2, \ldots, m_r$ respectivamente. Finalmente, como $\partial g < \partial f = n$, concluímos pela hipótese de indução que $g_1, f_2, \ldots, f_r \in K[x]$. Disso tiramos que $f_1 = g_1 p \in K[x]$ também. Ou seja, $f_1, \ldots, f_r \in K[x]$, como desejado. □

Em particular, se f for irredutível em $K[x]$ vemos que o polígono de Newton de f consistirá de um único segmento, que liga os pontos $(0, v(a_0))$ e $(n, v(a_n))$. Assim, para todo $0 \leq i \leq n$, o ponto $(a_i, v(a_i))$ está acima desse segmento ou sobre ele, de onde nós concluímos que $v(a_i) \geq \min\{v(a_0), v(a_n)\}$. Em termos do valor absoluto $|\cdot|$ associado a v, isso significa que $|a_i| \leq \max\{|a_0|, |a_n|\}$. Com isso, nós temos:

Corolário 10.40. *Seja $(K, |\cdot|)$ um corpo com valor absoluto não-arquimediano. Seja ainda $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ um polinômio irredutível. Suponhamos que $|\cdot|$ admita uma extensão única a um valor absoluto do corpo de decomposição de f. Então $|f| = \max\{|a_0|, |a_n|\}$.*

Note que obtivemos um resultado do mesmo tipo que o Corolário 10.7. Estamos na verdade fazendo o caminho inverso do que fizemos nas seções 10.1 e 10.2. Nelas, supondo um corpo completo, mostramos o Lema de Hensel, provamos a partir disso o Corolário 10.7 e então mostramos a existência e a unicidade de uma extensão. Aqui, supondo a existência e a unicidade de uma certa extensão, mostramos o Corolário 10.40. De fato, supondo a existência e a unicidade de todas as extensões algébricas, conseguimos voltar mais ainda e deduzir o Lema de Hensel:

Teorema 10.41. *Um corpo com valor absoluto não-arquimediano $(K, |\cdot|)$ é henseliano se e somente se o valor absoluto $|\cdot|$ de K admitir extensão única a qualquer extensão algébrica de K. Além disso, nesse caso, chamando de κ o corpo residual de K, vale a seguinte afirmação: dado um polinômio $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$ primitivo e irredutível com $a_0, a_n \neq 0$, temos duas opções para o polinômio induzido $\overline{f}(x) \in \kappa[x]$:*

- *$\overline{f}(x)$ é um polinômio constante não-nulo, ou*
- *$\partial \overline{f} = \partial f$ e $\overline{f}(x) = \overline{a}\,\overline{\varphi}(x)^m$, onde $\overline{a} \in \kappa^\times$ é uma constante, $\overline{\varphi}(x) \in \kappa[x]$ é irredutível mônico e m é um inteiro positivo.*

Demonstração. Denotemos $(K, v, |\cdot|, A, \mathfrak{p}, \kappa)$. A ida da primeira parte desse teorema segue do Teorema 10.31. Provemos portanto a volta. Suponhamos que $|\cdot|$ admita extensão única a qualquer extensão algébrica de K. Começaremos provando a última afirmação do enunciado. Consideremos $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$ primitivo e irredutível, com $a_0, a_n \neq 0$, e seja $\overline{f}(x) \in \kappa[x]$ seu polinômio induzido.

Como $|\cdot|$ possui única extensão ao corpo de decomposição de f, o fato de f ser irredutível implica que seu polígono de Newton é um único segmento, que liga $(0, v(a_0))$ a $(n, v(a_n))$. Aplicando o Corolário 10.40, concluímos que $|f| = \max\{|a_0|, |a_n|\}$. Sendo f primitivo, temos $|f| = 1$, logo $|a_0| = 1$ ou $|a_n| = 1$, isto é, $v(a_0) = 0$ ou $v(a_n) = 0$.

Se $v(a_n) > 0$, então $v(a_0) = 0$, e o polígono de Newton de f é o segmento não-horizontal que liga $(0, 0)$ a $(n, v(a_n))$. Mas note que isso significa que $v(a_i) > 0$ para todo $1 \leq i \leq n$. Desse modo, nesse caso temos $\overline{f}(x) = \overline{a}_0$ constante não-nulo.

Suponhamos então $v(a_n) = 0$. Assim, $a_n \notin \mathfrak{p}$, de modo que $\overline{a}_n \neq 0$ e nós temos $\partial \overline{f} = \partial f$. Seja L o corpo de decomposição de f sobre K. Então $(L, |\cdot|, B, \mathfrak{P}, \lambda)$ é um corpo com valor absoluto,

onde $|\cdot|$ é a única extensão a L do valor absoluto de K. Notemos que, para todo $\sigma \in \mathrm{Gal}(L/K)$, $|\sigma(\cdot)|\colon L \to \mathbb{R}_+$ é um valor absoluto de L que estende o valor absoluto de K. Assim, pela unicidade da extensão temos $|\sigma(\cdot)| = |\cdot|$.

Dado $\alpha \in B$, temos $|\alpha| \leq 1$, e portanto $|\sigma(\alpha)| = |\alpha| \leq 1$, o que mostra que $\sigma\alpha \in B$, onde $\sigma \in \mathrm{Gal}(L/K)$ é qualquer. Portanto, $\sigma B \subseteq B$. Da mesma forma, $\sigma^{-1}B \subseteq B \Rightarrow B \subseteq \sigma B$, o que prova que temos $\sigma B = B$ para todo $\sigma \in \mathrm{Gal}(L/K)$. Procedendo analogamente, concluímos que $\sigma\mathfrak{P} = \mathfrak{P}$ para todo $\sigma \in \mathrm{Gal}(L/K)$. Assim, cada automorfismo $\sigma \in \mathrm{Gal}(L/K)$ induz um automorfismo $\overline{\sigma} \in \mathrm{Gal}(\lambda/\kappa)$ dado por $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$.

Afirmamos que todas as raízes de f estão em B. Para isso, sejam $\alpha_1, \ldots, \alpha_n \in L$ as raízes de f, contadas com multiplicidade. Como f é irredutível, todas as suas raízes são conjugadas. Assim, para $1 \leq i \leq n$ existe $\sigma_i \in \mathrm{Gal}(L/K)$ tal que $\sigma_i(\alpha_1) = \alpha_i$. Desse modo, como $\sigma B = B$ para todo $\sigma \in \mathrm{Gal}(L/K)$, basta mostrarmos que $\alpha_1 \in B$. Supondo por absurdo que $\alpha_1 \notin B$, temos $|\alpha_1| > 1$, e portanto $|\alpha_i| = |\sigma_i(\alpha_1)| = |\alpha_1| > 1$ para todo $1 \leq i \leq n$. Desse modo:

$$|a_0| = \left|\prod_{i=1}^{n} \alpha_i\right| = \prod_{i=1}^{n} |\alpha_i| > 1,$$

um absurdo já que $a_0 \in A \Rightarrow |a_0| \leq 1$. Concluímos que $\alpha_1 \in B$, e assim $\alpha_1, \ldots, \alpha_n \in B$. Agora, para todo $1 \leq i \leq n$ nós temos $\overline{\sigma_i}(\overline{\alpha}_1) = \overline{\alpha}_i$, o que mostra que todas as raízes de $\overline{f}$ são conjugadas por automorfismos de $\mathrm{Gal}(\lambda/\kappa)$. Assim, $\overline{f} = \overline{a}\,\overline{\varphi}(x)^m$, onde $\overline{a} \in \kappa^\times$, $\overline{\varphi}$ é o polinômio minimal de $\overline{\alpha}_1$ em $\kappa[x]$ e m é um inteiro positivo, provando a última afirmação.

Seja agora $f(x) \in A[x]$ um polinômio primitivo qualquer, e seja $f(x) = f_1(x) \cdots f_r(x)$ sua fatoração em irredutíveis de $K[x]$. Pelo Lema de Gauss não-arquimediano, multiplicando $f_1, \ldots, f_r$ por constantes adequadas nós podemos supor que $f_1, \ldots, f_r \in A[x]$ são primitivos. Assim, em $\kappa[x]$ nós temos a fatoração $\overline{f}(x) = \overline{f}_1(x) \cdots \overline{f}_r(x)$. Como cada f_j é irredutível, pelo que vimos nós temos $\overline{f}_j$ ou constante não-nulo ou então $\partial\,\overline{f}_j = \partial\, f_j$ e $\overline{f}_j$ é a potência de um polinômio irredutível em $\kappa[x]$, a menos de constante.

Mostraremos que vale o Lema de Hensel para f. Assim, suponhamos que $\overline{f} = \overline{g}\,\overline{h}$ para alguns $\overline{g}, \overline{h} \in \kappa[x]$ primos entre si. Como cada $\overline{f}_j$ é ou constante não-nulo ou potência de irredutível a menos de constante, isso significa que existem uma partição $I \sqcup J = \{1, 2, \ldots, r\}$ e elementos $\overline{a}, \overline{b} \in \kappa^\times$ tais que $\overline{g} = \overline{a} \prod_{i \in I} \overline{f}_i$, $\overline{h} = \overline{b} \prod_{j \in J} \overline{f}_j$ e $\partial\,\overline{f}_i = \partial\, f_i$ para todo $i \in I$. Notemos que, como $\overline{f} = \overline{g}\overline{h}$, nós temos $\overline{ab} = 1$, ou seja, $\overline{b} = \overline{a}^{-1}$.

Seja $a \in A \setminus \mathfrak{p} = A^\times$ tal que $\overline{a} = a \pmod{\mathfrak{p}}$. Então $a^{-1} \in A$. Note ainda que temos $\overline{b} = \overline{a}^{-1} = a^{-1} \pmod{\mathfrak{p}}$. Definamos finalmente $g := a \prod_{i \in I} f_i$ e $h := a^{-1} \prod_{j \in J} f_j$. Então é claro que $g, h \in A[x]$ são tais que $gh = f$, $\overline{g}$ e $\overline{h}$ são os polinômios induzidos por g e h em $\kappa[x]$, respectivamente, e $\partial\, g = \sum_{i \in I} \partial\, f_i = \sum_{i \in I} \partial\,\overline{f}_i = \partial\,\overline{g}$. Isso prova que vale o Lema de Hensel para f, como queríamos. □

Como consequência imediata desse teorema, nós temos:

Corolário 10.42. *Seja (K, v) um corpo henseliano, e seja (L, w) uma extensão algébrica de K. Então (L, w) também é corpo henseliano.*

Demonstração. Segue imediatamente da caracterização de corpos henselianos por unicidade de extensão, uma vez que toda extensão algébrica de (L, w) também é uma extensão algébrica de (K, v). □

Em particular, o fecho algébrico $(\overline{K}, \overline{v})$ de um corpo henseliano (K, v) é henseliano. Também é fácil ver que o corpo de resíduos de $\overline{K}$ é um fecho algébrico do corpo de resíduos de K. Juntando tudo, nós temos o seguinte resultado:

Proposição 10.43. *Seja $(K, v, A, \mathfrak{p}, \kappa)$ um corpo henseliano. Então existe uma única extensão de v a uma valoração $\overline{v}$ de seu fecho algébrico $\overline{K}$, que torna $\overline{K}$ um corpo henseliano $(\overline{K}, \overline{v}, \overline{A}, \overline{\mathfrak{p}}, \overline{\kappa})$. Além disso, $\overline{\kappa}$ é um fecho algébrico de κ.*

10.6. Ramificações

Nessa seção, estudaremos os tipos de ramificações que ocorrem em extensões de corpos com valoração (não-arquimediana). Em certo sentido, a ramificação de uma extensão mede o quão bem se comporta a extensão de corpos de resíduos correspondente: quanto menos ramificação ocorre, mais bem-comportada é essa extensão. Comecemos definindo o que significa uma não-ramificação, o caso mais bem-comportado:

Definição (Extensão Finita Não-Ramificada)**.** Seja $(L, w, \lambda)/(K, v, \kappa)$ uma extensão finita de corpos henselianos. Dizemos que essa extensão é **não-ramificada** se a extensão λ/κ for separável e se $[L : K] = [\lambda : \kappa]$.

Note que numa extensão de corpos henselianos $(L, w, \lambda)/(K, v, \kappa)$, se v for discreta temos a identidade fundamental $ef = [L : K]$, onde e e f são o índice de ramificação e o grau de inércia de L/K, respectivamente. Como $f = [\lambda : \kappa]$, a igualdade $[L : K] = [\lambda : \kappa]$ é equivalente a $f = [L : K]$, e portanto a $e = 1$ pela identidade fundamental. Assim, L/K será finita não-ramificada se e só se λ/κ for separável e $e = 1$, o que justifica a nomenclatura não-ramificada.

Proposição 10.44. *Seja $(K, v, A, \mathfrak{p}, \kappa)$ um corpo henseliano.*

(a) Seja $(L, w, B, \mathfrak{P}, \lambda)$ uma extensão finita não-ramificada de K. Então existe $\alpha \in B$ tal que $L = K(\alpha)$ e $\lambda = \kappa(\overline{\alpha})$. Além disso, sendo $f(x) = P_{\alpha,K} \in A[x]$ o polinômio minimal de α sobre K e $\overline{f}(x) = f(x) \pmod{\mathfrak{p}} \in \kappa[x]$, temos que $\overline{f}$ é o polinômio minimal de $\overline{\alpha}$ sobre κ e é separável.

(b) Seja L'/K uma extensão finita de corpos com valoração, e suponhamos que L seja um corpo com $K \subseteq L \subseteq L'$. Então L'/K será finita não-ramificada se e somente se as extensões intermediárias L'/L e L/K forem ambas finitas não-ramificadas.

(c) Sejam L/K e K'/K extensões de corpos com valoração dentro de um fecho algébrico $\overline{K}/K$, e suponhamos que L/K seja finita não-ramificada. Então LK'/K' também é finita não-ramificada.

(d) Sejam L/K e K'/K extensões de corpos com valoração dentro de um fecho algébrico $\overline{K}/K$, e suponhamos que L/K e K'/K sejam ambas finitas não-ramificadas. Então LK'/K também é finita não-ramificada. Desse modo, o compositum de duas extensões finitas não-ramificadas também é uma extensão finita não-ramificada.

Demonstração. (a) Como λ/κ é separável, existe $\overline{\alpha} \in \lambda$ tal que $\lambda = \kappa(\overline{\alpha})$, onde $\alpha \in B$. Seja $n := [L : K] = [\lambda : \kappa]$. Então $1, \overline{\alpha}, \ldots, \overline{\alpha}^{n-1}$ formam uma base de λ/κ, de modo que pela demonstração da Proposição 10.11 vemos que $1, \alpha, \ldots, \alpha^{n-1} \in B$ são linearmente independentes sobre K, e portanto formam uma base de L/K. Assim, $L = K(\alpha)$. Notemos que $f(x) = P_{\alpha,K}(x)$ está de fato em $A[x]$, pois $B = \overline{A}^L$ pelo Teorema 10.31. Como $\partial \overline{f} = \partial f = n = [\kappa(\alpha) : \kappa]$ e $\overline{f}(\overline{\alpha}) = 0$, vemos que $\partial \overline{f}$ é o polinômio irredutível de $\overline{\alpha}$ sobre κ. Como a extensão λ/κ é separável, vemos que $\overline{\alpha}$ é separável.

(b) Denotemos (L, λ) e (L', λ').

($\Rightarrow$): Suponhamos que L'/K seja finita não-ramificada. Sabemos que λ'/κ é separável e que $[\lambda' : \kappa] = [L' : K]$. Como λ'/λ e λ/κ são subextensões da extensão separável λ'/κ, vemos que ambas extensões são separáveis. Além disso, pela Proposição 10.11, nós temos $[\lambda' : \lambda] \leq [L' : L]$ e $[\lambda : \kappa] \leq [L : K]$. Assim:

$$[\lambda' : \kappa] = [\lambda' : \lambda][\lambda : \kappa] \leq [L' : L][L : K] = [L' : K] = [\lambda' : \kappa].$$

Desse modo, todas as desigualdades acima são igualdades, e portanto $[\lambda' : \lambda] = [L' : L]$ e $[\lambda : \kappa] = [L : K]$. Isso prova que L'/L e L/K são finitas não-ramificadas.

