UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

DAVI NILSON MENDONÇA SOUZA

Equações lineares e quadráticas em corpos métricos

Recife

2025

DAVI NILSON MENDONÇA SOUZA

Equações lineares e quadráticas em corpos métricos

Dissertação apresentada ao Programa de Pós-graduação em Matemática da Universidade Federal de Pernambuco como requisito para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra comutativa

Orientador: Rodrigo José Gondim Neves

Recife

2025

.Catalogação de Publicação na Fonte. UFPE - Biblioteca Central

Souza, Davi Nilson Mendonça.
   Equações lineares e quadráticas em corpos métricos / Davi Nilson Mendonça Souza. - Recife, 2025.
   110f.: il.

   Dissertação (Mestrado) - Universidade Federal de Pernambuco, Centro de Ciências Exatas e da Natureza, Programa de Pós-Graduação em Matemática, 2025.
   Orientação: Rodrigo José Gondim Neves.
   Inclui referências.

   1. Princípio logal-global; 2. Corpos de classe; 3. Problema de Frobenius. I. Neves, Rodrigo José Gondim. II. Título.

UFPE-Biblioteca Central

DAVI NILSON MENDONÇA SOUZA

Equações lineares e quadráticas em corpos métricos

Dissertação apresentada ao Programa de Pós-graduação do Departamento de Matemática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestrado em Matemática.

Aprovada em: 21/02/2025

BANCA EXAMINADORA

Prof. Dr. Rodrigo José Gondim Neves (Orientador)
Universidade Federal Rural de Pernambuco

Prof. Dr. Roberto Carlos Alvarenga da Silva Júnior (Examinador Interno)
Universidade Estadual Paulista

Prof. Dr. Ramon Moreira Nunes (Examinador Externo)
Universidade Federal do Ceará

RESUMO

Esta dissertação visa apresentar o estudo de diferentes ferramentas da Teoria Algébrica dos Números tendo dois objetivos principais. O primeiro sendo compreender em detalhes o Teorema de Hasse-Minkowski para quádricas, que afirma que uma forma quadrática em n variáveis sobre um corpo de números K representa 0 se e somente se representa 0 em cada completamento $K_{\mathfrak{p}}$. Como pré-requisitos para isso, estudamos os números algébricos, a teoria de valoração e a teoria de corpos de classe. O segundo objetivo foi utilizar as ferramentas aprendidas ao longo do estudo para construir uma formulação original e resultados análogos ao problema de Frobenius para domínios com valor absoluto. Este é um problema inicialmente formulado sobre os números inteiros e que diferentes autores buscaram generalizar para outros ambientes matemáticos como polinômios e domínios de integridade.

Palavras-chaves: Números algébricos. p-ádicos. Corpos de classe. Hasse-Minkowski. Princípio local-global. Problema de Frobenius.

ABSTRACT

This dissertation aims to present the study of different tools of Algebraic Number Theory considering two main goals. The first goal was to understand in detail the Hasse-Minkowski Theorem for quadrics, which states a quadratic form in n variables over a number field K represents 0 if and only if it represents 0 in each completion $K_{\mathfrak{p}}$, and as prerequisites for that we studied the algebraic numbers, the valuation theory, and class field theory. The second goal was to use the tools learned to make an original formulation and prove results analogous to Frobenius problem for domains with absolute value. This problem was initially formulated over the integers, and different authors have been trying to generalize it for other mathematical environments such as polynomials and integral domains.

Keywords: Algebraic numbers. p-adics. Class fields. Hasse-Minkowski. Local-global principal. Frobenius problem.

SUMÁRIO

1 INTRODUÇÃO

A teoria dos números é uma área de matemática que busca estudar os números inteiros e os racionais. Alguns dos resultados como o Princípio Fundamental da Aritmética costumam ser provados a partir de argumentos elementares sobre os próprios inteiros sem ser necessário explorar conjuntos maiores. Para outros problemas é possível utilizar uma outra abordagem, como por exemplo, para determinar os números primos p que satisfazem uma equação do tipo

$$p = x^2 + y^2, \quad x, y \in \mathbb{Z},$$

podemos estudar essa equação nos inteiros gaussianos $\mathbb{Z}[i]$ e a partir disso deduzir resultados sobre $\mathbb{Z}$. Em muitos livros introdutórios de Teoria Algébrica dos Números esse é um dos problemas motivadores para se estudar os números algébricos, que é o que estudamos no capítulo 2, embora não exploremos este problema em específico. Buscamos definir o que é um corpo de números, seu anel de inteiros, descrever a estrutura do grupo de unidades do anel de inteiros e o comportamento dos ideais primos (que cumprem papel análogo aos números primos).

Outra técnica para estudar problemas sobre os inteiros, em especial equações diofantinas, é estudar módulo potência de número primo e junto com o Teorema Chinês dos Restos extrapolar para resultados para qualquer inteiro. A partir da necessidade de encontrar números inteiros que satisfaçam uma congruência para cada potência de um número primo p, surgem os números p-ádicos e o valor absoluto p-ádico. Provamos que todo valor absoluto em $\mathbb{Q}$ é equivalente, ou seja, gera a mesma topologia, que o valor absoluto usual de $\mathbb{R}$ ou a mesma topologia do valor absoluto p-ádico e usando este último valor absoluto para completar $\mathbb{Q}$, obtemos o corpo dos números p-ádicos. De forma mais geral, ao longo do capítulo 3 buscamos estudar os corpos com valor absoluto tendo como um dos resultados centrais o Teorema de Classificação de corpos localmente compactos, que afirma que dado um corpo com valor absoluto $(K, |\ |)$, existe um isomorfismo, que também é homeomorfismo, entre $(\hat{K}, |\ |)$ e

(i) $\mathbb{R}$ ou $\mathbb{C}$, se $(K, |\ |)$ é arquimediano;

(ii) uma extensão finita de $\mathbb{Q}_p$ (um corpo $\mathfrak{p}$-ádico), para algum primo p, se $(K, |\ |)$ é não arquimediano.

