Matheus Haddad Ribeiro

O completamento de corpos de números e extensões suavemente ramificadas

Vitória

12 de abril de 2023

Matheus Haddad Ribeiro

O completamento de corpos de números e extensões suavemente ramificadas

Dissertação de mestrado apresentada ao PPGMAT como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Orientador: Prof. Dr. Thiago Filipe da Silva

Vitória

12 de abril de 2023

Ficha catalográfica disponibilizada pelo Sistema Integrado de Bibliotecas - SIBI/UFES e elaborada pelo autor

---

Ribeiro, Matheus Haddad, 1992-
R484c O completamento de corpos de números e extensões suavemente ramificadas / Matheus Haddad Ribeiro. - 2023.
95 f. : il.

Orientador: Thiago Filipe da Silva.
Dissertação (Mestrado em Matemática) - Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Teoria algébrica dos números. I. Silva, Thiago Filipe da. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

O Completamento de Corpos de Números e Extensões Suavemente Ramificadas

Matheus Haddad Ribeiro

Dissertação submetida ao Programa de Pós-Graduação em Matemática da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do grau de Mestre em Matemática.

Aprovada em 12 de abril de 2023 por:

_____
Prof. Dr. Thiago Filipe da Silva
Universidade Federal do Espírito Santo
Orientador

_____
Prof. Dr. Renato Fehlberg Júnior
Universidade Federal do Espírito Santo

_____
Prof. Dr. Gregory Duran Cunha
Universidade Federal de Goiás

Universidade Federal do Espírito Santo
Vitória, Abril de 2023

Este texto é dedicado ao meu saudoso amigo Rafael da Silveira Cossetti, um matemático muito melhor do que eu. E que apesar de não gostar de Álgebra, tenho certeza que me ajudaria muito, como sempre ajudou, e estaria feliz com o resultado.

Agradecimentos

Gostaria de agradecer primeiramente ao meu orientador, Thiago Filipe da Silva, não somente pela orientação no trabalho, mas pela paciência, e principalmente por acreditar em mim, mesmo quando eu não acreditava. Agradeço também aos professores Renato Fehlberg Júnior e Grégory Duran Cunha pela disponibilidade e interesse em fazer parte da banca examinadora.

Não poderia deixar de agradecer aos meus grandes amigos e maiores incentivadores na vida acadêmica, Alancardek Araújo, João Paulo Costalonga e Matheus Brioschi Herkenhoff Vieira.

E por último, mas não menos importante, aos meus colegas do curso Guilherme Schultz Netto, Gustavo Panin Ramos, Lucas Venâncio da Silva Santos, Matheus dos Santos Lima, Nelson Prata Pravato Serrano, Ramon Aleixo da Silva e Willerson Costa Bernardino, com quem dividi horas de estudo nas disciplinas do programa, e aos professores Apoenã Passos Passamani, Fabiano Petronetto do Carmo e Wescley Bonomo, que mesmo com toda a dificuldade do período remoto, fizeram o máximo e conseguiram entregar aulas de muita qualidade que contruibuíram para minha formação acadêmica.

"Deus criou os números inteiros, todo o resto é obra do homem"
(Leopold Kronecker)

Resumo

Neste trabalho, nós estudamos os corpos de números, que são extensões finitas dos números racionais. Na primeira parte do trabalho fizemos uma breve revisão de conceitos básicos da Álgebra Comutativa. Em seguida, estudamos os anéis de inteiros destes corpos e a fatoração única de seus ideais. Por fim, temos os assuntos principais deste texto, os completamentos dos corpos de números com respeito a um valor absoluto e as ramificações suaves em extensões de corpos henselianos.

Palavras-chave: Corpos de números. Anéis de inteiros. Fatoração única de ideais. Completamentos. Corpos henselianos. Ramificação.

Abstract

In this work, we studied the number fields, which are finite extensions of the field of rational numbers. In the first part of the work we did a brief review of basic concepts of Commutative Algebra. Then, we studied the rings of integers in these fields and the unique factorization of its ideals. At last, we have the main subjects of this text, the completions of number fields with respect of an absolute value and the tame ramifications in extensions of henselian fields.

Keywords: Number fields. Rings of integers. Unique factorization of ideals. Completions. Henselian fields. Ramification.

Lista de símbolos

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Anel dos números inteiros
$\mathbb{Z}_+$	Conjunto dos números inteiros não negativos
$\mathbb{Q}$	Corpo do números racionais
$\overline{\mathbb{Q}}$	Fecho algébrico do corpo $\mathbb{Q}$
$\mathbb{R}$	Corpo dos números reais
$\mathbb{C}$	Corpo dos números complexos
$\mathcal{O}_K$	Anel de inteiros do corpo K
$\mathbb{Z}_p$	Anel dos inteiros p-ádicos
$\mathbb{Z}_{(p)}$	Localização de $\mathbb{Z}$ por $p\mathbb{Z}$
$\mathbb{Q}_p$	Corpo dos números p-ádicos
$A^\times$	Grupo de unidades do anel A
$S^{-1}A$	Localização do anel A pelo conjunto multiplicativo $S \subset A$
$A_\mathfrak{p}$	Localização do anel A pelo conjunto multiplicativo $A \setminus \mathfrak{p}$
$\mathrm{Spec}(A)$	Conjunto dos ideais primos do anel A
$\dim_K V$	Dimensão do K-espaço vetorial V
$(X_1, X_2, \ldots)$	Ideal gerado por $X_1, X_2, \ldots$
δ_{ij}	Delta de Kronecker
$\overline{A}$	Fecho integral do anel A

$ht(\mathfrak{p})$	Altura do ideal primo $\mathfrak{p}$
$\dim A$	Dimensão de Krull do anel A
$\mathrm{Specm}(A)$	Conjunto dos ideais maximais do anel A
$\mathrm{Gal}(L/K)$	Grupo de Galois da extensão de corpos L/K
$N(\alpha)$	Norma do elemento α
$Tr(\alpha)$	Traço do elemento α
$d(\alpha)$	Discriminante do elemento α
e	Índice de ramificação
f	Grau de inércia
$D_{\mathfrak{q}}$	Grupo de decomposição de $\mathfrak{q}$
$Z_{\mathfrak{q}}$	Corpo de decomposição de $\mathfrak{q}$
$v(x)$	Valorização do elemento x
$\lvert x\rvert_v$	Valor absoluto do elemento x com respeito à valorização v
$\lvert x\rvert_0$	Valor absoluto trivial
$\lvert x\rvert_\infty$	Valor absoluto usual de $\mathbb{R}$
$\mathbb{F}_p$	Corpo finito com p elementos
$\hat{K}$	Completamento do corpo K
K^h	Henselização do corpo K
K^{nr}	Extensão não ramificada maximal do corpo K
K^{suave}	Extensão suavemente ramificada maximal do corpo K

Sumário

Introdução

A Teoria dos Números é a área da Matemática que estuda os números inteiros. Um dos principais objetos de estudo dessa área são as equações diofantinas, que são equações polinomiais para as quais estamos interessados em encontrar soluções inteiras. Não há grande dificuldade em resolver equações diofantinas lineares, no entanto, ao considerarmos graus maiores, problemas podem surgir. Por exemplo:

Fixado n positivo, a equação

$$x^2 - y^2 = n$$

não nos oferece tantas dificuldades, basta fatorar o lado esquerdo para obter

$$(x + y)(x - y) = n$$

e utilizar o Teorema Fundamental da Aritmética para encontrar todas as formas de escrever n como produto de dois inteiros. Assim, para resolver a equação acima, precisamos resolver um sistema de duas equações diofantinas lineares. Agora, considere a equação

$$x^2 + y^2 = n$$

Neste caso, não conseguimos fatorar o primeiro membro em $\mathbb{Z}$. No entanto, é possível fatorá-lo em $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$ como

$$(x + yi)(x - yi) = n$$

O anel $\mathbb{Z}[i]$ é chamado de anel dos inteiros gaussianos e está para o corpo $\mathbb{Q}(i)$ assim como $\mathbb{Z}$ está para $\mathbb{Q}$.

Muitas vezes, ao tentarmos resolver um problema da Teoria dos Números, convém considerarmos corpos de números, que são extensões finitas dos racionais. Nestes corpos, existem elementos que fazem um papel parecido com o papel dos inteiros,

e por isso são chamados de inteiros algébricos. Veremos nesta dissertação que o conjunto dos inteiros algébricos num corpo de números forma um anel, chamado de *anel de inteiros*. Os corpos de números e seus anéis de inteiros são os principais objetos de estudo da Teoria Algébrica dos Números.

Infelizmente, existem anéis de inteiros para os quais não é possível realizar a fatoração única. Para tentar corrigir esta *falha*, podemos olhar para os ideais destes anéis ao invés de olharmos para seus elementos. Neste contexto surge o conceito de *domínio de Dedekind* e a *fatoração única de ideais*. Além disto, estamos interessados em saber como esses ideais se comportam em extensões, e para isso precisamos estudar a teoria de ramificação.

Por fim, assim como o corpo dos números reais pode ser visto como um completamento dos racionais num ponto de vista topológico, temos os completamentos de corpos de números, onde estudaremos as chamadas topologias p-ádicas.

Para uma boa compreensão desta dissertação, é recomendado que o leitor tenha um conhecimento em Álgebra Linear a nível de graduação e um conhecimento básico de Teoria de Galois e Teoria de Módulos. Além disto, no último capítulo serão utilizados alguns resultados básicos de Análise e Topologia.

1 Noções básicas de Álgebra Comutativa

O conteúdo aqui estudado pode ser encontrado nas referências (ATIYAH; MACDONALD, 1969) e (TENGAN; FILHO, 2015).

Vamos aqui admitir algumas condições:

1. Todo anel será comutativo com unidade 1;
2. Todos os subanéis contém a unidade 1;
3. Dado um homomorfismo de anéis $f : A \to B$, além das propriedades usuais de homomorfismo, vamos supor que $f(1_A) = 1_B$.
4. Em todo domínio, vamos supor $1 \neq 0$.

1.1 Localização

O corpo de frações Frac A de um domínio A é construído invertendo-se formalmente os elementos não nulos de A. Da mesma forma, dado um anel A e um subconjunto multiplicativo $S \subset A$, a localização $S^{-1}A$ é o anel obtido invertendo-se formalmente os elementos de S.

Definição 1.1.1. Seja A um anel. Um conjunto multiplicativo $S \subset A$ é um subconjunto de A que é fechado para o produto e tal que $1 \in S$.

Dado um anel A e um subconjunto multiplicativo $S \subset A$, a localização de A com respeito a S é o anel $S^{-1}A$ obtido invertendo-se os elementos de S. Formalmente, construímos $S^{-1}A$ quocientando $A \times S$ pela seguinte relação de equivalência

$$(a, s) \sim (b, t) \iff u(at - bs) = 0 \text{ para algum } u \in S$$

Denotaremos a classe de equivalência (a, s) por $\frac{a}{s}$. Assim, a soma e produto em $S^{-1}A$ são definidas da maneira usual

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st} \text{ e } \frac{a}{s}\frac{b}{t}=\frac{ab}{st}$$

Uma simples verificação mostra que as operações estão bem definidas, isto é, não dependem dos representantes de classe.

Com as operações acima, $S^{-1}A$ é um anel com zero igual a $\frac{0}{1}$ e unidade igual a $\frac{1}{1}$. Além disto, este anel possui um homomorfismo canônico

$$\begin{aligned} \iota : A &\to S^{-1}A \\ a &\mapsto \frac{a}{1} \end{aligned}$$

chamado de mapa de localização.

Observação 1.1.2. Se A for um domínio e $0 \notin S$ a relação de equivalência se reduz a

$$\frac{a}{s}=\frac{b}{t} \iff at=bs$$

Ou seja, $S^{-1}A$ pode ser visto como um subanel do corpo de frações de A e neste caso, o mapa de localização é um morfismo injetivo de anéis, de modo que o anel A pode ser visto como um subdomínio de $S^{-1}A$, ou seja, uma "inclusão". No entanto, para anéis mais gerais, o mapa de localização nem sempre será injetivo [1].

Podemos também localizar módulos. Dado um A-módulo M, a localização $S^{-1}M$ de M por um subconjunto multiplicativo $S \subset A$ é o $S^{-1}A$-módulo das frações $\frac{m}{s}$ com $m \in M$ e $s \in S$ tais que

$$\frac{m}{s}=\frac{n}{t} \iff u(mt-ns)=0 \text{ para algum } u \in S$$

O módulo $S^{-1}M$ é construído a partir de uma relação de equivalência em $M \times S$ de modo análogo ao que foi feito para se localizar anéis. As operações de soma e multiplicação são dadas por

$$\frac{m}{s}+\frac{n}{t}=\frac{mt+ns}{st} \text{ e } \frac{a}{t}\frac{m}{s}=\frac{am}{st}$$

[1] Exemplo 4.1.5 da referência (TENGAN; FILHO, 2015)

com $a \in A, s, t \in S$ e $m, n \in M$.

Na prática, os dois subconjuntos multiplicativos mais usados são os seguintes:

Exemplo 1.1.3. Seja A um anel e M um A-módulo.

1. Dado $f \in A$, o conjunto $S_f = \{f^n \mid n \in \mathbb{Z}_+\}$ é um subconjunto multiplicativo de A e denotamos por A_f e M_f as localizações de A e M por S_f, respectivamente;

2. Seja $\mathfrak{p}$ um ideal primo de A, o conjunto $S_\mathfrak{p} = A \setminus \mathfrak{p}$ é um subconjunto multiplicativo de A e denotamos por $A_\mathfrak{p}$ e $M_\mathfrak{p}$ as localizações de A e M por $S_\mathfrak{p}$, respectivamente.

Agora vamos provar a propriedade mais importante das localizações e que, de fato, as caracteriza. A chamada propriedade universal nos diz que dar um homomorfismo $\psi : S^{-1}A \to B$ é o mesmo que dar um homomorfismo $\varphi : A \to B$ tal que $\varphi(S) \subset B^\times$.

Teorema 1.1.4. Sejam A um anel, $S \subset A$ um subconjunto multiplicativo e $\iota : A \to S^{-1}A$ o mapa de localização. Se $\varphi : A \to B$ for um homomorfismo de anéis tal que $\varphi(s) \in B^\times$ para todo $s \in S$, então existe um único homomorfismo de anéis $\psi : S^{-1}A \to B$ definido por $\psi\left(\frac{a}{s}\right) = \varphi(s)^{-1}\varphi(a)$ tal que $\psi \circ \iota = \varphi$, isto é, tal que o diagrama abaixo comuta.

$$\begin{array}{ccc} A & \xrightarrow{\iota} & S^{-1}A \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \psi} \\ & & B \end{array}$$

Dem.: Vamos mostrar que ψ está bem definido. Sejam $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$ tais que $\frac{a}{s} = \frac{b}{t}$, então existe $u \in S$ tal que

$$uta = usb \implies \varphi(uta) = \varphi(usb) \iff \varphi(u)\varphi(t)\varphi(a) = \varphi(u)\varphi(s)\varphi(b)$$

Como $\varphi(u), \varphi(t), \varphi(s) \in B^\times$ segue que

$$\varphi(a)\varphi(s)^{-1} = \varphi(b)\varphi(t)^{-1} \iff \psi\left(\frac{a}{s}\right) = \psi\left(\frac{b}{t}\right)$$

Uma verificação direta mostra que φ é único homomorfismo de anéis tal que $\psi \circ \iota = \varphi$, isto é, tal que o diagrama comuta. ■

Como os elementos de S passam a ser invertíveis em $S^{-1}A$, este aumento no número de unidades reduz o número de ideais primos. Agora, vamos ver como a localização se relaciona com os ideais primos. Primeiramente, vamos apresentar o nome do conjunto dos ideais primos de um anel.

Definição 1.1.5. Seja A um anel. Chamamos de **espectro primo de** A o conjunto de todos os ideais primos de A e denotamos por $\mathrm{Spec}(A)$.

Definição 1.1.6. Chamamos o conjunto de todos os ideal maximais de A de **espectro maximal** e denotamos por $\mathrm{Specm}(A)$.

Teorema 1.1.7. Sejam A um anel e $S \subset A$ um subconjunto multiplicativo. Seja $\iota : A \to S^{-1}A$ o mapa de localização.

1. Se $\mathfrak{a}$ é um ideal de A então $S^{-1}\mathfrak{a}$ é um ideal de $S^{-1}A$.
2. Todo ideal $\mathfrak{b}$ de $S^{-1}A$ é da forma $S^{-1}\mathfrak{a}$ para algum ideal de $\mathfrak{a}$;
3. O mapa de espectros

$$\begin{aligned} \mathrm{Spec}(\iota) : \mathrm{Spec}(S^{-1}A) &\to \mathrm{Spec}(A) \\ \mathfrak{q} &\mapsto \iota^{-1}(\mathfrak{q}) \end{aligned}$$

é injetivo e tem como imagem o conjunto

$$D_S = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}$$

Dem.: 1. Uma verificação direta mostra que $S^{-1}\mathfrak{a}$ é um ideal de $S^{-1}A$.
2. Dado um ideal $\mathfrak{b}$ de $S^{-1}A$ sabemos da teoria de ideais que $\mathfrak{a} = \iota^{-1}\mathfrak{b}$ é um ideal de A. Vamos mostrar que $S^{-1}\mathfrak{a} = \mathfrak{b}$. Para a primeira inclusão temos que se $\frac{a}{s} \in S^{-1}\mathfrak{a}$, então $\frac{a}{s} = \left(\frac{1}{s}\right)\iota(a) \in \mathfrak{b}$. Reciprocamente, se $\frac{b}{s} \in \mathfrak{b}$, então $\iota(b) = \left(\frac{s}{1}\right)\left(\frac{b}{s}\right) \in \mathfrak{b}$,

isto é, $b \in \mathfrak{a}$, e portanto, $\dfrac{b}{s} \in S^{-1}\mathfrak{a}$.

3. Primeiramente, vamos mostrar que dados $\mathfrak{p} \in D_S, a \in A$ e $s \in S$ temos que

$$\frac{a}{s} \in S^{-1}\mathfrak{p} \iff a \in \mathfrak{p}$$

A implicação ($\Leftarrow$) é direta. Por outro lado, se $\dfrac{a}{s} \in S^{-1}\mathfrak{p}$, existem $p \in \mathfrak{p}$ e $t \in S$ tais que

$$\frac{a}{s} = \frac{p}{t} \iff u(at - ps) = 0 \text{ para algum } u \in S$$

e disto

$$uta = usp \in \mathfrak{p} \text{ com } ut \in S$$

Como $\mathfrak{p} \in D_S, ut \notin \mathfrak{p}$, e portanto $a \in \mathfrak{p}$, o que prova a implicação ($\Rightarrow$). Agora vamos mostrar que a imagem de $\mathrm{Spec}(\iota)$ está contida em D_S. Suponha por absurdo que $\mathfrak{p} \in \mathrm{Spec}(\iota)(\mathfrak{q})$ e $S \cap \mathfrak{p} \neq \emptyset$. Assim, $\mathfrak{p} = \iota^{-1}\mathfrak{q}$ e existe $s \in S \cap \mathfrak{p}$, então $\iota(s) \in \mathfrak{q}$, absurdo pois $\iota(s) \in (S^{-1}A)^\times$. Por outro lado, se $\mathfrak{p} \in D_S$, vamos mostrar que $S^{-1}\mathfrak{p} \in \mathrm{Spec}(S^{-1}A)$. Note que $S^{-1}\mathfrak{p}$ é um ideal próprio de $S^{-1}A$, pois, caso contrário, teríamos $\dfrac{1}{1} \in S^{-1}\mathfrak{p}$, e disto, $1 \in \mathfrak{p}$, que é um absurdo. Dados $a, b \in A$ e $s, t \in S$ temos que

$$\begin{aligned} \frac{a}{s}\frac{b}{t} \in S^{-1}\mathfrak{p} &\iff \frac{ab}{st} \in S^{-1}\mathfrak{p} \iff ab \in \mathfrak{p} \\ &\iff a \in \mathfrak{p} \text{ ou } b \in \mathfrak{p} \\ &\iff \frac{a}{s} \in S^{-1}\mathfrak{p} \text{ ou } \frac{b}{t} \in S^{-1}\mathfrak{p} \end{aligned}$$

o que mostra que $S^{-1}\mathfrak{p}$ é um ideal primo de $S^{-1}A$. Por fim, uma verificação direta mostra que o mapa $\mathrm{Spec}(\iota) : \mathrm{Spec}(S^{-1}A) \to D_S$ é uma bijeção, com inversa $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$. ■

Um corolário direto do Teorema 1.1.7 é o seguinte:

Corolário 1.1.8. Sejam A um anel e $\mathfrak{p} \in \mathrm{Spec}(A)$, temos uma bijeção

$$\begin{aligned} \{\mathfrak{q} \in \mathrm{Spec}(A) \mid \mathfrak{q} \subset \mathfrak{p}\} &\to \mathrm{Spec}(A_\mathfrak{p}) \\ \mathfrak{q} &\mapsto \mathfrak{p}A_\mathfrak{p} \end{aligned}$$

Agora daremos duas definições com respeito à quantidade de ideais primos de um anel.

Pelo Corolário 1.1.8 localização $A_{\mathfrak{p}}$ de um anel A com respeito a um ideal primo $\mathfrak{p} \in \mathrm{Spec}(A)$ possui um único ideal maximal $\mathfrak{p}A_{\mathfrak{p}}$. Anéis com esta propriedade possuem um papel importante na Álgebra Comutativa e devemos estudá-los.

Definição 1.1.9. Um anel A é dito local se possui um único ideal maximal $\mathfrak{m}$.

O nome anel local é um bom motivo para chamarmos as localizações por este nome. Um critério útil para identificar anéis locais é o seguinte:

Lema 1.1.10. Um anel A é local se, e somente se, $A \setminus A^{\times}$ é um ideal.

Dem.: Se A é local com ideal maximal $\mathfrak{m}$, então $u \in A^{\times}$ se, e somente se, $u \notin \mathfrak{m}$. Assim, $\mathfrak{m} = A \setminus A^{\times}$. Reciprocamente, se $\mathfrak{m} = A \setminus A^{\times}$ é um ideal, todo ideal próprio $\mathfrak{a}$ de A é tal que $\mathfrak{a} \cap A^{\times} = \emptyset$, ou seja, $\mathfrak{a} \subset \mathfrak{m}$, o que mostra que $\mathfrak{m}$ é o único ideal maximal de A. ■

Um dos principais resultados sobre anéis locais é o chamado Lema de Nakayama, que é de fato muito importante, então chamaremos de teorema.

Teorema 1.1.11. Sejam A um anel local, $\mathfrak{a}$ um ideal próprio de A e M um A-módulo finitamente gerado.

1. Se $\mathfrak{a}M = M$, então $M = \{0\}$;
2. Se N é um submódulo de M tal que $M = N + \mathfrak{a}M$, então $M = N$.

Dem.: 1. Usaremos o chamado "truque de determinante". Sejam $m_1, \ldots, m_n$ geradores de M. Por hipótese, existem $a_{ij} \in \mathfrak{a} \subset \mathfrak{m}$ tais que

$$\begin{aligned} m_1 &= a_{11}m_1 + \ldots + a_{1n}m_n \\ m_2 &= a_{21}m_1 + \ldots + a_{2n}m_n \\ &\vdots \\ m_n &= a_{n1}m_1 + \ldots + a_{nn}m_n \end{aligned}$$

Considere a matriz $T = (a_{ij}) \in M_n(A)$. Seja $I \in M_n(A)$ a matriz identidade. Podemos reescrever o sistema linear acima como a equação matricial

$$(I - T)\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Multiplicando pela matriz adjunta de $I - T$, obtemos $\det(I - T)m_i = 0$ para todo $i \in \{1, \ldots, n\}$. Porém

$$a_{ij} \in \mathfrak{m} \implies \det(I - T) \equiv \det I = 1 \mod \mathfrak{m} \implies \det(I - T) \in A^\times$$

e disto $m_i = 0$ para todo $i \in \{1, \ldots, n\}$, o que nos dá $M = 0$.
2. Basta tomar $M = \dfrac{M}{N}$ e aplicar o item 1. ■

Observação 1.1.12. Na demonstração do item 1. do Lema de Nakayama, poderíamos simplesmente ter resolvido o sistema linear isolando uma variável de cada vez. De fato,

$$m_1 = a_{11}m_1 + a_{12}m_2 + \ldots + a_{1n}m_n \iff (1 - a_{11})m_1 = a_{12}m_2 + \ldots + a_{1n}m_n$$

Como $a_{11} \in \mathfrak{m}$, temos que $1 - a_{11} \notin \mathfrak{m} \iff 1 - a_{11} \in A^\times$. Assim, dividindo por $1 - a_{11}$ obtemos $m_1 \in Am_2 + \ldots + Am_n$, ou seja, M pode ser gerado por $n - 1$ geradores. Repetindo o processo, eventualmente teremos $M = 0$.