($\Leftarrow$): Suponhamos que L'/L e L/K sejam ambas finitas não-ramificadas. Então λ'/λ e λ/κ são separáveis, e valem as igualdades $[\lambda' : \lambda] = [L' : L]$ e $[\lambda : \kappa] = [L : K]$. Concluímos que λ'/κ é também separável, e temos:

$$[\lambda' : \kappa] = [\lambda' : \lambda][\lambda : \kappa] = [L' : L][L : K] = [L' : K],$$

mostrando que L'/K é finita não-ramificada.

(c) Denotemos $(L, B, \mathfrak{P}, \lambda)$, $(K', A', \mathfrak{p}', \kappa')$ e $(LK', B', \mathfrak{P}', \lambda')$. Então sabemos que λ/κ é separável e $[L : K] = [\lambda : \kappa]$. Como $[LK' : K'] \leq [L : K]$, a extensão $[LK' : K']$ é finita. Assim, basta mostrarmos que λ'/κ' é separável e $[LK' : K'] = [\lambda' : \kappa']$.

Seja $\alpha \in B$ tal que $L = K(\alpha)$ e $\lambda = \kappa(\overline{\alpha})$, que sabemos existir por (a). Sejam ainda $f(x) \coloneqq P_{\alpha,K}(x) \in A[x]$ e $\overline{f}(x) \coloneqq f(x) \pmod{\mathfrak{p}}$. Desse modo, $LK' = K'(\alpha)$. Seja $g(x) \coloneqq P_{\alpha,K'}(x) \in K'[x]$. Como $\alpha \in B' = \overline{A'}^{LK'}$, vemos que de fato temos $g(x) \in A'[x]$.

Definamos $\overline{g}(x) \coloneqq g(x) \pmod{\mathfrak{p}'} \in \kappa'[x]$. Como $g(x) = P_{\alpha,K'}(x)$ e $f(x) = P_{\alpha,K}(x)$, vemos que $g \mid f$ em $A'[x]$, e portanto $\overline{g} \mid \overline{f}$ em $\kappa'[x]$. Assim, $\overline{g}$ é separável. Se $\overline{g}$ fosse redutível em $\kappa'[x]$, seus dois fatores seriam coprimos devido à separabilidade de $\overline{g}$, e portanto pelo Lema de Hensel em K' nós concluiríamos que g seria redutível em $A'[x]$, um absurdo! Logo $\overline{g}$ é irredutível em $\kappa'[x]$, e portanto $\overline{g}(x) = P_{\overline{\alpha},\kappa'}$. Então:

$$[\lambda' : \kappa'] \leq [LK' : K'] = \partial\, g = \partial\, \overline{g} = [\kappa'(\overline{\alpha}) : \kappa'] \leq [\lambda' : \kappa'].$$

Assim, todas as desigualdades acima são igualdades, de modo que $[LK' : K'] = [\lambda' : \kappa']$ e $[\kappa'(\overline{\alpha}) : \kappa'] = [\lambda' : \kappa']$. Agora, como $\kappa'(\overline{\alpha}) \subseteq \lambda'$, a igualdade de graus acima nos diz que $\lambda' = \kappa'(\overline{\alpha})$ é extensão separável de κ', já que o polinômio minimal $\overline{g}$ de $\overline{\alpha}$ sobre κ' o é. Isso prova que LK'/K' é extensão finita não-ramificada.

(d) Devido ao item (c), sabemos que LK'/K' é finita não-ramificada. Como K'/K também é finita não-ramificada, vemos pelo item (b) que LK'/K é finita não-ramificada, como queríamos.

□

Para podermos definir uma extensão infinita não-ramificada de corpos henselianos, nós precisamos do seguinte resultado:

Lema 10.45. *Seja K um corpo henseliano, e seja L uma extensão finita de K. Então são equivalentes:*

(i) *L/K é não-ramificada.*

(ii) *Toda subextensão de L/K é não-ramificada.*

(iii) *L é uma união de subextensões não-ramificadas de L/K.*

(iv) *L é um compositum de subextensões não-ramificadas de L/K.*

Demonstração. $(i) \Rightarrow (ii)$: Segue da proposição acima.

$(ii) \Rightarrow (iii)$: É claro, já que L é a união de todas as suas subextensões.

$(iii) \Rightarrow (iv)$: Suponhamos que $L = \bigcup_{\lambda\in\Lambda} L_\lambda$, onde cada L_λ/K é extensão finita não-ramificada. Então é claro que $L = \prod_{\lambda\in\Lambda} L_\lambda$ é o compositum de todas essas extensões.

$(iv) \Rightarrow (i)$: Suponhamos que $L = \prod_{\lambda\in\Lambda} L_\lambda$ seja o compositum dos L_λ, e que cada L_λ/K seja uma extensão finita não-ramificada. Como L/K é finita, vemos que L é de fato o compositum de um número finito dos L_λ's, digamos $L = \prod_{j=1}^n L_j$. Aplicando sucessivamente o item (d) da proposição acima, vemos que L é extensão finita não-ramificada de K, como queríamos. □

Com isso, nós temos:

Proposição 10.46. *Seja K um corpo henseliano, e seja L uma extensão algébrica de K. Então são equivalentes:*

(i) Toda subextensão finita de L/K é não-ramificada.

(ii) L é uma união de subextensões finitas não-ramificadas de L/K.

(iii) L é um compositum de subextensões finitas não-ramificadas de L/K.

Demonstração. $(i) \Rightarrow (ii)$: Segue do fato de L ser a união de todas as suas subextensões finitas.

$(ii) \Rightarrow (iii)$: Suponhamos que $L = \bigcup_{\lambda\in\Lambda} L_\lambda$, onde cada L_λ é uma subextensão finita não-ramificada de L/K. Então basta notar que temos $L = \prod_\lambda L_\lambda$.

$(iii) \Rightarrow (i)$: Suponhamos que $L = \prod_\lambda L_\lambda$, onde cada L_λ é uma subextensão finita não-ramificada de L/K. Seja M uma subextensão finita qualquer de L/K. Então $M \subseteq \prod_\lambda L_\lambda$, e como M/K é extensão finita vemos que M está contido no compositum de um número finito dos L_λ's, digamos $M \subseteq \prod_{j=1}^n L_j$. Aplicando $(iv) \Rightarrow (i)$ e $(i) \Rightarrow (ii)$ do lema acima, concluímos que M/K é extensão finita não-ramificada. Assim, toda subextensão finita de L/K é não-ramificada, como queríamos. □

Definição (Extensão Não-Ramificada/Ramificada)**.** Seja (K, v) um corpo henseliano e seja (L, w) uma extensão algébrica de K. Dizemos que a extensão L/K é **não-ramificada** se ela satisfazer alguma das três condições equivalentes da proposição acima. Caso contrário, dizemos que essa extensão é **ramificada**.

Observe que, se L/K for extensão finita, então essa definição coincide com a anterior, devido ao Lema 10.45. Notemos ainda que se L/K for extensão não-ramificada de corpos henselianos, e se λ e κ forem os corpos residuais de L e de K, respectivamente, então λ/κ será uma extensão separável, já que todas as suas subextensões finitas são separáveis.

Nós temos a seguinte versão mais geral da Proposição 10.44:

Proposição 10.47. *Seja (K, v) um corpo henseliano.*

(a) Seja L'/K uma extensão algébrica não-ramificada, e suponhamos que L seja um corpo com $K \subseteq L \subseteq L'$. Então as extensões intermediárias L'/L e L/K são ambas não-ramificadas.

(b) Sejam L/K e K'/K extensões de corpos dentro de um fecho algébrico $\overline{K}/K$, e suponhamos que L/K seja não-ramificada. Então LK'/K' também é não-ramificada.

(c) Sejam L/K e K'/K extensões de corpos dentro de um fecho algébrico $\overline{K}/K$, e suponhamos que L/K e K'/K sejam ambas não-ramificadas. Então LK'/K também é não-ramificada. Desse modo, o compositum de duas extensões não-ramificadas também é uma extensão não-ramificada.

(d) Sejam L_λ/K extensões de corpos dentro de um fecho algébrico $\overline{K}/K$, e suponhamos que L_λ/K seja não-ramificada para todo $\lambda \in \Lambda$. Então o compositum $L = \prod_{\lambda\in\Lambda} L_\lambda$ é uma extensão não-ramificada de K.

Demonstração. (b) Como L/K é não-ramificada, temos $L = \prod_{\lambda\in\Lambda} L_\lambda$, onde cada L_λ é uma subextensão finita não-ramificada de K. Então nós temos $LK' = \prod_{\lambda\in\Lambda} L_\lambda K'$, e pela Proposição 10.44 nós temos cada $L_\lambda K'/K'$ finita não-ramificada. Assim, LK' é o compositum de subextensões finitas não-ramificadas de LK'/K', de onde concluímos que LK'/K' é extensão não-ramificada.

(a) Toda subextensão finita de L/K também é subextensão finita de L'/K, e portanto é não-ramificada. Disso concluímos que L/K é não-ramificada. Para ver que L'/L também é não-ramificada, basta aplicar o item (b) para as extensões L'/K e L/K, observando que $L' = L'L$.

(c) Como L/K e K'/K são não-ramificadas, podemos escrever $L = \prod_{i\in I} L_i$ e $K' = \prod_{j\in J} K'_j$, onde cada L_i/K é subextensão finita não-ramificada de L/K, e cada K'_j/K é subextensão finita não-ramificada de K'/K. Notemos então que cada $L_iK'_j/K$ é subextensão finita não-ramificada de LK'/K, pela Proposição 10.44, e que temos $LK' = \prod_{i\in I}\prod_{j\in J} L_iK'_j$, de modo que LK'/K é extensão não-ramificada.

(d) Basta mostrarmos que toda subextensão finita de L/K é não-ramificada. Mas toda tal subextensão também é uma subextensão finita do compositum de um número finito de L_λ's, que já sabemos ser uma extensão não-ramificada de K. Assim, toda subextensão finita de L/K é não-ramificada, e concluímos que L/K é não-ramificada.

□

A proposição acima nos mostra que existe uma subextensão não-ramificada maximal de L/K:

Definição (Subextensão Não-Ramificada Maximal)**.** Seja L/K uma extensão algébrica de corpos henselianos. Então o compositum T de todas as subextensões não-ramificadas de L/K é chamada de **subextensão não-ramificada maximal** de L/K. No caso em que $L = \overline{K}$ é um fecho algébrico de K, denotamos T por K^{nr}, e o chamamos de **extensão não-ramificada maximal**.

Note que T/K é subextensão não-ramificada de L/K e toda subextensão não-ramificada de L/K está contida em T, o que justifica a nomenclatura. Essa subextensão tem as seguintes propriedades:

Proposição 10.48. *Seja $(L, w, B, \mathfrak{P}, \lambda)/(K, v, A, \mathfrak{p}, \kappa)$ uma extensão algébrica de corpos henselianos, e seja $(T, w, A_s, \mathfrak{p}_s, \lambda_s)$ a sua subextensão não-ramificada maximal. Então λ_s é o fecho separável de κ em λ, e $w(T^\times) = v(K^\times)$.*

Em particular, o corpo de resíduos de K^{nr} é o fecho separável $\overline{\kappa}_s$ de κ, e $w((K^{rn})^\times) = v(K^\times)$.

Demonstração. Chamemos de λ_{sep} o fecho separável de κ em λ. Como T/K é não-ramificada, temos $\lambda_s \subseteq \lambda_{\text{sep}}$. Seja agora $\overline{\alpha} \in \lambda_{\text{sep}}$. Seja $\overline{f}(x) := P_{\overline{\alpha},\kappa}(x) \in \kappa[x]$, e seja $f(x) \in A[x]$ tal que $f(\alpha) = 0$ e $\overline{f} = f \pmod{\mathfrak{p}}$. Como $\overline{f}$ é irredutível em $\kappa[x]$, temos f irredutível em $A[x]$. Além disso, como $x - \overline{\alpha}$ divide $\overline{f}$ e $\overline{f}$ é separável, vemos pelo Lema de Hensel em L que existe $\alpha \in B$ tal que $\overline{\alpha} = \alpha \pmod{\mathfrak{P}}$. Assim, f é o polinômio minimal de α sobre K, e nós temos:

$$[K(\alpha) : K] = \partial f = \partial \overline{f} = [\kappa(\alpha) : \kappa].$$

Desse modo, $\kappa(\alpha)/\kappa$ é uma extensão separável e $[K(\alpha) : K] = [\kappa(\alpha) : \kappa]$. Disso poderemos concluir que $K(\alpha)/K$ é uma extensão não-ramificada, se mostrarmos que o corpo de resíduos κ' de $K(\alpha)$ é igual a $\kappa(\alpha)$. Como $\alpha \in B \cap K(\alpha) = \overline{A}^{K(\alpha)}$, vemos que $\overline{\alpha} \in \kappa'$, e portanto $\kappa(\overline{\alpha}) \subseteq \kappa'$. Por outro lado, temos:

$$[\kappa' : \kappa] \leq [K(\alpha) : K] = [\kappa(\alpha) : \kappa],$$

o que mostra que devemos ter $\kappa' = \kappa(\alpha)$, como queríamos. Portanto, a extensão $K(\alpha)/K$ é não-ramificada, como queríamos, e $K(\alpha) \subseteq T$. Assim, $\overline{\alpha} \in \lambda_s$. Isso mostra que $\lambda_{\text{sep}} \subseteq \lambda_s$, e

provamos que $\lambda_s = \lambda_{\text{sep}}$.

Mostremos agora que $w(T^\times) = v(K^\times)$. Como T é a união de suas subextensões finitas, basta provarmos que $w(M^\times) = v(K^\times)$ para toda subextensão finita não-ramificada (M, w, λ_M) de L/K. Mas nós temos:

$$[M : K] \geq (w(M^\times) : v(K^\times))[\lambda_M : \kappa] = (w(M^\times) : v(K^\times))[M : K],$$

de onde obtemos $(w(M^\times) : v(K^\times)) = 1$, ou seja, $w(M^\times) = v(K^\times)$, como queríamos.

Finalmente, a afirmação sobre o corpo de resíduos de K^{nr} segue da Proposição 10.43. □

Seja $m \in \mathbb{N}$ não divisível pela característica do corpo de resíduos κ de K. Então sabemos que o polinômio $x^m - 1 \in \kappa[x]$ é separável, e portanto se decompõe em fatores lineares em $\overline{\kappa}_s[x]$. Aplicando o Lema de Hensel a K^{nr}, vemos que $x^m - 1 \in K[x]$ se decompõe em fatores lineares em $K^{nr}[x]$, e portanto K^{nr} contém todas as raízes m-ésimas da unidade.

A subextensão não-ramificada maximal se comporta bem com interseções:

Proposição 10.49. *Seja $M/L/K$ uma torre algébrica de corpos henselianos, e seja T a subextensão não-ramificada maximal de M/K. Então a subextensão não-ramificada maximal de L/K é $T \cap L$. Em particular, a subextensão não-ramificada maximal de L/K é $K^{nr} \cap L$.*

Demonstração. Chamemos de U a subextensão não-ramificada maximal de L/K. Como a extensão $(T \cap L)/K$ é uma subextensão da extensão não-ramificada T/K, essa extensão é não-ramificada, e portanto $T \cap L \subseteq U$. Por outro lado, é claro que $U \subseteq L$, e como essa é uma subextensão não-ramificada de M/K temos $U \subseteq T$, o que nos dá $U \subseteq T \cap L$. Assim, vale a igualdade desejada. □

Estudemos agora as extensões ramificadas. Existem dois tipos de ramificação: a ramificação mansa, que é melhor comportada, e a ramificação selvagem, que é pior comportada:

Definição (Extensão Mansamente/Selvagemente/Totalmente Ramificada)**.** Consideremos uma extensão algébrica ramificada de corpos henselianos $(L, w, \lambda)/(K, v, \kappa)$. Seja T a sua subextensão não-ramificada maximal e seja p o expoente característico de κ. Se L/K for finita, dizemos que a extensão L/K é **mansamente ramificada** se λ/κ for uma extensão separável e se tivermos $\text{mdc}([L : T], p) = 1$. No caso geral, dizemos que L/K é **mansamente ramificada** se λ/κ for uma extensão separável e se toda subextensão finita de L/T tiver grau primo com p.