No capítulo 4, desenvolvemos a Teoria de Corpos de Classe, com a qual conseguimos conectar as duas teorias desenvolvidas nos capítulos anteriores e estudar as extensões abelianas

$L|K$ de corpos de números e de corpos de números $\mathfrak{p}$-ádicos. Com essa teoria conseguimos demonstrar o Teorema da norma de Hasse, segundo o qual numa extensão cíclica de corpos de números $L|K$, a propriedade de um elemento $x \in K^*$ ser norma de um elemento de L é local, ou seja, é equivalente à propriedade de ser norma em qualquer completamento $L_{\mathfrak{P}}|K_{\mathfrak{p}}$. E a partir deste resultado, concluímos o Teorema de Hasse-Minkowski para quádricas, também conhecido como princípio local-global para quádricas, que afirma que uma forma quadrática em n variáveis sobre um corpo de números K representa 0 se e somente se representa 0 em cada completamento $K_{\mathfrak{p}}$.

Por fim, no capítulo 5, a partir das ferramentas desenvolvidas no capítulo 3, buscamos construir formulações originais e encontrar resultados para o problema de Frobenius em domínios com valor absoluto $(D, |\ |)$ de característica 0. Buscando generalizar o problema de Frobenius inicialmente formulado sobre $\mathbb{Z}$ para outros ambientes matemáticos assim como outros autores já fizeram por outras abordagens. Esta parte final do trabalho é a continuação de um estudo iniciado pelo orientador Rodrigo Gondim com o colaborador Ricardo Conceição da Gettysburg College. O problema de Frobenius clássico pode ser sintetizado da seguinte maneira: sejam $k \geq 2$ e $a_1, \ldots, a_k, c \in \mathbb{Z}_{>0}$ com $mdc(a_1, \ldots, a_n) = 1$ e considere uma equação linear

$$a_1x_1 + \cdots + a_kx_k = c$$

em $x_1, \ldots, x_k \in \mathbb{Z}$. Como se comportam as soluções não negativas ($x_i \geq 0, \forall i$) desta equação?

Na nossa formulação para domínios com valor absoluto $(D, |\ |)$, utilizamos a hipótese do completamento $(\hat{K}, |\ |)$ do corpo de frações K de D ser localmente compacto pois assim podemos descrevê-lo pelo Teorema de Classificação. No caso arquimediano real, utilizamos a noção de corpos ordenados arquimedianos e assim teremos uma noção de positividade intrínseca ao domínio D e a partir disso enunciamos e provamos resultados sobre o Problema de Frobenius. No caso não arquimediano, a formulação que propomos foi a seguinte: dado um corpo $(K, |\ |)$ com característica 0 e discreto com valor absoluto não arquimediano. Seja $\mathcal{O}$ seu anel de valoração, $\mathfrak{p}$ seu único ideal maximal. Dados $a_1, \ldots, a_k \in \mathcal{O} \setminus \{0\}$, dizemos que um elemento $c \in \mathfrak{p}^n \setminus \{0\}$ é representável se a equação

$$a_1x_1 + \cdots + a_kx_k = c$$

tem solução em $x_1, \ldots, x_k \in \mathfrak{p}^n \setminus \{0\}$. Provamos que a menor valoração possível de um elemento representável é $\gamma(a_1, \ldots, a_n) = \min_{1 \leq i \leq k} \{v(a_i)\} + n$. Além disso, cada elemento com

uma valoração maior é representável e nenhum elemento com valoração menor é representável. Também provamos alguns resultados sobre a infinitute de representações de um elemento representável fixado.

2 NÚMEROS ALGÉBRICOS

2.1 EXTENSÕES INTEGRAIS E EXTENSÕES DE CORPOS

Definição 1. *Seja $L|K$ uma extensão de corpos de grau n. O traço e a norma de $x \in L$ em K são definidas como o traço e determinante, respectivamente, do operador K - linear*

$$T_x : L \longrightarrow L$$
$$\alpha \longmapsto x\alpha.$$

Denotamos $Tr_{L|K}(x) = Tr(T_x)$ e $N_{L|K}(x) = det(T_x)$. O polinômio característico de x, que denotamos $f_x(t)$ é definido como o polinômio característico de T_x.

Escrevendo

$$f_x(t) = det\,(tI - T_x) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[t],$$

onde $n = [L : K]$ é possível ver que $a_1 = Tr_{L|K}(x)$ e $a_n = N_{L|K}(x)$.

Proposição 1. *Se $L|K$ é uma extensão separável e $\sigma : L \longrightarrow \overline{K}$ percorre os diferentes K-mergulhos de L em um fecho algébrico $\overline{K}$ de K, então*

(i) $f_x(t) = \prod_\sigma (t - \sigma x)$;

(ii) $Tr_{L|K}(x) = \sum_\sigma \sigma x$;

(iii) $N_{L|K}(x) \prod_\sigma \sigma x$.

Demonstração. Ver a proposição 2.6 do capítulo 1 de Neukirch (1999).