1.2 Anéis e módulos noetherianos

A maioria dos anéis comutativos encontrados em Teoria dos Números e Geometria Algébrica satisfazem certas condições de finitude que, de certa forma, funcionam como um substituto para o princípio de indução finita. Anéis que satisfazem tais condições são chamados de noetherianos, assim batizados em homenagem à matemática alemã Emmy Noether, que foi a pioneira no estudo de tais condições de finitude, provenientes das chamadas condições de cadeia para ideais e módulos.

Definição 1.2.1. Seja A um anel. Um A-módulo M é noetheriano se todo A-submódulo $N \subset M$ for finitamente gerado.

O teorema a seguir nos dá mais duas condições equivalentes que caracterizam um A-módulo noetheriano.

Teorema 1.2.2. Sejam A um anel e M um A-módulo. São equivalentes:

1. M é noetheriano;
2. Toda cadeia ascendente de A-submódulos de M é estacionária;
3. Todo subconjunto não vazio de A-submódulos de M possui um elemento maximal com relação à inclusão.

Dem.: $(1. \implies 2.)$: Seja $N_1 \subset N_2 \subset \ldots$ uma cadeia de A-submódulos de M e seja $N = \bigcup N_i$, que também é um A-submódulo de M. Por hipótese, N é finitamente gerado, digamos $N = An_1 + \ldots + An_k$. Tome i_0 suficientemente grande para que $n_1, \ldots, n_k \in N_{i_0}$, de modo que $N = N_{i_0}$, e portanto, $N_i = N_{i_0}$ para todo $i \geq i_0$.
$(2. \implies 3.)$: Seja $C \neq \emptyset$ um conjunto de A-submódulos de M e seja $N_1 \in C$. Se N_1 for maximal em C, nada a provar. Caso contrário, existe $N_2 \in C$ tal que $N_1 \subsetneq N_2$. Se N_2 for maximal em C, nada a provar. Caso contrário, repita o processo. Eventualmente, esse processo irá terminar, já que caso contrário teríamos uma cadeia ascendente não estacionária, o que contraria a hipótese. Portanto, C possui um elemento maximal com relação à inclusão.
$(3. \implies 1.)$: Sejam N um A-submódulo de M e C o conjunto dos A-submódulos de M que são finitamente gerados. Como $\{0\} \in C$, temos que $C \neq \emptyset$, logo por hipótese, C possui um elemento maximal N'. Vamos mostrar que $N = N'$. Por um lado, temos que $N' \subset N$. Suponha por absurdo que exista $x \in N \setminus N'$. Assim, $N' + Ax \in C$ e $N' \subsetneq N' + Ax$, contradizendo a maximalidade de N'. Portanto, $N = N'$. ■

Como corolário direto do Teorema 1.2.2 temos a caracterização dos anéis noetherianos.

Corolário 1.2.3. Seja A um anel. São equivalentes:

1. A é noetheriano;
2. Toda cadeia ascendente de ideais de A é estacionária;
3. Todo subconjunto não vazio de ideais de A possui um elemento maximal com relação à inclusão.

Vamos agora dar exemplos de anéis noetherianos para ilustrar o que apresentamos até agora.

Exemplo 1.2.4. Seja K um corpo. Então, um K-espaço vetorial V é noetheriano se, e somente se, $\dim_K V < \infty$. Basta usar o fato de que um K-espaço vetorial é finitamente gerado se, e somente se, tem dimensão finita.

Exemplo 1.2.5. Corpos e DIPs são noetherianos pois todos os seus ideais são finitamente gerados (por um único elemento).

Exemplo 1.2.6. Um exemplo de anel não noetheriano é o anel de polinômios em infinitas indeterminadas $X_1, X_2, \ldots$. Este anel possui uma cadeia ascendente estrita de ideais

$$(X_1) \subsetneq (X_1, X_2) \subsetneq \ldots$$

Como comentado na introdução desta seção, o conceito de anel noetheriano pode ser interpretado como um substituto para o princípio da indução finita ou para o princípio da boa ordem em $\mathbb{N}$. Mas antes vamos enunciar um importante resultado envolvendo ideais primos, conhecido como "Prime avoidance"ou numa tradução livre para o português, "Como evitar primos":

Teorema 1.2.7. Sejam A um anel, $\mathfrak{a} \subset A$ um ideal de A e $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideais primos de A. Então

$$\mathfrak{a} \subset \bigcup_{1 \leq i \leq n} \mathfrak{p}_i \iff \mathfrak{a} \subset \mathfrak{p}_i \text{ para algum } i$$

Dem.: Teorema 3.1.10 da referência (TENGAN; FILHO, 2015). ■

Como exemplo de aplicação de "indução noetheriana", temos o seguinte teorema:

Teorema 1.2.8. Seja A um anel noetheriano.

1. Todo ideal $\mathfrak{a}$ de A contém um produto finito de ideais primos;

2. A possui apenas um número finito de ideais primos minimais.

Dem.: 1. Suponha que o resultado seja falso. Seja P o conjunto dos ideais que não contêm produtos finitos de ideais primos, que é não vazio por hipótese. Seja $\mathfrak{m}$ um elemento maximal em P. Em particular, $\mathfrak{m}$ não é primo, logo, existem $a, b \notin \mathfrak{m}$ tais que $ab \in \mathfrak{m}$. Como $\mathfrak{a} = (a) + \mathfrak{m} \supsetneq \mathfrak{m}$ e $\mathfrak{b} = (b) + \mathfrak{m} \supsetneq \mathfrak{m}$, pela maximalidade de $\mathfrak{m}$, $\mathfrak{a}, \mathfrak{b} \notin P$, logo existem $\mathfrak{p}_i, \mathfrak{q}_i \in \mathrm{Spec}(A)$ tais que

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n \text{ e } \mathfrak{b} = \mathfrak{q}_1 \dots \mathfrak{q}_m$$

Como $ab \in \mathfrak{m}$, temos que

$$\mathfrak{m} \supset \mathfrak{ab} = \mathfrak{p}_1 \dots \mathfrak{p}_n \mathfrak{q}_1 \dots \mathfrak{q}_m$$

absurdo.
2. Pelo item 1., $\{0\} \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$ para certos $\mathfrak{p}_i \in \mathrm{Spec}(A)$. Logo, dado $\mathfrak{q} \in \mathrm{Spec}(A), \mathfrak{q} \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$, e portanto, $\mathfrak{q} \supset \mathfrak{p}_i$ para algum i, pelo Teorema 1.2.7. Assim, os primos minimais de A formam um subconjunto dos $\mathfrak{p}_i$ acima. ■

Os próximos resultados nos darão condições suficientes para que um A-módulo seja noetheriano.

Proposição 1.2.9. Sejam A um anel e

$$0 \to M' \to M \to M'' \to 0$$

uma sequência exata de A-módulos. Então M é noetheriano se, e somente se, M' e M'' forem noetherianos. Em particular, quocientes e submódulos de módulos noetherianos são noetherianos.

Dem.: Suponha sem perda de generalidade que M' é um submódulo de M e que $M'' = \dfrac{M}{M'}$.

($\Longrightarrow$) : Suponha M noetheriano. Todo A-submódulos de M é finitamente gerado, logo todo submódulo de M' é finitamente gerado, e portanto, é noetheriano. Pelo teorema de correspondência, toda cadeia ascendente de A-submódulos de M'' corresponde a uma cadeia ascendente de A-submódulos de M, contendo M', que é estacionária. Portanto, M'' é noetheriano.
($\Longleftarrow$) : Sejam M' e M'' noetherianos. Dada uma cadeia ascendente de A-submódulos de M

$$M_1 \subset M_2 \subset M_3 \subset \dots$$

temos por hipótese que as cadeias de A-submódulos

$$M_1 \cap M' \subset M_2 \cap M' \subset M_3 \cap M' \subset \dots \subset M'$$
$$\frac{M_1 + M'}{M'} \subset \frac{M_2 + M'}{M'} \subset \frac{M_3 + M'}{M} \subset \dots \subset \frac{M}{M'} = M''$$

são estacionárias para algum i suficientemente grande. Assim, basta mostrar que

$$\begin{cases} M_i \cap M' = M_{i+1} \cap M' \\ M_i + M' = M_{i+1} + M' \end{cases} \implies M_i = M_{i+1}$$

Como $M_i \subset M_{i+1}$ basta provar a inclusão contrária. Tome

$$m_{i+1} \in M_{i+1} \subset M_{i+1} + M' = M_i + M'$$

Assim, existem $m_i \in M_i$ e $m' \in M'$ tais que $m_{i+1} = m_i + m'$. Como

$$m' = m_{i+1} - m_i \in M_{i+1} \cap M' = M_i \cap M' \implies m' \in M_i$$

temos que $m_{i+1} = m_i + m' \in M_i$, o que prova que $M_{i+1} \subset M_i$. ■

Corolário 1.2.10. Seja M um A-módulo finitamente gerado. Se A é noetheriano, então M é noetheriano.

Dem.: Primeiramente, observe que um A-módulo livre A^n de posto n é noetheriano: o resultado vale para $n = 1$, pois A é noetheriano por hipótese. Suponha valer para $n - 1$, se $n > 1$ temos a sequência exata

$$0 \longrightarrow A^{n-1} \xrightarrow{\iota} A^n \xrightarrow{\pi} A \longrightarrow 0$$

Por hipótese de indução, A^{n-1} é noetheriano, logo A^n é noetheriano pela Proposição 1.2.9. Agora um A-módulo M finitamente gerado é um quociente de um A-módulo livre de posto finito: se $M = Am_1 + \ldots + Am_n$, temos uma sobrejeção

$$A^n \to M$$
$$(a_1, \ldots, a_n) \mapsto a_1m_1 + \ldots + a_nm_n$$

e novamente pela Proposição 1.2.9, M é noetheriano. ■

Veremos ainda que a classe de anéis noetherianos é fechada por quocientes e localizações.

Teorema 1.2.11. Seja A um anel noetheriano. Então

1. $\dfrac{A}{\mathfrak{a}}$ é noetheriano para todo ideal $\mathfrak{a}$ de A;
2. $S^{-1}A$ é noetheriano para todo subconjunto multiplicativo S de A.

Dem.: 1. Segue diretamente da Proposição 1.2.9 uma vez que um A-submódulo de $\dfrac{A}{\mathfrak{a}}$ nada mais é que um ideal de $\dfrac{A}{\mathfrak{a}}$.
2. Pelo Teorema 1.1.7, um ideal de $S^{-1}A$ é da forma $S^{-1}\mathfrak{a}$ para algum ideal $\mathfrak{a}$ de A. Se $\mathfrak{a}$ for finitamente gerado, digamos $\mathfrak{a} = (a_1, \ldots, a_n)$, então $S^{-1}\mathfrak{a} = \left(\dfrac{a_1}{1} \ldots, \dfrac{a_n}{1}\right)$ também é finitamente gerado, e portanto, A noetheriano implica $S^{-1}A$ noetheriano. ■

2 Dependência integral

O conteúdo aqui estudado pode ser encontrado novamente nas referências (ATIYAH; MACDONALD, 1969) e (TENGAN; FILHO, 2015).

2.1 Extensões integrais de anéis

Nesta seção vamos definir integralidade sobre um anel A. Dizemos que $A \subset B$ é uma extensão de anéis se A é um subanel de B.

Definição 2.1.1. Seja $A \subset B$ uma extensão de anéis. Dizemos que $x \in B$ é integral sobre A se x for raiz de um polinômio mônico com coeficientes em A. Dizemos que B é integral sobre A se todo elemento de B for integral sobre A.

O próximo teorema nos dará condições equivalentes que caracterizam o fato de um elemento ser integral sobre um anel. Mas primeiro, precisamos de um lema que pode ser visto como uma generalização do teorema de Cayley-Hamilton da Álgebra Linear, só que para módulos.

Lema 2.1.2. Seja $A \subset B$ uma extensão de anéis. Se M for um B-módulo finitamente gerado como A-módulo, então dado $b \in B$, existe um polinômio mônico $f(X) \in A[X]$ tal que $f(b)M = \{0\}$.

Dem.: Seja $M = \sum_{i=1}^{n} Am_i$. Como M é um B-módulo, existem elementos $a_{ij} \in A$ com $i, j \in \{1, \ldots, n\}$ tais que

$$bm_i = \sum_{j=1}^{n} a_{ij} m_j$$

Por outro lado, temos que

$$bm_i = \sum_{j=1}^{n} b\delta_{ij} m_j$$

para cada i. Então subtraindo as duas equações temos o sistema

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

Tome $c_{ij} = b\delta_{ij} - a_{ij} \in B$ e considere a matriz $C = (c_{ij}) \in M_n(B)$. Então, o sistema acima pode ser reescrito como

$$C\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

E aqui vamos usar o "truque do determinante", isto é, multiplicar a equação à esquerda pela adjunta de C. Assim,

$$\det C\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Como os m_i geram M, isto prova que $(\det C)M = 0$ e por um argumento análogo ao que fizemos no Teorema 1.1.11, segue o resultado. ■

Teorema 2.1.3. Seja $A \subset B$ uma extensão de anéis. Dado $b \in B$, as seguintes afirmações são equivalentes:

1. b é integral sobre A;
2. $A[b]$ é um A-módulo finitamente gerado;
3. Existe um A-submódulo C de B contendo $A[b]$ tal que C é finitamente gerado;
4. Existe um $A[b]$-módulo fiel M que é um A-módulo finitamente gerado.

Dem.: (1. $\implies$ 2.) : Como b é integral sobre A, existem $a_0, \ldots, a_{n-1} \in A$ tais que

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

Logo,

$$b^n \in M := \sum_{i=0}^{n-1} Ab^i$$

que é um A-módulo finitamente gerado. Por indução, segue que para todo $m \geq n, b^m \in M$, e portanto, $A[b] = M$. Logo, $A[b]$ é um A-módulo finitamente gerado.
(2. $\implies$ 3.) : Tome $C = A[b]$. Então, C é um A-módulo finitamente gerado por hipótese
(3. $\implies$ 4.) : Tome $M = C$. Como C contém $A[b]$, e $1 \in A[b]$ então $1 \in C$, e portanto, C é um A-módulo fiel.
(4. $\implies$ 1.) : Pelo Lema 2.1.2, $f(b)M = \{0\}$ para algum polinômio mônico $f(X) \in A[X]$, como M é fiel, $f(b) = 0$. Portanto, b é integral sobre A. ■

Corolário 2.1.4. Seja $A \subset B$ uma extensão de anéis e sejam $b_1, \ldots, b_n$ integrais sobre A. Então, $A[b_1, \ldots, b_n]$ é um A-módulo finitamente gerado.

Dem.: Vamos provar por indução sobre n. O caso $n = 1$ segue do Teorema 2.1.3. Para $n \geq 2$, suponha que $C = A[b_1, \ldots, b_{n-1}]$ seja um A-módulo finitamente gerado. Então, existem $c_1, \ldots, c_m \in C$ tais que

$$C = A[b_1, \ldots, b_{n-1}] = \sum_{i=1}^{m} Ac_i$$

Por hipótese, b_n é integral sobre A, logo, é integral sobre C. Então,

$$C[b_n] = \sum_{j=0}^{k-1} Cb_n^j$$

para algum $k \in \mathbb{N}$. Assim,

$$A[b_1, \ldots, b_n] = C[b_n] = \sum_{j=0}^{k-1} \sum_{i=1}^{m} Ac_i b_n^j$$

Em particular, $A[b_1, \ldots, b_n]$ é um A-módulo finitamente gerado. ■

Assim como para extensões de corpos existe o fecho algébrico, no caso de anéis temos o fecho integral.

Definição 2.1.5. Seja $A \subset B$ uma extensão de anéis. O fecho integral de A em B é o conjunto de todos os $b \in B$ que são integrais sobre A. Se A for igual ao seu fecho integral em B, dizemos que A é integralmente fechado em B.

Na teoria de corpos, tínhamos que o fecho algébrico em si era um corpo, analogamente, para o fecho integral temos o seguinte resultado.

Teorema 2.1.6. Seja $A \subset B$ uma extensão de anéis. Então o fecho integral de A em B é um subanel de B que contém A.

Dem.: Seja $\overline{A_B}$ o fecho integral de A em B. A inclusão, $A \subset \overline{A_B}$ é trivial, pois todo $a \in A$ é raiz do polinômio mônico $X - a \in A[X]$. Sejam $x, y \in \overline{A_B}$. Pelo Corolário 2.1.4, $A[x, y]$ é um A-módulo finitamente gerado, que é um subanel de B. Como $x - y, xy \in A[x, y]$, pelo Teorema 2.1.3 segue que $x - y, xy$ são integrais sobre A. ■

O próximo resultado nos mostrará que a integralidade é uma propriedade transitiva.

Proposição 2.1.7. Sejam $A \subset B$ e $B \subset C$ extensões integrais de anéis. Então, $A \subset C$ também é uma extensão integral de anéis.

Dem.: Seja $x \in C$. Devemos mostrar que x é integral sobre A. Primeiramente, como x é integral sobre B, existem $b_0, \ldots, b_{n-1} \in B$ tais que

$$x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0$$

Como $A \subset B$ é uma extensão integral, x é integral sobre $B' := A[b_0, \ldots, b_{n-1}]$. Pelo Corolário 2.1.4, B' é um A-módulo finitamente gerado, pois todos os b_i são integrais sobre A. Então existem elementos $y_1, \ldots, y_k \in B'$ que geram B' como A-módulo. Além disto, $B'[x]$ é um B'-módulo finitamente gerado pelos $x^j, j \in \{0, \ldots, m-1\}$. Temos que

$$A[x] \subset B'[x] = \sum_{j=0}^{m-1} B'x^j = \sum_{j=0}^{m-1} \sum_{i=1}^{k} Ay_i x^j$$

Logo, pelo Teorema 2.1.3, x é integral sobre A, e portanto, $A \subset C$ é uma extensão integral de anéis. ■

Corolário 2.1.8. Seja $A \subset B$ uma extensão de anéis. Então, o fecho integral $\overline{A_B}$ de A em B é integralmente fechado em B.

Dem.: Tome $b \in B$ integral sobre $\overline{A_B}$. Então, a extensão de anéis $\overline{A_B} \subset \overline{A_B}[x]$ é integral pelo Corolário 2.1.4 e a extensão $A \subset \overline{A_B}$ é integral pela definição de $\overline{A_B}$. Pela Proposição 2.1.7, segue que $A \subset \overline{A_B}[x]$ é integral. Em particular, x é integral sobre A. Portanto, $x \in \overline{A_B}$. ■

Vamos agora mostrar que um DFU é integralmente fechado. Em particular, um DIP é integralmente fechado.

Definição 2.1.9. Dizemos que um domínio A é integralmente fechado se for integralmente fechado no seu corpo de frações.

Proposição 2.1.10. Todo *DFU* é integralmente fechado.

Dem.: Sejam A um DFU e K seu corpo de frações. Tome $x \in K$ e escreva $x = \frac{a}{b}$ com $a, b \in A, b \neq 0$. Como A é um DFU, podemos supor que a e b são coprimos, isto é, não existe nenhum primo $p \in A$ que divida ambos a e b. Suponha que x seja integral sobre A. Então, existem elementos $a_0, \ldots, a_{n-1} \in A$ tais que

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \ldots + a_0 = 0$$

Multiplicando a equação por b^n ficamos com

$$a^n + a_{n-1}a^{n-1}b + \ldots + a_0 b^n = 0$$

Assim, $b \mid a^n \in A$, mas como a e b são coprimos, a^n e b são coprimos. Logo, $b \in A^\times$. Logo, $b^{-1} \in A$, e disto, $x = \frac{a}{b} = ab^{-1} \in A$, mostrando que A é integralmente fechado. ■

Exemplo 2.1.11. Os anéis $\mathbb{Z}$ e $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ são domínios euclidianos, em particular são DFUs, e portanto, são integralmente fechados.

Agora, consideraremos $A \subset B$ uma extensão de domínios e K o corpo de frações de A.

Teorema 2.1.12. Seja $A \subset B$ uma extensão integral de domínios. Então, A é um corpo se, e somente se, B é um corpo.

Dem.: ($\Longrightarrow$) : Seja A um corpo e tome $b \in B \setminus \{0\}$. Então b é integral sobre A e existem $a_0, \ldots, a_{n-1} \in A$ tais que

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

que pode ser reescrita como

$$b(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1) = -a_0$$

Escolha tal expressão com n minimal. Por hipótese, $b \neq 0$ e como n é minimal,

$$b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1 \neq 0$$

Como B é um domínio, segue que $a_0 \neq 0$, e como A é um corpo, existe $a_0^{-1} \in A$. Logo

$$b^{-1} = -a_0^{-1}(b^{n-1} + \ldots + a_1)$$

Logo $b \in B^\times$.
($\Longleftarrow$) : Seja B um corpo e tome $a \in A \setminus \{0\}$. Então, existe $a^{-1} \in B$. Como $A \subset B$ é integral, existem $a_i \in A$ tais que

$$a^{-n} + a_{n-1}a^{-(n-1)} + \ldots + a_0 = 0$$

Isolando a^{-n} no primeiro membro da equação e dividindo ambos os membros por a^{n-1} ficamos com

$$a^{-1} = -(a_{n-1} + \ldots + a_0 a^{n-1}) \in A$$

Logo, $a \in A^\times$. ■

O próximo resultado relaciona os conceitos de elemento algébrico sobre um corpo e elemento integral sobre um anel.

Proposição 2.1.13. Seja A um domínio integralmente fechado em seu corpo de frações K. Sejam L/K uma extensão finita e $\alpha \in L$ algébrico sobre K. Então α é integral sobre A se, e somente se, o polinômio minimal de f sobre K pertence a $A[X]$.

Dem.: ($\Longleftarrow$) : Segue da definição de integralidade.
($\Longrightarrow$) : Seja E um corpo de decomposição de f sobre K. Então

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i) \text{ com } \alpha_i \in E, \alpha_1 = \alpha$$

Como α é integral, existem K-isomorfismos

$$\sigma_i \colon K(\alpha) \to K(\alpha_i)$$
$$\alpha \mapsto \alpha_i$$

usando o fato que $K(\alpha_i) \cong \dfrac{K[X]}{(f(X))}$ para cada raiz α_i. Por hipótese, existe um polinômio mônico $g(X) \in A[X]$ tal que $g(\alpha) = 0$. Aplicando σ_i nesta equação, temos que

$$0 = \sigma_i(g(\alpha)) = g(\sigma_i(\alpha)) = g(\alpha_i)$$

Logo, α_i é integral sobre A para todo $i \in \{1, \ldots, n\}$. Segue que $f(X) = \prod_{i=1}^{n}(X - \alpha_i) \in K[X]$ tem coeficientes que são integrais sobre A. Como A é integralmente fechado, segue que $f \in A[X]$. ■

2.2 Extensões integrais de ideais

Nesta seção, vamos estudar os ideais em extensões integrais e como extensões se relacionam com localização.

Proposição 2.2.1. Seja $A \subset B$ uma extensão integral de anéis com $\mathfrak{a}$ e $\mathfrak{b}$ ideais de A e B respectivamente, tais que $\mathfrak{b} \cap A = \mathfrak{a}$. Então

1. $\dfrac{B}{\mathfrak{b}}$ é integral sobre $\dfrac{A}{\mathfrak{a}}$;
2. Se $\mathfrak{a} \in \text{Spec}(A)$ e $\mathfrak{b} \in \text{Spec}(B)$, então $\mathfrak{a}$ é maximal em A se, e somente se, $\mathfrak{b}$ é maximal em B.

Dem.: 1. Temos uma sequência $A \hookrightarrow B \twoheadrightarrow \dfrac{B}{\mathfrak{b}}$ onde o núcleo de $A \to \dfrac{B}{\mathfrak{b}}$ é $A \cap \mathfrak{b} = \mathfrak{a}$. Logo, temos uma injeção de $\dfrac{A}{\mathfrak{a}}$ em $\dfrac{B}{\mathfrak{b}}$ e podemos ver $\dfrac{A}{\mathfrak{a}} \hookrightarrow \dfrac{B}{\mathfrak{b}}$ como uma extensão de anéis. Tome $\overline{x} = x + \mathfrak{b} \in \dfrac{B}{\mathfrak{b}}$ para algum $x \in B$. Então, existem $a_i \in A$ tais que

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 \equiv 0 \mod \mathfrak{b} \implies \overline{x}^n + \overline{a_{n-1}}\overline{x}^{n-1} + \ldots + \overline{a_0} = \overline{0}$$

Os coeficientes da segunda equação estão em $\dfrac{A}{\mathfrak{a}}$, então temos que $\overline{x}$ é integral sobre $\dfrac{A}{\mathfrak{a}}$.

2. Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais primos, então $\dfrac{A}{\mathfrak{a}}$ e $\dfrac{B}{\mathfrak{b}}$ são domínios. Pelo item 1., podemos ver $\dfrac{A}{\mathfrak{a}} \hookrightarrow \dfrac{B}{\mathfrak{b}}$ como uma extensão integral de anéis, então pelo Lema 2.1.12, $\dfrac{B}{\mathfrak{b}}$ é um corpo se, e somente se, $\dfrac{A}{\mathfrak{a}}$ é um corpo. Portanto, $\mathfrak{b}$ é maximal se, e somente se, $\mathfrak{a}$ é maximal. ■

Proposição 2.2.2. Sejam $A \subset B$ uma extensão de anéis e $S \subset A$ um subconjunto multiplicativo.

1. Se $A \subset B$ for integral, então $S^{-1}A \subset S^{-1}B$ é integral;
2. Se C for o fecho integral de A em B, então $S^{-1}C$ é o fecho integral de $S^{-1}A$ em $S^{-1}B$.

Dem.: Existe um homomorfismo canônico

$$\begin{aligned} S^{-1}A &\to S^{-1}B \\ \frac{a}{b} &\mapsto \frac{a}{b} \end{aligned}$$

que está bem definido e é injetivo. Assim, podemos ver $S^{-1}A$ como um subanel de $S^{-1}B$.

1. Seja $\dfrac{b}{s} \in S^{-1}B$ com $b \in B$ e $s \in S$. Como b é integral sobre A, existem $a_0, \ldots, a_{n-1} \in A$ tais que

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

Aplicando o morfismo de localização $\iota : B \to S^{-1}B$ na equação acima e dividindo por s^n, ficamos com

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

Como agora cada coeficiente pertence a $S^{-1}A$, segue que $\dfrac{b}{s}$ é integral sobre $S^{-1}A$, e portanto, a extensão $S^{-1}A \subset S^{-1}B$ é integral.

2. Temos que $A \subset C \subset B$, então podemos considerar a torre de extensões de anéis $S^{-1}A \subset S^{-1}C \subset S^{-1}B$. Como $A \subset C$ é integral, pelo item anterior, segue que $S^{-1}A \subset S^{-1}C$ é integral. Seja $\dfrac{b}{s} \in S^{-1}B$, integral sobre $S^{-1}A$. Então, existem frações $\dfrac{a_0}{s_0}, \ldots, \dfrac{a_{n-1}}{s_{n-1}} \in S^{-1}A$ tais que

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{b}{s}\right)^{n-1} + \ldots + \frac{a_0}{s_0} = \frac{0}{1}$$

Multiplicando por s^n e pelo denominador comum das frações, podemos escrever

$$\left(t'\frac{b}{1}\right)^n + \frac{a'_{n-1}}{s_{n-1}}\left(\frac{b}{1}\right)^{n-1} + \ldots + \frac{a'_0}{1} = \frac{0}{1}$$

onde $t' \in S$ e $a'_i \in A$. Então, existe algum $t'' \in S$ tal que

$$t''(t'b^n + a'_{n-1}b^{n-1} + \ldots + a'_0) = 0$$

Tomando $t = t't'' \in S$, vemos que

$$tb^n + a''_{n-1}b^{n-1} + \ldots + a''_0 = 0, a''_i \in A$$

Multiplicando por t^{n-1}, ficamos com

$$(tb)^n + a''_{n-1}(tb)^{n-1} + \ldots + a''_0 t^{n-1} = 0$$

Portanto, tb é integral sobre A, isto é, $tb \in C$. Logo,

$$\frac{b}{s} = \frac{tb}{ts} \in S^{-1}C$$

E concluímos que $S^{-1}C$ é o fecho integral de $S^{-1}A$ em $S^{-1}B$. ■

Proposição 2.2.3. Seja $A \subset B$ uma extensão integral de anéis. Se $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}(B)$ são tais que $\mathfrak{q} \subset \mathfrak{q}'$ e $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$, então $\mathfrak{q} = \mathfrak{q}'$.

Dem.: Seja $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Então, $\mathfrak{p} \in \mathrm{Spec}(A)$. Se $S = A \setminus \mathfrak{p}$, então pela Proposição 2.2.2, $A_\mathfrak{p} \subset S^{-1}B$ é uma extensão integral. Pelo Corolário 1.1.8, $\mathfrak{p}A_\mathfrak{p}$ é o único ideal maximal do anel local $A_\mathfrak{p}$. Note que $S \cap \mathfrak{q}' = S \cap A \cap \mathfrak{q}' = S \cap \mathfrak{p} = \emptyset$. Analogamente, $S \cap \mathfrak{q} = \emptyset$. Assim, pelo Teorema 1.1.7, $S^{-1}\mathfrak{q} \subset S^{-1}\mathfrak{q}' \in \mathrm{Spec}(S^{-1}B)$. Além disto, $\frac{1}{1} \notin S^{-1}\mathfrak{q}'$, logo $S^{-1}\mathfrak{q}' \cap S^{-1}A \neq S^{-1}A$. Assim, $S^{-1}\mathfrak{q}' \cap S^{-1}A = \mathfrak{p}A_\mathfrak{p}$. Analogamente, $S^{-1}\mathfrak{q} \cap S^{-1}A = \mathfrak{p}A_\mathfrak{p}$. Como $\mathfrak{p}A_\mathfrak{p}$ é maximal em $S^{-1}A$, pela Proposição 2.2.1, temos que $S^{-1}\mathfrak{q}$ e $S^{-1}\mathfrak{q}'$ são ambos maximais em $S^{-1}B$. Portanto, $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{q}'$ e novamente pelo Teorema 1.1.7, temos que $\mathfrak{q} = \mathfrak{q}'$. ■

Lema 2.2.4. Seja $A \subset B$ uma extensão integral de anéis e $\mathfrak{p} \in \mathrm{Spec}(A)$. Então existe $\mathfrak{q} \in \mathrm{Spec}(B)$ tal que $\mathfrak{q} \cap A = \mathfrak{p}$.

Dem.: Seja $S = A \setminus \mathfrak{p}$ e considere o diagrama comutativo

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle j} \\ A_\mathfrak{p} & \hookrightarrow & S^{-1}B \end{array}$$

Tome um ideal maximal $\mathfrak{m}$ de $S^{-1}B$ e considere $\mathfrak{q} = j^{-1}(\mathfrak{m})$ que é um ideal primo de B pelo Teorema 1.1.7. Vamos provar que $\mathfrak{q} \cap A = \mathfrak{p}$. Como B é integral sobre A, pelo Lema 2.2.2, $S^{-1}B$ é integral sobre $S^{-1}A = A_\mathfrak{p}$. Então, pelo Lema 2.2.1, $\mathfrak{m}$ maximal em $S^{-1}B$ implica $\mathfrak{m} \cap A_\mathfrak{p}$ maximal em $A_\mathfrak{p}$. Mas $A_\mathfrak{p}$ é um anel local, logo $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Como o primeiro diagrama comuta, temos outro diagrama comutativo

$$\begin{array}{ccc} \mathfrak{q} \cap A & \hookrightarrow & \mathfrak{q} \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle j} \\ \mathfrak{p}A_\mathfrak{p} & \hookrightarrow & \mathfrak{m} \end{array}$$

Logo, $\mathfrak{q} \cap A = j^{-1}(\mathfrak{m}) \cap A = i^{-1}(\mathfrak{m} \cap A_\mathfrak{p}) = i^{-1}(\mathfrak{p}A_\mathfrak{p})$. Finalmente, pelo Teorema 1.1.7, temos que $\mathfrak{q} \cap A = \mathfrak{p}$. ■

A Proposição 2.2.3 e o Lema 2.2.4 combinados mostram que numa extensão integral $A \subset B$, qualquer $\mathfrak{p} \in \text{Spec}(A)$ levantado em B está contido num $\mathfrak{q} \in \text{Spec}(B)$. Isto pode ser generalizado no teorema a seguir, conhecido como going up.

Teorema 2.2.5. Sejam $A \subset B$ uma extensão integral de anéis, $\mathfrak{p}_1, \mathfrak{p}_2 \in \text{Spec}(A)$ e $\mathfrak{q}_1 \in \text{Spec}(B)$ onde $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ e $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Então existe $\mathfrak{q}_2 \in \text{Spec}(B)$ tal que $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2$ e $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

Dem.: Considere a extensão de anéis quocientes

$$\overline{A} = \frac{A}{\mathfrak{p}_1} \hookrightarrow \overline{B} = \frac{B}{\mathfrak{q}_1}$$

Pela Proposição 2.2.1, $\overline{B}$ é integral sobre $\overline{A}$. Pelo teorema de correspondência, $\overline{\mathfrak{p}}_2 = \dfrac{\mathfrak{p}_2}{\mathfrak{p}_1} \in \text{Spec}(\overline{A})$. Então pelo Lema 2.2.4, existe um ideal $\overline{\mathfrak{q}}_2 \in \text{Spec}(\overline{B})$ tal que $\overline{\mathfrak{q}_2} \cap \overline{A} = \overline{\mathfrak{p}}_2$. Seja $\mathfrak{q}_2$ a pré imagem $\pi^{-1}(\overline{\mathfrak{q}}_2)$ onde $\pi : B \to \overline{B}$ é a projeção canônica. Como $\overline{\mathfrak{p}}_1 \neq 0$, segue que $\mathfrak{q}_2 \supsetneq \mathfrak{q}_1$. Por fim, temos que $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. ■

Definição 2.2.6. Seja A um anel e $\mathfrak{p} \in \text{Spec}(A)$. A altura de $\mathfrak{p}$ é definida por

$$ht(\mathfrak{p}) = \sup\{l \geq 0 \mid \text{existe uma cadeia de ideais primos } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_{l-1} \subsetneq \mathfrak{p}\}$$

A dimensão de Krull de A é definida por

$$\dim A = \sup\{ht(\mathfrak{p}) \mid \mathfrak{p} \in \text{Spec}(A)\}$$

Observação 2.2.7. Se $\mathfrak{p}$ não for maximal, então $\mathfrak{p} \subset \mathfrak{m}$ para algum ideal maximal $\mathfrak{m}$ de A, então podemos reformular a dimensão de Krull como

$$\begin{aligned}\dim A &= \sup\{ht(\mathfrak{m}) \mid \mathfrak{m} \in \text{Specm}(A)\} \\ &= \sup\{l \geq 0 \mid \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_l \text{ é uma cadeia de ideais primos}\}\end{aligned}$$

Exemplo 2.2.8. Se K for um corpo, então $\dim K = 0$, pois $\{0\}$ é o único ideal maximal de K.

Exemplo 2.2.9. Se A for um domínio, então $\dim A = 0 \iff A$ é um corpo. Mas existem anéis que não são domínios e têm dimensão 0[1].

[1]Teorema 7.3.3 da referência (TENGAN; FILHO, 2015)

Exemplo 2.2.10. Se A for um DIP que não é corpo, então $\dim A = 1$.
A estratégia aqui será mostrar que todo ideal primo não nulo é maximal. De fato, seja $\mathfrak{a} \in \mathrm{Spec}(A), \mathfrak{a} \neq \{0\}$. Como A é um DIP, podemos escrever $\mathfrak{a} = (a), a \in A$. Como $\mathfrak{a} \neq \{0\}, a \neq 0$. Suponha que $\mathfrak{a} \subset \mathfrak{b} \subset A$ para algum ideal $\mathfrak{b}$ de A e escreva $\mathfrak{b} = (b)$ para algum $b \in A$. O elemento $a \in (a) \subset (b)$, então existe $c \in A$ tal que $a = bc$. Como $\mathfrak{a} \in \mathrm{Spec}(A)$ e $a = bc \in \mathfrak{a}$, temos que $b \in \mathfrak{a}$ ou $c \in \mathfrak{a}$. Se $b \in \mathfrak{a}$, segue que $\mathfrak{b} = (b) \subset \mathfrak{a}$, e portanto, $\mathfrak{a} = \mathfrak{b}$. Se $c \in \mathfrak{a} = (a)$, existe $d \in A$ tal que $c = ad$. Assim, $a = bc = bad$ e como A é um domínio e $a \neq 0$, temos que $bd = 1$. Logo, $b \in A^\times$, e portanto, $\mathfrak{b} = A$.

Vamos agora provar alguns resultados a cerca da dimensão de Krull.

Proposição 2.2.11. Seja $\mathfrak{p} \in \mathrm{Spec}(A)$. Então

1. $ht(\mathfrak{p}) = \dim A_{\mathfrak{p}}$;
2. $ht(\mathfrak{p}) + \dim \dfrac{A}{\mathfrak{p}} \leq \dim A$.

Dem.: 1. Pelo Corolário 1.1.8, existe uma correspondência biunívoca entre $\mathrm{Spec}(A_{\mathfrak{p}})$ e $\mathfrak{q} \in \mathrm{Spec}(A)$ tais que $\mathfrak{q} \subset \mathfrak{p}$. Assim, qualquer cadeia

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq p_{n-1} \subsetneq \mathfrak{p}$$

em $\mathrm{Spec}(A)$ corresponde a uma cadeia

$$S^{-1}\mathfrak{p}_0 \subsetneq S^{-1}\mathfrak{p}_1 \subsetneq \ldots \subsetneq S^{-1}p_{n-1} \subsetneq S^{-1}\mathfrak{p}$$

em $\mathrm{Spec}(A_{\mathfrak{p}})$. E isto prova que $\dim A_{\mathfrak{p}} \geq ht(\mathfrak{p})$. Reciprocamente, qualquer cadeia

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_{l-1} \subsetneq S^{-1}\mathfrak{p}$$

em $\mathrm{Spec}(A_{\mathfrak{p}})$ corresponde a uma cadeia

$$i^{-1}(\mathfrak{q}_0) \subsetneq i^{-1}(\mathfrak{q}_1) \subsetneq \ldots \subsetneq i^{-1}(\mathfrak{q}_{l-1}) \subsetneq i^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$$

em $\mathrm{Spec}(A)$. E isto prova que $\dim A_{\mathfrak{p}} \leq ht(\mathfrak{p})$, e portanto, $ht(\mathfrak{p}) = \dim A_{\mathfrak{p}}$.
2. Suponha que $\dim \dfrac{A}{\mathfrak{p}} = l$ e seja

$$\overline{\mathfrak{q}_0} \subsetneq \overline{\mathfrak{q}_1} \subsetneq \ldots \subsetneq \overline{\mathfrak{q}_l}$$

uma cadeia maximal em $\mathrm{Spec}\left(\frac{A}{\mathfrak{p}}\right)$. Pelo teorema de correspondência de ideais, isto é levantado a uma cadeia

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_l$$

em $\mathrm{Spec}(A)$ tal que cada $\mathfrak{q}_i \supset \mathfrak{p}$. Claro que sempre podemos adicionar $\mathfrak{p}$ no início de tal cadeia, então se l é maximal, devemos ter que $\mathfrak{q}_0 = \mathfrak{p}$. Agora, dada uma cadeia

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}$$

em $\mathrm{Spec}(A)$, podemos criar uma nova cadeia

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p} = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_l$$

em $\mathrm{Spec}(A)$. Isto mostra que $\dim A \geq n + l$. Em particular, isto vale para qualquer $n \leq ht(\mathfrak{p})$, então temos que

$$\dim A \geq ht(\mathfrak{p}) + l = ht(\mathfrak{p}) + \dim \frac{A}{\mathfrak{p}}$$

■

Teorema 2.2.12. Se $A \subset B$ é uma extensão integral de anéis, então $\dim A = \dim B$.

Dem.: Seja

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_l$$

uma cadeia em $\mathrm{Spec}(B)$, então

$$\mathfrak{q}_0 \cap A \subsetneq \mathfrak{q}_1 \cap A \subsetneq \ldots \subsetneq \mathfrak{q}_l \cap A$$

é uma cadeia em $\mathrm{Spec}(A)$. O fato das inclusões serem estritas segue da Proposição 2.2.3. Assim, $\dim B \leq \dim A$. Por outro lado, se

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_l$$

for uma cadeia em $\mathrm{Spec}(A)$, pelo going up, temos uma cadeia

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_l$$

em $\mathrm{Spec}(B)$, com $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para cada $i \in \{0, \ldots, l\}$. Logo, $\dim A \leq \dim B$, e portanto, $\dim A = \dim B$. ■

Existe um resultado análogo do going up para cadeias descendentes de ideais primos, mas que necessita de condições adicionais. Para isso precisamos provar dois lemas.

Lema 2.2.13. Dados uma extensão de anéis $A \subset B$ e $\mathfrak{p} \in \mathrm{Spec}(A)$, existe $\mathfrak{q} \in \mathrm{Spec}(B)$ tal que $\mathfrak{q} \cap A = \mathfrak{p}$ se, e somente se, $\mathfrak{p}B \cap A \subset \mathfrak{p}$.

Dem.: ($\Longrightarrow$) : Se $\mathfrak{q} \in \mathrm{Spec}(A)$ é tal que $\mathfrak{q} \cap A = \mathfrak{p}$, então

$$\mathfrak{p}B \cap A = (\mathfrak{q} \cap A)B \cap A \subset \mathfrak{q} \cap A = \mathfrak{p}.$$

($\Longleftarrow$) : Seja $S = A \setminus \mathfrak{p}$. Por hipótese, $\mathfrak{p}B \cap A \subset \mathfrak{p}$ implica que $(\mathfrak{p}B \cap A) \cap S = \emptyset$. Logo, $S^{-1}(\mathfrak{p}B) \neq S^{-1}B$, então existe um ideal maximal $\mathfrak{m}$ em $S^{-1}B$ tal que $S^{-1}(\mathfrak{p}B) \subset \mathfrak{m}$. Pelo Teorema 1.1.7, existe um $\mathfrak{q} \in \mathrm{Spec}(B)$ tal que $\mathfrak{q} \cap S = \emptyset$ e $\mathfrak{m} = S^{-1}\mathfrak{q}$. Então

$$\mathfrak{p} \subset \mathfrak{p}B \cap A \subset \mathfrak{q} \cap A \subset \mathfrak{q} \cap \mathfrak{p} \subset \mathfrak{p}$$

Portanto, $\mathfrak{p} = \mathfrak{q} \cap A$. ■

Lema 2.2.14. Seja $A \subset B$ uma extensão integral de domínios com $K = Frac A$ e A integralmente fechado. Se $\mathfrak{p} \in \mathrm{Spec}(A)$ e $\alpha \in \mathfrak{p}B$, então os coeficientes do polinômio minimal, exceto o líder, f de α sobre K pertencem a $\mathfrak{p}$.

Dem.: Pelo Lema 2.1.13, os coeficientes de f devem pertencer a A. Seja $\alpha = b_1p_1 + \ldots + b_kp_k$ com $b_i \in B$ e $p_i \in \mathfrak{p}$. Substituindo B por $A[b_1, \ldots, b_k]$, podemos supor que B é um A-módulo finitamente gerado por $x_1, \ldots, x_n$. Para cada $i \in \{1, \ldots, n\}$, escreva

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

com $a_{ij} \in \mathfrak{p}$. Então

$$\sum_{j=1}^{n} (\delta_{ij}\alpha x_i - a_{ij}) = 0$$

Pelo truque do determinante temos que

$$\det(\delta_{ij}\alpha x_i - a_{ij})x_j = 0 \text{ para todo } j \in \{1, \ldots, n\}$$

Logo, αx_i é raiz de um polinômio mônico com coeficientes em $\mathfrak{p}$. Como isto vale para todo gerador x_i, segue que o próprio α é raiz deste polinômio, digamos, $g \in \mathfrak{p}[X]$. Seja f o polinômio minimal de α sobre K, então $f \mid g$, isto é, $g = fh$ para algum $h \in A[X]$. Reduzindo módulo $\mathfrak{p}$, temos que

$$X^{\deg g} = \overline{g} = \overline{fh} \in \frac{A}{\mathfrak{p}}[X]$$

Como $\mathfrak{p} \in \operatorname{Spec}(A), \dfrac{A}{\mathfrak{p}}$ é um domínio, então $\overline{f}$ e $\overline{h}$ devem ser potências de X. Portanto, todo coeficiente não líder de f pertence a $\mathfrak{p}$. ■

O próximo teorema é conhecido como going down.

Teorema 2.2.15. Seja $A \subset B$ uma extensão integral de domínios, onde A é integralmente fechado. Sejam $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec}(A)$ e $\mathfrak{q}_1 \in \operatorname{Spec}(B)$ onde $\mathfrak{p}_1 \supsetneq \mathfrak{p}_2$ e $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Então existe $\mathfrak{q}_2 \in \operatorname{Spec}(B)$ tal que $\mathfrak{q}_1 \supsetneq \mathfrak{q}_2$ e $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

Dem.: Como B é um domínio, o mapa $B \to B_{\mathfrak{q}_1}$ é injetivo. Seja $B' = B_{\mathfrak{q}_1} = S^{-1}B$, onde $S = B \setminus \mathfrak{q}_1$. Temos uma torre de extensões de anéis $A \subset B \subset B'$. Temos que mostrar que existe um $\mathfrak{q}' \in \operatorname{Spec}(B')$ não nulo tal que $\mathfrak{q}' \cap A = \mathfrak{p}_2$, e pelo Teorema 1.1.7, teremos que

$$\mathfrak{p}_2 = \mathfrak{q}' \cap A = (\mathfrak{q}' \cap B) \cap A = \mathfrak{q}_2 \cap A$$

Tome $\mathfrak{p} = \mathfrak{p}_2$. Pelo Lema 2.2.13, mostrar a existência de $\mathfrak{q}' \in \operatorname{Spec}(B')$ tal que $\mathfrak{q}' \cap A = \mathfrak{p}$ é equivalente a mostrar que $\mathfrak{p}B' \cap A \subset \mathfrak{p}$. Se $\mathfrak{p}B' \cap A = \{0\}$, nada a

provar. Caso contrário, seja $a \in \mathfrak{p}B'$ não nulo e escreva $a = \alpha s$ para algum $\alpha \in \mathfrak{p}B$ e $s \in S$. Seja f o polinômio minimal de α sobre K. Pelo Lema 2.2.14 temos que

$$f = X^n + c_{n-1}X^{n-1} + \ldots + c_0, c_i \in \mathfrak{p}$$

Como $a \in A$, podemos escrever

$$\frac{1}{a^n}f(aX) = X^n + \frac{c_{n-1}}{a}X^{n-1} + \ldots + \frac{c_0}{a^n} = X^n + c'_{n-1}X^{n-1} + \ldots + c'_0$$

com $c'_i = \dfrac{c_i}{a^{n-i}}$. Então, $\dfrac{1}{a^n}$ também é irredutível, e tomando $X = s$ temos

$$\frac{1}{a^n}f(as) = \frac{1}{a^n}f(\alpha) = 0$$

Segue que $\dfrac{1}{a^n}f(aX)$ é o polinômio minimal de s sobre K. Logo, cada $c'_i \in A$ para $i \in \{1, \ldots, n-1\}$. Suponha que $a \notin \mathfrak{p}$. Então, como $\mathfrak{p}$ é primo, $c'_{n-i}a^i = c_{n-i} \in \mathfrak{p}$ implica que $c'_{n-i} \in \mathfrak{p}$ para cada $i \in \{0, \ldots, n-1\}$. Como $s \in B$, temos que

$$s^n = -c'_{n-1}s^{n-1} - \ldots - c'_0 \in \mathfrak{p}B' \subset \mathfrak{p}_1 B \subset \mathfrak{q}_1$$

Então, $s \in \mathfrak{q}_1$ pois $\mathfrak{q}_1$ é primo, mas isto contradiz o fato de $s \in S = B \setminus \mathfrak{q}_1$. Portanto, $a \in \mathfrak{p}$, e disto, $\mathfrak{p}B' \cap A \subset \mathfrak{p}$. ■

Até o final desta seção, seja A um domínio com corpo de frações K. Se $S \subset A \setminus \{0\}$, podemos considerar o anel $S^{-1}A$ como um subanel de K. Em particular, $A_\mathfrak{p} \subset K$ para todo $\mathfrak{p} \in \mathrm{Spec}(A)$.

Proposição 2.2.16. Todo domínio A pode ser escrito como

$$A = \bigcap_{\mathfrak{m} \in \mathrm{Specm}(A)} A_\mathfrak{m}$$

Dem.: Seja D a interseção dos $A_\mathfrak{m}$ sobre todos os ideais maximais $\mathfrak{m}$ de A. Então, $D \subset K$. Fixado um $x \in D$, considere o ideal $\mathfrak{a} = \{a \in A \mid ax \in A\}$ de A. Se $\mathfrak{m}$ for um ideal maximal de A fixado, por hipótese, $x \in A_\mathfrak{m}$, então existem $a, b \in A$ com $a \notin \mathfrak{m}$ e tais que $x = \dfrac{b}{a}$. Segue que $ax = b \in A$, então $a \in \mathfrak{a}$. Como tomamos

$a \notin \mathfrak{m}$, isto implica que $\mathfrak{a} \not\subset \mathfrak{m}$. Como $\mathfrak{m}$ foi arbitrário, temos que $A = \mathfrak{a}$. Logo, $1 \in \mathfrak{a}$, isto é, $x = x \cdot 1 \in A$, e portanto, $A = D$. ■

Proposição 2.2.17. Dado um domínio A são equivalentes:

1. A é integralmente fechado;
2. $A_{\mathfrak{p}}$ é integralmente fechado para todo $\mathfrak{p} \in \mathrm{Spec}(A)$;
3. $A_{\mathfrak{m}}$ é integralmente fechado para todo $\mathfrak{m} \in \mathrm{Specm}(A)$.