Se L/K não for mansamente ramificada, dizemos que L/K é **selvagemente ramificada**. Além disso, dizemos que L/K é **totalmente ramificada** se $T = K$.

Suponhamos v discreta, L/K finita e λ/κ separável. Nesse caso, como já vimos, L/K será não-ramificada se e só se $e = 1$. Notemos que $[T : K] = [\lambda_s : \kappa] = [\lambda : \kappa] = f$. Assim, $[L : T] = [L : K]/f = e$. Ou seja, nesse caso L/K será mansamente ramificada se e só se $e > 1$ e $p \nmid e$, e será selvagemente ramificada se e só se $e > 1$ e $p \mid e$. De todo modo, temos o seguinte diagrama:

$$\begin{array}{ccc} L & & \lambda \\ {\scriptstyle e}\big| & & {\scriptstyle 1}\big| \\ T & & \lambda_s = \lambda \\ {\scriptstyle f}\big| & & {\scriptstyle f}\big| \\ K & & \kappa \end{array}$$

Observemos ainda que, nessas condições, L/K será totalmente ramificada se e só se $T = K$, e portanto se e só se $f = 1$.

É possível mostrar que o compositum de extensões mansamente ramificadas também é uma extensão mansamente ramificada (veja por exemplo a Seção II.7 de [2]). Assim, dada uma extensão L/K de corpos henselianos, sempre existe uma **subextensão mansamente ramificada maximal** V de L/K.

No caso em que L/K é uma extensão finita galoisiana, a valoração é discreta e λ/κ é finita, podemos mostrar que a subextensão não-ramificada maximal de L/K é igual ao seu corpo de inércia:

Proposição 10.50. *Seja $(L, w, B, \mathfrak{P}, \lambda)/(K, v, A, \mathfrak{p}, \kappa)$ uma extensão finita galoisiana de corpos henselianos, e suponhamos que v seja discreta e que λ/κ seja separável. Então T_w é a subextensão não-ramificada maximal de L/K.*

Demonstração. Nós temos o seguinte diagrama:

$$\begin{array}{ccccc}
\mathfrak{P} \lhd B & \hookrightarrow & L = Q(B) & \text{---------} & 1 \\
{\scriptstyle p^t}\big| & & {\scriptstyle p^t}\big| & & {\scriptstyle p^t}\big| \\
\mathfrak{P}_V \lhd B_V & \hookrightarrow & V_w = Q(B_V) & \text{------} & R_w \\
{\scriptstyle \tilde{e}}\big| & & {\scriptstyle \tilde{e}}\big| & & {\scriptstyle \tilde{e}}\big| \\
\mathfrak{P}_T \lhd B_T & \hookrightarrow & T_w = Q(B_T) & \text{-------} & I_w \qquad \lambda = B_T/\mathfrak{P}_T \\
{\scriptstyle f}\big| & & {\scriptstyle f}\big| & & {\scriptstyle f}\big| \qquad\qquad \big| \\
\mathfrak{p} \lhd A & \hookrightarrow & K = Q(A) & \text{--------} & G \qquad\qquad \kappa
\end{array}$$

Seja T a subextensão não-ramificada maximal de L/K. Nós temos:

$$[B_T/\mathfrak{P}_T : \kappa] = [\lambda : \kappa] = f = [T_w : K].$$

Assim, T_w/K é extensão não-ramificada, de modo que $T_w \subseteq T$. Como $[T_w : K] = f = [T : K]$, concluímos que $T_w = T$, como queríamos. □

Similarmente, pode-se mostrar que nesse caso a subextensão não-ramificada maximal de L/K é o corpo de ramificação V_w (veja por exemplo a Seção II.9 de [2]).

Capítulo 11

O Teorema de Kronecker-Weber

Nosso objetivo nesse capítulo é provar o importante **Teorema de Kronecker-Weber**:

Teorema 11.1 (Teorema de Kronecker-Weber)**.** *Toda extensão finita abeliana de* $\mathbb{Q}$ *está contida em uma extensão ciclotômica. Isto é, se* $K/\mathbb{Q}$ *for uma extensão finita galoisiana com* $\mathrm{Gal}(K/\mathbb{Q})$ *abeliano, então existe uma raiz da unidade* $\zeta \in \mathbb{C}$ *tal que* $K \subseteq \mathbb{Q}(\zeta)$*.*

Para demonstrarmos esse teorema, aplicaremos o chamado **Princípio Local-Global**, que nos permite obter resultados sobre $\mathbb{Q}$ olhando para cada corpo p-ádico $\mathbb{Q}_p$ e depois "juntando tudo". Assim, provaremos o Teorema de Kronecker-Weber utilizando o **Teorema de Kronecker-Weber Local**:

Teorema 11.2 (Teorema de Kronecker-Weber Local)**.** *Seja* p *um primo. Toda extensão finita e abeliana de* $\mathbb{Q}_p$ *está contida em uma extensão ciclotômica. Isto é, se* $K/\mathbb{Q}_p$ *for uma extensão finita galoisiana com* $\mathrm{Gal}(K/\mathbb{Q}_p)$ *abeliano, então existe uma raiz da unidade* $\zeta \in \overline{\mathbb{Q}}_p$ *tal que* $K \subseteq \mathbb{Q}_p(\zeta)$*.*

Nós provaremos esse teorema local dividindo no caso de extensões não-ramificadas, mansamente ramificadas e selvagemente ramificadas.

Nesse capítulo, utilizaremos a notação ζ_n para indicar uma raiz primitiva n-ésima da unidade.

11.1. O Caso Local

Para provarmos o Teorema de Kronecker-Weber Local, podemos nos restringir às extensões cíclicas de grau potência de primo. Para ver isso, comecemos com o seguinte lema:

Lema 11.3. *Seja* L/K *uma extensão finita galoisiana, e suponhamos que* G_1, G_2 *sejam grupos tais que* $\mathrm{Gal}(L/K) \cong G_1 \times G_2$*. Então* $L = L_1L_2$*, onde* L_1, L_2 *são extensões finitas galoisianas de* K*, com* $L_1 \cap L_2 = K$*,* $\mathrm{Gal}(L_1/K) \cong G_1$ *e* $\mathrm{Gal}(L_2/K) \cong G_2$*.*

Demonstração. Sem perda de generalidade, reconheçamos G_1 e G_2 com suas identificações dentro de $\mathrm{Gal}(L/K)$. Então $\mathrm{Gal}(L/K) = G_1 \odot G_2$. Definimos L_1 e L_2 como os corpos fixos de G_2 e G_1, respectivamente. Desse modo, $\mathrm{Gal}(L/L_1) = G_2$ e $\mathrm{Gal}(L/L_2) = G_1$. Como nós temos $\mathrm{Gal}(L/K) = G_1 \odot G_2$, $G_1, G_2 \lhd \mathrm{Gal}(L/K)$. Assim, L_1/K e L_2/K são extensões finitas galoisianas, com $\mathrm{Gal}(L_1/K) \cong \mathrm{Gal}(L/K)/G_2 \cong G_1$ e $\mathrm{Gal}(L_2/K) \cong \mathrm{Gal}(L/K)/G_1 \cong G_2$.

Além disso, o corpo fixo de $\mathrm{Gal}(L/K) = G_1G_2$ é $L_1 \cap L_2$, de modo que $L_1 \cap L_2 = K$, e L_1L_2 é o corpo fixo de $G_1 \cap G_2 = 1$, de modo que $L_1L_2 = L$. □

Com isso, conseguimos a redução desejada:

Proposição 11.4. *Seja p um primo. Suponhamos que toda extensão finita cíclica K de $\mathbb{Q}_p$ com grau potência de primo esteja contida em uma extensão ciclotômica. Então vale o Teorema de Kronecker-Weber Local para p.*

Demonstração. Seja K uma extensão finita abeliana qualquer de $\mathbb{Q}_p$. Então, pelo Teorema de Classificação dos Grupos Abelianos Finitos, nós temos:

$$\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z},$$

para $p_1, \ldots, p_r$ primos e $k_1, \ldots, k_r$ inteiros positivos. Aplicando várias vezes o lema acima, concluímos que $K = K_1 \cdots K_r$, onde $K_1, \ldots, K_r$ são extensões finitas galoisianas de $\mathbb{Q}_p$ com $\mathrm{Gal}(K_j/\mathbb{Q}_p) \cong \mathbb{Z}/p_j^{k_j}\mathbb{Z}$, para todo $1 \leq j \leq r$. Por hipótese, nós temos $K_j \subseteq \mathbb{Q}_p(\zeta_{n_j})$, para algum inteiro positivo n_j. Tomemos $n \coloneqq n_1 \cdots n_r$. Então:

$$K = K_1 \cdots K_r \subseteq \mathbb{Q}_p(\zeta_{n_1}) \cdots \mathbb{Q}_p(\zeta_{n_r}) \subseteq \mathbb{Q}_p(\zeta_n),$$

concluindo a demonstração. □

A partir de agora, fixemos um número primo p. Pelo resultado acima, para demonstrar o Teorema de Kronecker-Weber Local para p basta estudarmos as extensões finitas galoisianas $K/\mathbb{Q}_p$ com $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/\ell^r\mathbb{Z}$, onde $\ell \in \mathbb{N}$ é um primo e r é um inteiro positivo. Como veremos, convém dividir o nosso estudo nos casos $\ell \neq p$ e $\ell = p$. O primeiro caso é mais simples, enquanto o segundo requer um cuidado maior.

Nessa seção, estudaremos como as extensões de corpos sobre $\mathbb{Q}_p$ se comportam em termos de ramificação, e também como são as extensões ciclotômicas sobre $\mathbb{Q}_p$. Ao longo dessa seção, L/K sempre denotará uma extensão finita de corpos, onde ambos $(L, |\cdot|_p, B, \mathfrak{P}, \lambda)$ e $(K, |\cdot|_p, A, \mathfrak{p}, \kappa)$ são extensões finitas de $\mathbb{Q}_p$. Observemos em particular que κ é um corpo finito de característica p, digamos $\kappa = \mathbb{F}_q$, onde q é uma potência de p. Sendo κ finito, vemos que λ/κ é sempre separável. Assim, podemos ignorar essa condição quando tratarmos do tipo de ramificação.

Denotaremos por e e por f o índice de ramificação e o grau de inércia de L/K, respectivamente. Observemos que vale a identidade fundamental $ef = [L : K]$, já que essa é uma extensão finita de corpos completos com uma valoração discreta.

Proposição 11.5. *Suponhamos que L/K seja uma extensão finita não-ramificada. Então existe uma raiz n-ésima da unidade $\zeta \in \overline{\mathbb{Q}}_p$, com $n \in \mathbb{N}$ primo com p, tal que $L = K(\zeta)$.*

Em particular, toda extensão finita não-ramificada de $\mathbb{Q}_p$ é ciclotômica.

Demonstração. Como L/K é não-ramificada, temos $[L : K] = [\lambda : \kappa]$. Sendo $\kappa = \mathbb{F}_q$, temos $\lambda = \kappa(\overline{\zeta})$, onde $\overline{\zeta} \in \lambda$ é uma raiz n-ésima da unidade, e $n = q^k - 1$ para algum k inteiro positivo. Em particular, $p \nmid n$. Como $\overline{\zeta} \in \lambda$ é raiz do polinômio separável $x^n - 1 \in \mathbb{F}_p[x]$, vemos pelo Lema de Hensel que existe $\zeta \in L$ tal que $\zeta^n = 1$ e $\zeta \pmod{\mathfrak{p}} = \overline{\zeta}$. Agora, notemos que $[K(\zeta) : K] \geq [\kappa(\overline{\zeta}) : \kappa]$ pela demonstração da Proposição 10.11, e assim:

$$[L : K] \geq [K(\zeta) : K] \geq [\kappa(\overline{\zeta}) : \kappa] = [\lambda : \kappa] = [L : K].$$

Então todas as desigualdades acima são igualdades, e vemos que $L = K(\zeta)$, como queríamos. □

Note que o resultado acima resolve o Teorema de Kronecker-Weber Local para o caso de extensões não-ramificadas. Além disso, a "volta" desse resultado também vale:

Proposição 11.6. *Suponhamos que $L = K(\zeta)$, onde ζ é uma raiz primitiva n-ésima da unidade, para $p \nmid n$. Então temos:*

(a) A extensão L/K é não-ramificada de grau f, onde f é o menor número natural tal que $q^f \equiv 1 \pmod{n}$, isto é, f é a ordem de q em $(\mathbb{Z}/n\mathbb{Z})^\times$.

(b) As extensões L/K e λ/κ são galoisianas e seus grupos de Galois são canonicamente isomorfos. Além disso, $\mathrm{Gal}(L/K)$ *é gerado pelo automorfismo* $\zeta \mapsto \zeta^q$.

(c) $B = A[\zeta]$.

Demonstração. (a) Seja $P(x) := P_{\zeta,K}(x)$. Então $\overline{P}(x) := P(x) \pmod{\mathfrak{p}} \in \kappa[x]$ é igual ao polinômio minimal de $\overline{\zeta}$ sobre κ. De fato, $\overline{P}(x)$ é separável, pois divide o polinômio separável $x^n - 1 \in \kappa[x]$. Desse modo, pelo Lema de Hensel, $\overline{P}$ é irredutível, pois caso contrário P seria redutível. Assim:

$$[L : K] = [K(\zeta) : K] \geq [\kappa(\overline{\zeta}) : \kappa] = \partial\,\overline{P} = \partial\,P = [L : K].$$

Concluímos então que $[\kappa(\overline{\zeta}) : \kappa] = [L : K] \geq [\lambda : \kappa] \geq [\kappa(\overline{\zeta}) : \kappa]$. Assim, $\kappa(\overline{\zeta}) = \lambda$ e a extensão L/K é não-ramificada. Para calcularmos o grau dessa extensão, devemos determinar o grau de $\kappa(\overline{\zeta})/\kappa$, ou seja, de $\mathbb{F}_q(\overline{\zeta})/\,\mathbb{F}_q$. Mas o grau dessa extensão é exatamente a ordem de q em $(\mathbb{Z}\,/n\,\mathbb{Z})^\times$, devido ao Teorema 2.31.

(b) Sendo geradas por raízes da unidade, é claro que L/K e λ/κ são ambas galoisianas. Consideremos agora $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\lambda/\kappa)$ dado por $\sigma \mapsto \overline{\sigma}$, onde $\overline{\sigma}(\overline{\zeta}) = \overline{\sigma(\zeta)}$. O fato desse homomorfismo ser uma bijeção segue de os conjugados de $\overline{\zeta}$ serem as classes dos conjugados de ζ. Finalmente, como $\kappa = \mathbb{F}_q$, sabemos que $\mathrm{Gal}(\lambda/\kappa)$ é gerado por $\overline{\zeta} \mapsto \overline{\zeta}^q$, de onde vemos que $\mathrm{Gal}(L/K)$ é gerado por $\zeta \mapsto \zeta^q$.

(c) Dado $b \in B$ qualquer, como $\lambda = \kappa(\overline{\zeta})$ temos $\overline{b} = \overline{a}_0 + \overline{a}_1\overline{\zeta} + \cdots + \overline{a}_{f-1}\overline{\zeta}^{f-1}$, para alguns $a_0, \ldots, a_{f-1} \in A$. Assim, $b = a_0 + a_1\zeta + \cdots + a_{f-1}\zeta^{f-1} + p$ para algum $p \in \mathfrak{P}$. Isso prova que $B = A[\zeta] + \mathfrak{P}$. Como L/K é não-ramificado, temos $e = 1$, e portanto $\mathfrak{p}\,B = \mathfrak{P}$. Assim, $B = A[\zeta] + \mathfrak{p}\,B$. Como $B = \overline{A}^L$ é um A-módulo finitamente gerado, concluímos pelo Lema de Nakayama que $B = A[\zeta]$.