□

O **discriminante** de uma base $\alpha_1, \ldots \alpha_n$ de uma extensão separável $L|K$ é definido como

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

onde $\sigma_i, i = 1, \ldots, n$, percorre os K-mergulhos $L \longrightarrow \overline{K}$. Por causa da relação

$$Tr_{L|K}(\alpha_i \alpha_j) = \sum_k (\sigma_k \alpha_i)(\sigma_k \alpha_j),$$

a matriz $(Tr_{L|K}(\alpha_i \alpha_j))$ é o produto das matrizes $(\sigma_k \alpha_i)^t$ e $(\sigma_k \alpha_j)$, então podemos escrever

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

No caso especial de uma base do tipo $1, \theta, \ldots, \theta^{n-1}$ temos que o discriminante é o determinante de uma matriz de Vandermonde

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

onde $\theta_i = \sigma_i \theta$.

Ao longo deste capítulo vamos agora considerar um domínio integralmente fechado A com corpo de frações K e seu fecho integral B em uma extensão finita e separável $L|K$. Se $x \in B$, então todos os seus conjugados σx também estão em B. Como A é integralmente fechado, $A = B \cap K$, logo

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

e

$$x \in B^* \iff N_{L|K}(x) \in A^*.$$

A implicação $(\Rightarrow)$ segue do fato de todos so conjugados estarem em B e portanto também serem unidade. A implicação $(\Leftarrow)$ é provada da seguinte forma: se $aN_{L|K}(x) = 1$ com $a \in A$ então $1 = a \prod_\sigma \sigma x = yx$ com $y \in B$ pois todos os conjugados de x estão em B.

Proposição 2. *Na notação dos parágrafos acima, seja $\alpha_1, \ldots \alpha_n$ uma base de $L|K$ contida em B, de discriminante $d = d(\alpha_1, \ldots, \alpha_n)$. Então*

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

Demonstração. Ver lema 2.9 do capítulo 1 de Neukirch (1999).

□

Um conjunto de elementos $\omega_1, \ldots, \omega_n \in B$ tal que todo $b \in B$ pode ser escrito de maneira única como uma combinação A-linear

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

é chamado de base integral de B sobre A ou uma A-base de B. Já que toda base integral é automaticamente uma base de $L|K$, então $n = [L : K]$.

Proposição 3. *Na notação dos parágrafos anteriores, se $L|K$ é uma extensão finita e separável e A é um domínio de ideais principais, então todo B-submódulo $M \neq 0$ de L, finitamente gerado, é um A-módulo livre de posto $[L : K]$. Em particular, B admite uma base integral sobre A.*

Demonstração. Ver proposição 2.10 do capítulo 1 de Neukirch (1999).

□

Definição 2. *Dizemos que uma extensão finita $K|\mathbb{Q}$ é um corpo de números e definimos o anel de inteiros de K como o fecho integral de $\mathbb{Z}$ em K, que denotamos $\mathcal{O}_K$.*

Se $[K:\mathbb{Q}] = n$, segue da proposição anterior que todo $\mathcal{O}_K$-submódulo finitamente gerado $\mathfrak{a}$ de K admite uma $\mathbb{Z}$-base $\alpha_1, \ldots, \alpha_n$,

$$\mathfrak{a} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n.$$

O discriminante

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

independe da escolha da $\mathbb{Z}$-base pois se $\beta_1, \ldots . \beta_n$ é outra base então a matriz mudança de base e sua inversa possuem coeficientes inteiros logo tem determinante ± 1. Então podemos definir o discriminante de $\mathfrak{a}$

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

No caso especial $\mathfrak{a} = \mathcal{O}_K$, denotamos $d_K = d(\mathcal{O}_K)$ o discriminante do corpo de números K.

Proposição 4. *Se $\mathfrak{a} \subseteq \mathfrak{a}'$ são $\mathcal{O}_K$-submódlos de K finitamente gerados e não nulos, então o índice $(\mathfrak{a}' : \mathfrak{a})$ é finito e satisfaz*

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

Demonstração. Ver teorema 2.12 do capítulo 1 de Neukirch (1999) e teorema 1.17 de Stewart e Tall (2016).

□

É possível mostrar que diferente de $\mathbb{Z}$ o anel de inteiros $\mathcal{O}_K$ de um corpo de números K nem sempre é domínio de fatoração única, por outro lado ele possui uma propriedade análoga interessante: a fatoração única em ideais primos. Vamos estudar essa propriedade e suas consequências para objetos mais gerais, conhecidos como domínios de Dedekind. Outra questão que buscaremos compreender é a estrutura do grupo de unidades $\mathcal{O}_K^*$ e para isso utilizaremos uma abordagem geométrica conhecida como Teoria de Minkowski.

2.2 DOMÍNIOS DE DEDEKIND

2.2.1 Fatoração única em ideais primos

Proposição 5. *Seja $\mathcal{O}_K$ o anel de inteiros de um corpo de números K. Temos que $\mathcal{O}_K$ é noetheriano, integralmente fechado e todo ideal primo $\mathfrak{p} \neq 0$ é ideal maximal.*

Demonstração. Ver teorema 3.1 do capítulo 1 de Neukirch (1999).

□

Definição 3. *Um domínio noetheriano, integralmente fechado em que todo ideal primo é maximal é chamado de domínio de Dedekind.*

Daqui em diante, em vez de considerarmos o anel de inteiros $\mathcal{O}_K$ de um corpo de números K, vamos trabalhar com um domínio de Dededekind $\mathcal{O}$ arbitrário com corpo de frações K.