Dem.: (1. $\implies$ 2.) : Seja $\mathfrak{p} \in \mathrm{Spec}(A)$ e considere $S = A \setminus \mathfrak{p}$. Por hipótese, A é o fecho integral de A em K, e pelo Lema 2.2.2, $S^{-1}A = A_{\mathfrak{p}}$ é integralmente fechado em K, que também é o corpo de frações de $S^{-1}A$.
(2. $\implies$ 3.) : Segue do fato de todo ideal maximal ser um ideal primo.
(3. $\implies$ 1.) : Seja $\mathfrak{m} \in \mathrm{Specm}(A)$, temos que $A \subset A_{\mathfrak{m}} \subset K$. Como $A_{\mathfrak{m}}$ é integralmente fechado, segue que o fecho integral de A em K está contido em $A_{\mathfrak{m}}$ para qualquer $m \in \mathrm{Specm}(A)$. Pelo Lema 2.2.16, segue que A é integralmente fechado. ■

3 Corpos de Números

O conteúdo aqui estudado pode ser encontrado nas referências (NEUKIRCH, 2013), (CASSELS; FRÖHLICH, 1986), (JANUSZ, 1996), (MARCUS; SACCO, 1977), (WEIL, 2013), (ENDLER, 1986), (MILNE, 2017) e (SUTHERLAND, 2017).

3.1 Anéis de inteiros

Vamos começar esta seção definindo os dois objetos mais importantes da Teoria Algébrica dos Números.

Definição 3.1.1. Um corpo de números K é uma extensão finita de $\mathbb{Q}$.

Definição 3.1.2. Dado um corpo de números K, seu anel de inteiros $\mathcal{O}_K$ é o fecho integral de $\mathbb{Z}$ em K.

O próximo exemplo mostra como podemos determinar o anel de inteiros de um caso particular de corpo de números.

Exemplo 3.1.3. Seja K um corpo quadrático, isto é, um corpo de números tal que $[K : \mathbb{Q}] = 2$. Então, $K = \mathbb{Q}(\sqrt{d})$ para algum inteiro livre de quadrados $d \in \mathbb{Z} \setminus \{0, 1\}$, isto é, existem primos dois a dois distintos $p_i \in \mathbb{Z}$ tais que

$$d = \pm p_1 p_2 \dots p_r$$

Queremos encontrar o anel de inteiros de K. Como $K/\mathbb{Q}$ é uma extensão galoisiana, existe um $\mathbb{Q}$-automorfismo não trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$

$$\begin{aligned} \sigma : K &\to K \\ a + b\sqrt{d} &\mapsto a - b\sqrt{d} \end{aligned}$$

Usando a norma e o traço para $K/\mathbb{Q}$, temos que

$$\alpha \in \mathcal{O}_K \iff N(\alpha) = \alpha\sigma(\alpha) \text{ e } Tr(\alpha) = \alpha + \sigma(\alpha) \in \mathbb{Z}$$

De fato, suponha que $f(\alpha) = 0$ para algum polinômio mônico $f(X) \in \mathbb{Z}[X]$. Então,

$$0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$$

Logo, $\sigma(\alpha) \in \mathcal{O}_K$. Como $\mathcal{O}_K$ é um anel, $N(\alpha) = \alpha\sigma(\alpha), Tr(\alpha) = \alpha + \sigma(\alpha) \in \mathcal{O}_K$. Mas a norma e o traço tomam valores em $\mathbb{Q}$, logo, $N(\alpha), Tr(\alpha) \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. Reciprocamente, se $\alpha\sigma(\alpha), \alpha + \sigma(\alpha) \in \mathbb{Z}$ então α é uma raiz do polinômio mônico

$$(X - \alpha)(X - \sigma(\alpha)) = X^2 - (\alpha + \sigma(\alpha))X + \alpha\sigma(\alpha) \in \mathbb{Z}[X]$$

Portanto, $\alpha \in \mathcal{O}_K$. Assim, temos que

$$\begin{aligned} \mathcal{O}_K &= \{a + b\sqrt{d} \mid a, b \in \mathbb{Q} \text{ e } a^2 - b^2 d, 2a \in \mathbb{Z}\} \\ &= \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{se } d \equiv 2, 3 \mod 4 \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & \text{se } d \equiv 1 \mod 4 \end{cases} \end{aligned}$$

O segundo caso segue do fato que se $d \equiv 1 \mod 4$, então $\omega = \dfrac{1+\sqrt{d}}{2}$ satisfaz a equação $\omega^2 - \omega + \dfrac{1-d}{4}$.

Observação 3.1.4. Pelo Lema 2.1.13, podemos escrever

$$\mathcal{O}_K = \{\alpha \in K / f_\alpha \in \mathbb{Z}[X]\}$$

onde f_α é o polinômio minimal de α sobre $\mathbb{Q}$.

Como vimos no exemplo, duas aplicações importantes para entender os corpos de números são a norma e traço. Seja L/K uma extensão finita de corpos e fixe $x \in L$.

Definição 3.1.5. A norma de x é o elemento $N_{L/K}(x) = \det T_x \in K$, onde

$$\begin{aligned} T_x \colon L &\to L \\ \alpha &\mapsto \alpha x \end{aligned}$$

é uma aplicação K-linear.

Definição 3.1.6. O traço de x é $Tr_{L/K}(x) = trT_x$, onde tr denota o traço.

Note que a norma e o traço estão definidos para qualquer extensão finita L/K, e não apenas para corpos de números. Quando a extensão de corpos estiver subentendida, escreveremos apenas $N(x)$ e $Tr(x)$ para a norma e o traço do elemento x.

Lema 3.1.7. Dado $x \in L$, o polinômio característico p de T_x é tal que

$$p(X) = (f(X))^{[L:K(x)]}$$

onde f é o polinômio minimal de x sobre K. Logo,

$$Tr_{L/K}(x) = [L : K(x)]Tr_{K(x)/K}(x)$$

Dem.: Sejam $m = [L : K(x)]$ e $n = [K(x) : K]$. Se $m = 1$, então $L = K(x)$ e disto, $\deg f = [L : K] = n$. Pelo teorema de Cayley-Hamilton, $f \mid p$, mas por definição, ambos são mônicos e $\deg p = n$, então temos que $p = f$. No caso geral, sejam $\{v_1, \ldots, v_m\}$ uma base de $K(x)/K$ e $\{u_1, \ldots, u_n\}$ uma base de $L/K(x)$. Sabemos que o conjunto

$$\{v_i u_j \mid i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}\}$$

é uma base para L/K. Seja $B = (b_{kl})$ a matriz canônica para T_x na extensão $K(x)/K$. Então

$$xv_i = \sum_{k=1}^{r} b_{ki} v_k$$

e portanto,

$$x(v_i u_j) = \sum_{k=1}^{r} b_{ki}(v_k u_j)$$

Escrevendo a base $\{v_i u_j\}$ como $\{v_1 u_1, v_2 u_1, \ldots, v_r u_1, v_1 u_2, \ldots, v_r u_m\}$ então a matriz canônica de T_x em L/K tem m blocos, cada um deles igual a B, assim

$$p(X) = [\det(XI - B)]^m$$

e pelo caso $m = 1$,

$$\det(XI - B) = f(X)$$

Portanto, $p(X) = (f(X))^m$. ■

Teorema 3.1.8. Seja L/K uma extensão finita e separável de corpos. Sejam $\sigma_1, \ldots, \sigma_n$ as imersões distintas $L \hookrightarrow \overline{K}$ onde $\overline{K}$ é o fecho algébrico de K. Então, dado $x \in L$,

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x) \text{ e } Tr_{L/K} = \sum_{i=1}^{n} \sigma_i(x)$$

Dem.: Suponha $\sigma_i(x) \neq \sigma_j(x)$ se $i \neq j$. Uma base de L/K é $\{1, x, \ldots, x^{n-1}\}$ e a matriz de T_x nesta base é

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

onde $f(X)$ é o polinômio minimal de x sobre K. Neste caso, temos que f também é o polinômio característico de x. Então, $Tr(x)$ é igual à soma das raízes de f e $N(x)$ é igual ao produto. ■

Exemplo 3.1.9. Seja $K = \mathbb{Q}(\sqrt{d})$ com d um inteiro livre de quadrados. Então um elemento $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ tem

$$N(x) = a^2 - b^2 d \text{ e } Tr(x) = 2a$$

Até o final desta seção, considere L/K uma extensão finita e separável de corpos e sejam $\{\alpha_1, \ldots, \alpha_n\}$ uma K-base de L, tal que $[L : K] = n$. Além disto, sejam $\sigma_1, \ldots, \sigma_n : L \hookrightarrow \overline{K}$ as n K-imersões distintas de L no fecho algébrico de K.

Definição 3.1.10. O discriminante da base $\{\alpha_1, \ldots, \alpha_n\}$ é

$$d_{L/K}(\alpha_1, \ldots, \alpha_n) = [\det(\sigma_i(\alpha_j))]^2$$

Proposição 3.1.11. Seja $A = (Tr_{L/K}(\alpha_i\alpha_j))$. Então, $d_{L/K}(\alpha_1, \ldots, \alpha_n) = \det A$. Em particular, $d_{L/K}(\alpha_1, \ldots, \alpha_n)$ pertence a K.

Dem.: Pelo Teorema 3.1.8,

$$Tr_{L/K}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$$

Logo, $A = BC$ onde

$$B = (\sigma_k(\alpha_i))^T \text{ e } C = (\sigma_k(\alpha_j))$$

Calculando o determinante, segue que

$$\det A = (\det B)(\det C) = (\det C)^2 = d_{L/K}(\alpha_1, \ldots, \alpha_n)$$

■

Um caso interessante é quando $L = K(\alpha)$ é uma extensão simples e $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma K-base para L. Então, definimos o discriminante de α como

$$d_{L/K}(\alpha) = d_{L/K}(1, \alpha, \ldots, \alpha^{n-1})$$

Lema 3.1.12. Dado um elemento $\alpha \in L$ algébrico sobre $K, d_{L/K}(\alpha)$ é igual ao discriminante do polinômio minimal de α.

Dem.: Seja $L = K(\alpha)$ e tome $\alpha_i = \sigma_i(\alpha)$ para cada imersão $\sigma_i : L \hookrightarrow \overline{K}$. Então

$$d_{L/K}(\alpha) = \det \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{pmatrix}$$

Que é um determinante de Vandermonde, isto é

$$d_{L/K}(\alpha) = \prod_{1 \leq i < j \leq n, i \neq j} (\alpha_i - \alpha_j) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

Como $K(\alpha)/K$ é separável, $d_{L/K}(\alpha) \neq 0$. E a fórmula acima é exatamente o discriminante de f, o polinômio minimal de α sobre K. ■

Proposição 3.1.13. Dada uma K-base $\{\alpha_1, \ldots, \alpha_n\}$ de L, $d_{L/K}(\alpha_1, \ldots, \alpha_n) \neq 0$.

Dem.: Como L/K é finita e separável, pelo teorema do elemento primitivo, $L = K(\beta)$ para algum $\beta \in L$. Então pelo Lema 3.1.12, $d_{L/K}(1, \beta, \ldots, \beta^{n-1}) \neq 0$. Seja $A \in GL_n(K)$ a matriz de mudança de base de $\{\alpha_1, \ldots, \alpha_n\}$ para $\{1, \beta, \ldots, \beta^{n-1}\}$. Então para cada $i, j \in \{1, \ldots, n\}$

$$\det(\sigma_i(\alpha_j)) = (\det A)(\det(\sigma_i(\beta^{j-1}))$$

Ambos os determinantes do lado direito são não nulos, logo $\det(\sigma_i(\alpha_j)) \neq 0$, o que implica $d_{L/K}(\alpha_1, \ldots, \alpha_n) \neq 0$ pela definição de discriminante. ■

A prova da Proposição 3.1.13 nos dá uma fórmula bem útil: Sejam B, B' duas K-bases para L com matriz de mudança de base A, então

$$d_{L/K}(B) = (\det A)^2 d_{L/K}(B')$$

Boa hora para um exemplo de como encontrar o discriminante na prática.

Exemplo 3.1.14. Vamos ao nosso exemplo favorito, $K = \mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadrados. Então, $\{1, \sqrt{d}\}$ é uma base de K, e seu discriminante é

$$d_{K/\mathbb{Q}}(1, \sqrt{d}) = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = (-2\sqrt{d})^2 = 4d$$

Que coincide com o discriminante de $X^2 - d$, como esperado.

Seja A um domínio integralmente fechado com corpo de frações K. Seja B o fecho integral de A em L, que é uma extensão finita de K. Se $x \in B$ então cada $\sigma_i(x)$ em $\overline{K}$ também é integral sobre K. Como A é integralmente fechado, $N_{L/K}(x), Tr_{L/K}(x) \in A$.

Lema 3.1.15. Se $x \in B^\times$, então $N(x) \in A^\times$.

Dem.: Segue do fato de $N_{L/K} : L^\times \to K^\times$ ser um homomorfismo de grupos. ■

Lema 3.1.16. Suponha $\alpha_1, \ldots, \alpha_n \in B$ formem uma K-base para L. Seja $d = d_{L/K}(\alpha_1, \ldots, \alpha_n)$. Então

$$dB \subset A\alpha_1 + \ldots + A\alpha_n$$

Dem.: Sejam $a_1, \ldots, a_n \in K$ tais que $\alpha = \sum_{i=1}^{n} a_i\alpha_i \in B$. Então $(a_1, \ldots, a_n)$ é solução do sistema linear

$$Tr_{L/K}(\alpha_i\alpha) = \sum_{j=1}^{n} Tr_{L/K}(\alpha_i\alpha_j)x_j, i \in \{1, \ldots, n\}$$

A matriz do sistema tem determinante d pela Proposição 3.1.11. Logo, cada a_j pode ser escrito como $\frac{1}{d}$ vezes uma combinação A-linear de $Tr(\alpha_i\alpha)$. Como $\alpha_i, \alpha \in B, Tr(\alpha_i\alpha) \in A$ e $d\alpha_j \in A$ para cada j. Assim

$$d\alpha = \sum_{j=1}^{n} da_j\alpha_j \in A\alpha_1 + \ldots + A\alpha_n$$

Como $\alpha \in B$ foi arbitrário, mostramos que $dB \subset A\alpha_1 + \ldots + A\alpha_n$. ■

Proposição 3.1.17. Sejam A um DIP, B o fecho integral de A em L e $M \subset L$ um B-módulo finitamente gerado. Então M é um A-módulo livre de posto $n = [L : K]$. Em particular, B é um A-módulo livre de posto n.

Dem.: Seja $\{\alpha_1, \ldots, \alpha_n\} \subset B$ uma base para L/K. Pelo Teorema B.4.1 da referência (TENGAN; FILHO, 2015), sabemos que o posto de B, que está bem definido sobre um DIP, é no máximo n. Por outro lado, como os α_i são LI, o posto de B é pelo menos n. Portanto, o posto de B é igual a n. Agora suponha que M seja uma B-módulo finitamente gerado por $\beta_1, \ldots, \beta_r$. Então existe $a \in A$ tal que $a\beta_i \in B$ para cada i. Logo, pelo Lema 3.1.16

$$da\beta_i \in M_0 = A\alpha_1 + \ldots + A\alpha_n$$

Então, $daM \subset M_0$. Novamente pelo teorema B.4.1 da referência (TENGAN; FILHO, 2015), como M_0 é livre, segue que daM também é livre. Logo, M é livre de posto no máximo n. Por outro lado, por hipótese, o posto de M é pelo menos

o posto de B, logo vale a igualdade. A segunda afirmação segue se tomarmos $M = B$. ■

Definição 3.1.18. Uma A-base de B na situação da Proposição 3.1.17 é chamada de base integral.

Para nós, o caso mais importante de base integral é quando $K = \mathbb{Q}, A = \mathbb{Z}$ e $B \subset L$ é o fecho integral de A num corpo de números L.

Exemplo 3.1.19. Seja K um corpo de números. Então existe uma $\mathbb{Q}$-base de K, $\{\alpha_1, \ldots, \alpha_n\}$, que é uma $\mathbb{Z}$-base de $\mathcal{O}_K$, isto é, uma base integral de K. Em particular, a Proposição 3.1.17 nos mostra que $\mathcal{O}_K$ é um grupo livre abeliano de posto $n = [K : \mathbb{Q}]$. No caso em que $K = \mathbb{Q}(\sqrt{d})$, o anel de inteiros $\mathcal{O}_K = \mathbb{Z} \bigoplus \mathbb{Z}\omega$, com

$$\omega = \begin{cases} \sqrt{d} & \text{se } d \equiv 2, 3 \mod 4 \\ \dfrac{1+\sqrt{d}}{2} & \text{se } d \equiv 1 \mod 4 \end{cases}$$

Portanto, $\{1, \omega\}$ é uma base integral de $\mathcal{O}_K$.

Observação 3.1.20. A Proposição 3.1.17 não é válida se L/K não for uma extensão separável, como veremos na próxima seção.

Proposição 3.1.21. Sejam $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_n\}$ duas bases integrais de um corpo de números K. Então

$$d_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = d_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$$

Dem.: Sejam $d = d_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ e $d' = d_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$. Então, $d = (\det M)^2 d'$ para alguma matriz $M \in GL_n(\mathbb{Z})$. Portanto, $\det M = \pm 1$ e $d = d'$. ■

Como o discriminante de um corpo de números K independe da escolha da base integral, podemos definir:

Definição 3.1.22. O discriminante de um corpo de números K é

$$d_K = d_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$$

para alguma $\mathbb{Z}$-base $\{\alpha_1, \ldots, \alpha_n\}$ de $\mathcal{O}_K$.

Exemplo 3.1.23. O corpo quadrático $\mathbb{Q}(\sqrt{2})$ tem base integral $\{1, \sqrt{2}\}$. Então, $d_K = 8$. Em geral, para um corpo quadrático $K = \mathbb{Q}(\sqrt{d})$, o discriminante é dado por

$$d_K = \begin{cases} 4d & \text{se } d \equiv 2, 3 \mod 4 \\ d & \text{se } d \equiv 1 \mod 4 \end{cases}$$

Vamos terminar esta seção com um resultado que relaciona o discriminante com a norma.

Proposição 3.1.24. Sejam $K = \mathbb{Q}(\alpha)$ e f o polinômio minimal de α. Então

$$d_{K/\mathbb{Q}}(\alpha) = \pm N_{K/\mathbb{Q}}(f'(\alpha))$$

Dem.: Sejam $\sigma_1, \ldots, \sigma_n$ as $\mathbb{Q}$-imersões de K em $\overline{\mathbb{Q}}$. Podemos supor sem perda de generalidade que $\sigma_1 = id : K \hookrightarrow \overline{\mathbb{Q}}$. Então, pelo Lema 3.1.12

$$d_{K/\mathbb{Q}}(\alpha) = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

Pela regra do produto da derivada, temos que

$$f'(\alpha) = \prod_{i=2}^{n} (\alpha - \sigma_i(\alpha))$$

Por fim, vamos calcular a norma

$$\begin{aligned} N_{K/\mathbb{Q}}(f'(\alpha)) &= \prod_{1 \leq j \leq n} \sigma_j(\prod_{i=2}^{n} (\alpha - \sigma_i(\alpha))) \\ &= \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha)) \\ &= \pm \prod_{1 \leq j < i \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = d_{K/\mathbb{Q}}(\alpha) \end{aligned}$$

■

3.2 Fatoração de ideais

Seja K um corpo de números. No próximo exemplo vamos ver que a fatoração única pode falhar em $\mathcal{O}_K$.

Exemplo 3.2.1. O corpo quadrático $K = \mathbb{Q}(\sqrt{-5})$ tem anel de inteiros $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Neste anel, o número 6 tem duas fatorações diferentes:

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

Portanto, a fatoração única falha em $\mathbb{Z}[\sqrt{-5}]$. Para ver que estas são as duas únicas fatorações do 6, observe que $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, mas não existem soluções inteiras para as equações $N(a + b\sqrt{-5}) = a^2 + 5b^2 = 2$ e $N(a + b\sqrt{-5}) = a^2 + 5b^2 = 3$.

Nosso objetivo nesta seção é tentar de alguma forma consertar a falha da fatoração única em $\mathcal{O}_K$, e mais geralmente num domínio de Dedekind A (como definiremos mais adiante). Então estudaremos o problema de determinar todas as fatorações de um elemento numa extensão integral. Para o problema da fatoração única no exemplo anterior, seria interessante que existissem elementos $p_1, p_2, p_3, p_4 \in \mathbb{Z}[\sqrt{-5}]$ tais que

$$2 = p_1 p_2, 1 + \sqrt{-5} = p_1 p_3$$
$$3 = p_2 p_3, 1 - \sqrt{-5} = p_2 p_4$$

Na verdade, os objetos que estamos procurando são exatamente os ideais primos em $\mathcal{O}_K$. Para descrever uma fatoração única em ideais primos, vamos recordar que dados ideais $\mathfrak{a}, \mathfrak{b}$ de A, seu produto é o ideal

$$\mathfrak{ab} = \{\sum_{i=1}^{n} a_i b_i / a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

Vamos agora definir o principal objeto de estudo desta seção.

Definição 3.2.2. Um domínio A é um domínio de Dedekind se

1. A é integralmente fechado;

2. A é noetheriano;

3. $\dim A = 1$, isto é, todo ideal primo não nulo de A é maximal.

Observe que a condição 3. da Definição 3.2.2 significa que um corpo não é um domínio de Dedekind. A seguir um exemplo de anel que satisfaz as três condições:

Exemplo 3.2.3. Todo DIP que não é um corpo é um domínio de Dedekind. Em particular, $\mathbb{Z}$ é um domínio de Dedekind.

Domínios de Dedekind têm papel fundamental na Teoria Algébrica dos Números, pois veremos a seguir que dado qualquer corpo de números K, seu anel de inteiros $\mathcal{O}_K$ é um domínio de Dedekind. Vamos mostrar que num domínio de Dedekind todo ideal não nulo se fatora unicamente como produto de ideais primos, o que nos permite generalizar as propriedades de fatoração única em $\mathbb{Z}$.

Teorema 3.2.4. Sejam A um domínio de Dedekind com corpo de frações K e L/K uma extensão finita e separável de corpos. Então, o fecho integral B de A em L é um domínio de Dedekind.

Dem.: Primeiramente, B é integralmente fechado pelo Corolário 2.1.8. Além disto, como L/K é uma extensão separável, pelo Lema 3.1.16, existe uma K-base $\{v_1, \ldots, v_n\}$ de L tal que $B \subset \sum_{i=1}^{n} Av_i$. Como A é noetheriano, temos que B é noetheriano. Finalmente, como $A \subset B$ é uma extensão integral, $\dim A = \dim B = 1$ pelo Teorema 2.2.12. ■

Corolário 3.2.5. Seja K um corpo de números. Então $\mathcal{O}_K$ é um domínio de Dedekind.

Dem.: Como $\mathbb{Q}$ é um corpo perfeito, a extensão $K/\mathbb{Q}$ é separável e o resultado segue do Teorema 3.2.4. ■

Como $\mathbb{Z}$ é um domínio de Dedekind, a fatoração única nos inteiros pode ser escrita em termos de fatoração única de ideais. Associado a cada primo $p \in \mathbb{Z}$ temos um ideal primo $(p) = p\mathbb{Z}$. Por exemplo, em $\mathbb{Z}[\sqrt{-5}]$ temos que

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

Lema 3.2.6. Seja A um domínio de Dedekind, então todo ideal não nulo $\mathfrak{a}$ de A contém um produto finito de ideais primos.

Dem.: Como A é noetheriano, o resultado segue do Teorema 1.2.8. ■

A prova clássica de fatoração única nos inteiros depende da capacidade de cancelarmos os ideais primos através da divisão, então para imitar a prova em termos de ideais primos, precisamos criar uma analogia de inversos para ideais.

Definição 3.2.7. Seja $\mathfrak{a}$ um ideal de A. O ideal fracionário gerado por $\mathfrak{a}$ é o A-módulo

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset A\}$$

onde K é o corpo de frações de A.

Note que dado um ideal $\mathfrak{a}$ de A, $\mathfrak{a}^{-1}$ é um A-submódulo de K. Além disto, $\mathfrak{a}^{-1} \supset A$, então dado um ideal próprio $\mathfrak{a}$ de A, $\mathfrak{a}^{-1}$ não é um ideal de A. Mas observe que $\mathfrak{a}\mathfrak{a}^{-1}$ é um ideal de A.

Antes de provar o teorema, precisaremos provar alguns resultados auxiliares. Aqui iremos assumir que os ideais $\mathfrak{p} \in \mathrm{Spec}(A)$ são não nulos.