□

Suponhamos agora que L/K seja uma extensão ramificada. Como a característica de κ é p, essa extensão será mansamente ramificada se tivermos $\mathrm{mdc}(e, p) = 1$ e selvagemente ramificada se tivermos $\mathrm{mdc}(e, p) > 1$. Comecemos estudando as ramificações mansas:

Proposição 11.7. *Seja L/K uma extensão finita totalmente ramificada mansa. Então existem $\pi \in K$ um normalizador e $\alpha \in L$ uma raiz e-ésima de π tais que $L = K(\alpha)$. Além disso, nesse caso α é um normalizador de L.*

Demonstração. Tomemos $\pi_0 \in K$ e $\beta \in L$ normalizadores. Então temos $\beta^e = u\pi_0$, para algum $u \in B^\times$. Como L/K é uma extensão totalmente ramificada, temos $f = 1 \Rightarrow \lambda = \kappa$. Assim, existe $u_0 \in A^\times$ tal que $u \equiv u_0 \pmod{\mathfrak{P}}$. Então $u = u_0 + x$, para algum $x \in \mathfrak{P}$. Chamemos $\pi := u_0\pi_0$. Então é claro que π também é um normalizador de K, e nós temos:

$$\beta^e = u\pi_0 = (u_0 + x)\pi_0 = u_0\pi_0 + x\pi_0 = \pi + x\pi_0 \Rightarrow |\beta^e - \pi|_p = |x\pi_0|_p < |\pi_0|_p = |\pi|_p.$$

Consideremos o polinômio $f(x) = x^e - \pi \in A[x]$, e sejam $\alpha_1, \ldots, \alpha_e$ suas raízes em $\overline{\mathbb{Q}}_p$. Notemos que $\alpha_j^e = \pi \Rightarrow |\alpha_j|_p = \sqrt[e]{|\pi|_p}$, para todo $1 \leq j \leq e$. Agora:

$$\prod_{j=1}^{e} |\beta - \alpha_j|_p = |f(\beta)|_p = |\beta^e - \pi|_p < |\pi|_p.$$

Assim, devemos ter $|\beta - \alpha_j|_p < \sqrt[e]{|\pi|_p} = |\alpha_1|_p$ para algum $1 \leq j \leq e$. Suponhamos sem perda de generalidade que isso valha para $j = 1$. Observemos ainda que, para todo $2 \leq j \leq e$, temos $|\alpha_1 - \alpha_j|_p \leq \max\{|\alpha_1|_p, |\alpha_j|_p\} = |\alpha_1|_p$. Agora:

$$\prod_{j=2}^{e} |\alpha_1 - \alpha_j|_p = |f'(\alpha_1)| = |e\alpha_1^{e-1}|_p = |\alpha_1|_p^{e-1},$$

uma vez que $p \nmid e$. Desse modo, devemos ter $|\alpha_1 - \alpha_j|_p = |\alpha_1|_p$, para todo $2 \leq j \leq e$. Seja agora $(M, |\cdot|)$ o fecho normal, e portanto galoisiano, da extensão $L(\alpha_1)/L$, e seja $\sigma \in \mathrm{Gal}(M/L)$ qualquer. Como $|\sigma(\cdot)|_p$ é um valor absoluto de M, pela unicidade do Teorema 10.9 temos que $|\sigma(\cdot)|_p = |\cdot|_p$. Assim:

$$|\beta - \sigma(\alpha_1)|_p = |\sigma(\beta - \alpha_1)|_p = |\beta - \alpha_1|_p < |\alpha_1|_p.$$

Mas então, para todo $2 \leq j \leq e$, temos:

$$|\alpha_1 - \sigma(\alpha_1)|_p \leq \max\{|\alpha_1 - \beta|_p, |\beta - \sigma(\alpha_1)|_p\} < |\alpha_1|_p = |\alpha_1 - \alpha_j|_p,$$

o que mostra que $\sigma(\alpha_1) \neq \alpha_j$. Como $\sigma(\alpha_1)$ é raiz de f, concluímos que $\sigma(\alpha_1) = \alpha_1$. Mas isso vale para todo $\sigma \in \mathrm{Gal}(M/L)$, o que significa que $\alpha_1 \in L$. Aplicando agora o critério de Eisenstein a $f(x) = x^e - \pi$, ou equivalentemente observando que seu polígono de Newton é um único segmento, vemos que f é irredutível sobre K, e portanto $[K(\alpha_1) : K] = e = [L : K]$. Isso mostra que $L = K(\alpha_1)$. Tomemos $\alpha := \alpha_1$. Finalmente, notemos que $|\alpha|_p^e = |\pi|_p = |\pi_0|_p = |\beta|_p^e$, e portanto $|\alpha|_p = |\beta|_p$, o que mostra que α é um normalizador de L. □

Para demonstrarmos o Teorema de Kronecker-Weber no caso ramificado, precisamos estudar o comportamento das extensões ciclotômicas sobre $\mathbb{Q}_p$ geradas por raízes p^m-ésimas da unidade.

Proposição 11.8. *Seja ζ uma raiz primitiva p^m-ésima da unidade, para m inteiro positivo. Então temos:*

(a) $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ *é uma extensão totalmente ramificada de grau* $\varphi(p^m) = (p-1)p^{m-1}$.

(b) $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ *é canonicamente isomorfo a* $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

(c) $1-\zeta$ *é um normalizador de* $\mathbb{Q}_p[\zeta]$, *e* $N_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}(1-\zeta) = p$.

(d) $\mathbb{Z}_p[\zeta]$ *é o DVD de* $\mathbb{Q}_p(\zeta)$.

Demonstração. Seja $\xi := \zeta^{p^{m-1}}$. Então ξ é uma raiz primitiva p-ésima da unidade, e portanto temos $1 + \xi + \cdots + \xi^{p-1} = 0$. Assim, temos $1 + \zeta^{p^{m-1}} + \cdots + \zeta^{(p-1)p^{m-1}} = 0$. Denotemos

$$\varphi(x) := x^{(p-1)p^{m-1}} + \cdots + x^{p^{m-1}} + 1.$$

Então $\varphi(\zeta) = 0$. Notemos que $\zeta - 1$ é raiz de $\varphi(x+1)$. Mas nós temos:

$$\varphi(x) = \frac{(x^{p^{m-1}})^p - 1}{x^{p^{m-1}} - 1} = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} \equiv \frac{(x-1)^{p^m}}{(x-1)^{p^{m-1}}} = (x-1)^{(p-1)p^{m-1}} \pmod{p}.$$

Desse modo, $\varphi(x+1) \equiv x^{(p-1)p^{m-1}} \pmod{p}$ e o coeficiente independente desse polinômio é igual a $\varphi(0+1) = \varphi(1) = p$. Assim, pelo Critério de Eisenstein, vemos que $\varphi(x+1)$ é irredutível em $\mathbb{Q}_p[x]$, e portanto $\varphi(x)$ também o é. Isso prova que $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ tem grau $(p-1)p^{m-1} = \varphi(p^m)$.

Pelo Teorema 2.25, $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ é canonicamente isomorfo a um subgrupo de $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Como $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ e $(\mathbb{Z}/p^m\mathbb{Z})^\times$ têm ambos ordem $\varphi(p^m)$, concluímos que esse é um isomorfismo. Notemos agora que:

$$N(1-\zeta) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)} \sigma(1-\zeta) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)} (1 - \sigma(\zeta)) = \varphi(1) = p.$$

Chamemos de w a valoração estendida de v_p em $\mathbb{Q}_p(\zeta)$. Então:

$$w(1-\zeta) = \frac{1}{\varphi(p^m)} v_p(N(1-\zeta)) = \frac{1}{\varphi(p^m)} v_p(p) = \frac{1}{\varphi(p^m)}.$$

Isso mostra que $e \geq \varphi(p^m)$, e portanto pela identidade fundamental devemos ter $e = \varphi(p^m)$ e $f = 1$. Isso prova que $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ é totalmente ramificada. Como $1/e$ é o menor valor positivo assumido por w, e $w(1-\zeta) = 1/e$, vemos que $1-\zeta$ é um normalizador de $\mathbb{Q}_p(\zeta)$.

Finalmente, notemos que pela demonstração da Proposição 10.13, utilizando o fato de que $f = 1$ e tomando $\omega_1 := 1$ e $\Pi := 1-\zeta$, nós obtemos que o DVD de $\mathbb{Q}_p(\zeta)$ é $\mathbb{Z}_p[1-\zeta] = \mathbb{Z}_p[\zeta]$, como queríamos. □

Precisaremos ainda do seguinte lema:

Lema 11.9. *Temos $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$, onde $(-p)^{1/(p-1)}$ denota uma raiz $(p-1)$-ésima qualquer de $-p$.*

Demonstração. Se $p = 2$, então ambos os corpos indicados são $\mathbb{Q}_p$, de modo que o resultado é óbvio. Suponhamos então $p > 2$. Nesse caso, como já vimos, $\zeta_p \notin \mathbb{Q}_p$, uma vez que as únicas raízes da unidade de $\mathbb{Q}_p$ são as $(p-1)$-ésimas. Notemos que todas as raízes $(p-1)$-ésimas de $-p$ geram o mesmo corpo sobre $\mathbb{Q}_p$, já que uma difere de outra por uma raiz primitiva $(p-1)$-ésima da unidade, e todas essas raízes estão em $\mathbb{Q}_p$. Assim, basta provarmos isso para uma raiz $(p-1)$-ésima qualquer de $-p$.

Denotemos $\varphi(x) = x^{p-1} + \cdots + x + 1$ e $\psi(x) = \varphi(x+1)$. Então, como vimos na demonstração do teorema anterior, esses são polinômios irredutíveis, e $1-\zeta_p$ é normalizador de $\mathbb{Q}_p(\zeta_p)$. Notemos que

$$\psi(x) = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1}x + p.$$

Como $e = \varphi(p) = p-1$, temos $(1-\zeta_p)^{p-1} = tp$ para algum $t \in \mathbb{Z}_p[\zeta_p]^\times$. Assim, $(1-\zeta_p)^{p-1}$ divide p em $\mathbb{Z}_p[\zeta_p]$, de modo que:

$$\begin{aligned} & (\zeta_p - 1)^{p-1} + \binom{p}{p-1}(\zeta_p-1)^{p-2} + \cdots + \binom{p}{1}(\zeta_p - 1) + p \\ \equiv\ & (\zeta_p - 1)^{p-1} + p \pmod{(1-\zeta_p)^p}. \end{aligned}$$

Logo:

$$0 = \psi(\zeta_p - 1) \equiv (\zeta_p-1)^{p-1} + p = (t+1)p \pmod{(1-\zeta_p)^p} \Rightarrow t+1 \equiv 0 \pmod{1-\zeta_p}.$$

Dessa forma, $u := -t \equiv 1 \pmod{1-\zeta_p}$. Notemos que $u = \frac{(1-\zeta_p)^{p-1}}{-p} \in \mathbb{Z}_p[\zeta_p]^\times$. Consideremos agora o polinômio $f(x) = x^{p-1} - u \in \mathbb{Q}_p(\zeta_p)[x]$. Então $f(1) = 1 - u \equiv 0 \pmod{1-\zeta_p}$, e $f'(1) = p-1 \not\equiv 0 \pmod{1-\zeta_p}$. Pelo Lema de Hensel, concluímos que existe $u_1 \in \mathbb{Z}_p[\zeta_p]$ tal que $f(u_1) = 0$, isto é, $u_1^{p-1} = u$. Com isso:

$$-p = \frac{(1-\zeta_p)^{p-1}}{u} = \frac{(1-\zeta_p)^{p-1}}{u_1^{p-1}} = \left(\frac{1-\zeta_p}{u_1}\right)^{p-1} \Rightarrow (-p)^{1/(p-1)} = \frac{1-\zeta_p}{u_1} \in \mathbb{Q}_p\,.$$

Isso prova que $\mathbb{Q}_p((-p)^{1/(p-1)}) \subseteq \mathbb{Q}_p(\zeta_p)$. Por outro lado, $x^{p-1} + p \in \mathbb{Q}_p[x]$ é um polinômio irredutível pelo critério de Eisenstein, de modo que $\mathbb{Q}_p((-p)^{1/(p-1)})/\mathbb{Q}_p$ é uma extensão de grau $p-1$, assim como $\mathbb{Q}_p(\zeta_p)$. Isso prova que $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$. □

Com isso, podemos demonstrar o Teorema de Kronecker-Weber Local para extensões mansamente ramificadas. Isso em particular demonstrará o teorema para extensões cíclicas de grau ℓ^r com $\ell \neq p$.

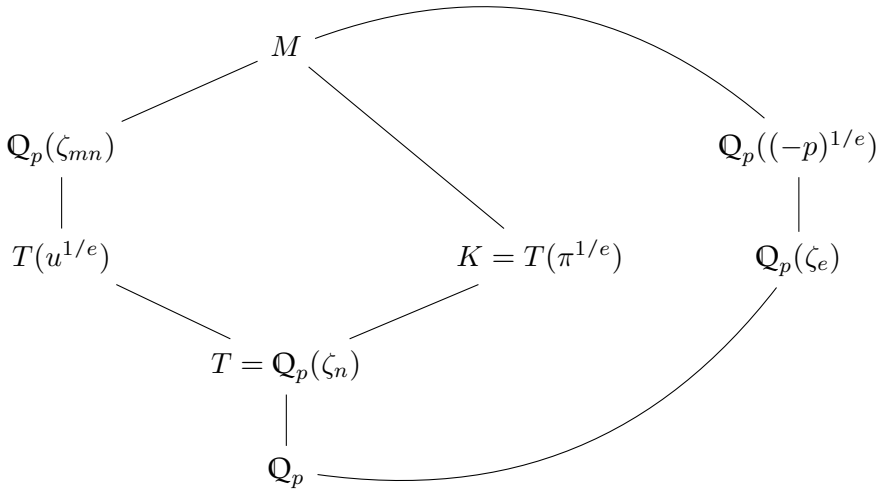
Proposição 11.10. *Seja $K/\mathbb{Q}_p$ uma extensão finita abeliana mansamente ramificada. Então existe uma raiz da unidade $\zeta \in \overline{\mathbb{Q}}_p$ tal que $K \subseteq \mathbb{Q}_p(\zeta)$. Em particular, isso ocorre caso nós tenhamos $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/\ell^r\mathbb{Z}$, onde $\ell \neq p$ é um primo e r é um inteiro positivo.*

Demonstração. Seja $T/\mathbb{Q}_p$ a subextensão não-ramificada maximal de $K/\mathbb{Q}_p$. Então pela Proposição 11.5 existe um inteiro positivo n não divisível por p tal que $T = \mathbb{Q}_p(\zeta_n)$. Chamemos de e e de f o índice de ramificação e o grau de inércia de $K/\mathbb{Q}_p$, respectivamente. Então K/T é uma extensão totalmente ramificada de índice e, de modo que pela Proposição 11.7 existe um normalizador $\pi \in K$ tal que $K = T(\pi^{1/e})$.

Como $T/\mathbb{Q}_p$ é uma extensão não-ramificada, temos $\pi = -up$ para alguma unidade u no DVD de T. Consideremos agora o polinômio $x^e - u$. Como u é unidade, o polinômio induzido $x^e - \overline{u}$ no corpo de resíduos de T é separável, já que $p \nmid e$, e portanto aplicando o Lema de Hensel em T^{nr} nós encontramos $u^{1/e} \in T^{nr}$ raiz desse polinômio. Então a extensão $T(u^{1/e})/T$ é finita não-ramificada. Assim, pela Proposição 11.5 existe m inteiro positivo não divisível por p tal que

$$T(u^{1/e}) = T(\zeta_m) = \mathbb{Q}_p(\zeta_m, \zeta_n) \subseteq \mathbb{Q}_p(\zeta_{mn}).$$

Seja M o compositum de K e de $\mathbb{Q}_p(\zeta_{mn})$. Como $K/\mathbb{Q}_p$ e $\mathbb{Q}_p(\zeta_{mn})/\mathbb{Q}_p$ são extensões galoisianas, $M/\mathbb{Q}_p$ também é extensão galoisiana, com $\mathrm{Gal}(M/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{mn})/\mathbb{Q}_p)$. Assim, a extensão $M/\mathbb{Q}_p$ é abeliana. Observemos agora que $\pi^{1/e}, u^{1/e} \in M$, e portanto nós temos $(-p)^{1/e} := \pi^{1/e}/u^{1/e} \in M$. Assim, $\mathbb{Q}_p((-p)^{1/e}) \subseteq M$. Sendo uma subextensão de $M/\mathbb{Q}_p$, vemos que $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ é uma extensão abeliana.