Lema 1. *Se $\mathfrak{a} \neq 0$ é um ideal de $\mathcal{O}$ então existem ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ tais que*

$$a \supseteq \mathfrak{p}_1 \ldots \mathfrak{p}_r.$$

Demonstração. Segue do fato de $\mathcal{O}$ ser noetheriano. Ver a proposição 7.6.4 de Ash (2006). □

Lema 2. *Seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}$ e definimos*

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

Então $\mathfrak{a}\mathfrak{p}^{-1} := \{\sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a}$, para todo ideal $\mathfrak{a} \neq 0$.

Demonstração. Ver lema 3.5 do capítulo 1 de Neukirch (1999).

□

Teorema 1. *Todo ideal $\mathfrak{a}$ de $\mathcal{O}$ diferente de (0) e (1) admite uma fatoração*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

em ideais primos não nulos $\mathfrak{p}_i$ de $\mathcal{O}$ unicamente determinados a menos de ordem dos fatores.

Demonstração. existência da fatoração em ideais primos: Seja X o conjunto de todos os ideais de $\mathcal{O}$ diferentes e (0) e de (1) que não admitem uma fatoração em produtos de ideais

primos e suponha por absurdo que $X \neq \emptyset$. Como $\mathcal{O}$ é noetheriano, X possui um elemento maximal $\mathfrak{a}$ e seja $\mathfrak{p}$ ideal maximal contendo $\mathfrak{a}$. Como $\mathcal{O} \subseteq \mathfrak{p}^{-1}$, segue que

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

Como $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$ e $\mathfrak{p}$ é ideal maximal, segue que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Como $\mathfrak{a} \neq \mathfrak{p}$ e $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ então $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$ e já que $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$, segue $\mathfrak{a}\mathfrak{p}^{-1}$ admite uma fatoração em ideais primos, sendo assim

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r \Rightarrow \mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p},$$

o que é absurdo.

Unicidade: Se $\mathfrak{a}, \mathfrak{b}, \mathfrak{p}$ forem ideais com $\mathfrak{p}$ primo, então $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ ou $\mathfrak{b} \subseteq \mathfrak{p}$, ou seja

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

Considere agora

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

duas fatorações de $\mathfrak{a}$ em ideais primos. Então $\mathfrak{p}_1|\mathfrak{q}_i$ para algum i, digamos $\mathfrak{q}_1$ e como $\mathfrak{q}_1$ é maximal, segue que $\mathfrak{p}_1 = \mathfrak{q}_1$. Como $\mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$, temos que

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

e o resultado segue por indução.

□

Proposição 6 (Teorema Chinês do Resto)**.** *Sejam $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideais num anel $\mathcal{O}$ tais que $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{O}$ para $i \neq j$. Então se $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i$, temos que*

$$\mathcal{O}/\mathfrak{a} \simeq \bigoplus_{i=1}^{n} \mathcal{O}/\mathfrak{a}_i$$

.

Demonstração. Ver proposição 3.6 do capítulo 1 de Neukirch (1999). □

Definição 4. *Um ideal fracionário de K é um $\mathcal{O}$-submódulo finitamente gerado $\mathfrak{a} \neq 0$ de K. Chamamos os ideais fracionários contidos em $\mathcal{O}$, ou seja, os ideais de $\mathcal{O}$, de ideais integrais.*

Proposição 7. *Os ideais fracionários, com a operação de multiplicação de ideais, formam um grupo abeliano, o grupo ideal J_K de K. O elemento neutro é $(1) = \mathcal{O}$ e o inverso de $\mathfrak{a}$ é*

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

Demonstração. Ver proposição 3.8 de Neukirch (1999).

□

Corolário 1. *Todo ideal fracionário* $\mathfrak{a}$ *admite uma única representação como produto*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}},$$

com $v_{\mathfrak{p}} \in \mathbb{Z}$ *e* $v_{\mathfrak{p}} = 0$ *para quase todo* $\mathfrak{p}$*.*

Demonstração. Ver corolário 3.9 do capítulo 1 de Neukirch (1999).

□

Os ideais fracionários principais $(a) = a\mathcal{O},\ a \in K^*$ formam um subgrupo de J_K que denotamos P_K e definimos o grupo de classes de ideias (ou grupo de classe)

$$Cl_K = J_K/P_K$$

e temos assim a sequência exata

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1.$$

2.2.2 Localização

Definição 5. *Seja* A *um domínio com corpo de frações* K *e seja* $S \subseteq A \setminus \{0\}$ *um subconjunto multiplicativo, ou seja,* $1 \in S$ *e este conjunto é fechado por multiplicação. Definimos a localização de* A *por* S *como o conjunto*

$$AS^{-1} = \left\{ \frac{a}{s} \in K \mid a \in A, s \in S \right\}$$

que é claramente um subanel de K*. O caso mais importante é quando* $S = A \setminus \mathfrak{p}$*, em que* $\mathfrak{p}$ *é um ideal primo de* A*. Neste caso denotamos a localização como* $A_{\mathfrak{p}}$ *e chamamos de localização de* A *em* $\mathfrak{p}$*.*

Proposição 8. *Os mapas*

$$\mathfrak{q} \longmapsto \mathfrak{q}S^{-1} \quad e \quad \mathfrak{Q} \longmapsto \mathfrak{Q} \cap A$$

são correspondências $1-1$*, mutualmente inversíveis, entre os ideais primos* $\mathfrak{q} \subseteq A \setminus S$ *de* A *e os ideais primos* $\mathfrak{Q}$ *de* AS^{-1}

Demonstração. Ver proposição 11.1 do capítulo 1 de Neukirch (1999).