Lema 3.2.8. Se $\mathfrak{p} \in \mathrm{Spec}(A)$, então $\mathfrak{p}^{-1} \neq A$.

Dem.: Seja $x \in \mathfrak{p}$. Pelo Lema 3.2.6, temos que

$$(x) \supset \mathfrak{p}_1 \dots \mathfrak{p}_r$$

com $\mathfrak{p}_i \in \mathrm{Spec}(A)$. Suponha r minimal. Vamos mostrar que $\mathfrak{p} = \mathfrak{p}_i$ para algum $i \in \{1, \dots, r\}$. Caso contrário, existiria $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ para cada i, pela maximalidade dos ideais primos. Então

$$a_1 \dots a_r \in \mathfrak{p}_1 \dots \mathfrak{p}_r \subset (x) \subset \mathfrak{p}$$

uma contradição. Logo, $\mathfrak{p} = \mathfrak{p}_i$ para algum i. Suponha sem perda de generalidade que $\mathfrak{p} = \mathfrak{p}_1$. Então pela minimalidade de r, temos que

$$(x) \supsetneq \mathfrak{p}_2 \dots \mathfrak{p}_r$$

Seja $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r \setminus (x)$. Então, $x^{-1}b \notin A$, mas $x^{-1}b\mathfrak{p} \subset A$. Portanto, $x^{-1}b \in \mathfrak{p}^{-1} \setminus A$. ■

Lema 3.2.9. Se $\mathfrak{a}$ é um ideal de A e $\mathfrak{p} \in \text{Spec}(A)$, então $\mathfrak{a}\mathfrak{p}^{-1} \supsetneq \mathfrak{a}$.

Dem.: Como $\mathfrak{p}^{-1} \supset A$, segue que $\mathfrak{a}\mathfrak{p}^{-1} \supset \mathfrak{a}$. Suponha por absurdo que $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ e seja $x \in \mathfrak{p}^{-1}$. Então, $x\mathfrak{a} \subset \mathfrak{a}$, em particular, a multiplicação à esquerda por x é um elemento da A-álgebra [1] $End_A(\mathfrak{a})$. Como A é noetheriano, $End_A(\mathfrak{a})$ é finitamente gerada[2]. Além disto, $End_A(\mathfrak{a})$ é um A-módulo fiel. Segue do Teorema 2.1.3 que x é integral sobre A. Como A é integralmente fechado, $x \in A$. Mostramos assim que $\mathfrak{p}^{-1} = A$, mas isto contradiz o Lema 3.2.8. Portanto, $\mathfrak{a}\mathfrak{p}^{-1} \supsetneq \mathfrak{a}$. ■

Corolário 3.2.10. Dado $\mathfrak{p} \in \text{Spec}(A), \mathfrak{p}\mathfrak{p}^{-1} = A$.

Dem.: Pelo Lema 3.2.9, temos que $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subset A$. Como $\mathfrak{p}\mathfrak{p}^{-1}$ é um ideal de A e ideais primos não nulos são maximais num domínio de Dedekind, então $\mathfrak{p}\mathfrak{p}^{-1} = A$. ■

Corolário 3.2.11. Dados um ideal $\mathfrak{a}$ de A e $\mathfrak{p} \in \text{Spec}(A), \mathfrak{p} \supsetneq \mathfrak{a}$, temos que $\mathfrak{a}\mathfrak{p}^{-1} \subsetneq A$.

Dem.: Se $\mathfrak{a}\mathfrak{p}^{-1} = A$, então $\mathfrak{p} = \mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{a}$, absurdo. ■

Agora estamos preparados para provar o teorema de fatoração única para ideais não nulos num domínio de Dedekind.

Teorema 3.2.12. Se A for um domínio de Dedekind, então todo ideal não nulo $\mathfrak{a}$ de A tem fatoração

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$$

em ideais primos distintos $\mathfrak{p}_i \in \text{Spec}(A)$ que são únicos a menos da ordem.

[1] Um anel B munido de um homomorfismo de anéis $A \to B$ é dito uma A-Álgebra (MILNE, 2017)

[2] Proposição 7.8 da referência (ATIYAH; MACDONALD, 1969)

Dem.: Seja $\mathcal{P}$ o conjunto dos ideais próprios não nulos de A que não possuem fatoração em ideais primos. Vamos mostrar que $\mathcal{P} = \emptyset$. Suponha por absurdo que $\mathcal{P} \neq \emptyset$. Como A é noetheriano, $\mathcal{P}$ possui um elemento maximal $\mathfrak{a}$. Como $\mathfrak{a}$ não pode ser escrito como um produto de ideais primos, ele mesmo não pode ser primo. Então $\mathfrak{a}$ está contido num ideal primo $\mathfrak{p}$. Pelo Lema 3.2.9, $\mathfrak{a}\mathfrak{p}^{-1} \supsetneq \mathfrak{a}$, então $\mathfrak{a}\mathfrak{p}^{-1} \notin \mathcal{P}$. Por outro lado, o Corolário 3.2.11 nos diz que $\mathfrak{a}\mathfrak{p}^{-1} \neq (1)$, então

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

Multiplicando por $\mathfrak{p}$, temos que

$$\mathfrak{a} = \mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_r$$

o que mostra que $\mathfrak{a}$ possui uma fatoração, absurdo. Logo, $\mathcal{P} = \emptyset$. E isto prova a existência da fatoração única. Para a unicidade, suponha que

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

com $\mathfrak{p}_i, \mathfrak{q}_j \in \operatorname{Spec}(A)$. Então pela prova do Lema 3.2.8, $\mathfrak{p}_1 \supset \prod_j \mathfrak{q}_j$ implica que $\mathfrak{p}_1 = \mathfrak{q}_j$ para algum $j \in \{1, \dots, s\}$. Multiplicando ambos os lados por $\mathfrak{p}_1^{-1}$ cancelamos este termo, chegando numa fatoração menor de $\mathfrak{a}$ em primos. Por indução, segue que as duas fatorações são iguais. ■

Observação 3.2.13. Dados um ideal $\mathfrak{a}$ de A e um ideal $\mathfrak{p} \in \operatorname{Spec}(A)$, usaremos as expressões $\mathfrak{p} \supset \mathfrak{a}$ ($\mathfrak{p}$ contém $\mathfrak{a}$) e $\mathfrak{p} \mid \mathfrak{a}$ ($\mathfrak{p}$ divide $\mathfrak{a}$) para dizer que $\mathfrak{p}$ aparece na fatoração única de $\mathfrak{a}$.

Mas as coisas não acabam por aqui, ainda existem perguntas que precisam ser respondidas a respeito dos ideais primos.

Exemplo 3.2.14. Seja $K = \mathbb{Q}(\sqrt{-5})$. Já vimos que $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Mas como 2 e 3 se fatoram como ideais em $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$? Segue que

$$2\mathcal{O}_K = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) \text{ e } 3\mathcal{O}_K = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$

Este comportamento se deve ao fato do polinômio minimal $X^2 + 5$ de $\sqrt{-5}$ se decompor de forma diferente mod 2 e mod 3:

$$X^2 + 5 \equiv (X+1)^2 \mod 2 \text{ e } X^2 + 5 \equiv (X-1)(X+1) \mod 3$$

O Exemplo 3.2.14 nos motiva a estudar o comportamento dos ideais primos e assim surge a chamada teoria de ramificação, que é um dos objetos centrais nesta dissertação. Antes de definir o que é a ramificação, vamos provar alguns resultados.

Até o final desta seção, seja L/K uma extensão finita separável de corpos, seja $\mathcal{O}_K$ um domínio de Dedekind com corpo de frações K e seja $\mathcal{O}_L$ o fecho integral de $\mathcal{O}_K$ em L. Tome $n = [L : K]$.

Lema 3.2.15. $\mathcal{O}_L$ é um domínio de Dedekind.

Dem.: A prova é a mesma do Corolário 3.2.5. ■

Lema 3.2.16. Se $\mathfrak{p} \in \text{Spec}(\mathcal{O}_K)$, então $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$.

Dem.: Tome $x \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$, que existe pelo Lema 3.2.8. Então $x\mathfrak{p} \subset \mathcal{O}_K$ e $x\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$. Se $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, então teríamos $x\mathfrak{p}\mathcal{O}_L = x\mathcal{O}_L \subsetneq \mathcal{O}_L$, o que é uma contradição. Portanto, $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. ■

Agora fixe um $\mathfrak{p} \in \text{Spec}(\mathcal{O}_K)$ não nulo. Pelo Teorema 3.2.12, o ideal de $\mathcal{O}_L$ gerado $\mathfrak{p}$ tem fatoração única

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_g^{e_g}$$

onde $\mathfrak{q}_i \in \text{Spec}(\mathcal{O}_L)$ são distintos e cada $e_i \geq 1$. Note que para cada i, $\dfrac{\mathcal{O}_L}{\mathfrak{q}_i}$ é um $\dfrac{\mathcal{O}_K}{\mathfrak{p}}$-espaço vetorial de dimensão finita. Isto segue do fato de $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$. Dizemos que $\mathfrak{q}_i \in \text{Spec}(\mathcal{O}_L)$ estão acima de $\mathfrak{p}$. Pela fatoração única, segue que estes são os únicos primos acima de $\mathfrak{p}$.

Definição 3.2.17. Dado um primo $\mathfrak{q}_i$ da fatoração de $\mathfrak{p}\mathcal{O}_L$, o índice $f_i = \left[\dfrac{\mathcal{O}_L}{\mathfrak{q}_i} : \dfrac{\mathcal{O}_K}{\mathfrak{p}}\right]$ é chamado de grau de inércia de $\mathfrak{q}_i$ sobre $\mathfrak{p}$ e o expoente e_i é chamado de índice de ramificação de $\mathfrak{q}_i$ sobre $\mathfrak{p}$. Dizemos que o primo $\mathfrak{p}$

1. Se decompõe totalmente se $e_i = f_i = 1$ para todo $i \in \{1, \dots, g\}$;

2. É totalmente ramificado se $g = 1$ e $f_1 = 1$;

3. É inerte se $g = 1$ e $e_1 = 1$.

Definição 3.2.18. Se algum $e_i > 1$ ou se a extensão $\dfrac{\mathcal{O}_L}{\mathfrak{q}_i}/\dfrac{\mathcal{O}_K}{\mathfrak{p}}$ for inseparável, dizemos que o primo $\mathfrak{p}$ é ramificado em $\mathcal{O}_L$. Caso contrário, dizemos que é não ramificado.

O teorema a seguir é conhecido como a identidade fundamental da teoria de ramificação.

Teorema 3.2.19. Dado $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ com fatoração em primos $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$ temos que

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

Dem.: Pelo teorema chinês dos restos podemos escrever

$$\frac{\mathcal{O}_L}{\mathfrak{p}\mathcal{O}_L} = \frac{\mathcal{O}_L}{\prod_{i=1}^{g} \mathfrak{q}_i^{e_i}} \cong \bigoplus_{i=1}^{g} \frac{\mathcal{O}_L}{\mathfrak{q}_i^{e_i}}$$

Para provar o teorema, precisamos mostrar que $\left[\dfrac{\mathcal{O}_L}{\mathfrak{p}\mathcal{O}_L} : \dfrac{\mathcal{O}_K}{\mathfrak{p}}\right] = n$ e $\left[\dfrac{\mathcal{O}_L}{\mathfrak{q}_i^{e_i}} : \dfrac{\mathcal{O}_K}{\mathfrak{p}}\right] = e_i f_i$ para cada $i \in \{1, \ldots, g\}$. Para a primeira igualdade, seja $\{v_1, \ldots, v_m\}$ uma base para $\dfrac{\mathcal{O}_L}{\mathfrak{p}\mathcal{O}_L}$ como um $\dfrac{\mathcal{O}_K}{\mathfrak{p}}$-espaço vetorial. Levante esses elementos a $w_1, \ldots, w_m \in \mathcal{O}_L$ e suponha que

$$a_1 w_1 + \ldots + a_n w_m = 0, a_i \in \mathcal{O}_K$$

Seja $\mathfrak{a} = (a_1, \ldots, a_m)$ um ideal de $\mathcal{O}_K$ e seja $x \in \mathfrak{a}^{-1} \setminus \mathfrak{a}\mathfrak{p}$. Tal elemento existe pelo Lema 3.2.8. Então $xa_i \in \mathcal{O}_K$ para todo i, mas $xa_i \notin \mathfrak{p}$ para algum i. Substituindo a_i por xa_i e reduzindo módulo $\mathfrak{p}$ temos uma dependência linear, contradizendo o fato de que $v_1, \ldots, v_m$ formavam uma base. Portanto, $w_1, \ldots, w_m$ devem ser linearmente independentes em $\mathcal{O}_K$. Agora vamos mostrar que eles geram $\mathcal{O}_K$. Seja $M = w_1\mathcal{O}_K + \ldots + w_m\mathcal{O}_K \subset \mathcal{O}_L$. Como os v_i geram $\dfrac{\mathcal{O}_L}{\mathfrak{p}\mathcal{O}_L}$, temos que $M = \mathfrak{p}\mathcal{O}_L$. Ou seja, $\mathfrak{p}\left(\dfrac{\mathcal{O}_L}{M}\right) = \dfrac{\mathcal{O}_L}{M}$. Pelo lema de Nakayama, segue que $\dfrac{\mathcal{O}_L}{M}$ é

anulado por algum $x \in 1 + \mathfrak{p}$. Em particular, $x \neq 0$ e disto $x\mathcal{O}_L \subset M$. Logo, $\frac{w_1}{x}\mathcal{O}_K + \ldots + \frac{w_m}{x}\mathcal{O}_K \supset \mathcal{O}_L$. Assim, $\frac{w_1}{x}K + \ldots + \frac{w_m}{x}K = L$. Então, os w_i geram $\mathcal{O}_L$ como $\mathcal{O}_K$-espaço vetorial. Isto só é possível se $m = n$, e disto temos a primeira igualdade. Agora considere a sequência

$$\frac{\mathcal{O}_L}{\mathfrak{q}_i^{e_i}} \supset \frac{\mathfrak{q}_i}{\mathfrak{q}_i^{e_i}} \supset \frac{\mathfrak{q}_i^2}{\mathfrak{q}_i^{e_i}} \supset \ldots \supset \frac{\mathfrak{q}_i^{e_i-1}}{\mathfrak{q}_i^{e_i}} \supset \{0\}$$

Tomando cada quociente da cadeia, temos algo da forma $\frac{\mathfrak{q}_i^r}{\mathfrak{q}_i^{r+1}}$, e pela fatoração única, cada um desses quocientes é não trivial. Podemos escolher $x \in \mathfrak{q}_i^r \setminus \mathfrak{q}_i^{r+1}$. Considere a função

$$\begin{aligned} \varphi \colon \mathcal{O}_L &\to \frac{\mathfrak{q}_i^r}{\mathfrak{q}_i^{r+1}} \\ \alpha &\mapsto x\alpha \end{aligned}$$

Como $\mathfrak{q}_i \subset \ker\varphi$ e todos os ideais primos são maximais em $\mathcal{O}_K$, segue que $\ker\varphi = \mathfrak{q}_i$. Além disto, como $\mathfrak{q}_i^{r+1} \subsetneq (x) + \mathfrak{q}_i^{r+1} \subset \mathfrak{q}_i^r$, isto é, $(x) + \mathfrak{q}_i^{r+1} = \mathfrak{q}_i^r$, segue que φ é sobrejetiva. Logo, $\frac{\mathcal{O}_L}{\mathfrak{q}_i} \cong \frac{\mathfrak{q}_i^r}{\mathfrak{q}_i^{r+1}}$ como $\frac{\mathcal{O}_K}{\mathfrak{p}}$-espaços vetoriais. Assim,

$$\dim_{\frac{\mathcal{O}_K}{\mathfrak{p}}} \frac{\mathcal{O}_L}{\mathfrak{q}^{e_i}} = \sum_{j=1}^{e_i} \dim_{\frac{\mathcal{O}_K}{\mathfrak{p}}} \frac{\mathcal{O}_L}{\mathfrak{q}_i} = e_i f_i$$

Portanto,

$$n = \sum_{i=1}^{g} e_i f_i$$

■

Agora vamos discutir a teoria de ramificação de Hilbert. Suponha que L/K seja uma extensão galoisiana e seja $G = \mathrm{Gal}(L/K)$. Note que $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ para todo $\sigma \in G$. Se $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ e $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$, então cada $\sigma \in G$ age nos primos acima de $\mathfrak{p}$: $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$ para algum $j \in \{1, \ldots, g\}$. Uma observação importante é que essa ação é transitiva.

Proposição 3.2.20. Dado $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K), G = \mathrm{Gal}(L/K)$ age transitivamente [3] nos primos de $\mathcal{O}_L$ acima de $\mathfrak{p}$.

Dem.: Suponha por absurdo que não. Então existe um par de primos $\mathfrak{q}_i, \mathfrak{q}_j$ acima de $\mathfrak{p}$ tais que $\sigma(\mathfrak{q}_j) \neq \mathfrak{q}_i$ para todo $\sigma \in G$. Pelo teorema chinês dos restos, existe $x \in \mathfrak{q}_j$ tal que

$$x \equiv 1 \mod \sigma(\mathfrak{q}_i)$$

para todo $\sigma \in G$. Então,

$$N_{L/K}(x) \in \mathfrak{q}_j \cap \mathcal{O}_K = \mathfrak{p}$$

Por outro lado

$$N_{L/K} = \prod_{\sigma \in G} \sigma(x)$$

mas $\sigma(x) \notin \mathfrak{q}_i$ para todo i, então $N_{L/K}(x) \notin \mathfrak{p}$. Absurdo, então deve existir algum $\sigma \in G$ tal que $\sigma(\mathfrak{q}_j) = \mathfrak{q}_i$. ■

Corolário 3.2.21. Quando a extensão L/K for galoisiana, dado um primo $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, todos os índices de ramificação e_i e todos os graus de inércia f_i de primos acima de $\mathfrak{p}$ são iguais, e portanto,

$$[L : K] = efg$$

onde g é a quantidade de ideais primos da fatoração, $e = e_i$ e $f = f_i$ para qualquer primo $\mathfrak{q}_i \mid \mathfrak{p}$.

Dem.: Um ideal $\mathfrak{q}_i^r$ divide $\mathfrak{p}\mathcal{O}_L$ se, e somente se, $\sigma(\mathfrak{q}_i^r)$ divide $\mathfrak{p}\mathcal{O}_L$ para todo $\sigma \in G$, o que pela Proposição 3.2.20 é equivalente a $\mathfrak{q}_j^r$ dividir $\mathfrak{p}\mathcal{O}_L$ para todo $j \in \{1, \ldots, g\}$. Assim, os índices de ramificação são iguais e seja e tal índice. Agora, dados $i, j \in \{1, \ldots, g\}$, suponha que $\sigma \in G$ seja uma permutação de $\mathfrak{q}_j$ em $\mathfrak{q}_i$, isto

[3] Uma ação de um grupo G num conjunto X é transitiva se dados $x, y \in X$ existe um $g \in G$ tal que $gx = y$

é, $\mathfrak{q}_i = \sigma(\mathfrak{q}_j)$. Então σ determina um isomorfismo $\dfrac{\mathcal{O}_L}{\mathfrak{q}_j} \to \dfrac{\mathcal{O}_L}{\mathfrak{q}_i}$. Logo, $f_i = f_j = f$. Finalmente, pelo Teorema 3.2.19 temos que

$$[L : K] = \sum_{i=1}^{g} ef = efg$$

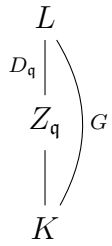
■

Fixe $\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_L)$ acima de $\mathfrak{p}$.

Definição 3.2.22. O subgrupo $D_\mathfrak{q} = \{\sigma \in G / \sigma(\mathfrak{q}) = \mathfrak{q}\}$ de G é chamado de grupo de decomposição de $\mathfrak{q}$.

Pelo teorema estabilizador-órbita, $|D_\mathfrak{q}| = ef$, onde e e f são o índice de ramificação e o grau de inércia de $\mathfrak{q}$ sobre $\mathfrak{p}$ respectivamente. Pela teoria de Galois, existe uma extensão de corpos $Z_\mathfrak{q}/K$ correspondendo ao subgrupo $D_\mathfrak{p}$, que é explicitamente o corpo fixado $Z_\mathfrak{q} = L^{D_\mathfrak{q}}$.

Definição 3.2.23. Dado um primo $\mathfrak{q} \mid \mathfrak{p}$, o corpo $Z_\mathfrak{q}$ é chamado de corpo de decomposição de $\mathfrak{q}$.



4 O completamento de corpos de números e extensões suavemente ramificadas

O conteúdo aqui estudado pode ser encontrado nas referências (NEUKIRCH, 2013), (CASSELS; FRÖHLICH, 1986), (JANUSZ, 1996), (MARCUS; SACCO, 1977), (WEIL, 2013), (TENGAN; FILHO, 2015), (MILNE, 2017) e (SUTHERLAND, 2017).

4.1 Valorizações

Começaremos esta seção definindo uma versão local de um domínio de Dedekind.

Definição 4.1.1. Um domínio de Dedekind local A é chamado de anel de valorização discreta. Seu corpo residual é definido como o quociente $k = \frac{A}{\mathfrak{m}}$, onde $\mathfrak{m}$ é o único ideal maximal de A.

A próxima definição e a próxima proposição explicam o motivo do nome "anel de valorização discreta".

Definição 4.1.2. Seja A um anel. Uma valorização em A é uma função $v : A \setminus \{0\} \to \mathbb{Z}_+$ tal que dados $x, y \in A \setminus \{0\}$ temos que

1. $v(x) = 0 \iff x \in A^\times$;
2. $v(xy) = v(x) + v(y)$;
3. $v(x + y) \geq \min\{v(x), v(y)\}$

Uma valorização v é discreta se for sobrejetiva. É comum estender uma valorização v em A ao corpo de frações K de A pondo $v(0) = \infty$ e $v\left(\frac{a}{b}\right) = v(a) - v(b)$ e considerando a função $v : K \to \mathbb{Z} \cup \{\infty\}$.

Proposição 4.1.3. Seja K um corpo e seja $v : K \to \mathbb{Z} \cup \{\infty\}$ uma valorização discreta. O anel de valorização discreta associado a v é o anel local

$$\mathcal{O}_v := \{a \in K \mid v(a) \geq 0\}$$

com ideal maximal

$$\mathfrak{m}_v := \{a \in K \mid v(a) > 0\}.$$

Dem.: Note que de fato $\mathcal{O}_v$ é um subanel de K já que $v(a) \geq 0$ e $v(b) \geq 0$ implica $v(a+b) \geq \min\{v(a), v(b)\} \geq 0$ e $v(ab) = v(a) + v(b) \geq 0$. Além disso, $v(a) \geq 0$ e $v(a^{-1}) \geq 0$ implica $v(a) = 0$, ou seja,

$$\mathcal{O}_v^\times = \{a \in K \mid v(a) = 0\} = \mathcal{O}_v \setminus \mathfrak{m}_v$$

o que mostra que $\mathcal{O}_v$ é um anel local. ■

Proposição 4.1.4. Todo anel de valorização discreta é um DIP que não é corpo.

Dem.: Como v é sobrejetor, existe $\pi \in A$ com $v(\pi) = 1$ de modo que $\pi \in \mathfrak{m}_v = \mathfrak{m} \implies \mathfrak{m} \neq 0$, e portanto, A não é corpo. Agora tome $\mathfrak{a} \subset A$ um ideal não nulo; vamos mostrar que $\mathfrak{a} = (t)$ é principal com $t \in \mathfrak{a}$ um elemento de valorização mínima dentre os elementos de $\mathfrak{a}$ (note que t existe pois $\mathfrak{a} \neq 0$ e $v(\mathfrak{a}) \subset \mathbb{N} \cup \{\infty\}$). Temos que $\mathfrak{a} \supset (t)$; para mostrar a inclusão contrária, tome $a \in \mathfrak{a}$: segue que $v(a) \geq v(t)$ pela escolha de t, logo, $v\left(\frac{a}{t}\right) = v(a) - v(t) \geq 0$, ou seja, $\frac{a}{t} \in A = \mathcal{O}_v$, e portanto, $\mathfrak{a} = (t)$. ■

Exemplo 4.1.5. Seja p primo e considere a localização de $\mathbb{Z}$ no ideal primo (p) :

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, p \nmid b\right\}$$

Então, $\mathbb{Z}_{(p)}$ é um anel de valorização discreta com valorização $v\left(\frac{a}{b}\right) = r$ se pudermos escrever

$$\frac{a}{b} = p^r \frac{a'}{b'}$$

para inteiros a', b' não divisíveis por p.

A valorização do Exemplo 4.1.5 é chamada de valorização p-ádica e agora vamos definir e provar algumas propriedades básicas dos números p-ádicos. Os números p-ádicos foram descobertos por Kurt Hensel. Sua ideia original para definir tais números veio quando estudava expansões de séries de potência em Análise, mas rapidamente ele percebeu sua utilidade na teoria de números.