Sendo uma extensão de Galois, todas as raízes e-ésimas de $-p$ estão em $\mathbb{Q}_p((-p)^{1/e})$, digamos $r_1 = (-p)^{1/e}, \ldots, r_e$. Note que essas raízes são todas distintas, pois como $p \nmid e$ o polinômio $x^e + p$ é separável. Assim, $1, r_1/r_2, \ldots, r_1/r_e \in \mathbb{Q}_p((-p)^{1/e})$ são todas as e raízes e-ésimas da unidade. Isso prova que $\zeta_e \in \mathbb{Q}_p((-p)^{1/e})$. Notemos agora que a extensão $\mathbb{Q}_p((-p)^{1/e})$ é totalmente ramificada. De fato, isso segue do Teorema 4.28, uma vez que $(-p)^{1/e}$ é raiz de $x^e + p = 0$, que satisfaz o Critério de Eisenstein.

Como $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ é subextensão de $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$, ela é totalmente ramificada. Mas $p \nmid e$, e portanto pela Proposição 11.6 a única forma disso ocorrer é se essa for a extensão trivial, ou seja, $\zeta_e \in \mathbb{Q}_p$. Pela Proposição 10.5, devemos ter $e \mid p-1$ ou $e = 2$ e $p = 2$. Como $p \nmid e$, concluímos que $e \mid p-1$. Desse modo, $\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$, pelo lema acima. Assim:

$$K = T(\pi^{1/e}) \subseteq T(u^{1/e}, (-p)^{1/e}) \subseteq \mathbb{Q}_p(\zeta_{mn}, \zeta_p) = \mathbb{Q}_p(\zeta_{mnp}),$$

como desejado.

Suponhamos agora $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/\ell^r\mathbb{Z}$. Seja T a subextensão não-ramificada maximal de $K/\mathbb{Q}_p$. Então K/T é uma extensão de grau que divide ℓ^r, e portanto $\mathrm{mdc}([K:T], p) = 1$. Isso prova que $K/\mathbb{Q}_p$ é uma extensão mansamente ramificada, como gostaríamos. □

Assim, resta mostrarmos o Teorema de Kronecker-Weber Local para extensões $K/\mathbb{Q}_p$ tais que $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/p^r\mathbb{Z}$, para algum inteiro positivo r. Para tratarmos desse caso, utilizaremos sem demonstração o seguinte resultado:

Lema 11.11. *Seja $p > 2$ um primo. Então não existem extensões de $\mathbb{Q}_p$ com grupo de Galois isomorfo a $(\mathbb{Z}/p\mathbb{Z})^3$. Além disso, não existem extensões de $\mathbb{Q}_2$ com grupo de Galois isomorfo a $(\mathbb{Z}/2\mathbb{Z})^4$ ou $(\mathbb{Z}/4\mathbb{Z})^3$.*

Esse resultado se demonstra utilizando resultados básicos da chamada **Teoria de Kummer**. Para uma demonstração desse fato, veja por exemplo o Capítulo 20 de [3] ou o Capítulo 14 de [8]. Nós também utilizaremos resultados elementares sobre os grupos de unidades de $\mathbb{Z}/n\mathbb{Z}$ para n inteiro positivo, que podem ser encontrados no Capítulo 4 de [12].

Finalmente, conseguimos concluir a demonstração do Teorema de Kronecker-Weber Local, tratando do caso de uma extensão $K/\mathbb{Q}_p$ com $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/p^r\mathbb{Z}$.

Teorema 11.12. *Seja $K/\mathbb{Q}_p$ uma extensão cíclica de grau p^r, para r inteiro positivo. Então $K \subseteq \mathbb{Q}_p(\zeta_n)$, para algum inteiro positivo n.*

Demonstração. Suponhamos inicialmente $p \neq 2$. Comecemos considerando as extensões ciclotômicas $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$ e $\mathbb{Q}_p(\zeta_{p^{r+1}})$ de $\mathbb{Q}_p$. Pela Proposição 11.6, a extensão $\mathbb{Q}_p(\zeta_{p^{p^r}-1})/\mathbb{Q}_p$ é cíclica não-ramificada de grau p^r, e pela Proposição 11.8 a extensão $\mathbb{Q}_p(\zeta_{p^{r+1}})/\mathbb{Q}_p$ é totalmente ramificada de grau $\varphi(p^r) = (p-1)p^r$, com grupo de Galois isomorfo a:

$$(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^r\mathbb{Z} \cong \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

Assim, $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$ e o subcorpo de $\mathbb{Q}_p(\zeta_{p^{r+1}})$ fixo pelo subgrupo de $(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times$ isomorfo a $\mathbb{Z}/p^r\mathbb{Z}$ são ambas extensões cíclicas de $\mathbb{Q}_p$ de grau p^r. Definamos $n := (p^{p^r}-1)p^{r+1}$.

Mostraremos agora que $\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{p^{p^r}-1})\,\mathbb{Q}_p(\zeta_{p^{r+1}})$ e $\mathbb{Q}_p(\zeta_{p^{p^r}-1}) \cap \mathbb{Q}_p(\zeta_{p^{r+1}}) = \mathbb{Q}_p$. A primeira igualdade é clara. Para a segunda, basta notar que $\mathbb{Q}_p(\zeta_{p^{p^r}-1}) \cap \mathbb{Q}_p(\zeta_{p^{r+1}})$ é ao mesmo tempo uma extensão não-ramificada e totalmente ramificada de $\mathbb{Q}_p$, e portanto deve ser igual a $\mathbb{Q}_p$. Com isso:

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) &\cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{p^r}-1})/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{r+1}})/\mathbb{Q}_p) \\
&\cong \mathbb{Z}/p^r\mathbb{Z} \times (\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \\
&\cong \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.
\end{aligned}$$

Afirmamos que $K \subseteq \mathbb{Q}_p(\zeta_n)$. De fato, suponhamos por absurdo que $K \not\subseteq \mathbb{Q}_p(\zeta_n)$. Então $K(\zeta_n) = K\,\mathbb{Q}_p(\zeta_n)$ é uma extensão de Galois de $\mathbb{Q}_p$, cujo grupo de Galois é um subgrupo de $\mathrm{Gal}(K/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) = (\mathbb{Z}/p^r\mathbb{Z})^3 \times \mathbb{Z}/(p-1)\mathbb{Z}$. Em particular, essa é uma extensão abeliana. Além disso, como $(\mathbb{Z}/p^r\mathbb{Z})^3$ e $\mathbb{Z}/(p-1)\mathbb{Z}$ têm ordens primas entre si, é fácil ver que devemos ter $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_p) = G \times H$, para $G \leq (\mathbb{Z}/p^r\mathbb{Z})^3$ e $H \leq \mathbb{Z}/(p-1)\mathbb{Z}$.

Notemos que $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_p(\zeta_n))$ é canonicamente isomorfo a um subgrupo de $K/\mathbb{Q}_p$, e portanto isomorfo a $\mathbb{Z}/p^s\mathbb{Z}$ para algum $1 \leq s \leq r$ (note que $s > 0$, pois $K \not\subseteq \mathbb{Q}_p(\zeta_n)$). Além disso, note que esse grupo está contido em G, uma vez que H contém apenas elementos de ordem não divisível por p. Agora:

$$\begin{aligned}
&\frac{\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_p)}{\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_p(\zeta_n))} \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \\
\Rightarrow\quad &\frac{G \times H}{\mathbb{Z}/p^s\mathbb{Z}} \cong (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/(p-1)\mathbb{Z} \\
\Rightarrow\quad &\frac{G}{\mathbb{Z}/p^s\mathbb{Z}} \times H \cong (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/(p-1)\mathbb{Z}.
\end{aligned}$$

Como H possui apenas elementos de ordem não divisível por p, H deve ser levado por esse isomorfismo num subgrupo de $\mathbb{Z}/(p-1)\mathbb{Z}$. Da mesma forma, $\frac{G}{\mathbb{Z}/p^s\mathbb{Z}}$ deve ser levado num subgrupo de $(\mathbb{Z}/p^r\mathbb{Z})^2$. Isso mostra que devemos ter $\frac{G}{\mathbb{Z}/p^s\mathbb{Z}} \cong (\mathbb{Z}/p^r\mathbb{Z})^2$ e $H \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Sejam $x, y \in G$ tais que $\overline{x}$ e $\overline{y}$ geram $(\mathbb{Z}/p^r\mathbb{Z})^2$, e seja $z \in G$ um gerador de $\mathbb{Z}/p^s\mathbb{Z}$. Então x e y devem ter ordem múltipla de p^r, e portanto essa ordem deve ser exatamente p^r, uma vez que $G \leq (\mathbb{Z}/p^r\mathbb{Z})^3$. Notemos que todo elemento de $\frac{G}{\mathbb{Z}/p^s\mathbb{Z}}$ se escreve como $a\overline{x} + b\overline{y}$, onde nós temos $0 \leq a, b < p^r$ inteiros. Como isso nos dá $(p^r)^2$ elementos, e essa é exatamente a ordem de $\frac{G}{\mathbb{Z}/p^s\mathbb{Z}} \cong (\mathbb{Z}/p^r\mathbb{Z})^2$, vemos que todos esses elementos são distintos. Isso prova que $\langle x, y\rangle \cap \langle z\rangle = 0$. Notemos ainda que $G = \langle x, y\rangle\langle z\rangle$, uma vez que $\frac{G}{\langle z\rangle} = \langle \overline{x}, \overline{y}\rangle$. Sendo G abeliano, $\langle x, y\rangle, \langle z\rangle \lhd G$, e nós concluímos que $G = \langle x, y\rangle \odot \langle z\rangle$. Assim:

$$G \cong \langle x, y\rangle \times \langle z\rangle \cong (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/p^s\mathbb{Z}.$$

Finalmente, nós obtemos:

$$\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_p) = G \times H \cong (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

Em particular, $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_p)$ possui um subgrupo isomorfo a $(\mathbb{Z}/p\mathbb{Z})^3$. Sendo $K(\zeta_n)/\mathbb{Q}_p$ uma extensão abeliana, vemos que existe um subgrupo L dessa extensão com grupo de Galois $\mathrm{Gal}(L/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^3$, um absurdo pelo lema acima! Concluímos que $K \subseteq \mathbb{Q}_p(\zeta_n)$, como desejávamos.

Suponhamos agora $p = 2$. Então, pela Proposição 11.6, a extensão $\mathbb{Q}_2(\zeta_{2^{2^r}-1})/\mathbb{Q}_2$ é cíclica não-ramificada de grau 2^r, e pela Proposição 11.8 a extensão $\mathbb{Q}_2(\zeta_{2^{r+2}})/\mathbb{Q}_2$ é totalmente ramificada de grau 2^{r+1}, com grupo de Galois isomorfo a $(\mathbb{Z}/2^{r+2}\mathbb{Z})^\times$. Definindo $n := (2^{2^r}-1)2^{r+2}$, vemos do mesmo modo que no caso anterior que $\mathbb{Q}_2(\zeta_n)$ é o compositum dessas duas extensões e que $\mathbb{Q}_2$ é a interseção delas, de modo que

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}_2(\zeta_n)/\mathbb{Q}_2) &\cong \mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{2^r}-1})/\mathbb{Q}_2) \times \mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{r+2}})/\mathbb{Q}_2)\\ &\cong \mathbb{Z}/2^r\mathbb{Z} \times (\mathbb{Z}/2^{r+2}\mathbb{Z})^\times\\ &\cong \mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.\end{aligned}$$

Afirmamos que $K \subseteq \mathbb{Q}_2(\zeta_n)$. De fato, suponhamos por absurdo que $K \not\subseteq \mathbb{Q}_2(\zeta_n)$. Então $K(\zeta_n) = K\,\mathbb{Q}_2(\zeta_n)$ é uma extensão de Galois de $\mathbb{Q}_2$, cujo grupo de Galois é um subgrupo do grupo $\mathrm{Gal}(K/\mathbb{Q}_2) \times \mathrm{Gal}(\mathbb{Q}_2(\zeta_n)/\mathbb{Q}_2) \cong (\mathbb{Z}/2^r\mathbb{Z})^3 \times \mathbb{Z}/2\mathbb{Z}$. De forma análoga ao caso anterior, vemos que $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2(\zeta_n)) \cong \mathbb{Z}/2^s\mathbb{Z}$ para algum $1 \leq s \leq r$. Agora:

$$\begin{aligned}&\frac{\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2)}{\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2(\zeta_n))} \cong \mathrm{Gal}(\mathbb{Q}_2(\zeta_n)/\mathbb{Q}_2)\\ \Rightarrow\quad &\frac{\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2)}{\mathbb{Z}/2^s\mathbb{Z}} \cong (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}.\end{aligned}$$

Sejam $x, y, z \in \mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2)$ tais que $\frac{\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2)}{\mathbb{Z}/2^s\mathbb{Z}} = \langle \overline{x}, \overline{y}, \overline{z}\rangle$, onde o isomorfismo acima leva $\langle x\rangle$ no primeiro fator $\mathbb{Z}/2^r\mathbb{Z}$, $\langle y\rangle$ no segundo fator $\mathbb{Z}/2^r\mathbb{Z}$ e $\langle z\rangle$ em $\mathbb{Z}/2\mathbb{Z}$. Então x e y possuem ordens múltiplas de 2^r, e portanto iguais a 2^r já que $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2) \leq (\mathbb{Z}/2^r\mathbb{Z})^3 \times \mathbb{Z}/2\mathbb{Z}$. Seja ainda w um gerador de $\mathbb{Z}/2^s\mathbb{Z}$. Então $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2) = \langle x, y, z, w\rangle$.

Afirmamos que $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2) = \langle x\rangle \odot \langle y\rangle \odot \langle z, w\rangle$. Comecemos mostrando que nós temos $\langle x, y\rangle \cap \langle z, w\rangle = 0$. Note que o isomorfismo acima leva $\langle x, y\rangle$ em $\langle \overline{x}, \overline{y}\rangle$, e ambos $\langle x, y\rangle$ e $\langle \overline{x}, \overline{y}\rangle$ têm $(2^r)^2$ elementos. Sejam $0 \leq a, b < 2^r$ inteiros. Suponhamos que $ax + by \in \langle z, w\rangle$, com $0 \leq a, b < 2^r$. Então $ax + by$ é levado pelo isomorfismo acima em $0 \times 0 \times \mathbb{Z}/2\mathbb{Z}$. Mas isso é um absurdo, pois então $\langle \overline{x}, \overline{y}\rangle$ teria menos de $(2^r)^2$ elementos.

Agora, $\langle x\rangle \cap \langle y\rangle = 0$, pois argumentando de forma similar veríamos que $\langle \overline{x}, \overline{y}\rangle$ teria menos de $(2^r)^2$ elementos. Assim, $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2) = \langle x\rangle \odot \langle y\rangle \odot \langle z, w\rangle \cong (\mathbb{Z}/2^r\mathbb{Z})^2 \times \langle z, w\rangle$. Notemos que $\langle z, w\rangle$ tem ordem 2^{s+1}, uma vez que w tem ordem 2^s e $\overline{z}$ tem ordem 2 em $\frac{\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2)}{\langle w\rangle}$. Temos dois casos:

- $\langle z, w\rangle$ é cíclico: nesse caso, $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2) \cong (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2^{s+1}\mathbb{Z}$. Como esse é um subgrupo de $(\mathbb{Z}/2^r\mathbb{Z})^3 \times \mathbb{Z}/2\mathbb{Z}$, concluímos que $r \geq s+1 \geq 2$, de modo que $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2)$ possui um subgrupo isomorfo a $(\mathbb{Z}/4\mathbb{Z})^3$. Assim, existe um subcorpo L de $K(\zeta_n)$ com $\mathrm{Gal}(L/\mathbb{Q}_2) \cong (\mathbb{Z}/4\mathbb{Z})^3$, um absurdo pelo lema acima!