□

Corolário 2. *Se $\mathfrak{p}$ é um ideal primo de A, então $A_{\mathfrak{p}}$ é anel local, ou seja, possui um único ideal maximal, que é $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$.*

Demonstração. Ver corolário 11.2 do capítulo 1 de Neukirch (1999).

□

Perceba que em um anel local A com ideal maximal $\mathfrak{m}$, todo elemento de $a \in A \setminus \mathfrak{m}$ é unidade pois o ideal (a) não está contido em nenhum ideal maximal, logo $(a) = A$.

Definição 6. *Um anel de valoração discreta é um domínio de ideais principais $\mathcal{o}$ com um único ideal maximal $\mathfrak{p} \neq 0$.*

O único ideal maximal é da forma $\mathfrak{p} = (\pi) = \pi\mathcal{o}$, para algum elemento primo $\pi \in \mathcal{o}$. Como todo elemento fora de $\mathfrak{p}$ é unidade e $\mathcal{o}$ é domínio de fatoração única, segue que a menos de elementos associados, π é o único elemento primo de $\mathcal{o}$ e todo elemento de $\mathcal{o}$ pode ser escrito de maneira única na forma $\varepsilon\pi^n$, para algum $\varepsilon \in \mathcal{o}^*$ e $n \geq 0$ e disso segue que todo elemento não nulo $a \in K$ do corpo de frações de $\mathcal{o}$ pode ser escrito de maneira única na forma

$$a = \varepsilon\pi^n, \quad \varepsilon \in \mathcal{o}^*, \quad n \in \mathbb{Z}.$$

O expoente n é chamado de valoração de a e denotamos por $v(a)$. Perceba que $v(a)$ é caracterizado pela equação

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

e assim temos definida uma função

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

que estendemos para todo K pela convenção $v(0) = \infty$. Assim é fácil verificar que esta função satisfaz para todos $a, b \in K$

$$v(ab) = v(a) + v(b), \quad v(a+b) \geq \min\{v(a), v(b)\}.$$

Proposição 9. *Se $\mathcal{o}$ é um domínio de Dedekind e $S \subseteq \mathcal{o} \setminus \{0\}$ é um conjunto multiplicativo, então $\mathcal{o}S^{-1}$ também é um domínio de Dedekind.*

Demonstração. Ver proposição 11.4 do capítulo 1 de Neukirch (1999).

□

Proposição 10. *Se $\mathcal{o}$ é um domínio de Dedekind e $\mathfrak{p} \neq 0$ é um ideal primo, então a localização $\mathcal{o}_\mathfrak{p}$ é um anel de valoração discreta.*

Demonstração. Ver proposição 11.5 do capítulo 1 de Neukirch (1999).

□

Para um domínio de Dedekind $\mathcal{o}$, temos para cada ideal primo $\mathfrak{p} \neq 0$, o anel de valoração discreta $\mathcal{o}_\mathfrak{p}$ e a valoração correspondente

$$v_\mathfrak{p} : K^* \longrightarrow \mathbb{Z},$$

onde K é o corpo de frações de $\mathcal{o}$, que é também o corpo de frações de $\mathcal{o}_\mathfrak{p}$. Agora note que se $x \in K^*$ e

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

é a fatoração em ideais primos do ideal fracionário principal gerado por x, então afirmamos que para cada $\mathfrak{p}$, temos que

$$v_\mathfrak{p} = v_\mathfrak{p}(x).$$

Com efeito, fixado um ideal primo não nulo $\mathfrak{q}$ de $\mathcal{o}$, como para $\mathfrak{p} \neq \mathfrak{q}$, temos que $\mathfrak{p}\mathcal{o}_\mathfrak{q} \neq \mathcal{o}_\mathfrak{q}$, segue que

$$x\mathcal{o}_\mathfrak{q} = \left(\prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}}\right) \mathcal{o}_\mathfrak{q} = \mathfrak{q}^{v_\mathfrak{q}}\mathcal{o}_\mathfrak{q} = {\mathfrak{m}_\mathfrak{q}}^{v_\mathfrak{q}},$$

portanto, $v_\mathfrak{q}(x) = v_\mathfrak{q}$.

2.2.3 Ramificação de ideais primos

Proposição 11. *Seja $\mathcal{o}$ um domínio de Dedekind com corpo de frações K, seja $L|K$ uma extensão finita e $\mathcal{O}$ o fecho integral de $\mathcal{o}$ em L. Então*

(i) $\mathcal{O}$ é integralmente fechado;

(ii) Todo ideal primo não nulo $\mathfrak{P}$ de $\mathcal{O}$ é maximal;

(iii) Se $L|K$ for separável, então $\mathcal{O}$ é um $\mathcal{o}$-módulo finitamente gerado;

(iv) Se $L|K$ for separável, então $\mathcal{O}$ é noetheriano e junto com (i) e (ii), temos que $\mathcal{O}$ é Dedekind.

É possível provar através de outros métodos que o item (iv) é verdade mesmo que $L|K$ não seja separável mas não precisaremos disso ao longo deste trabalho. Para uma demonstração desse fato, ver a proposição 12.8 do capítulo 1 de Neukirch (1999).