Seja K um corpo e tome um polinômio $f(X) \in K[X]$. Dado $a \in K$, podemos escrever

$$f(X) = \sum_{i=0}^{n} a_i(X-a)^i \text{ para alguns } a_i \in K$$

Observe que os coeficientes a_i estão relacionados às derivadas $f^{(i)}(a)$, como no teorema de Taylor. Se ao invés, tivermos uma função racional

$$f(X) = \frac{g(X)}{h(X)} \in K[X]_{(X-a)}$$

para $g, h \in K[X]$ com $h(a) \neq 0$, ainda podemos escrever uma expansão em séries de potência formais de $f(X)$ em torno de $X = a$:

$$\frac{f(X)}{g(X)} \approx \sum_{i=0}^{\infty} a_i(X-a)^i \text{ para } a_i \in K$$

A noção de aproximação ficará mais clara quando falarmos de convergência num corpo qualquer. Assim podemos relacionar o anel dos inteiros $\mathbb{Z}$ e anéis de polinômios sobre corpos. Dado um inteiro positivo $x \in \mathbb{Z}$, podemos escrever

$$x = \sum_{i=0}^{n} a_i p^i \text{ para } a_i \in \{0, 1, \ldots, p-1\}$$

Se $x \in \mathbb{Z}_{(p)}$, a localização em (p) dada no exemplo 4.1.5, então podemos escrever uma série de potência formal que representa x

$$\sum_{i=0}^{\infty} a_i p^i$$

com $a_i \in \{0, 1, \ldots, p-1\}$.

Exemplo 4.1.6. Sejam $p = 5$ e $x = 233$. Então a expansão 5-ádica nos dá uma série de potência para 233

$$233 = 3 \cdot 5^0 + 1 \cdot 5 + 4 \cdot 5^2 + 1 \cdot 5^3 + 0 \cdot 5^4 + \dots$$

Definição 4.1.7. Dado um primo p, um inteiro p-ádico é uma soma infinita formal

$$\sum_{i=0}^{\infty} a_i p^i$$

para $a_i \in \{0, 1, \dots, p-1\}$. O conjunto de todos os inteiros p-ádicos é denotado por $\mathbb{Z}_p$.

Note que todo inteiro p-ádico tem uma classe residual bem definida módulo p^n para cada $n \geq 0$. Por outro lado, todo elemento do anel local $\mathbb{Z}_{(p)}$ tem uma classe residual bem definida módulo p^n. Dado $x \in \mathbb{Z}_{(p)}$, escrevemos

$$x = \sum_{i=0}^{\infty} a_i p^i$$

se ambos os objetos tiverem o mesmo resídulo módulo p^n para todo $n \geq 0$. Em outras palavras, temos uma função $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$. Esta função é injetiva. De fato, sejam $x, y \in \mathbb{Z}_{(p)}$ com $x = \sum_{i=0}^{\infty} a_i p^i = y$. Então $x - y \equiv 0 \mod p^n$ para todo $n \geq 0$, e portanto, $x = y$.

Exemplo 4.1.8. Nem sempre essas p-séries de potência se comportam como no caso analítico. Por exemplo, tome $x = -1$, então para cada $n \geq 0$,

$$\sum_{i=0}^{n-1} (p-1)p^i = p^n - 1 \equiv -1 \mod p^n$$

Logo, -1 tem expansão p-ádica $\sum_{i=0}^{\infty} (p-1)p^i$ para qualquer primo p. Se $p = 2$, temos

$$-1 = 1 + 2 + 4 + 8 + 16 + \dots$$

Nos inteiros, tal sequência não converge, mas nos números 2-ádicos sim. Alternativamente, a série de potência

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots$$

não converge para $x = 2$, mas converge nos números 2-ádicos. Em geral, temos que

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \dots$$

é válido em $\mathbb{Z}_p$.

Mais a frente veremos que $\mathbb{Z}_p$ é o completamento de $\mathbb{Z}_{(p)}$ com respeito a uma certa topologia, que chamaremos de topologia p-ádica.

Definição 4.1.9. O corpo de frações de $\mathbb{Z}_p$ é chamado de corpo dos inteiros p-ádicos e denotado por $\mathbb{Q}_p$.

Por definição, qualquer elemento de $\mathbb{Q}_p$ pode ser escrito como $p^{-m}x$ para algum $x \in \mathbb{Z}_p$ e $m \geq 0$. A soma em $\mathbb{Q}_p$ é dada por

$$p^{-m}x + p^{-r}y = p^{-m}(x + p^{m-r}y)$$

se $m \geq r$. Enquanto a multiplicação é simplesmente

$$(p^{-m}x)(p^{-r}y) = p^{-(m+r)}xy$$

Note que $\mathbb{Q}_p$ é um corpo de característica 0, então ele contém $\mathbb{Q}$ como subcorpo. Mais formalmente, existe uma imersão canônica $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ que faz o seguinte diagrama comutar

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}_p \\ \uparrow & & \uparrow \\ \mathbb{Z}_{(p)} & \hookrightarrow & \mathbb{Z}_p \end{array}$$

Os elementos de $\mathbb{Q}_p$ podem ser vistos como séries de Laurent p-ádicas $\sum_{i=-m}^{\infty} a_i p^i$ com $a_i \in \{0, \dots, p-1\}$.

Definição 4.1.10. Para todo primo $p \in \mathbb{Z}$ a valorização p-ádica em $\mathbb{Q}$ é a valorização estendida $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ definida por $v_p(x) = m$ se $x = p^m \frac{a}{b}$ com $a, b \in \mathbb{Z}$ e $p \nmid ab$, e $v(0) = \infty$.

Definição 4.1.11. Uma valorização v num anel A é chamada de não arquimediana se dados $x, y \in A$

$$v(x+y) \geq \min\{v(x), v(y)\}$$

com igualdade se, e somente se, $v(x) \neq v(y)$.

Definição 4.1.12. Dado um primo p, o valor absoluto (normalizado) p-ádico em $\mathbb{Q}$ é definido por $|x|_p = p^{-v_p(x)}$ para $x \neq 0$ e $|0|_p = 0$.

As demonstrações dos próximos dois lemas são apenas verificações e serão suprimidas aqui.

Lema 4.1.13. Toda valorização p-ádica em $\mathbb{Q}$ é não arquimediana.

Lema 4.1.14. O valor absoluto p-ádico é uma norma em $\mathbb{Q}$ para todo p primo.

Toda valorização p-ádica dá origem a uma topologia em $\mathbb{Q}$ através da métrica

$$d_p(x, y) = |x - y|_p$$

Esta topologia é chamada de topologia p-ádica em $\mathbb{Q}$. Para o valor absoluto usual de $\mathbb{Q}$ herdado de $\mathbb{R}$, escreveremos $|\cdot|_\infty$.

Teorema 4.1.15. Seja $x \in \mathbb{Q}^\times$. Então

$$\prod_p |x|_p = 1$$

onde o produto varia entre todos os primos p e ∞.

Dem.: Como normas são multiplicativas, basta mostrar que a fórmula do produto vale para x primo e $x = -1$. Quando $x = -1, |-1|_p = 1$ para todo primo p e $|-1|_\infty = 1$, então a fórmula do produto é válida. Se $x = q$ é primo, então

$$|q|_p = \begin{cases} q & \text{se } p = \infty \\ \dfrac{1}{q} & \text{se } p = q \\ 1 & \text{caso contrário} \end{cases}$$

Portanto, a fórmula do produto vale também neste caso. ■

O próximo lema nos mostra um dos aspectos curiosos das topologias definidas em valores absolutos não arquimedianos.

Lema 4.1.16. Dados p primo e $a \in \mathbb{Q}$, definimos a bola p-ádica de centro a e raio r

$$B_p(a,r) = \{c \in \mathbb{Q} \mid |c-a|_p < r\}$$

Então todo ponto $b \in B_p(a,r)$ é na verdade o centro da bola, ou seja, $B_p(b,r) = B_p(a,r)$. O mesmo vale para toda bola fechada $B_p[a,r]$.

Dem.: Tome $c \in B_p(a,r)$, vamos mostrar que $c \in B_p(b,r)$. Temos que $|a-c|_p < r$. Como $b \in B_p(a,r)$, temos que

$$|b-c|_p = |b-a+a-c|_p \leq \max\{|b-a|_p, |a-c|_p\} < r$$

Portanto, $c \in B_p(b,r)$, e disto $B_p(a,r) \subset B_p(b,r)$. Mudando os papéis de a e b temos que $B_p(a,r) = B_p(b,r)$. ■

Não é difícil mostrar que $\mathbb{Q}$ não é completo com respeito a $|\cdot|_p$ para todo primo p, e sabemos da Análise Real que $\mathbb{Q}$ não é completo com respeito à $|\cdot|_\infty$. Então podemos completar $\mathbb{Q}$ com respeito a qualquer uma dessas topologias construindo o anel das sequências de Cauchy e tomando o quociente pelo ideal das sequências cujo limite é 0.

Lema 4.1.17. O completamento de $\mathbb{Q}$ com respeito a qualquer valorização $|\cdot|_p$ para p primo ou ∞ é um corpo topológico. Além disto, seu completamento é exatamente $\mathbb{Q}_p$ se p for primo e $\mathbb{R}$ se $p = \infty$. Finalmente, se p for primo, $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p < 1\}$.

Dem.: O caso $p = \infty$ é assunto para um curso de Análise Real, aqui vamos nos ater ao caso em que p é um número primo. Podemos identificar qualquer número p-ádico $\sum_{i=-m}^{\infty} a_i p^i$ com a sequência de Cauchy (s_n) dada por

$$s_n = \sum_{i=-m}^{n} a_i p^i \in \mathbb{Q}$$

Por outro lado, dado n, toda sequência de Cauchy é eventualmente constante módulo p^n. Então podemos associar tal sequência (s_n) com uma soma

$$\sum_{i=-m}^{n-1} a_i p^i$$

para cada $n \in \mathbb{N}$. Dada esta identificação, podemos tratar $\sum_{i=-m}^{\infty} a_i p^i$ com uma série de potência convergente em $\mathbb{Q}_p$. Sabemos que

$$|\sum_{i=-m}^{\infty} a_i p^i|_p = p^m$$

pela propriedade ultramétrica[1], então

$$y = \sum_{i=-m}^{\infty} a_i p^i \in \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\} \iff m \leq 0 \iff y \in \mathbb{Z}_p$$

Portanto, o inteiros p-ádicos são como descritos acima. ■

Podemos interpretar o corpo dos números p-ádicos $\mathbb{Q}_p$ de três maneiras distintas:

1. Séries de potência formais (Análise);
2. O corpo de frações de $\mathbb{Z}_p$ (Álgebra);
3. O completamento de $\mathbb{Q}$ com respeito a uma norma $|\cdot|_p$ (Topologia)

E este é um dos motivos pelos quais é tão interessante, e até necessário, estudarmos os números p-ádicos. Claro que nesta dissertação, nosso foco maior é a interpretação algébrica, mas sem deixar as outras duas de lado. A seguir faremos dois resultados sobre o anel dos inteiros p-ádicos $\mathbb{Z}_p$, um topológico e o outro algébrico.

Proposição 4.1.18. Dado um primo $p, \mathbb{Z}_p$ é o fecho de $\mathbb{Z}$ em $\mathbb{Q}_p$

Dem.: Se $x \in \mathbb{Z}_p$, escreva $x = \sum_{i=0}^{\infty} a_i p^i$. Então x é o limite da sequência $s_n = \sum_{i=0}^{n} a_i p^i \in \mathbb{Z}$. Por outro lado, se $x \notin \mathbb{Z}_p$, então $|x|_p > 1$, mas nenhuma sequência (y_n) em $\mathbb{Z}$ pode convergir para x, pois $|y_n|_p \leq 1$ para todo n. Portanto, $\mathbb{Z}_p = \overline{\mathbb{Z}}$. ■

[1]Que é uma versão mais forte da desigualdade triangular e diz que $|a+b|_p \leq \max\{|a|_p, |b|_p\}$

Note que $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$. Esta descrição das unidades será útil mais tarde.

Teorema 4.1.19. Dado um primo p

$$\mathbb{Z}_p \cong \frac{\mathbb{Z}[[X]]}{(X-p)}$$

como anéis.

Dem.: Considere a função

$$\begin{aligned} \varphi\colon \mathbb{Z}[[X]] &\to \mathbb{Z}_p \\ \sum_{i=0}^{\infty} a_i X^i &\mapsto \sum_{i=0}^{\infty} a_i p^i \end{aligned}$$

onde a série de potência na direita é convergente pelos resultados anteriores. Pela definição de $\mathbb{Z}_p$, temos que φ é sobrejetiva. Além disto, é um homomorfismo de anéis por construção e $(X-p) \subset \ker\varphi$. Seja $y \in \ker\varphi$. Então $y = \sum\limits_{i=0}^{\infty} a_i X^i$ tal que $\sum\limits_{i=0}^{n} a_i p^i \equiv 0 \mod p^{n+1}$ para todo $n \geq 0$. Para cada n, seja $b_n = -\dfrac{1}{p^{n+1}}(a_0 + a_1 p + \ldots + a_n p^n)$. Então

$$(b_0 + b_1 X + b_2 X^2 + \ldots)(X-p) = (a_0 + a_1 p + a_2 p^2 + \ldots)$$

e $y \in (X-p)$, logo $\ker\varphi = (X-p)$ e pelo primeiro teorema de isomorfismo de anéis segue o resultado. ■

4.2 Completamentos

Agora vamos generalizar a noção de valor absoluto para qualquer corpo K.

Definição 4.2.1. Seja K um corpo. Um valor absoluto em K é uma função $|\cdot| : K \to \mathbb{R}_+$ tal que dados $x, y \in K$ temos que

1. $|x| = 0 \iff x = 0$;
2. $|xy| = |x||y|$;

3. $|x+y| \leq |x| + |y|$.

Observação 4.2.2. O item 3. nos diz que $|\xi_n| = 1$ para qualquer $\xi_n \in K$ tal que $\xi_n^n = 1$.

Definição 4.2.3. Um valor absoluto $|\cdot| : K \to \mathbb{R}_+$ é dito não arquimediano se $|x+y| \leq \max\{|x|, |y|\}$ para todos $x, y \in K$. Caso contrário, $|\cdot|$ é dito arquimediano.

Definições geralmente merecem exemplos, vamos a eles:

Exemplo 4.2.4. O valor absoluto trivial está definido para qualquer corpo K:

$$|x|_0 = \begin{cases} 1 & \text{se } x \neq 0 \\ 0 & \text{se } x = 0 \end{cases}$$

Exemplo 4.2.5. O valor absoluto usual:

$$|x|_\infty = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}$$

é um valor absoluto arquimediano em $\mathbb{Q}$.

Exemplo 4.2.6. Dado qualquer primo $p \in \mathbb{Z}$ o valor absoluto p-ádico da Definição 4.1.12 é um valor absoluto não arquimediano em $\mathbb{Q}$.

O próximo resultado nos fornece uma condição de verificar quando um valor absoluto é não arquimediano.

Lema 4.2.7. Um valor absoluto $|\cdot| : K \to \mathbb{R}_+$ é não arquimediano se, e somente se, $|n \cdot 1_K| \leq 1$ para todo $n \in \mathbb{Z}$.

Dem.: ($\Longrightarrow$) : Direto da Definição 4.2.3.
($\Longleftarrow$) : Dados $x, y \in K$, suponha sem perda de generalidade que $|x| \geq |y|$. Então,

$|x|^k|y|^{n-k} \leq |x|^n$ para todo $k \in \{0, \ldots, n\}$ e temos que

$$\begin{aligned}
|x+y|^n &= |(x+y)^n| \\
&= \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \text{ (pelo teorema binomial)} \\
&\leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k|y|^{n-k} \text{ (pela desigualdade triangular)} \\
&\leq \sum_{i=1}^{n} |x|^n \left(\text{pois} \binom{n}{k} \in \mathbb{Z}\right) \\
&= (n+1)|x|^n
\end{aligned}$$

Então $|x+y| \leq \sqrt[n]{n+1}|x|$. Tendendo $n \to \infty, (n+1)^{\frac{1}{n}}$ converge para 1, então $|x+y| \leq |x|$. Portanto, $|\cdot|$ é não arquimediano. ■

Um corolário direto do Lema 4.2.7 é o seguinte:

Corolário 4.2.8. Num corpo de característica $p > 0$ todo valor absoluto é não arquimediano.

Vamos agora preparar o terreno para o importante teorema de Ostrowski, que caracteriza completamente os completamentos de $\mathbb{Q}$.

Definição 4.2.9. Dois valores absolutos $|\cdot|_1$ e $|\cdot|_2$ em K são ditos equivalentes, e escrevemos $|\cdot|_1 \sim |\cdot|_2$, se eles induzem a mesma topologia em K, isto é, se existem constantes $r, s > 0$ tais que dados $x, y \in K$

$$|x-y|_2 \leq |x-y|_1^r \text{ e } |x-y|_1 \leq |x-y|_2^s$$

Proposição 4.2.10. Sejam $|\cdot|_1$ e $|\cdot|_2$ dois valores absolutos equivalentes não triviais em K. Então existe uma constante $s > 0$ tal que $|x|_1 = |x|_2^s$ para todo $x \in K$.

Dem.: Note que se $|\cdot|_1 \sim |\cdot|_2$ então $x^n \to 0$ em $|\cdot|_1$ se, e somente se, $x^n \to 0$ em $|\cdot|_2$. Isto implica que $|\cdot|_1 < 1$ se, e somente se, $|x|_2 < 1$. Agora seja $y \in K$ tal que $|y|_1 < 1$ e tome $x \in K^\times$ tal que $|x|_1 = |y|_1^\alpha$ para algum $\alpha \in \mathbb{R}$. Sejam $m_i, n_i \in \mathbb{Z}$ sequências de inteiros tais que cada $n_i > 0$ e $\dfrac{m_i}{n_i}$ converge por cima para α, mas $\dfrac{m_i}{n_i} \neq \alpha$ para nenhum i, então $|x|_1 < |y|_1^\alpha < |y|_1^{\frac{m_i}{n_i}}$ para todo i. Logo,

$$\left|\frac{x^{n_i}}{y^{m_i}}\right|_1 < 1 \implies \left|\frac{x^{n_i}}{y^{m_i}}\right|_2 < 1 \implies |x|_2 < |y|_2^{\frac{m_i}{n_i}}$$

Quando $i \to \infty$ temos que $\dfrac{m_i}{n_i} \to \alpha$, então $|x|_2 \leq |y|_2^{\alpha}$. Logo

$$\frac{\log |x|_1}{\log |x|_2} = \frac{\log |y|_1}{\log |y|_2}$$

para todo $x \in K^{\times}$. Isto mostra que a função $s = \dfrac{\log |x|_1}{\log |x|_2}$ é uma função constante. Logo, segue que $|x|_1 = |x|_2^s$ para todo $x \in K$. ■

Um corolário direto da Proposição 4.2.10 é o seguinte:

Corolário 4.2.11. Cada classe de equivalência de valores absolutos num corpo K é caracterizada unicamente pelo conjunto $\{x \in K \mid |x| < 1\}$ para qualquer $|\cdot|$ na classe.

Agora estamos prontos para provar o Teorema de Ostrowski para $\mathbb{Q}$.

Teorema 4.2.12. Todo valor absoluto não trivial $|\cdot|$ em $\mathbb{Q}$ é equivalente a $|\cdot|_p$ para algum primo p se $|\cdot|$ for não arquimediano ou é equivalente a $|\cdot|_\infty$ se $|\cdot|$ for arquimediano.

Dem.: Suponha que $|\cdot| : \mathbb{Q} \to \mathbb{R}_+$ seja não arquimediano. Seja $p \in \mathbb{N}$ minimal tal que $|p| < 1$, que existe pois $|\cdot|$ é não trivial e multiplicativo. O fato de ser multiplicativo implica que podemos tomar p primo. Considere

$$\mathfrak{a} = \{x \in \mathbb{Z} \mid |x| < 1\}$$

que é um ideal de $\mathbb{Z}$ pela propriedade não arquimediana e pelo Lema 4.2.7. Temos que $(p) \subset \mathfrak{a}$ e como (p) é maximal, segue que $\mathfrak{a} = (p)$. Logo, se $a \in \mathbb{Z}$ e $p \nmid a$, $|a| = 1$. Dado qualquer $m \in \mathbb{Z}$ tal que $p \nmid m$, temos que

$$|p^n m| = |p|^n |m| = |p|^n$$

Isto mostra que $|\cdot| = |\cdot|_p^s$ onde s é o único número positivo tal que $|p| = \left(\dfrac{1}{p}\right)^s$. Logo, todos os valores não arquimedianos em $\mathbb{Q}$ são equivalentes a um valor absoluto

p-ádico. O valor absoluto com $s = 1$ é o valor absoluto p-ádico normalizado da Definição 4.1.12. Agora suponha que $|\cdot|$ seja arquimediano e suponha também que dados $m, n \in \mathbb{Z}$ com $m, n > 1$, o valor absoluto satisfaça a seguinte propriedade:

$$|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log n}}$$

Então para $s > 0$ tal que $e^s = |n|^{\frac{1}{\log n}}$, para qualquer $n > 1$, temos que

$$|m| = (|n|^{\frac{1}{\log n}})^{\log m} = e^{s \log m} = m^s = |m|^s$$

Portanto, $|m| = |m|_\infty^s$ e isto vale para todo $m \in \mathbb{Q}$ pela multiplicatividade. Assim, é suficiente verificar que qualquer valor absoluto arquimediano satisfaz a propriedade $|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log n}}$. Fixe $m, n \in \mathbb{Z}$ com $m, n > 1$ e escreva m na base n

$$m = a_0 + a_1 n + \ldots + a_r n^r$$

com $a_i \in \{0, \ldots, n\}$. Note que

$$r \leq \frac{\log m}{\log n}$$

Então

$$\begin{aligned}
|m| &= |a_0 + a_1 n + \ldots + a_r n^r| \\
&\leq \sum_{i=0}^{r} |a_i||n|^i \text{ (pela desigualdade triangular)} \\
&\leq \left(1 + \frac{\log m}{\log n}\right) |n||n|^{\frac{\log m}{\log n}} \\
&= \left(1 + \frac{\log m}{\log n}\right) |n|^{1+\frac{\log m}{\log n}}
\end{aligned}$$

Substituindo m por m^k para $k > 1$, ficamos com

$$|m|^k \leq \left(1 + \frac{k \log m}{\log n}\right) |n|^{1+\frac{k \log m}{\log n}} \implies |m| \leq \left(1 + \frac{k \log m}{\log n}\right)^{\frac{1}{k}} |n|^{\frac{1}{k}+\frac{\log m}{\log n}}$$

Fazendo $k \to \infty$, temos que $|m| \leq |n|^{\frac{\log m}{\log n}}$, ou $|m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{\log n}}$. Mudando os papéis de m e n obtemos a outra desigualdade, provando a propriedade e completando a prova do teorema. ■

O próximo teorema pode ser visto como uma generalização do teorema chinês dos restos.

Teorema 4.2.13. Sejam $|\cdot|_1, \ldots, |\cdot|_n$ valores absolutos não equivalentes em K e tome $a_1, \ldots, a_n \in K$. Então dado $\epsilon > 0$, existe $x \in K$ tal que $|x - a_i|_i < \epsilon$.

Dem.: Se $n = 1$ nada a provar, suponha $n \geq 2$. Como $|\cdot|_1$ e $|\cdot|_n$ não são equivalentes, sabemos que existe $\alpha \in K$ tal que $|\alpha|_1 < 1$, mas $|\alpha|_n \geq 1$. Analogamente, existe $\beta \in K$ tal que $|\beta|_1 \geq 1$ e $|\beta|_n < 1$. Seja $y = \dfrac{\beta}{\alpha}$, então $|y|_1 > 1$ e $|y|_n < 1$. Vamos mostrar que existe algum $z \in K$ tal que $|z|_1 > 1$, mas $|z|_j < 1$ para todo $j \in \{2, \ldots, n\}$. O caso base da indução já foi provado, então tome $z \in K$ tal que $|z|_1 > 1$ e $|z|_j < 1$ para todo $j \in \{2, \ldots, n-1\}$. Se $|z|_n < 1$ nada a provar. Se $|z|_n = 1$, então $z^m y$ vai funcionar para m suficientemente grande. Finalmente, se $|z|_n > 1$ tome $t_m = \dfrac{z^m}{1+z^m}$, então se $m \to \infty, |t_m|_1 \to 1, |t_m|_n \to 1$ e $|t_m|_j \to 0$ para todo $j \in \{2, \ldots, n-1\}$. Logo, $t_m y$ vai funcionar para m suficientemente grande. Agora, dado $z \in K$ tal que $|z|_1 < 1$ para todo $j \in \{2, \ldots, n\}$, considere a mesma sequência t_m. Se $m \to \infty$, temos que

$$|t_m|_1 = \left|\frac{z^m}{1+z^m}\right|_1 = \left|1 - \frac{1}{1+z^m}\right|_1 \to 1$$
$$|t_m|_j = \left|\frac{z^m}{1+z^m}\right|_j \leq |z^m|_j \to 0$$

para todo $j \in \{2, \ldots, n\}$. Então podemos encontrar z_1 tal que $|z_1 - 1|_1 < \epsilon$ e $|z_1|_j < \epsilon$ para todo $j \in \{2, \ldots, n\}$. Repetindo este processo, podemos encontrar $z_2, \ldots, z_n$ com $|z_j - 1|_j < \epsilon$ e $|z_j|_l < \epsilon$ se $l \neq j$. Então o elemento

$$x = a_1 z_1 + \ldots + a_n z_n$$

satisfaz as condições desejadas. ■

Vamos agora relacionar a teoria dos valores absolutos não arquimedianos com as valorizações discretas em K.