- $\langle z, w\rangle$ não é cíclico: nesse caso, como a ordem de w é 2^s e $\langle z, w\rangle$ tem ordem 2^{s+1}, devemos ter $\langle z, w\rangle \cong \mathbb{Z}/2^s\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, e portanto $\mathrm{Gal}(K(\zeta_n)/\mathbb{Q}_2) \cong (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2^s\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Em particular, esse grupo possui um subgrupo isomorfo a $(\mathbb{Z}/2\mathbb{Z})^4$. Assim, existe um subcorpo L de $K(\zeta_n)$ com $\mathrm{Gal}(L/\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^4$, um absurdo pelo lema acima!

Esses absurdos nos mostram que $K \subseteq \mathbb{Q}_2(\zeta_n)$, concluindo a demonstração. □

11.2. O Caso Global

Finalmente, mostremos que o caso local implica o caso global. Ou seja, que como o Teorema de Kronecker-Weber Local vale para todo primo p, então também vale o Teorema de Kronecker-Weber. Comecemos com dois lemas:

Lema 11.13. *Seja L/K uma extensão galoisiana, onde L e K são extensões finitas galoisianas de $\mathbb{Q}_p$, para p primo. Sejam I_L e I_K os grupos de inércia de $L/\mathbb{Q}_p$ e $K/\mathbb{Q}_p$, respectivamente. Então temos um homomorfismo sobrejetor $I_L \to I_K$.*

Demonstração. Seja T a subextensão não-ramificada maximal de $L/\mathbb{Q}_p$. Então a subextensão não-ramificada maximal de $K/\mathbb{Q}_p$ é $T \cap K$, pela Proposição 10.49. Também sabemos que os grupos de inércia de $L/\mathbb{Q}_p$ e $K/\mathbb{Q}_p$ são isomorfos a $\mathrm{Gal}(T/\mathbb{Q}_p)$ e a $\mathrm{Gal}((T\cap K)/\mathbb{Q}_p)$, respectivamente, pela Proposição 10.50. Desse modo, o resultado segue do fato do homomorfismo de restrição $\mathrm{Gal}(T/\mathbb{Q}_p) \to \mathrm{Gal}((T\cap K)/\mathbb{Q}_p)$ ser sobrejetor. □

Lema 11.14. *Seja n um inteiro positivo. Então o grupo de inércia da extensão $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ é isomorfo a $(\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^\times$.*

Demonstração. Seja $e := v_p(n)$. Então podemos escrever $n = p^e m$, onde $p \nmid m$. Pela Proposição 11.6, a extensão $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ é não-ramificada. Isso significa em particular que p é um normalizador de $\mathbb{Q}_p(\zeta_m)$. Com isso, podemos reproduzir a demonstração da Proposição 11.8 substituindo $\mathbb{Q}_p$ por $\mathbb{Q}_p(\zeta_m)$, para concluir que a extensão $\mathbb{Q}_p(\zeta_m)(\zeta_{p^e})/\mathbb{Q}_p(\zeta_m)$ é totalmente ramificada com grupo de Galois isomorfo a $(\mathbb{Z}/p^e\mathbb{Z})^\times$. Mas $\mathbb{Q}_p(\zeta_m)(\zeta_{p^e}) = \mathbb{Q}_p(\zeta_n)$. Assim, a extensão $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p(\zeta_m)$ é totalmente ramificada e $\mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p(\zeta_m)) \cong (\mathbb{Z}/p^e\mathbb{Z})^\times$.

Desse modo, pela Proposição 10.50, teremos o resultado desejado se mostrarmos que $\mathbb{Q}_p(\zeta_m)$ é a subextensão não-ramificada maximal de $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$. Seja T essa subextensão não-ramificada maximal. Como $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ é não-ramificada, temos $T \supseteq \mathbb{Q}_p(\zeta_m)$. Além disso, $T/\mathbb{Q}_p(\zeta_m)$ é extensão não-ramificada, pelo item (b) da Proposição 10.44.

Sendo $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p(\zeta_m)$ uma extensão totalmente ramificada, é fácil ver pela Proposição 10.49 que a subextensão $T/\mathbb{Q}_p(\zeta_m)$ também é totalmente ramificada. Desse modo, $T/\mathbb{Q}_p(\zeta_m)$ é uma extensão ao mesmo tempo não-ramificada e totalmente ramificada, de onde $T = \mathbb{Q}_p(\zeta_m)$, concluindo a demonstração. □

Demonstração. (Do Teorema de Kronecker-Weber) Seja $K/\mathbb{Q}$ uma extensão finita abeliana qualquer. Para cada primo $p \in \mathbb{N}$ que se ramifica em K, tomemos $\mathfrak{p} \lhd \mathcal{O}_K$ primo sobre p. Então, pela Proposição 10.29, $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \cong G_\mathfrak{p}(K/\mathbb{Q}) \subseteq \mathrm{Gal}(K/\mathbb{Q})$. Em particular, a extensão $K_\mathfrak{p}/\mathbb{Q}_p$ é finita abeliana. Assim, pelo Teorema de Kronecker-Weber Local nós concluímos que existe

um inteiro positivo n_p para o qual $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{n_p})$. Denotemos, para cada um desses primos p, $e_p := v_p(n_p)$, e definamos:

$$n := \prod_{p \text{ ramifica em } K} p^{e_p}.$$

Esse produto é finito, pelo Corolário 4.26. Mostraremos que $K \subseteq \mathbb{Q}(\zeta_n)$, o que concluirá a demonstração. Para isso, mostraremos que $K(\zeta_n) = \mathbb{Q}(\zeta_n)$. Seja $L := K(\zeta_n)$. Observe que $L = K\,\mathbb{Q}(\zeta_n)$, e portanto $\mathrm{Gal}(L/\mathbb{Q})$ é isomorfo a um subgrupo de $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Em particular, a extensão $L/\mathbb{Q}$ é finita abeliana. Para cada $\mathfrak{p} \mid p$ escolhido, fixemos um primo $\mathfrak{P} \lhd \mathcal{O}_L$ sobre $\mathfrak{p}$. Então de forma análoga ao que fizemos acima podemos concluir que a extensão $L_\mathfrak{P}/\mathbb{Q}_p$ é finita abeliana, já que $L_\mathfrak{P} = K_\mathfrak{p}(\zeta_n) = K_\mathfrak{p}\,\mathbb{Q}_p(\zeta_n)$.

Denotemos $I_\mathfrak{P}(L/\mathbb{Q}) := I_p$, e chamemos de T_p o seu corpo fixo. Pela Proposição 10.29, nós temos $I_p \cong I_{L_\mathfrak{P}}$, onde $I_{L_\mathfrak{P}}$ é o grupo de inércia da extensão $L_\mathfrak{P}/\mathbb{Q}_p$. Note que:

$$L_\mathfrak{P} = K_\mathfrak{p}(\zeta_n) \subseteq \mathbb{Q}_p(\zeta_{n_p}, \zeta_n) = \mathbb{Q}_p(\zeta_{\mathrm{mmc}(n_p,n)}) = \mathbb{Q}_p(\zeta_{p^{e_p}n'}),$$

onde n' é um inteiro positivo com $p \nmid n'$. Assim, $\mathbb{Q}_p(\zeta_n) \subseteq L_\mathfrak{P} \subseteq \mathbb{Q}_p(\zeta_{p^{e_p}n'})$. Denotemos por $I_{\mathbb{Q}_p(\zeta_n)}$ e por $I_{\mathbb{Q}_p(\zeta_{p^{e_p}n'})}$ os grupos de inércia de $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ e de $\mathbb{Q}_p(\zeta_{p^{e_p}n'})/\mathbb{Q}_p$, respectivamente. Pelo Lema 11.14, ambos os grupos $I_{\mathbb{Q}_p(\zeta_n)}$ e $I_{\mathbb{Q}_p(\zeta_{p^{e_p}n'})}$ são isomorfos a $(\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$. Agora, pelo Lema 11.13 temos uma sequência de homomorfismos sobrejetores $I_{\mathbb{Q}_p(\zeta_{p^{e_p}n'})} \to I_{L_\mathfrak{P}} \to I_{\mathbb{Q}_p(\zeta_n)}$, de onde concluímos que $I_{L_\mathfrak{P}} \cong (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$. Desse modo, $I_p \cong I_{L_\mathfrak{P}} \cong (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$. Seja I o subgrupo de $\mathrm{Gal}(L/\mathbb{Q})$ gerado por $\bigcup_{p|n} I_p$. Como $\mathrm{Gal}(L/\mathbb{Q})$ é abeliano, $\prod_{p|n} I_p$ é um grupo que contém $\bigcup_{p|n} I_p$, e portanto:

$$|I| \leq \prod_{p|n} |I_p| = \prod_{p|n} |(\mathbb{Z}/p^{e_p}\mathbb{Z})^\times| = \prod_{p|n} \varphi(p^{e_p}) = n = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]. \tag{11.1}$$

Seja M o corpo fixo de I. Fixado $p \mid n$, nós sabemos que toda a ramificação de p na extensão $L/\mathbb{Q}$ ocorre em L/T_p. Assim, p não se ramifica em T_p. Agora, $I_p \subseteq I \Rightarrow M \subseteq T_p$, de modo que p também não se ramifica em M. Fixemos agora $p \nmid n$. Provaremos que p também não se ramifica em M. Para isso, basta ver que p não se ramifica em L, já que $M \subseteq L$.

Seja $\mathfrak{P} \lhd \mathcal{O}_L$ primo sobre p qualquer. Queremos mostrar que $e(\mathfrak{P} \mid p) = 1$. Sabemos que p não se ramifica em K, já que $p \nmid n$. Isso também nos diz que p não se ramifica em $\mathbb{Q}(\zeta_n)$, pelo Teorema 5.17. Assim, $e(\mathfrak{P} \cap K \mid p) = e(\mathfrak{P} \cap \mathbb{Q}(\zeta_n)) = 1$, e portanto pela Proposição 6.15 nós concluímos que $T_\mathfrak{P} \supseteq K$ e $T_\mathfrak{P} \supseteq \mathbb{Q}(\zeta_n)$. Ou seja, $T_\mathfrak{P} \supseteq K\,\mathbb{Q}(\zeta_n) = L$, o que mostra que $T_\mathfrak{P} = L$. Desse modo, $I_\mathfrak{P} = 1$, e temos $e(\mathfrak{P} \mid p) = |I_\mathfrak{P}| = 1$, como queríamos.

Essa análise nos mostra que todo primo $p \in \mathbb{N}$ é não-ramificado em M, e portanto pelo Teorema 7.21 obtemos $M = \mathbb{Q}$. Assim, $I = \mathrm{Gal}(L/\mathbb{Q})$, e (11.1) nos dá:

$$[L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})| \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}],$$

e como $\mathbb{Q}(\zeta_n) \subseteq L$ nós obtemos $L = \mathbb{Q}(\zeta_n)$, concluindo a demonstração. □

Capítulo 12

Introdução à Teoria dos Corpos de Classes

No capítulo anterior, vimos como pode ser útil estudar "coisas locais" (isto é, completamentos) para concluir "coisas globais". Chamamos essa ideia de **Princípio Local-Global**. O desenvolvimento desse princípio é o que chamamos de **Teoria dos Corpos de Classes**. Nesse capítulo, faremos uma breve introdução dessa importante teoria, que é uma sequência natural do que vínhamos estudando. Os resultados aqui enunciados podem ser encontrados em [2], [3], [11] e [15].

O principal objetivo da Teoria dos Corpos de Classes é estudar a relação entre as extensões de **corpos globais** e de **corpos locais** com a **aritmética** desses corpos.

12.1. Um Pouco de Geometria Algébrica

Consideremos o anel de funções $\mathbb{C}[t]$. Os seus ideais primos não-nulos são os ideais da forma $\langle t-\alpha\rangle$, para $\alpha \in \mathbb{C}$. Assim, esses ideais podem ser identificados com os pontos de $\mathbb{C}$. Dado $\alpha \in \mathbb{C}$ qualquer, podemos considerar a **avaliação** em α como sendo o homomorfismo $\mathbb{C}[t] \to \mathbb{C}$ dado por $f(t) \mapsto f(\alpha)$. Em termos de ideais, podemos considerar para cada ideal primo não-nulo $\mathfrak{p} \lhd \mathbb{C}[t]$ a **avaliação** em $\mathfrak{p}$ como sendo o homomorfismo $\mathbb{C}[t] \to \mathbb{C}[t]/\mathfrak{p}$ dado por $f(t) \mapsto f(t) \pmod{\mathfrak{p}}$.

Podemos generalizar essa ideia para um domínio de Dedekind A qualquer. Dado um primo não-nulo $\mathfrak{p} \lhd A$, definimos a **avaliação** em $\mathfrak{p}$ como sendo o homomorfismo $A \to A/\mathfrak{p}$ dado por $a \mapsto a(\mathfrak{p}) \coloneqq a \pmod{\mathfrak{p}}$. Desse ponto de vista, enxergamos os elementos de A como sendo funções nos ideais primos não-nulos de A, que assumem valores nos corpos de resíduos de A.

Consideremos agora o corpo de funções $\mathbb{C}(t) = Q(\mathbb{C}[t])$. Para cada $f(t) \in \mathbb{C}(t)$ e cada ponto $\alpha \in \mathbb{C}$, podemos representar f como uma série de Laurent em $\mathbb{C}((t-\alpha))$. Podemos ainda considerar a **ordem** de f em α como sendo:

$$\operatorname{ord}_\alpha(f) \coloneqq \begin{cases} m, & \text{se } \alpha \text{ for um zero de ordem } m \text{ de } f; \\ -m, & \text{se } \alpha \text{ for um polo de ordem } m \text{ de } f; \\ 0, & \text{caso contrário.} \end{cases}$$

Nós podemos ainda acrescentar a $\mathbb{C}$ o **ponto no infinito**. Nesse caso, dado $f(t) \in \mathbb{C}(t)$ podemos considerar sua **série de Laurent no infinito** como sendo sua expansão em $\mathbb{C}((1/t))$, e sua **ordem no infinito** como sendo $\operatorname{ord}_\infty(f) \coloneqq -\partial f$. É fácil ver que as ordens nos diferentes pontos de $\mathbb{C}$ se relacionam pela expressão $\sum_{\alpha \in \mathbb{C} \cup \{\infty\}} \operatorname{ord}_\alpha(f) = 0$.

Essas expansões em séries de Laurent possuem uma generalização para domínios de Dedekind em geral. Sejam A um domínio de Dedekind e $K = Q(A)$. Seja $\mathfrak{p} \lhd A$ primo não-nulo. Então para

cada $a \in A$ nós podemos considerar a expansão de a como uma série de Laurent no completamento $K_\mathfrak{p}$, devido à Proposição 9.14. Além disso, as valorações $\mathfrak{p}$-ádicas $v_\mathfrak{p}$ em K generalizam as ordens ord_α de $\mathbb{C}(t)$. Já a fórmula $\sum_{\alpha \in \mathbb{C} \cup \{\infty\}} \mathrm{ord}_\alpha(f) = 0$ corresponde em $\mathbb{Z}$ à **Fórmula do Produto** (Proposição 9.18), que nos diz que para todo $x \in \mathbb{Q}^\times$ temos $\prod_p |x|_p = 1$, onde p varia entre os primos de $\mathbb{N}$ e ∞. De fato, temos uma generalização dessa fórmula para **corpos globais**.

12.2. Corpos Globais e Locais

Os dois principais conceitos em Teoria dos Corpos de Classes são os de **corpos globais** e de **corpos locais**:

Definição (Corpo Global/ Corpo Local)**.** Um corpo K é chamado de **corpo global** se ele for uma extensão finita de $\mathbb{Q}$ (isto é, um corpo de números algébricos) ou de $\mathbb{F}_q(t)$, para q potência de primo (nesse caso, chamamos K de **corpo de funções global**).