Demonstração. (i) Como $\mathcal{O}$ é o fecho integral de o em L e L é o corpo de frações de $\mathcal{O}$, então $\mathcal{O}$ é integralmente fechado. (ii) Agora seja $\mathfrak{P}$ um ideal primo de o, então $\mathfrak{p} = \mathfrak{P} \cap o$ é um ideal primo de o e é não nulo, pois se $y \in \mathfrak{P} \setminus \{0\}$ e $f(X) \in o[X]$ é seu polinômio mínimo, então $f(0) \in \mathfrak{P} \cap o \setminus \{0\}$. Agora seja $\alpha \in \mathcal{O}$, então

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

com $a_0, \ldots a_{n-1} \in o$ e passando ao quociente módulo $\mathfrak{P}$, deduzimos que

$$\frac{o}{\mathfrak{p}}(\overline{\alpha}) = \frac{o}{\mathfrak{p}}[\overline{\alpha}] \subseteq \frac{\mathcal{O}}{\mathfrak{P}},$$

logo $\overline{\alpha}^{-1} \in \frac{o}{\mathfrak{p}}(\overline{\alpha}) \subseteq \frac{o}{\mathfrak{P}}$, portanto $\mathcal{O}/\mathfrak{P}$ é corpo, ou seja, $\mathfrak{P}$ é ideal maximal.

(iii) Supondo que a extensão $L|K$ é separável, seja $\alpha_1, \ldots, \alpha_n$ uma base de $L|K$ contida em $\mathcal{O}$ de discriminante de $d = d(\alpha_1, \ldots, \alpha_n)$. Sabemos de 2 que

$$\mathcal{O} \subseteq o\frac{\alpha_1}{d} + \cdots + o\frac{\alpha_n}{d}$$

e do lado direito temos um o-módulo noetheriano pois é finitamente gerado sobre um anel noetheriano, logo $\mathcal{O}$ é também um o-módulo finitamente gerado. Por fim (iv), segue do fato de $\mathcal{O}$ ser um módulo finitamente gerado sobre o anel noetheriano o, logo $\mathcal{O}$ é um o-módulo noetheriano. Se $\mathfrak{a}$ é um ideal de $\mathcal{O}$, então é um o-submódulo, logo é finitamente gerado sobre $o \subseteq \mathcal{O}$, e também sobre $\mathcal{O}$. Sendo assim, $\mathcal{O}$ é anel noetheriano. □

No que segue, além do domínio de Dedekind o com corpo de frações K, vamos considerar também uma extensão finita $L|K$ e $\mathcal{O}$, o fecho integral de o em L, que sabemos ser domínio de Dedekind e claramente L é seu corpo de frações. Se $\mathfrak{p}$ for um ideal primo não nulo de o, temos que $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$. Com efeito, tome $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, logo $\pi o = \mathfrak{p}\mathfrak{a}$ com $\mathfrak{p} \nmid \mathfrak{a}$, logo $\mathfrak{p} + \mathfrak{a} = o$. Escrevendo $1 = b + s$, com $b \in \mathfrak{p}$ e $s \in \mathfrak{a}$, temos que $s \notin \mathfrak{p}$ e $s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi o$. Suponha por absurdo que $\mathfrak{p}\mathcal{O} = \mathcal{O}$, então teríamos que $s\mathcal{O} = s\mathfrak{p}\mathcal{O} \subseteq \pi\mathcal{O}$, logo $s = \pi x$, com $x \in \mathcal{O} \cap K = o$, logo $x \in \mathfrak{p}$, o que é absurdo.

Escrevemos

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

com cada $\mathfrak{P}_i$ ideal primo de $\mathcal{O}$. Note que os ideais primos $\mathfrak{P}_i$ ocorrendo na fatoração de $\mathfrak{p}\mathcal{O}$ são precisamente os ideais primos $\mathfrak{P}$ de $\mathcal{O}$ que estão sobre $\mathfrak{p}$ ou seja, tais que

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

O expoente $e_i = e(\mathfrak{P}_i|\mathfrak{p})$ é chamado de índice de ramificação de $\mathfrak{P}_i$ sobre $\mathfrak{p}$ e o grau da extensão

$$f_i = f(\mathfrak{P}_i|\mathfrak{p}) = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$$

chamamos de grau de inércia de $\mathfrak{P}_i$ sobre $\mathfrak{p}$. Se a extensão $L|K$ for separável, então os números e_i, f_i e o grau $n = [L : K]$ estão relacionados da seguinte forma:

Teorema 2. *Seja $L|K$ extensão separável. Então temos a identidade fundamental*

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

Demonstração. Pelo Teorema Chinês dos restos, temos que

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

e tanto $\mathcal{O}/\mathfrak{p}\mathcal{O}$ quanto $\mathcal{O}/\mathfrak{B}_i^{e_i}, i = 1, \ldots, r$ são espaços vetoriais sobre o corpo $\kappa = o/\mathfrak{p}$, então basta mostrar que

$$dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n \quad \text{e} \quad dim_\kappa(\mathcal{O}/\mathfrak{B}_i^{e_i}) = e_i f_i, \ i = 1, \ldots, r.$$