Definição 4.2.14. Dado um valor absoluto não arquimediano $|\cdot|$ num corpo K, defina

$$\begin{aligned}
\mathcal{O} &= \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\} = \{x \in K^\times \mid |x| \leq 1\} \cup \{0\} \\
\mathcal{O}^\times &= \{x \in K \mid v(x) = 0\} = \{x \in K \mid |x| = 1\} \\
\mathfrak{m} &= \{x \in K \mid v(x) > 0\} = \{x \in K \mid |x| < 1\} \\
k &= \frac{\mathcal{O}}{\mathfrak{m}}
\end{aligned}$$

chamados, respectivamente, de anel de valorização, grupo de unidades, ideal de valorização e corpo residual de $|\cdot|$.

Exemplo 4.2.15. A partir dos conceitos da Definição 4.2.14 temos a seguinte analogia entre um corpo K com o corpo dos números p-ádicos $\mathbb{Q}_p$.

$(K, \lvert\cdot\rvert)$	$(\mathbb{Q}_p, \lvert\cdot\rvert_p)$
$\mathcal{O}$	$\mathbb{Z}_p$
$\mathcal{O}^\times$	$\mathbb{Z}_p^\times$
$\mathfrak{m}$	$p\mathbb{Z}_p$
k	$\mathbb{F}_p$

Definição 4.2.16. Se K é um corpo com um valor absoluto não arquimediano e valorização discreta associada, chamamos a tripla $(K, |\cdot|, v)$ de corpo de valorização discreta.

Se $(K, |\cdot|, v)$ é um corpo de valorização discreta, temos as cadeias

$$\begin{aligned}
\mathcal{O} \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^3 \supset \dots \text{ (de ideais)} \\
\mathcal{O}^\times \supset U^{(1)} \supset U^{(2)} \supset U^{(3)} \supset \dots \text{ (de subgrupos)}
\end{aligned}$$

onde $U^{(n)} = \{x \in \mathcal{O}^\times / x \equiv 1 \mod \mathfrak{m}^n\} = \{x \in \mathcal{O}^\times / v(x) \geq n\}$

Proposição 4.2.17. Seja $(K, |\cdot|, v)$ um corpo de valorização discreta. Então dado n

1. $\dfrac{\mathcal{O}^\times}{U^{(n)}} \cong \left(\dfrac{\mathcal{O}}{\mathfrak{m}^n}\right)^\times$
2. $\dfrac{U^{(n)}}{U^{(n+1)}} \cong \dfrac{\mathcal{O}}{\mathfrak{m}} = k$

Dem.: 1. O homomorfismo $\mathcal{O}^\times \to \left(\frac{\mathcal{O}}{\mathfrak{m}^n}\right)^\times$ é sobrejetivo e tem núcleo $U^{(n)}$.
2. Seja π um gerador de $\mathfrak{m}$. Então o homomorfismo

$$\begin{aligned} U^{(n)} &\to \frac{\mathcal{O}}{\mathfrak{m}} \\ 1+\pi^n a &\mapsto a \mod \mathfrak{m} \end{aligned}$$

é sobrejetivo com núcleo $U^{(n+1)}$. ■

Se v é uma valorização discreta em K, podemos formar o completamento $\hat{K}$ de K com respeito ao valor absoluto $|\cdot| = |\cdot|_v$. Similar ao Lema 4.1.17, temos:

Lema 4.2.18. Dada uma valorização v num corpo K

1. O completamento $\hat{K}$ com respeito a $|\cdot|$ é um corpo;
2. $|\cdot|$ se estende unicamente a um valor absoluto em $\hat{K}$;
3. K é um subconjunto denso de $\hat{K}$.

Também denotaremos por $|\cdot|$ a única extensão de $|\cdot|$ em $\hat{K}$. Definimos os completamentos do anel de valorização e do ideal de valorização em $\hat{K}$:

$$\begin{aligned} \hat{\mathcal{O}} &= \{x \in \hat{K}^\times \mid |x| \leq 1\} \cup \{0\} \\ \hat{\mathfrak{m}} &= \{x \in \hat{K}^\times \mid |x| < 1\} \end{aligned}$$

e diretamente das definições temos o seguinte lema:

Lema 4.2.19. Dado um valor absoluto $|\cdot|$ em K,

$$\frac{\hat{\mathcal{O}}}{\hat{\mathfrak{m}}} = \frac{\mathcal{O}}{\mathfrak{m}}$$

Seja R um sistema de representantes de $\frac{\mathcal{O}}{\mathfrak{m}}$ tal que $0 \in R$. Então todo elemento de $\hat{K}$ pode ser escrito unicamente como

$$\pi^m(a_0 + a_1\pi + a_2\pi^2 + \ldots)$$

com $a_i \in R$ e $m \leq 0$ e π o gerador do ideal maximal $\mathfrak{m}$. Isto generaliza a construção de $\mathbb{Q}_p$.

Para o resto da seção, seja K um corpo completo com respeito a um valor absoluto discreto não arquimediano $|\cdot|$. O próximo teorema é chamado de lema de Hensel e é um resultado central nesta dissertação, principalmente na próxima seção quando estudaremos os corpos henselianos. Considere também $\overline{f}$ o polinômio f com os coeficientes dados pelas classes de seus coeficientes módulo $\mathfrak{m}$ no corpo residual $k = \dfrac{\mathcal{O}}{\mathfrak{m}}$. Neste caso, dizemos que f é um levantamento de $\overline{f}$.

Teorema 4.2.20. Seja $f(X) \in \mathcal{O}[X]$ um polinômio mônico de grau n e $\overline{f}(X) \in k[X]$ que admite uma fatoração

$$\overline{f}(X) = \overline{g}(X)\overline{h}(X)$$

para $\overline{g}, \overline{h}$ coprimos e mônicos sobre k de graus r e $n-r$, respectivamente. Então

$$f(X) = g(X)h(X)$$

para $g(X), h(X) \in \mathcal{O}[X]$ com $\deg g = r, \deg h = n-r, \overline{g}(X) \equiv g(X) \mod \mathfrak{m}$ e $\overline{h}(X) \equiv h(X) \mod \mathfrak{m}$.

Dem.: A ideia é encontrar $g_k, h_k \in \mathcal{O}[X]$ indutivamente tais que $g_k h_k - f \in \mathfrak{m}^k$ para todo $k \in \mathbb{N}$, satisfazendo as condições $\deg g_k = r, \deg h_k = n-r, \overline{g} \equiv g_k \mod \mathfrak{m}$ e $\overline{h} \equiv h_k \mod \mathfrak{m}$. Para $k = 1$, sejam g_1 e h_1 quaisquer levantamentos mônicos de $\overline{g}, \overline{h} \in \mathcal{O}[X]$ com os graus apropriados. Suponha que g_k, h_k existam. Por hipótese, $(\overline{g}) + (\overline{h}) = (1)$ em $k[X]$ então para todo $\overline{q} \in k[X]$, existem $\overline{a}, \overline{b} \in k[X]$ tais que $\overline{a}\overline{g} + \overline{b}\overline{h} = \overline{q}$. Se $\deg \overline{q} < n$, então podemos tomar $\deg \overline{a} < n-r$ e $\deg \overline{b} < r$. Seja $\mathfrak{m} = (\pi)$ e escreva $g_k h_k - f = q\pi^k$ para algum $q \in \mathcal{O}[X]$ com $\deg q < n$. Agora, sejam $\overline{a}, \overline{b} \in k[X]$ como acima para $\overline{q}$, a redução de q módulo $\mathfrak{m}$. Sejam $a, b \in \mathcal{O}[X]$ levantamentos de $\overline{a}, \overline{b}$ com os mesmos graus e considere

$$g_{k+1} = g_k - \pi^k b \text{ e } h_{k+1} = h_k - \pi^k a$$

Então temos

$$\begin{aligned} g_{k+1}h_{k+1} &= (g_k - \pi^k b)(h_k - \pi^k a) \\ &= g_k h_k - \pi^k b h_k - \pi^k a g_k + \pi^{2k} ab \\ &\equiv g_k h_k - \pi^k (a g_k + b h_k) \mod \pi^{k+1} \\ &\equiv g_k h_k - \pi^k q \mod \pi^{k+1} \\ &\equiv f \mod \pi^{k+1} \text{ por indução} \end{aligned}$$

Portanto, g_{k+1}, h_{k+1} estão construídos. Note que os coeficientes das sequências (g_k) e (h_k) formam uma sequência de Cauchy em K. Como K é completo, cada sequência de coeficientes converge e podemos definir os limites

$$g = \lim_{k\to\infty} g_k \text{ e } h = \lim_{k\to\infty} h_k$$

que existem em $\mathcal{O}[X]$. Basta uma verificação de rotina para ver que g, h são as funções que estávamos procurando. ■

O próximo resultado muitas vezes é chamado de Lema de Hensel, mas na verdade é apenas um caso particular.

Corolário 4.2.21. Se $f(X) \in \mathcal{O}[X]$ é tal que $\overline{f}(X) \in k[X]$ tem uma raiz simples em k então $f(X)$ tem uma raiz simples em $\mathcal{O}$.

Dem.: Basta aplicar o Teorema 4.2.20 com $r = 1$. ■

Boa hora para um exemplo.

Exemplo 4.2.22. Considere $f(X) = X^2 - 14$ em $\mathbb{Z}_5$. Então seu corpo residual é $\mathbb{F}_5$ e

$$X^2 - 14 \equiv (X-2)(X+2) \mod 5$$

Logo, pelo lema de Hensel, $X^2 - 14 = (X - \alpha)(X + \alpha)$ para algum $\alpha \in \mathbb{Z}_5$. Em particular, $\sqrt{14} \in \mathbb{Z}_5$.

Corolário 4.2.23. Para cada primo p, todas as raízes $(p-1)$-ésimas da unidade estão em $\mathbb{Z}_p$.

Dem.: Considere o polinômio $f(X) = X^{p-1} - 1$. Então, $f(X)$ se fatora completamente em $\mathbb{F}_p$ e, em particular, não possui raízes múltiplas. Logo, pelo lema de Hensel, $X^{p-1} - 1$ se fatora completamente em $\mathbb{Z}_p$. Então todas as raízes $(p-1)$-ésimas estão em $\mathbb{Z}_p$. ■

Definição 4.2.24. Um polinômio $f \in \mathcal{O}[X]$ é dito ser primitivo se algum coeficiente de f for uma unidade em $\mathcal{O}$.

Uma versão do lema de Hensel muito útil, cuja prova pode ser encontrada na aula 9 da referência (SUTHERLAND, 2017) é a seguinte:

Teorema 4.2.25. Seja $f(X) \in \mathcal{O}[X]$ um polinômio primitivo tal que $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$ em $k[X]$, com $\overline{g}, \overline{h}$ coprimos. Então, $f(X) = g(X)h(X)$ em $\mathcal{O}[X]$, com $g, h \in \mathcal{O}[X]$ tais que $\deg g = \deg \overline{g}, \deg h = \deg \overline{h}, g \equiv \overline{g} \mod \mathfrak{m}$ e $h \equiv \overline{h} \mod \mathfrak{m}$.

Exemplo 4.2.26. Seja $K = \mathbb{Q}_5$ e considere o polinômio $f(X) = 5X^2 + 8X + 5$. Então, $\overline{f}(X) = 8X$ é uma fatoração coprima em $\mathbb{F}_5$, isto é, existem $g, h \in \mathbb{Z}_5[X]$, cada um de grau 1, tais que $f(X) = g(X)h(X)$.

Corolário 4.2.27. Sejam K um corpo completo não arquimediano e $f(X) = \sum_{i=0}^{n} a_i x^i \in K[X]$ um polinômio irredutível, mônico com $a_0 \in \mathcal{O}$. Então todo $a_i \in \mathcal{O}$.

Dem.: Podemos manipular f para que ele seja primitivo em $\mathcal{O}[X]$. Seja r o menor inteiro tal que $a_r \in \mathcal{O}^\times$. Então

$$\overline{f}(X) \equiv X^r(a_r + \ldots + X^{n-r}) \mod \mathfrak{m}$$

Se $r \in \{1, \ldots, n-1\}$, isto contradiz o Teorema 4.2.25 e a irredutibilidade de f. Se $r = 0$, então a_0 pode ser manipulado para ser uma unidade. Análogo para $r = n$. Em todos os casos, f deve ser primitivo, então todos os coeficientes pertencem a $\mathcal{O}$. ■

4.3 Teoria de ramificação

As propriedades que estamos interessados em estudar podem ser obtidas a partir do Lema de Hensel, então nesta seção vamos enfraquecer a hipótese da completude.

Definição 4.3.1. Um corpo K é henseliano se existir um valor absoluto não arquimediano $|\cdot|$ em K com anel de valorização $\mathcal{O}$ tal que o Lema de Hensel seja válido para polinômios irredutíveis em $\mathcal{O}[X]$.

Exemplo 4.3.2. Pelo Lema de Hensel, corpos de valorização discreta completos são henselianos.

Seja $(K, |\cdot|, v)$ um corpo não arquimediano. Tomando seu completamento $\hat{K}$, podemos considerar a subextensão $K \subset K^h \subset \hat{K}$ dada por

$$K^h = \{\alpha \in \hat{K} \mid \alpha \text{ é separável sobre } K\}$$

Então v e $|\cdot|$ se estendem unicamente em $\hat{K}$ pelo Lema 4.2.18. Denote suas restrições em K^h também por v e $|\cdot|$. Assim, K^h é um corpo não arquimediano com anel de valorização $\mathcal{O}^h = \mathcal{O}_{K^h}$. Note que $\mathcal{O} \subset \mathcal{O}_h \subset \hat{\mathcal{O}}$. Como os grupos de valorização e os corpos residuais de K e $\hat{K}$ são os mesmos, o mesmo ocorre em $\mathcal{O}^h$.

Lema 4.3.3. K^h é henseliano.

Dem.: Podemos fatorar um polinômio mônico $f(X) \in K[X]$ sobre o fecho algébrico $\overline{K}$ de K se pudermos fatorar em qualquer extensão de K. Portanto, o lema de Hensel vale para $\overline{K} \cap \hat{K} = K^{sep} \cap \hat{K} = K^h$. ■

Definição 4.3.4. Dado um corpo não arquimediano $(K, |\cdot|, v)$, o corpo $K^h \subset \hat{K}$ é chamado de henselização de K.

Vamos agora estudar as extensões dos valores absolutos em extensões de corpos henselianos.

Teorema 4.3.5. Sejam K um corpo henseliano e L/K uma extensão algébrica. Então existe um único valor absoluto $|\cdot|_L$ em L que estende $|\cdot|$. Além disto, se L/K for uma extensão finita de grau n, então

$$|x|_L = \sqrt[n]{|N_{L/K}(x)|}$$

e L é completo com respeito a $|\cdot|_L$ se K for completo com relação a $|\cdot|$.

Dem.: Seja $|x|_L = \sqrt[n_0]{|N_{L_0/K}(x)}$ para alguma extensão finita L_0/K contendo x, onde $n_0 = [L_0 : K]$. Temos que $|x|_L$ independe da escolha de L_0, então podemos mostrar o teorema quando L/K é uma extensão finita. Vamos mostrar que $|\cdot|_L$ é um valor absoluto não arquimediano em L. Dados $x, y \in L, |xy|_L = |x|_L|y|_L$ pela multiplicatividade da norma. Além disto, $|x|_L = 0$ se, e somente se, $N_{L/K}(x) = 0$ se, e somente se, $x = 0$. Por fim, dados $\alpha, \beta \in L$ com $|\alpha| \leq |\beta|$, temos que

$$\left|\frac{\alpha}{\beta} + 1\right| \leq \max\left\{\left|\frac{\alpha}{\beta}\right|, 1\right\} = 1 \iff |x| \leq 1 \text{ implica que } |x+1| \leq 1 \text{ para todo } x \in L$$

Logo, basta provar que $\mathcal{O}_L = \{x \in L \mid |x|_L \leq 1\}$ é um anel e é o fecho integral de $\mathcal{O}$ em L. Dado $x \in L$, temos que

$$\begin{aligned}
x \text{ é integral sobre } \mathcal{O} &\iff x^d + \ldots + a_1 x + a_0 = 0 \text{ irredutível com } a_i \in \mathcal{O} \\
&\iff x^d + \ldots + a_1 x + a_0 = 0 \text{ irredutível com } a_i \in K, a_0 \in \mathcal{O} \\
&\iff N_{L/K}(x) \in \mathcal{O} \\
&\iff |N_{L/K}(x)| \leq 1 \\
&\iff |x|_L \leq 1
\end{aligned}$$

Segue que $\mathcal{O}_L$ é o fecho integral de $\mathcal{O}$ em L. Agora, $|x| \leq 1 \iff |x+1| \leq 1$ para todo $x \in L$, então $|\cdot|_L$ é um valor absoluto em L. Para provar a unicidade, suponha que $|\cdot|'_L$ também estenda $|\cdot|$ em L. Seja $\mathcal{O}'_L = \{x \in L \mid |x|'_L \leq 1\}$. Se $x \in \mathcal{O}_L, x \neq 0$, então $f(x) = 0$ para algum polinômio mônico irredutível $f(X) = X^+ \ldots + a_1 X + a_0$ com $a_i \in \mathcal{O}$. Dividindo por x^d, temos $1 + \ldots + a_1 x^{1-d} + a_0 x^{-d} = 0$, que pode ser escrito como

$$1 = -a_{d-1}x^{-1} - \ldots - a_1 x^{1-d} - a_0 x^{-d}$$

Pela propriedade não arquimediana, $|a_i|'_L \leq 1$ para todo i, então se $|x|'_L < 1$ teríamos $|x^{-1}|'_L$, e portanto, a equação acima implicaria que $|1|'_L < 1$, absurdo. Logo, $|x|'_L \leq 1$, isto é, $x \in \mathcal{O}'_L$. Segue que $|\cdot|_L$ e $|\cdot|'_L$ são equivalentes, caso contrário, pelo Teorema 4.2.13 existiria $y \in L$ tal que $|y|'_L > 1$, mas $|y|_L < 1$, o que acabamos de mostrar que é impossível. Como os valores absolutos coincidem em K, eles são iguais. A prova da completude pode ser encontrada no Teorema $II.4.9$ da referência (NEUKIRCH, 2013). ■

Exemplo 4.3.6. O Teorema 4.3.5 pode não funcionar se K não for henseliano. Por exemplo, $K = \mathbb{Q}$ com o valor absoluto 5-ádico $|\cdot| = |\cdot|_5$ não é henseliano. Se $L = \mathbb{Q}(i)$ então podemos definir dois valores absolutos distintos em L:

$$|x|_1 = 5^{-m} \text{ se } x = (1+2i)^m \frac{a}{b} \text{ e } |x|_1 = 5^{-m} \text{ se } x = (1-2i)^m \frac{a}{b}$$

Ambos estendem $|\cdot|_5$ em L, mas não são equivalentes.

A recíproca do Teorema 4.3.5 é verdadeira, isto é, a propriedade da unicidade de extensão de valores absolutos caracteriza os corpos henselianos. Por esse motivo, vamos nos restringir a estudá-los ao invés dos corpos completos.

Teorema 4.3.7. Seja K um corpo não arquimediano tal que $|\cdot|$ se estende unicamente em qualquer extensão algébrica L/K. Então K é henseliano.

Dem.: Vamos provar que K satisfaz o lema de Hensel para polinômios mônicos. Seja $f \in \mathcal{O}[X]$ mônico com termo constante não nulo. Se f for irredutível, seja L/K um corpo de decomposição de f. Por hipótese, $|\cdot|$ se estende unicamente em L, então $\mathcal{O}_L, \mathfrak{m}_L, \pi_L$ e $\lambda = \dfrac{\mathcal{O}_L}{\mathfrak{m}_L}$ estão definidos neste corpo. Observe que qualquer $\sigma \in G = \mathrm{Gal}(L/K)$ preserva $|\cdot|$, caso contrário, $|x|' = |\sigma(x)|$ seria um valor absoluto distinto estendendo $|\cdot|$. Então, G age em $\mathcal{O}_L, \mathfrak{m}_L$ e λ. Seja $\alpha \in L$ uma raiz de $f(X)$. Então a_0 é uma potência $\prod\limits_{\sigma \in G} \sigma(\alpha)$ e

$$|\alpha_0| = \prod_{\sigma \in G} |\sigma(\alpha)|^\mu = |\alpha|^\mu$$

para algum μ. Como $|a_0| \leq 1$, devemos ter $|\alpha| \leq 1$, então $\alpha \in \mathcal{O}_L$. Logo, α tem uma imagem $\overline{\alpha} \in \lambda$. Como cada $\sigma(\alpha) \in \mathcal{O}_L$ e $\sigma \in G$, estas são todas as raízes de f e todas as raízes de $\overline{f}$ em λ devem ser da forma $\overline{\sigma}(\overline{\alpha})$ onde $\sigma \in G$ e $\overline{\sigma}$ é o automorfismo em $\overline{G} = \mathrm{Gal}(\lambda/k)$ induzido por σ. Então todas as raízes de $\overline{f}$ em λ são conjugadas. A única possibilidade é $\overline{f}(X) = \overline{\varphi}(X)^m$ para algum $m \in \mathbb{N}$ e algum polinômio irredutível $\overline{\varphi} \in k[X]$. Seja $f \in \mathcal{O}[X]$ mônico, mas não necessariamente irredutível. Escreva $f = f_1 \dots f_r$ com $f_j \in \mathcal{O}[X]$ mônicos e irredutíveis. Então $\overline{f} = \overline{f_1} \dots \overline{f_r} \in k[X]$ e pelo caso irredutível acima, cada $\overline{f_j}$ é potência de um polinômio irredutível. Se $\overline{f} = \overline{g}\overline{h}$ é uma fatoração mônica coprima em $k[X]$, então

$$\overline{g} = \prod_{j \in J} \overline{f}_j \text{ e } \overline{h} = \prod_{j \notin J} \overline{f}_j$$

para algum $J \subset \{1, \ldots, r\}$. Tome $g = \prod_{j \in J} f_j$ e $h = \prod_{j \notin J} f_j$, temos que $f = gh$ em $\mathcal{O}$. Portanto, K é henseliano. ■

Corolário 4.3.8. Toda extensão algébrica de um corpo henseliano é henseliana. Em particular, toda extensão finita de um corpo henseliano é henseliana.

Dem.: Segue imediatamente da caracterização de corpos henselianos pela unicidade da extensão. ■

Corolário 4.3.9. Seja K um corpo completo não arquimediano e L/K uma extensão algébrica. Então existe um único valor absoluto $|\cdot|_L$ em L que estende $|\cdot|$ e é da forma $|x|_L = \sqrt[n]{|N_{L/K}(x)|}$ se L/K for finita de grau $[L : K] = n$. Além disto, L é completo com respeito a $|\cdot|_L$.

Dem.: Todo corpo completo é henseliano e o resultado segue do Teorema 4.3.5. ■

Sejam K um corpo não arquimediano e L/K uma extensão algébrica. Então, a extensão de valores absolutos a L induz uma valorização estendida

$$\begin{aligned} w \colon L^\times &\to \mathbb{Z} \\ \alpha &\mapsto v(N_{L/K}(\alpha)) \end{aligned}$$

Além disto, se K for um corpo henseliano então w é a única valorização em L que estende v.

Definição 4.3.10. Sejam K um corpo henseliano com valorização v e L uma extensão algébrica de K com valorização w. O índice de ramificação é

$$e = e_{L/K} = [w(L^\times) : v(K^\times)]$$

e o grau de inércia é

$$f = f_{L/K} = [\lambda : k]$$

onde $\lambda = \dfrac{\mathcal{O}_L}{\mathfrak{m}_L}$.

Note que se v for uma valorização discreta e w sua extensão em L/K, temos que

$$w(\pi_L^e) = ew(\pi_L) = v(\pi_K) = w(\pi_K)$$

e então $(\pi_L^e) = (\pi_K)$ em $\mathcal{O}_L$, isto é, $\mathfrak{m}_L^e = \mathfrak{m}_K\mathcal{O}_L$. Em particular, isto coincide com a teoria de ramificação do capítulo anterior, pois um anel de valorização discreta é um domínio de Dedekind local.