Um corpo com valoração (L, v) é chamado de **corpo local** se ele for localmente compacto em relação à topologia induzida por $|\cdot|_v := e^{-v}$.

A definição de corpo global é resultado da analogia entre domínios de Dedekind e corpos de funções vista acima. De fato, embora o interesse da Teoria Algébrica dos Números a princípio seja apenas nos corpos de números algébricos, muitos resultados envolvendo os corpos de funções globais se traduzem em resultados sobre corpos de números algébricos (e vice-versa). De fato, em geral é mais fácil estudar corpos de funções, de modo que é comum a estratégia de primeiro estudar um problema sobre corpos de funções e então buscar desenvolver técnicas análogas sobre corpos de números. Essa estratégia é abordada em [16].

É claro que $\mathbb{R}$ e $\mathbb{C}$ são corpos locais. Pode-se mostrar que todo corpo local é completo. Como os únicos corpos arquimedianos completos são $\mathbb{R}$ e $\mathbb{C}$, falta determinarmos os corpos locais não-arquimedianos. Temos a seguinte caracterização:

Proposição 12.1. *Seja (L, v) um corpo com valoração discreta. Então esse corpo será local se e só se ele for completo e se seu corpo de resíduos associado for finito.*

Nesse caso, denotamos a cardinalidade de seu corpo de resíduos por q, e sendo A seu domínio de valoração discreta e $\mathfrak{p} \lhd A$ seu único ideal maximal, denotamos sua valoração por $v_\mathfrak{p}$. O valor absoluto associado a $v_\mathfrak{p}$ que consideramos nessa situação é $|\cdot|_\mathfrak{p}$ dado por $|x|_\mathfrak{p} := q^{-v_p(x)}$ (ou seja, nesse caso temos uma escolha canônica para a base de exponenciação). Temos ainda como caracterizar mais precisamente os corpos locais:

Teorema 12.2. *Seja (L, v) um corpo local. Se v for arquimediana, então temos $L \cong \mathbb{R}$ ou $L \cong \mathbb{C}$. Se v for não-arquimediana, então L é isomorfo a uma extensão finita de $\mathbb{Q}_p$ ou de $\mathbb{F}_q((t))$, onde $p \in \mathbb{N}$ é primo e $q \in \mathbb{N}$ é potência de primo.*

Seja agora K um corpo de números algébricos. Então, pelo Teorema 10.22, toda valoração não-arquimediana de K é a menos de equivalência uma valoração $\mathfrak{p}$-ádica para um ideal primo não-nulo $\mathfrak{p} \lhd \mathcal{O}_K$. Assim, todo completamento de K é da forma $K_\mathfrak{p}$. Note que $K_\mathfrak{p}$ é completo com relação a uma valoração discreta (a extensão de $v_\mathfrak{p}$) e seu corpo de resíduos associado é isomorfo a $(\mathcal{O}_K)_\mathfrak{p} / \mathfrak{p}_\mathfrak{p} \cong \mathcal{O}_K / \mathfrak{p}$, pela Proposição 9.13 e pelo Teorema 3.25. Mas $|\mathcal{O}_K / \mathfrak{p}| = \mathfrak{N}(\mathfrak{p}) < \infty$. Assim, $K_\mathfrak{p}$ é corpo local. Suponhamos agora que v seja uma valoração arquimediana de K. Nesse caso, sabemos pelo Teorema de Ostrowski que seu completamento é isomorfo a $\mathbb{R}$ ou $\mathbb{C}$, que são locais. Isso prova que todo completamento de um corpo de números algébricos é um corpo local. De forma similar, pode-se determinar quais são as valorações dos corpos da forma $\mathbb{F}_q(t)$, e utilizando o Teorema da Extensão pode-se mostrar que todo completamento de um corpo de funções global é um corpo local. Concluímos:

Proposição 12.3. *Seja K um corpo global e v uma valoração de K. Então o completamento K_v de K com relação a v é um corpo local.*

Isso dá sentido às nossas definições de corpo local e corpo global: para estudarmos os corpos globais por meio do Princípio Local-Global, nós devemos estudar seus completamentos, que são corpos locais. Na verdade, vale também a volta: todo corpo local é o completamento de algum corpo global com relação a um certo valor absoluto.

12.3. Lugares

Completando $\mathbb{Q}$, nós obtemos os corpos $\mathbb{Q}_2, \mathbb{Q}_3, \ldots, \mathbb{Q}_\infty$. Note que esses completamentos estão em bijeção com as classes de equivalência de valores absolutos em $\mathbb{Q}$. Do mesmo modo, dado um corpo global K, seus completamentos estão em bijeção com as classes de equivalência de valores absolutos em K.

Definição (Lugar)**.** Um **lugar** (também chamado de **primo**) de um corpo global K é uma classe de equivalência de valores absolutos de K. Se essa classe for composta de valores absolutos não-arquimedianos, ela é chamada de **lugar (ou primo) finito**, e se for composta de valores absolutos arquimedianos ela é chamada de **lugar (ou primo) infinito**.

Seja K um corpo de números algébricos. Então cada lugar finito de K é a classe de equivalência de algum $|\cdot|_\mathfrak{p}$ para $\mathfrak{p} \lhd \mathcal{O}_K$ primo não-nulo, pelo Teorema 10.22. A classe de $|\cdot|_\mathfrak{p}$ pode ser denotada por $\mathfrak{p}$, o que justifica a nomenclatura **primo**. Os lugares infinitos, por sua vez, correspondem às imersões $\tau\colon K \to \mathbb{C}$, devido ao Teorema da Extensão. Dizemos que um lugar infinito é um **lugar (ou primo) real** se $\tau(K) \subseteq \mathbb{R}$ e é um **lugar (ou primo) complexo** se $\tau(K) \not\subseteq \mathbb{R}$.

Sendo $\mathfrak{p}$ um lugar infinito associado à imersão $\tau\colon K \to \mathbb{C}$, nós definimos o valor absoluto $|\cdot|_\mathfrak{p}\colon K \to \mathbb{R}$ por $|x|_\mathfrak{p} = |\tau x|_\infty$, onde $|\cdot|_\infty\colon \mathbb{C} \to \mathbb{R}$ é o valor absoluto usual.

Por meio de lugares, nós conseguimos generalizar a Fórmula do Produto para um corpo de números algébricos K qualquer. De fato, é possível mostrar que para todo $x \in K^\times$ nós temos $\prod_\mathfrak{p} |x|_\mathfrak{p} = 1$, para $\mathfrak{p}$ variando entre os lugares de K (onde na verdade esse produto é finito, pois pode-se mostrar que $|x|_\mathfrak{p} \neq 1$ para apenas um número finito de lugares $\mathfrak{p}$).

12.4. Adèles e Idèles

A um corpo global K estão associados vários corpos locais: para cada lugar v de K temos o completamento K_v. É desejável que consigamos trabalhar com todos esses completamentos simultaneamente, por exemplo para conseguirmos aplicar o Princípio Local-Global. Uma forma natural de fazer isso seria considerar o anel $\prod_v K_v$, onde v varia entre todos os lugares de K. Um problema que surge é que esse produto não é localmente compacto, embora cada K_v o seja. Para corrigir isso, nós consideramos o **anel de adèles** $\mathbb{A}_K$ de K como sendo:

$$\mathbb{A}_K \;:=\; \left\{(a_v) \in \prod_v K_v \colon a_v \in \mathcal{O}_v \text{ para quase todo lugar finito } v\right\},$$

onde $\mathcal{O}_v$ é o DVD associado a K_v (note que esse anel só está bem-definido se v for um lugar finito) e "para quase todo" significa "para todo, exceto por um número finito". Os elementos de $\mathbb{A}_K$ são chamados de **adèles**. Note que temos uma imersão canônica de anéis $K \hookrightarrow \mathbb{A}_K$ dada por $x \mapsto (x)$. Assim, conseguimos ver K como subanel de $\mathbb{A}_K$. Os elementos de K são chamados de **adèles principais**. É possível colocar uma topologia em $\mathbb{A}_K$ de modo que esse conjunto se torne um anel topológico localmente compacto. Além disso, K é um subconjunto discreto de $\mathbb{A}_K$ e $\mathbb{A}_K / K$ é um grupo topológico compacto.

Podemos ainda definir o **grupo de idèles** I_K de K como sendo:

$$I_K := \left\{ (a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ para quase todo lugar finito } v \right\}.$$

É fácil ver que o grupo de idèles é igual ao grupo das unidades $\mathbb{A}_K^\times$ do anel de adèles. Seus elementos são chamados de **idèles**. Além disso, temos uma imersão canônica de grupos $K^\times \hookrightarrow I_K$ dada por $x \mapsto (x)$. Assim, conseguimos ver $K^\times$ como subgrupo de I_K. Os elementos de $K^\times$ são chamados de **idèles principais**. Podemos definir uma topologia em I_K que torna esse conjunto um grupo topológico localmente compacto. Essa topologia **não** é a topologia induzida por $\mathbb{A}_K$.

Definimos ainda o **grupo de classes de idèles** como sendo o quociente $C_K := I_K / K^\times$. Esse grupo topológico não é compacto. Para corrigir isso, definimos uma norma em $\mathbb{A}_K$. Então, chamando de $\mathbb{A}_K^1$ o subgrupo de I_K de elementos de norma 1, temos $K^\times$ discreto em $\mathbb{A}_K^1$ e $C_K^1 := \mathbb{A}_K^1 / K^\times$ compacto.

A compacidade de C_K^1 nos permite reobter o Teorema da Finitude do Número de Classes. De fato, pode-se mostrar que existe um homomorfismo sobrejetor contínuo $C_K^1 \to \mathscr{C}\ell(\mathcal{O}_K)$, onde $\mathscr{C}\ell(\mathcal{O}_K)$ é visto com a topologia discreta. Como a imagem de um conjunto compacto por uma função contínua é compacta, o grupo $\mathscr{C}\ell(\mathcal{O}_K)$ é compacto e discreto, e portanto finito.

Utilizando a teoria de adèles e idèles, também consegue-se uma outra demonstração do Teorema das Unidades de Dirichlet. Assim, a linguagem de adèles e idèles é útil tanto para a obtenção de novos resultados quanto para um entendimento mais profundo de resultados já provados.

12.5. Leis de Decomposição e Reciprocidade

No Capítulo 5, nós estudamos a decomposição de ideais primos em corpos quadráticos e ciclotômicos. Como nós vimos, a decomposição de um primo $p \in \mathbb{N}$ em um corpo K dessa forma obedece a uma **lei de decomposição**: ela depende apenas da classe de congruência de p módulo um certo inteiro positivo N, que por sua vez depende somente de K. Assim, é natural tentarmos encontrar uma generalização dessa lei para um corpo de números algébricos qualquer.

Infelizmente, essa generalização não existe[1], mas vale para extensões abelianas. De fato, vale o seguinte: se K for um corpo de números algébricos, então existirá um inteiro positivo N de modo que o tipo de decomposição de um primo $p \in \mathbb{N}$ em K dependa somente de $p \pmod N$ se e só se $K / \mathbb{Q}$ for uma extensão abeliana.

Na verdade vale algo ainda mais forte: uma extensão finita abeliana de $\mathbb{Q}$ está completamente determinada pela sua lei de decomposição. Por exemplo, suponhamos que $K / \mathbb{Q}$ seja um corpo de números algébricos, e que um primo $p \in \mathbb{N}$ se decomponha completamente em K se e só se $p \equiv 1 \pmod 4$. Então é possível mostrar que $K = \mathbb{Q}(i)$.

A existência de uma lei de decomposição para as extensões abelianas de $\mathbb{Q}$ segue de uma análise do que ocorre para os subcorpos dos corpos ciclotômicos e do Teorema de Kronecker-Weber. Seja N um inteiro positivo, e consideremos o corpo ciclotômico $\mathbb{Q}(\zeta_N)$. A teoria de Galois nos dá uma correspondência entre os subcorpos de $\mathbb{Q}(\zeta_N)$ e os subgrupos de $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. O interessante é que, dado um subcorpo $K \subseteq \mathbb{Q}(\zeta_N)$, a lei de decomposição em K está associada à identificação de $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/K)$ dentro de $(\mathbb{Z}/N\mathbb{Z})^\times$. De fato, temos o seguinte resultado, que generaliza o Teorema 5.17:

Teorema 12.4. *Sejam N um inteiro positivo, K um subcorpo de $\mathbb{Q}(\zeta_N)$ e H o subgrupo de $(\mathbb{Z}/N\mathbb{Z})^\times$ correspondente a K. Então, dado um primo $p \in \mathbb{N}$ que não divide N, temos:*

(a) p não se ramifica em K.

[1] Na verdade, existe mas não é tão forte. A Teoria dos Corpos de Classes não-abeliana vem se desenvolvendo bastante nos últimos anos.

(b) Seja f a ordem de $(p \pmod N)H$ em $(\mathbb{Z}/N\mathbb{Z})^\times/H$, isto é, o menor inteiro positivo tal que $p^f \pmod N \in H$. Então p se decompõe em $\mathcal{O}_K$ como um produto de $[K:\mathbb{Q}]/f$ ideais primos distintos.

Em particular, p será totalmente decomposto em K se e só se $p \pmod N \in H$.

Além disso, também temos uma versão mais forte do Teorema de Kronecker-Weber:

Teorema 12.5 (Teorema de Kronecker-Weber Forte)**.** *Seja K um corpo de números algébricos.*

(a) $K/\mathbb{Q}$ será uma extensão abeliana se e só se existir um inteiro positivo N tal que $K \subseteq \mathbb{Q}(\zeta_N)$.

(b) Seja N um inteiro positivo. Então $K \subseteq \mathbb{Q}(\zeta_N)$ se e só se o fato de um primo $p \in \mathbb{N}$ ser completamente decomposto em K depender somente de $p \pmod N$.

(c) Suponhamos que $K/\mathbb{Q}$ seja uma extensão abeliana, e que N seja o menor inteiro positivo para o qual $K \subseteq \mathbb{Q}(\zeta_N)$. Então um número primo $p \in \mathbb{N}$ será ramificado em K se e só se $p \mid N$.

A Teoria dos Corpos de Classes também possui generalizações para extensões abelianas de corpos de números. Por exemplo, consideremos a extensão abeliana $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}(\zeta_3)$. Verifica-se que o tipo de decomposição de um ideal primo de $\mathbb{Q}(\zeta_3)$ em $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ depende unicamente de seu "resto" módulo $6\mathcal{O}_{\mathbb{Q}(\zeta_3)}$. Algo curioso envolvendo essa extensão é a torre de corpos $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}(\zeta_3)/\mathbb{Q}$. Ambas as extensões $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ e $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}(\zeta_3)$ são abelianas. Assim, temos uma lei de decomposição para primos de $\mathbb{Q}$ em $\mathbb{Q}(\zeta_3)$ e para primos de $\mathbb{Q}(\zeta_3)$ em $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Entretanto, não temos uma lei de decomposição para primos de $\mathbb{Q}$ em $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$, já que a extensão $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ não é abeliana.

A Teoria dos Corpos de Classes também se interessa pela seguinte questão: dado um polinômio $f(x) \in \mathbb{Z}[x]$, determinar quais são os primos $p \in \mathbb{N}$ para os quais existe $n \in \mathbb{Z}$ tal que $p \mid f(n)$. Por simplicidade, diremos que se isso ocorrer então $p \mid f$. Consideremos por exemplo o polinômio $f(x) = x^2 + 1$. Então sabemos que $p \mid f$ se e só se $p = 2$ ou $\left(\frac{-1}{p}\right) = 1$, o que como já vimos ocorre se e só se $p \equiv 1 \pmod 4$. O objetivo é tentar generalizar isso para uma lei na forma: "dado um polinômio $f(x) \in \mathbb{Z}[x]$, existe um inteiro positivo N de modo que o fato de um primo $p \in \mathbb{N}$ dividir f dependa apenas de $p \pmod N$". Em alguns casos, existe tal N. Por exemplo, para $f(x) = x^4 + x^3 + x^2 + x + 1$ temos $N = 5$, e para $f(x) = x^3 + x^2 - 2x - 1$ temos $N = 7$. Entretanto, para $f(x) = x^3 - 2$ não existe um tal N.