$\underline{dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n}$: Como a extensão $L|K$ é separável, sabemos que $\mathcal{O}$ é um o-módulo finitamente gerado, logo $dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) < \infty$. Seja $\overline{w}_1, \ldots, \overline{w}_m$ uma κ-base de $\mathcal{O}/\mathfrak{p}\mathcal{O}$, então basta provarmos que $w_1, \ldots, w_m$ é uma base de $L|K$. Suponha por absurdo que esses vetores são LD sobre K e logo sobre o, então existem $a_1, \ldots, a_m \in o$ não todos nulos tais que

$$a_1 w_1 + \cdots a_m w_m = 0.$$

Considere o ideal $\mathfrak{a} = (a_1, \ldots, a_m)$ de o e escolha $a \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{p}$, logo $a\mathfrak{a} \not\subseteq \mathfrak{p}$, pois caso contrário existiria um ideal $\mathfrak{b}$ de o tal que

$$\mathfrak{p}\mathfrak{b} = (a)\mathfrak{a} \Rightarrow (a) = \mathfrak{a}^{-1}\mathfrak{p}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{p},$$

o que seria absurdo. Sendo assim os elementos $aa_1, \ldots, aa_m$ estão todos em o mas algum não está em $\mathfrak{p}$, logo módulo $\mathfrak{p}$ teríamos a seguinte relação de dependência linear não trivial

$$\overline{aa_1}.\overline{w_1} + \cdots \overline{aa_m}.\overline{w_m} = \overline{0}, \tag{2.1}$$

o que é absurdo.

Agora vamos provar que os w_i geram L como K-espaço vetorial. Considere os módulos

$$M = \mathfrak{o}w_1 + \cdots + \mathfrak{o}w_m \text{ e } N = \mathcal{O}/M.$$

Como $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, temos que $\mathfrak{p}N = N$. Como $L|K$ é separável, sabemos que $\mathcal{O}$ é um $\mathfrak{o}$-módulo finitamente gerado, logo N também é. Se $\alpha_1, \ldots, \alpha_s$ é um conjunto de geradores de N sobre $\mathfrak{o}$, então

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

com $a_{ij} \in \mathfrak{p}$. Denote $A = (a_{ik}) - I_s$, logo

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$$

e como $A \cdots adj(A) = det(A) \cdots I_s$, segue que $det(A)\alpha_i = 0, \forall i$, logo $dN = 0$, logo

$$d\mathcal{O} \subseteq M = \mathfrak{o}w_1 + \cdots \mathfrak{o}w_m.$$

Então se $x \in L$, escrevemos $x = \alpha/\beta$ com $\alpha, \beta \in \mathcal{O}$ e teremos que

$$x = \frac{1}{d\beta} d\alpha = \frac{1}{d\beta} \sum_{i=1}^{s} c_i w_i = \sum_{i=1}^{s} \frac{c_i}{d\beta} w_i,$$

com $c_i \in \mathcal{O}$, logo $c_i/d\beta \in K$.

$\underline{dim_\kappa(\mathcal{O}/\mathfrak{B}_i^{e_i}) = e_i f_i,\ i = 1, \ldots, r}$: Considere a cadeia descendente

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)$$

de κ-espaços vetoriais. Se mostrarmos que os quocientes sucessivos $\mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}, v = 0, \ldots, e_i - 1$, são todos κ-isomorfos a $\mathcal{O}/\mathfrak{P}_i$ como espaços vetoriais, teremos que

$$dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{v=0}^{e_i-1} dim_\kappa(\mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}) = e_i f_i.$$

Mostremos agora os isomorfismos. Para cada $v \in \{0, \ldots, e_i - 1\}$, escolha $\alpha \in \mathfrak{P}_i^v \setminus \mathfrak{P}_i^{v+1}$, então a aplicação

$$\mathcal{O} \longrightarrow \mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}, \quad a \longmapsto a\alpha$$

é homomorfismo de $\mathfrak{o}$-módulos de núcleo $\mathfrak{P}_i$ e é sobrejetiva pois $\mathfrak{P}_i^v = \alpha\mathcal{O} + \mathfrak{P}_i^{v+1}$. Logo temos um isomorfismo

$$\mathcal{O}/\mathfrak{P}_i \longrightarrow \mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}$$

de $\mathfrak{o}$-módulos que também é isomorfismo de κ-módulos. □

Definição 7. *Seja $L|K$ uma extensão separável e seja $\theta \in \mathcal{O}$ com polinômio mínimo $p(X) \in o[X]$. Definimos o condutor do anel $o[\theta]$ como o maior ideal $\mathfrak{F}$ de $\mathcal{O}$ que está contido em $o[\theta]$. Ou seja,*

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

Como $\mathcal{O}$ é um o-módulo finitamente gerado, temos que $\mathfrak{F} \neq 0$.

Proposição 12. *Seja $\mathfrak{p}$ um ideal primo de o com $\mathfrak{p}\mathcal{O}$ relativamente primo com o condutor $\mathfrak{F}$ de $o[\theta]$ e seja*

$$\overline{p}(X) = \overline{p_1}(X)^{e_1} \cdots \overline{p_r}(X)^{e_r},$$

a fatoração do polinômio $\overline{p}(X) = p(X) \ mod \ \mathfrak{p}$ em fatores irredutíveis $\overline{p_i}(X) = p_i(X) \ mod \ \mathfrak{p}$ sobre o corpo de resíduos $o/\mathfrak{p}$ com $p_i(X) \in o[X]$ mônico. Então

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

são os diferentes ideais primos de $\mathcal{O}$ sobre $\mathfrak{p}$. O grau de inércia f_i de $\mathfrak{P}_i$ é o grau do polinômio $\overline{p_i}(X)$ e

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Demonstração. Ver proposição 8.3 do capítulo 1 de Neukirch (1999).

□

Definição 8. *Diz-se que o ideal primo $\mathfrak{p}$ se decompõe totalmente/completamente sobre L (ou é totalmente/completamente decomponível) se na decomposição*

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

tivermos $r = n = [L : K]$, logo $e_i = f_i = 1$ para todo $i = 1, \ldots, r$. O ideal $\mathfrak{p}$ é dito indecomponível ou que não se decompõe se $r = 1$, ou seja, se há um único ideal primo de L sobre $\mathfrak{p}$.