Proposição 4.3.11. Sejam K um corpo henseliano, L/K uma extensão finita e $e = e_{L/K}$ e $f = f_{L/K}$ o índice de ramificação e o grau de inércia, respectivamente. Então, $[L : K] \geq ef$, com igualdade se, e somente se, v é uma valorização discreta e L/K é separável.

Dem.: Sejam $v_1, \ldots, v_f \in \mathcal{O}_L$ cujas reduções módulo $\mathfrak{m}_K$ formam uma base para λ/k. Sejam também $\pi_0, \pi_1, \ldots, \pi_{e-1} \in L^\times$ tais que $w(\pi_0), w(\pi_1), \ldots, w(\pi_{e-1})$ são representantes de $\dfrac{w(L^\times)}{v(K^\times)}$. Vamos provar que os produtos $v_i\pi_j$ são linearmente independentes sobre K. Suponha que

$$\sum a_{ij}v_i\pi_j = 0$$

com $a_{ij} \in K$ não todos nulos. Tomando os termos de valorização minimal nesta soma, basta mostrar que a soma destes termos tem a mesma valorização que cada um individualmente. Observe que todos estes termos devem ter o mesmo índice j, pois

$$w(a_{ij}v_i\pi_j) = w(a_{ij}) + w(\pi_j) \equiv w(\pi_j) \mod w(K^\times)$$

e então índices diferentes correspondem a valorizações diferentes. Fixe j e considere

$$\sum_{i\in I} a_{ij}v_j\pi_j$$

onde $I \subset \{1, \ldots, f\}$ corresponde ao subconjunto dos termos de valorização minimal. Então $w(a_{ij})$ é constante sobre $i \in I$, digamos $w(a_{ij}) = a$, então $a_{ij} = cb_{ij}$ para certos $c \in K^\times$ e b_{ij} tal que $w(b_{ij}) = 0$. Logo,

$$c\pi_j \sum b_{ij}v_j \not\equiv \mod \mathfrak{m}_L$$

pois $\overline{v}_1, \ldots, \overline{v}_f$ formam uma base para λ/k. Então

$$w(\sum a_{ij}v_i\pi_j) = w(c\pi_j) = w(a_{ij}) = a$$

e a independência linear está provada. Agora suponha que v seja discreta e que L/K seja separável. Então cada $\pi_j = \pi_L^j$. Defina os $\mathcal{O}_L$-submódulos

$$M = \sum \mathcal{O}_K v_i \pi_j = \sum \mathcal{O}_K w_i \pi_L^j$$
$$N = \sum \mathcal{O}_K v_i$$

Então $M = N + \pi_L N + \ldots + \pi_L^{e-1} N$. Vamos mostrar que $M = \mathcal{O}_L$.

$$\begin{aligned}
\mathcal{O}_L &= N + \pi_L \mathcal{O}_L \\
&= N + \pi_L(N + \pi_L \mathcal{O}_L) \\
&= N + \pi_L(N + \pi_L(N + \pi_L \mathcal{O}_L)) \\
&= N + \pi_L N + \pi_L^2 N + \ldots + \pi_L^{e-1} N + \pi_L^e \mathcal{O}_L \\
&= M + \pi_L^e \mathcal{O}_L = M + \pi_K \mathcal{O}_L
\end{aligned}$$

Como $\mathcal{O}_K$ é um anel local e L/K é separável, $\mathcal{O}_L$ é um $\mathcal{O}_K$-módulo finitamente gerado. Pelo lema de Nakayama, $\mathcal{O}_L = M$. Portanto, $[L : K] = ef$. ■

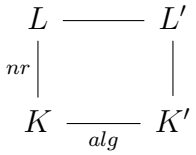
Observação 4.3.12. Para corpos completos com valorizações discretas, a igualdade fundamental da Proposição 4.3.11 vale sem a condição de L/K ser separável.

Seja K um corpo henseliano com anel de valorização $\mathcal{O}_K$, ideal maximal $\mathfrak{m}_K$, corpo de decomposição k e valorização v, e seja L/K uma extensão algébrica com extensões $\mathcal{O}_L, \mathfrak{m}_L, \lambda$ e w dos objetos correspondentes em K.

Definição 4.3.13. Dizemos que uma extensão finita L/K é não ramificada se $f_{L/K} = [L : K]$ e λ/k é separável. Se L/K for infinita, dizemos que a extensão é não ramificada se for união de extensões finitas não ramificadas. Em todos os outros casos, L/K é ramificada.

Note que para uma extensão finita, $f_{L/K} = [L : K]$ implica que $e_{L/K} = 1$.

Proposição 4.3.14. Suponha que L/K seja uma extensão não ramificada, K'/K uma extensão algébrica e $L' = LK'$ o compósito dentro de um fecho algébrico fixado $\overline{K}/K$. Então L'/K' é uma extensão não ramificada.



Dem.: Podemos supor que L/K e K'/K são finitas. Por hipótese, λ/k é separável, e então $\lambda = k(\overline{\alpha})$ para algum $\overline{\alpha} \in \lambda$ pelo teorema do elemento primitivo. Levante $\overline{\alpha}$ a algum $\alpha \in L$. Então

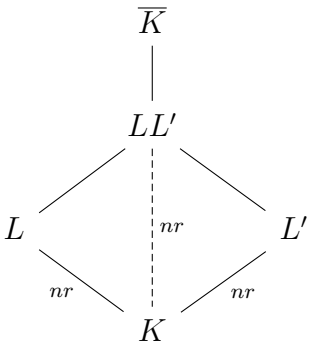
$$[L : K] = f_{L/K} = [\lambda : k] = \deg(\overline{\alpha}) \leq \deg(\alpha) \leq [L : K]$$

o que implica que $\deg(\alpha) = [L : K]$, então $L = K(\alpha)$. Isto significa que $L' = K'(\alpha)$. Seja g o polinômio minimal de α sobre K' e f o polinômio minimal de α sobre K. Como $\overline{f}$ é separável e $g \mid f, \overline{g}$ é separável. Se $\overline{g}$ fosse redutível, g seria redutível pelo lema de Hensel, mas isto é impossível, pois g é um polinômio minimal. Logo, $\overline{g}$ é irredutível sobre $k' = \dfrac{\mathcal{O}_{K'}}{\mathfrak{m}_{K'}}$ e separável. Se λ' é o corpo residual de L', então

$$[\lambda' : k'] \geq \deg \overline{g} = \deg g = [L' : K']$$

Por outro lado, a Proposição 4.3.11 nos diz que $[\lambda' : k'] \leq [L' : K']$, então temos a igualdade. Além disto, λ' é o corpo de decomposição de $\overline{g}$ sobre k', então λ'/k' é separável, e portanto, L'/K' é não ramificada. ■

Corolário 4.3.15. Seja K um corpo de números completo, L, L' extensões algébricas não ramificadas de K e $LL' \subset \overline{K}$ seu compósito dentro de um fecho algébrico $\overline{K}$. Então LL'/K é não ramificada.



Dem.: Suponha que todas as extensões sejam finitas. Para o caso infinito, basta tomar a união das extensões finitas não ramificadas. Pela Proposição 4.3.14, LL'/K e LL'/L são não ramificadas. Além disto, torres de extensões de corpos separáveis são separáveis e f é multiplicativo em torres, segue que

$$f_{LL'/K} = f_{L/K} f_{LL'/L} = [L : K][LL' : L] = [LL' : K]$$

Portanto, LL'/K é não ramificada. ■

Corolário 4.3.16. Se L/K é uma extensão algébrica então existe uma extensão não ramificada maximal $K \subset T \subset L$.

Dem.: Pelo Corolário 4.3.15, podemos tomar T como o compósito dentro de um fecho algébrico $\overline{K}/K$ de todas as extensões não ramificadas L/K. ■

Definição 4.3.17. A extensão não ramificada maximal de um corpo henseliano K é a extensão intermediária maximal de $\overline{K}/K$, denotada por K^{nr}.

Lema 4.3.18. Seja L/K uma extensão algébrica com subextensão não ramificada maximal $K \subset T \subset L$. O corpo residual τ de T é igual ao fecho separável de k em λ.

Dem.: Seja k^{sep} o fecho separável de k em λ e seja τ o corpo residual de T. Temos que $\tau \subset k^{sep} \cap \lambda$. Por outro lado, dado $\overline{\alpha} \in k^{sep} \cap \lambda$ com polinômio minimal $\overline{f}$ sobre k, temos que $\overline{f}$ é separável. Levante $\overline{f}$ a um polinômio mônico f em $L[X]$. Pelo lema de Hensel, f tem uma raiz $\alpha \in L$ levantando $\overline{\alpha}$. Então $K(\alpha)/K$ é não ramificada, pois

$$[K(\alpha) : K] \leq \deg f = \deg \overline{f} = [k(\overline{\alpha}) : k]$$

e $k(\overline{\alpha})/k$ é separável. Portanto, $K(\alpha) \subset T$, e $\overline{\alpha} \in \tau$. ■

Um corolário imediato do Lema 4.3.18 é o seguinte:

Corolário 4.3.19. Em qualquer corpo henseliano K com corpo residual k,

$$K^{nr} \cong k^{sep}.$$

Vamos agora definir o segundo objeto de estudo que dá nome a esta dissertação.

Definição 4.3.20. Seja K um corpo henseliano, com $car(k) = p$ e L/K uma extensão algébrica. Se L/K for finita, λ/k for separável e $p \nmid [L : T]$, onde T é a subextensão não ramificada maximal de L/K, dizemos que L/K é suavemente ramificada. Se L/K for infinita, dizemos que L/K é suavemente ramificada se toda subextensão finita $T \subset M \subset L$ for suavemente ramificada.

Se K for um corpo de característica 0 com corpo residual perfeito k de característica 0, dizer que L/K é suavemente ramificada é o mesmo que dizer que $p \nmid e_{L/K}$.

Lema 4.3.21. Seja L/K uma extensão suavemente ramificada e $e_{L/K} = f_{L/K} = 1$, então $L = K$.

Dem.: Suponha por absurdo que exista $\alpha \in L \setminus K$. Sendo $m = \deg(\alpha)$ e note que $p \nmid m$, pois L/K é suavemente ramificada. Considere $\beta = \alpha - \dfrac{1}{m} Tr_{L/K}(\alpha)$. Então

$$Tr(\beta) = Tr(\alpha) - \frac{1}{m} m Tr(\alpha) = 0$$

Como $e_{L/K} = 1$, existe $b \in K^\times$ com $v(b) = w(\beta)$. Seja $\epsilon = \dfrac{\beta}{b}$. Então $Tr(\epsilon) = 0 = w(\epsilon)$. Além disto, $f_{L/K} = 1$ implica que $\overline{Tr_{L/K}(\epsilon)} = m\bar{\epsilon}$, pois todos os conjugados de ϵ num fecho normal de L/K têm a mesma imagem em $\lambda = k$. Mas $\overline{Tr(\epsilon)} = 0$ implica que $m\bar{\epsilon} = 0$, e isto contradiz o fato de $w(\epsilon) = 0$. Portanto, $L = K$. ■

Temos a seguinte caracterização de extensões suavemente ramificadas num corpo henseliano.

Teorema 4.3.22. Suponha que L/K seja uma extensão finita, com subextensão não ramificada maximal T. Então L/K é suavemente ramificada se, e somente se, L/T for gerada por raízes m-ésimas de elementos de T tais que $car(k) = p \nmid m$.

Dem.: Por definição, L/K é suavemente ramificada se, e somente se, L/T é suavemente ramificada, então podemos supor $K = T$.
$(\implies)$: Seja L/K uma extensão suavemente ramificada com $n = [L : K]$. Então $p \nmid m$. Dado $\alpha \in L$, $w(\alpha) = \dfrac{1}{n} v(N_{L/K}(\alpha))$, e temos que $p \nmid [w(L^\times : v(K^\times)] = e_{L/K}$.

Seja $\beta \in L$ tal que $w(\beta) \notin v(K^\times)$. Seja m a ordem de $w(\beta)$ em $w(L^\times)/v(K^\times)$. Então $p \nmid m$ e podemos escrever $\beta^m = c\epsilon$ para $c \in K$ e $\epsilon \in L$ tal que $w(\epsilon) = 0$. Como $\lambda = k$, podemos supor $\overline{\epsilon} = 1$ em λ. Pelo lema de Hensel, ϵ é uma potência m-ésima em L. Escreva $\epsilon = (\epsilon')^m$ com $\epsilon' \in L$. Portanto, $\left(\frac{\beta}{\epsilon'}\right)^m = c \in K^\times$. Agora, substitua K por $K\left(\frac{\beta}{\epsilon'}\right) = K(\sqrt[m]{c})$ e repita o processo até que $w(L^\times) = v(K^\times)$. Assim, $e_{L/K} = 1 = f_{L/K}$, e portanto, $L = K$ pelo Lema 4.3.21.
$(\Longleftarrow)$: Adjuntando as raízes e aplicando indução, podemos supor que $L = K(\sqrt[m]{a})$ para algum $a \in K$ e $p \nmid m$. Se $m \nmid v(a)$ em $v(K^\times)$, então $e_{L/K} = m$ e $[L : K] = m$. Como $p \nmid m$, isto significa que $f_{L/K} = 1$, e então L/K é suavemente ramificada. Por outro lado, se $m \mid v(a)$ então podemos multiplicar a por uma potência m-ésima de um elemento de K para obter $v(a) = 0$. Assim, $\overline{a}$ é uma potência m-ésima em k, ou $k(\sqrt[m]{\overline{a}})$ é uma extensão inseparável de k, contradizendo $K = T$. Mas $\overline{a} \in (k^\times)^m$ implica que $a \in (k^\times)^m$ pelo segundo lema de Hensel. Portanto, $L = K(\sqrt[m]{a}) = K$, em todos os casos, L/K é suavemente ramificada. ■

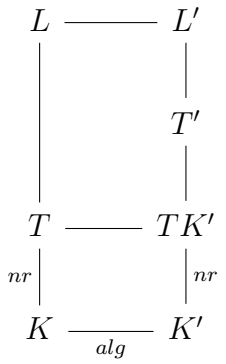
Diretamente do Teorema 4.3.22 temos o seguinte corolário.

Corolário 4.3.23. A igualdade fundamental $[L : K] = ef$ vale para toda extensão finita suavemente ramificada $[L : K]$.

Corolário 4.3.24. Sejam L/K uma extensão suavemente ramificada e K'/K uma extensão algébrica com compósito $L' = LK' \subset \overline{K}$. Então L'/K' também é suavemente ramificada.

$$\begin{array}{ccc} L & \text{———} & L' \\ {\scriptstyle suave}\,\big| & & \big| \\ K & \underset{alg}{\text{———}} & K' \end{array}$$

Dem.: Pelo Corolário 4.3.16, existe uma subextensão não ramificada maximal $K \subset T \subset L$. Então, pela Proposição 4.3.14, TK'/K' também é não ramificada. Seja T' a subextensão não ramificada maximal da extensão L'/K'. Então temos o seguinte diagrama:



Pelo Teorema 4.3.22, L/T é gerada por raízes m-ésimas, e então L'/TK' é gerado por raízes m-ésimas e o mesmo ocorre com L'/T'. Novamente pelo Teorema 4.3.22 segue que L'/K' é suave. ■

Corolário 4.3.25. Sejam L, L' duas extensões algébricas suavamente ramificadas de K. Então seu compósito $LL' \subset \overline{K}$ é suavemente ramificado.

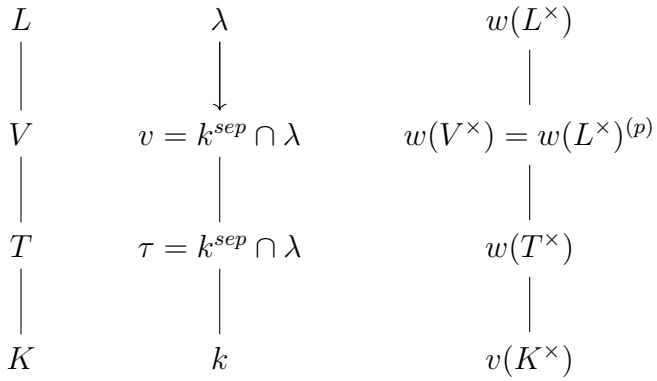
Dem.: A mesma do Corolário 4.3.15. ■

Assim como tínhamos a extensão não ramificada maximal, temos também a extensão suavamente ramificada maximal.

Corolário 4.3.26. Seja L/K uma extensão algébrica. Então existe uma subextensão suavemente ramificada maximal $K \subset V \subset L$.

Definição 4.3.27. A extensão suavemente ramificada maximal de um corpo henseliano K é a extensão suavemente ramificada maximal de $\overline{K}/K$, denotada por K^{suave}.

Em analogia com a torre de corpos de decomposição e inércia no caso geral, temos a seguinte torre de corpos henselianos, com seus respectivos corpos residuais e grupos de valorização.



Para finalizar o texto, vamos ilustrar o que falamos com um importante exemplo. Para maiores detalhes, a página 158 da referência (NEUKIRCH, 2013) pode ser consultada.

Exemplo 4.3.28. Seja $K = \mathbb{Q}_p$ e considere a extensão ciclotômica $K(\xi_n)/K$ com ξ_n uma raiz n-ésima primitiva da unidade. Suponha que $p \nmid n$ e tome $k = \mathbb{F}_q$ onde $p \mid q$. Se $f = ord_n q$, isto é, $q^f \equiv 1 \mod n$, então vamos mostrar que $K(\xi_n)/K$ é não ramificada de grau f. Note que $\mathbb{F}_{q^f}/\mathbb{F}_q$ é a menor extensão de $\mathbb{F}_q$ contendo uma raiz n-ésima da unidade. Seja $g(X)$ o polinômio minimal de ξ_n sobre K. Então g é separável e $\overline{g}$ é irredutível em $\mathbb{F}_q[X]$. Caso contrário, g teria raízes múltiplas, mas todas as raízes n-ésimas da unidade tem reduções distintas em $\mathbb{F}_q^f$, então isto é impossível. Logo, $\deg \overline{g} = f$ e disto $\deg g = f$. Portanto, $K(\xi_n)/K$ é não ramificada de grau f.

Lema 4.3.29. Dado $n \leq 1$, $\mathcal{O}_K(\xi_n) = \mathcal{O}_K[\xi_n]$.

Dem.: Seja $L = K(\xi_n)$. Então $\mathcal{O}_L = \mathcal{O}_K[\xi_n] + \mathfrak{m}_L\mathcal{O}_L$, mas como $\mathcal{O}_L$ e $\mathcal{O}_K$ são anéis locais, pelo Lema de Nakayama temos que $\mathcal{O}_L = \mathcal{O}_K[\xi_n]$. ■

Agora suponha que $p \mid n$. Por simplicidade, considere $n = p^m$ para algum $m \geq 1$.

Lema 4.3.30. A extensão $K(\xi_n)/K$ é totalmente ramificada, com $\mathrm{Gal}(K(\xi_n)/K) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$, $\mathcal{O}_{K(\xi_n)} = \mathbb{Z}_p[\xi_n]$ e $\mathfrak{m}_{K(\xi_n)} = (1 - \xi_n)$, onde $|N(1 - \xi_n)| = p$.

Dem.: Seja

$$\begin{aligned} h(X) &= \frac{(X+1)^n - 1}{(X+1)^{\frac{n}{p}} - 1} = \frac{(X+1)^{p^m} - 1}{(X+1)^{p^{m-1}} - 1} \\ &= 1 + (X+1)^{p^{m-1}} + \ldots + (X+1)^{(p-1)p^{m-1}} \end{aligned}$$

o polinômio minimal de $1 - \xi_n$ sobre K. Então $h(X)$ é um polinômio de Eisenstein cujo coeficiente constante é p. Logo $h(X)$ é irredutível, então

$$\begin{aligned} h(X) &= 1 + (X+1)^{p^{m-1}} + \ldots + (X+1)^{(p-1)p^{m-1}} \\ &= 1 + (X^{p^{m-1}} + 1) + (X^{p^{m-1}} + 1)^2 + \ldots + (X^{p^{m-1}} + 1)^{p-1} + A \text{ com } p \mid A \\ &= X^{(p-1)p^{m-1}} + p + A' \text{ com } p \mid A'. \end{aligned}$$

Assim $\mathrm{Gal}(K(\xi_n)/K) \hookrightarrow (\mathbb{Z}/p^m\mathbb{Z})^\times$ mas ambos os grupos têm ordem $\varphi(p^m) = (p-1)p^{m-1}$, então temos um isomorfismo. Como $1 - \xi_n$ é um elemento primo de $K(\xi_n)$, então é um uniformizador. Além disto

$$N(1 - \xi_n) = \prod_{\sigma \in \mathbb{Z}/p^m\mathbb{Z})^\times} (1 - \sigma(\xi_n)) = h(1) = \pm p.$$

Seja w a extensão de $v = v_p$ de K em $K(\xi_n)$. Então

$$\begin{aligned} w(1 - \xi_n) &= \frac{1}{\varphi(n)} v(N(1 - \xi_n)) \\ &= \frac{1}{\varphi(n)} \cdot v(p) = \frac{1}{\varphi(n)} = \frac{1}{[K(\xi_n) : K]}. \end{aligned}$$

Segue que $e_{K(\xi_n)/K} = [K(\xi) : K]$ e esta extensão é totalmente ramificada. ■

Para o caso geral, seja $n = p^m n'$ onde $p \nmid n'$. Assim, pelo Lema 4.3.29, temos que $\mathcal{O}_{K(\xi_n)} = \mathbb{Z}_p[\xi_n]$, e temos a seguinte torre:

$$\begin{array}{ccccc} L & = & \mathbb{Q}_p(\xi_n) & & \\ | & & | & & \\ V & = & \mathbb{Q}_p(\xi_{pn'}) & = & T(\xi_p) \\ | & & | & & \\ T & = & \mathbb{Q}_p(\xi_{n'}) & & \\ | & & | & & \\ K & = & \mathbb{Q}_p & & \end{array}$$

Considerações finais

Assim como em muitas áreas da ciência, a Matemática está em constante expansão, de modo que as coisas estudadas aqui podem seguir diversos caminhos. Por exemplo, um deles pode ser estudarmos as ramificações selvagens em extensões de corpos henselianos.

Outro caminho seria generalizar o que fizemos aqui em termos de completamento, para além dos corpos de números. Corpos de números são apenas um de dois tipos de corpos globais; os outros são os corpos de funções. Associado a cada corpo global, existe uma coleção infinita de corpos locais que correspondem aos completamentos dos corpos globais com respeito aos seus valores absolutos.

A teoria que estuda a relação entre as extensões de corpos globais e de corpos locais com a aritmética desses corpos é a Teoria de Corpos de Classes, que é uma sequência natural do que estudamos aqui.

Esta teoria busca responder perguntas do tipo: dado um número natural n, quando um número primo pode ser escrito na forma $x^2 + ny^2$? Embora esta questão pareça elementar, ela necessita de ferramentas bastante sofisticadas para ser respondida completamente. Mas isto é assunto para outra hora, quem sabe para uma tese de doutorado?

Referências

ATIYAH, M.; MACDONALD, I. G. *Introduction to commutative algebra*. [S.l.]: CRC Press, 1969. Citado 3 vezes nas páginas 14, 26 e 55.

CASSELS, J.; FRÖHLICH, A. *Algebraic number theory, London*. [S.l.]: Academic Press Inc.[Harcourt Brace Jovanovich Publishers]. Reprint of the . . . , 1986. Citado 2 vezes nas páginas 43 e 62.

ENDLER, O. *Teoria dos números algébricos*. [S.l.]: Instituto de Matemática Pura e Aplicada, CNPq, 1986. v. 15. Citado na página 43.

JANUSZ, G. J. *Algebraic number fields*. [S.l.]: American Mathematical Soc., 1996. v. 7. Citado 2 vezes nas páginas 43 e 62.

MARCUS, D. A.; SACCO, E. *Number fields*. [S.l.]: Springer, 1977. v. 1995. Citado 2 vezes nas páginas 43 e 62.

MILNE, J. S. *Algebraic number theory (v3. 07)*. 2017. Citado 3 vezes nas páginas 43, 55 e 62.

NEUKIRCH, J. *Algebraic number theory*. [S.l.]: Springer Science & Business Media, 2013. v. 322. Citado 4 vezes nas páginas 43, 62, 82 e 92.

SUTHERLAND, A. *18.785 Number Theory I, Fall 2017*. 2017. Citado 3 vezes nas páginas 43, 62 e 80.

TENGAN, E.; FILHO, H. M. B. *Álgebra comutativa em quatro movimentos*. [S.l.]: IMPA, 2015. Citado 7 vezes nas páginas 14, 15, 22, 26, 36, 49 e 62.

WEIL, A. *Basic number theory*. [S.l.]: Springer Science & Business Media, 2013. v. 144. Citado 2 vezes nas páginas 43 e 62.