A Teoria dos Corpos de Classes ainda se preocupa com uma terceira pergunta: dado um polinômio $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$, quais são os números primos $p \in \mathbb{N}$ que se escrevem na forma $p = f(n_1, \ldots, n_k)$, para alguns $n_1, \ldots, n_k \in \mathbb{Z}$? Um exemplo disso é determinar quais primos se escrevem na forma $x^2 + y^2$. Como já vimos no estudo de $\mathbb{Z}[i]$, isso ocorre se e só se $p = 2$ ou se $p \equiv 1 \pmod 4$. Dessa vez, buscamos uma lei da forma: "dado $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$, existe um inteiro positivo N de modo que o fato de $p \in \mathbb{N}$ estar na imagem de $f\colon \mathbb{Z}^k \to \mathbb{Z}$ dependa apenas de $p \pmod N$". Novamente, existem generalizações mas não para qualquer f. Por exemplo, para $f(x, y) = x^2 + 5y^2$ temos $N = 20$, e para $f(x, y) = x^2 + 6y^2$ temos $N = 24$, mas para $f(x, y) = x^2 + 26y^2$ não existe um tal N.

Lembre que a lei de decomposição para corpos quadráticos foi obtida por meio da Lei de Reciprocidade Quadrática. Da mesma forma que temos a Lei de Reciprocidade Quadrática, podem ser demonstradas outras leis de reciprocidade, como a **Lei de Reciprocidade Cúbica** e a **Lei de Reciprocidade Quártica**, que podem ser utilizadas para resolver casos particulares das perguntas acima. Todas essas leis aparecem como casos particulares da **Lei de Reciprocidade de Artin**, um dos principais resultados da Teoria dos Corpos de Classes. Para entendermos essa lei, comecemos definindo os **elementos de Frobenius**.

Sejam A um domínio de Dedekind, $K = Q(A)$, L uma extensão finita galoisiana de K com grupo de Galois G e $B = \overline{A}^L$. Suponhamos que, para todo primo não-nulo $\mathfrak{p} \lhd A$, tenhamos $|A/\mathfrak{p}| < \infty$. Note que isso sempre ocorre se K for um corpo global. Para todo $\mathfrak{p} \lhd A$ primo não-nulo, denotaremos $\mathbb{F}_\mathfrak{p} \coloneqq A/\mathfrak{p}$, e para todo $\mathfrak{P} \lhd B$ primo não-nulo nós denotaremos $\mathbb{F}_\mathfrak{P} \coloneqq B/\mathfrak{P}$.

Dados $\mathfrak{P} \mid \mathfrak{p}$ primos não-nulos quaisquer, sabemos que $\mathbb{F}_\mathfrak{P}$ é uma extensão finita de $\mathbb{F}_\mathfrak{p}$. Como $A/\mathfrak{p}$ é finito, sabemos da Teoria de Galois que a extensão $(B/\mathfrak{P})/(A/\mathfrak{p})$ é galoisiana, e que $\mathrm{Gal}(\mathbb{F}_\mathfrak{P} / \mathbb{F}_\mathfrak{p})$ é um grupo cíclico de ordem $f_\mathfrak{P}$ gerado pelo **automorfismo de Frobenius** $\overline{x} \mapsto \overline{x}^{|\mathbb{F}_\mathfrak{p}|}$. Lembre que temos a sequência exata:

$$1 \longrightarrow I_\mathfrak{P} \longrightarrow G_\mathfrak{P} \xrightarrow{\pi_\mathfrak{P}} \mathrm{Gal}(\mathbb{F}_\mathfrak{P} / \mathbb{F}_\mathfrak{p}) \longrightarrow 1$$

onde $\pi_\mathfrak{P}$ é dado por $\sigma \mapsto \overline{\sigma}$. Suponhamos agora que $\mathfrak{p}$ não se ramifique em L. Então nós temos $|I_\mathfrak{P}| = e_\mathfrak{P} = 1 \Rightarrow I_\mathfrak{P} = 1$. Assim, vemos que $G_\mathfrak{P} \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P} / \mathbb{F}_\mathfrak{p})$ por meio do isomorfismo $\pi_\mathfrak{P}$. Desse modo, $G_\mathfrak{P}$ é cíclico, gerado pela imagem do automorfismo de Frobenius por $\pi_\mathfrak{P}^{-1}$. Denotamos esse gerador por $\sigma_\mathfrak{P}$, e o chamamos de **elemento de Frobenius** de $\mathfrak{P}$. É fácil ver que esse é o único automorfismo $\sigma \in G$ tal que $\sigma(x) \equiv x^{|\mathbb{F}_\mathfrak{p}|} \pmod{\mathfrak{P}}$ para todo $x \in B$.

Dado um outro primo $\mathfrak{P}' \mid \mathfrak{p}$, sabemos que $\mathfrak{P}' = \tau\mathfrak{P}$ para algum $\tau \in G$. Disso é fácil ver que $\sigma_{\mathfrak{P}'} = \tau\sigma_\mathfrak{P}\tau^{-1}$. Ou seja, todos os elementos de Frobenius de primos sobre $\mathfrak{p}$ são conjugados. Assim, vemos que o conjunto dos elementos de Frobenius de primos sobre $\mathfrak{p}$ é igual à classe de conjugação de $\sigma_\mathfrak{P}$ em G. Esse conjunto é chamado de **classe de Frobenius** de $\mathfrak{p}$, e é denotado $\mathrm{Frob}_\mathfrak{p}$.

Nós diremos que um primo não-nulo $\mathfrak{P} \lhd B$ é **não-ramificado** se $\mathfrak{P} \cap A$ for não-ramificado em L. Nós definimos o **símbolo de Artin** como a função $\{\text{Primos Não-Ramificados de } L\} \to G$ dada por $\mathfrak{P} \mapsto \sigma_\mathfrak{P}$. Nós denotamos ainda $\left(\dfrac{L/K}{\mathfrak{P}}\right) \coloneqq \sigma_\mathfrak{P}$. Suponhamos agora que L/K seja uma extensão abeliana. Nesse caso, todos os elementos de Frobenius de primos sobre um $\mathfrak{p} \lhd K$ coincidem, e $\mathrm{Frob}_\mathfrak{p}$ possui um único elemento. Assim, podemos falar no **elemento de Frobenius de** $\mathfrak{p}$, que pode ser denotado por $\sigma_\mathfrak{p}$, $\mathrm{Frob}_\mathfrak{p}$ ou ainda $\left(\dfrac{L/K}{\mathfrak{p}}\right)$. Nesse contexto, vemos o símbolo de Artin como uma função $\{\text{Primos não-ramificados de } K\} \to G$.

Observemos ainda que, sendo σ o elemento de Frobenius de $\mathfrak{p}$, nós temos $\sigma(x) \equiv x^{|\mathbb{F}_\mathfrak{p}|} \pmod{\mathfrak{P}}$ para todo primo $\mathfrak{P} \mid \mathfrak{p}$ e para todo $x \in B$. Como $\mathfrak{p}$ é não-ramificado, sua fatoração em B é da forma $\mathfrak{p}\,B = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, e pelas congruências acima nós vemos que $\sigma(x) \equiv x^{|\mathbb{F}_\mathfrak{p}|} \pmod{\mathfrak{p}\,B}$, para todo $x \in B$. Denotaremos $\sigma(x) \equiv x^{|\mathbb{F}_\mathfrak{p}|} \pmod{\mathfrak{p}}$.

A ideia é tentar estender o símbolo de Artin para obter um homomorfismo $I(A) \to G$, mas isso não é simples porque $\pi_\mathfrak{P}$ não é um isomorfismo para $\mathfrak{P}$ ramificado. Para contornar o problema nós consideramos, para cada conjunto S de ideais primos não-nulos de A, o subgrupo abeliano livre I_A^S de $I(A)$ gerado pelos primos que não estão em S. Tomemos S como o conjunto (finito) dos primos ramificados em L. Então nós definimos o **mapa de Artin** como sendo o homomorfismo $\left(\dfrac{L/K}{\cdot}\right)\colon I_A^S \to G$ dado por $\displaystyle\prod_{i=1}^m \mathfrak{p}_i^{e_i} \mapsto \prod_{i=1}^m \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}$. Podemos ainda denotar o mapa de Artin como $\psi_{L/K}^S\colon I_A^S \to G$.

Exemplo 12.6. *Suponhamos $K = \mathbb{Q}$ e $L = \mathbb{Q}(\sqrt{d})$, para algum $d \in \mathcal{D}$. Então nós temos $\mathrm{Gal}(L/K) \cong \{\mathrm{id}, \tau\}$, onde $\tau(\sqrt{d}) = -\sqrt{d}$. Seja $p \in \mathbb{N}$ primo que não se ramifica em L. Como já vimos, isso significa que $p \nmid d_L$. Nós temos $|\mathbb{Z}/p\mathbb{Z}| = p$. Assim, o símbolo de Artin de p é o automorfismo σ que satisfaz $\sigma(x) \equiv x^p \pmod{p}$, para todo $x \in \mathcal{O}_L$. Em particular, nós temos $\sigma(\sqrt{d}) \equiv (\sqrt{d})^p \pmod{p}$. Note que $\sigma(\sqrt{d}) = \pm\sqrt{d}$. Suponhamos p ímpar. Assim, para determinar σ, basta determinar $(\sqrt{d})^{p-1} \pmod{p}$. Se $(\sqrt{d})^{p-1} \equiv 1 \pmod{p}$, então $\sigma = \mathrm{id}$, e se $(\sqrt{d})^{p-1} \equiv -1 \pmod{p}$, então $\sigma = \tau$ (note que, como $p > 2$, temos $1 \not\equiv -1 \pmod{p}$). Observemos agora que $(\sqrt{d})^{p-1} = d^{(p-1)/2}$. Assim, basta determinarmos se $d^{(p-1)/2}$ deixa resto 1 ou -1 módulo p. Mas pelo critério de Euler temos $d^{(p-1)/2} \equiv \left(\dfrac{d}{p}\right) \pmod{p}$. Assim, reconhecendo*

$\mathrm{Gal}(L/K)$ *com o grupo* $\{1,-1\}$*, nós concluímos que* $\left(\dfrac{L/K}{p\,\mathbb{Z}}\right)=\left(\dfrac{d}{p}\right)$*. Isso mostra que, em certo sentido, o mapa de Artin generaliza o símbolo de Legendre.*

Suponhamos agora $p=2$*. Nesse caso, como* $2\nmid d_L$*, vemos que* $d\equiv 1 \pmod 4$*. Assim, o símbolo de Artin satisfaz* $\sigma\left(\frac{1+\sqrt{d}}{2}\right)\equiv\left(\frac{1+\sqrt{d}}{2}\right)^2=\frac{1+d+2\sqrt{d}}{4}\pmod 2$*. Note que temos:*

$$\begin{aligned}\sigma=\mathrm{id}\iff \frac{1+\sqrt{d}}{2}\equiv\frac{1+d+2\sqrt{d}}{4}\pmod 2 &\iff 2+2\sqrt{d}\equiv 1+d+2\sqrt{d}\pmod 8\\ &\iff d\equiv 1\pmod 8.\end{aligned}$$

Assim, $\left(\dfrac{L/K}{2\,\mathbb{Z}}\right)=1$*, se* $d\equiv 1\pmod 8$*, e* $\left(\dfrac{L/K}{2\,\mathbb{Z}}\right)=-1$*, se* $d\equiv 5\pmod 8$*.*

Um dos principais resultados de Teoria dos Corpos de Classes é a sobrejetividade do mapa de Artin. Devido a isso, nós obtemos um isomorfismo $\mathrm{Gal}(L/K)\cong I_A^S/\ker\psi_{L/K}^S$. A **Lei de Reciprocidade de Artin** nos diz ainda mais:

Seja L/K uma extensão finita galoisiana de corpos globais, não necessariamente abeliana. Denotemos por C_K e por C_L os corpos de classes de idèles de K e de L, respectivamente. A norma $N_{L/K}$ induz um homomorfismo $N_{L/K}:=C_L\to C_K$. A Lei de Reciprocidade de Artin afirma que existe um isomorfismo canônico de grupos $\theta\colon C_K/N_{L/K}(C_L)\to\mathrm{Gal}(L/K)^{\mathrm{ab}}$, onde $\mathrm{Gal}(L/K)^{\mathrm{ab}}$ denota a **abelianização** do grupo de Galois $\mathrm{Gal}(L/K)$.

Embora não pareça a princípio, em geral temos mais informações sobre o grupo $C_K/N_{L/K}(C_L)$ do que sobre $\mathrm{Gal}(L/K)$. Assim, essa lei nos ajuda a entender melhor $\mathrm{Gal}(L/K)$, especialmente no caso L/K abeliano, quando temos $\mathrm{Gal}(L/K)\cong C_K/N_{L/K}(C_L)$. Mais especificamente, esse isomorfismo nos dá uma correspondência (que inverte a ordem de continência) entre as extensões abelianas finitas de K dentro de um fecho algébrico fixado e os subgrupos abertos de C_K. Por meio dele, conseguimos de fato classificar as extensões abelianas finitas de corpos globais. Ou seja, a Teoria dos Corpos de Classes funciona como uma espécie de Teoria de Galois para extensões abelianas finitas de corpos globais!

Referências Bibliográficas

[1] ENDLER, Otto. *Teoria dos Números Algébricos*. IMPA, Rio de Janeiro, 2014.

[2] NEUKIRCH, Jürgen. *Algebraic Number Theory*. Springer-Verlag, Berlin, 1999.

[3] SUTHERLAND, Andrew. *Number Theory I*. MIT OpenCourseWare, 2019.
https://ocw.mit.edu/courses/mathematics/18-785-number-theory-i-fall-2019/lecture-notes/MIT18_785F19_full_notes.pdf

[4] BORGES, Herivelto; TENGAN, Eduardo. *Álgebra Comutativa em Quatro Movimentos*. IMPA, Rio de Janeiro, 2015.

[5] MARTINEZ, Fábio; MOREIRA, Carlos; SALDANHA, Nicolau; TENGAN, Eduardo. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. IMPA, Rio de Janeiro, 2013.

[6] STEVENHAGEN, Peter. *Number rings*. Mastermath course, Leiden University, 2012.
http://websites.math.leidenuniv.nl/algebra/ant.pdf

[7] ORDULU, Nizameddin H. *A Simple Proof of Kronecker-Weber Theorem*. 2005.
https://wstein.org/129-05/final_papers/Nizameddin_Ordulu.pdf

[8] WASHINGTON, Lawrence C. *Introduction to cyclotomic fields*, 2nd Ed. Springer-Verlag, New York, 1997.

[9] SIM, Jae H. *The p-adic numbers and a proof of the Kronecker-Weber Theorem*. 2018.
http://math.uchicago.edu/~may/REU2018/REUPapers/Sim.pdf

[10] MARCUS, Daniel A. *Number Fields*, Springer-Verlag, New York-Heidelberg, 1977.

[11] KATO, Kazuya; KUROKAWA, Nobushige; SAITO, Takeshi. *Number Theory 2: Introduction to Class Field Theory*. (Vol. 186). American Mathematical Society, 2011.

[12] IRELAND, Kenneth; ROSEN, Michael. *A Classical Introduction to Modern Number Theory*, 2nd Ed. Springer-Verlag, New York, 1990.

[13] SUN, Lawrence. *Cyclotomic Polynomials in Olympiad Number Theory*. 2013.

[14] LANG, Serge. *Algebraic Number Theory*, 2nd Ed. Springer-Verlag, New York, 1994.

[15] WEIL, André. *Basic Number Theory*, 3rd Ed. Springer-Verlag, New York-Berlin, 1974.

[16] ROSEN, Michael. *Number theory in function fields*. Springer-Verlag, New York, 2002.

[17] ATIYAH, Michael F.; MACDONALD, Ian G. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, 1969.

[18] BARNES, E.S.; Swinnerton-Dyer, H.P.F. The inhomogeneous minima of binary quadratic forms (I). Acta Mathematika 87 (1952), 259-323.

Índice Remissivo