Definição 9. *Seja $\mathfrak{p}$ um ideal primo de o. Na decomposição $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, o ideal primo $\mathfrak{P}_i$ é dito não ramificado sobre o ou sobre K se $e_i = 1$ e se a extensão dos corpos de resíduos $\mathcal{O}/\mathfrak{P}_i|o/\mathfrak{p}$ for separável. Se não, dizemos que é ramificado e dizemos ser totalmente ramificado se também tivermos $f_i = 1$. Dizemos que o ideal primo $\mathfrak{p}$ não se ramifica em L (ou que é não ramificado em L) se todos os $\mathfrak{P}_i$ forem não ramificados e caso contrário é dito que se ramifica (ou que é ramificado). A extensão $L|K$ é dita não ramificada se todos os ideais primos $\mathfrak{p}$ de K forem não ramificados.*

Teorema 3. *Se $L|K$ é separável, então existe uma quantidade finita de ideais primos de K que se ramificam em L.*

Demonstração. Seja $\theta \in \mathcal{O}$ um elemento primitivo de $L|K$, ou seja, tal que $L = K(\theta)$ e seja $p(X) \in o[X]$ seu polinômio mínimo. Seja

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

o discrimintante de $p(X)$. Então todo ideal primo $\mathfrak{p}$ de K tal que $\mathfrak{p}\mathcal{O}$ é primo com $d\mathcal{O}$ e com o condutor $\mathfrak{F}$ de $o[\theta]$ é não ramificado, logo a quantidade de ideais primos que se ramificam é finita. Com efeito, o discriminante $\overline{d} = d \mod \mathfrak{p}$ de $\overline{p}$ é não nulo, logo $\overline{p}(X) = p(X)\ mod\ \mathfrak{p}$ não tem raízes repetidas e portanto, todos seus fatores irredutíveis tem multiplicidade 1, ou seja $e_i = 1, \forall i$. E como para cada i, denotado $\overline{\theta} = \theta \mod \mathfrak{P}_i$, temos que

$$\frac{\mathcal{O}}{\mathfrak{P}_i} = \frac{o}{\mathfrak{p}}(\overline{\theta})$$

e $\overline{\theta}$ é separável. Segue que $\mathcal{O}/\mathfrak{P}_i | o/\mathfrak{p}$ é extensão separável. Portanto, $\mathfrak{p}$ é não ramificado. □

2.2.4 Teoria de ramificação de Hilbert

Se $L|K$ for Galoisiana, dado a um elemento no anel de inteiros $\mathcal{O}$ de L, os conjugados σa também estão em $\mathcal{O}$ para todo $\sigma \in G(L|K)$ e se $\mathfrak{P}$ é um ideal primo de $\mathcal{O}$ sobre $\mathfrak{p}$, então é fácil ver que $\sigma\mathfrak{P}$ também é um ideal primo sobre $\mathfrak{p}$ para cada $\sigma \in G(L|K)$. Vamos fixar essa notação ao longo desta subseção.

Proposição 13. *O grupo de Galois $G = G(L|K)$ age transitivamente sobre o conjuntos dos ideais primos $\mathfrak{P}$ de $\mathcal{O}$ sobre $\mathfrak{p}$.*

Demonstração. Ver proposição 9.1 do capítulo 1 de Neukirch (1999).

□

Definição 10. *Se $\mathfrak{P}$ é um ideal primo de $\mathcal{O}$ sobre o ideal primo $\mathfrak{p}$ de K, então o subgrupo*

$$G_{\mathfrak{B}|\mathfrak{p}} = G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

é chamado de grupo de decomposição de $\mathfrak{P}$ sobre K. O corpo fixado

$$Z_{\mathfrak{P}|\mathfrak{p}} = Z_{\mathfrak{P}} = \{x \in L \mid \sigma x = x,\ \forall \sigma \in G_{\mathfrak{P}}\}$$

é chamado de corpo de decomposição de $\mathfrak{P}$ sobre K.

Proposição 14. *Denotando $G = G(L|K)$ o grupo de Galois de uma extensão Galoisiana, o grupo de decomposição $G_{\mathfrak{P}}$ de um ideal primo de $\mathcal{O}$ sobre K goza das seguintes propriedades*

(i) Se σ percorre um sistema completo de representantes das classes laterais de $G/G_{\mathfrak{P}}$, então $\sigma\mathfrak{P}$ percorre os diferentes ideais primos de $\mathcal{O}$ sobre $\mathfrak{p}$, cada um exatamente uma vez. Em particular, o número de ideais primos de $\mathcal{O}$ sobre $\mathfrak{p}$ é $(G : G_{\mathfrak{P}})$;

(ii) $G_{\mathfrak{P}} = 1 \iff \mathfrak{p}$ se decompõe totalmente;

(iii) $G_{\mathfrak{P}} = G \iff \mathfrak{p}$ não se decompõe;

(iv) Se $\sigma \in G$, então $G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}}\sigma^{-1}$. Em particular, no caso das extensões abelianas o grupo de decomposição $G_{\mathfrak{P}}$ é o mesmo para qualquer ideal primo de L sobre $\mathfrak{p}$ então neste caso é comum escrevermos $G_{\mathfrak{p}}$ para nos referirmos a $G_{\mathfrak{P}}$.

Demonstração. (i) Seja $\sigma_1, \ldots, \sigma_r$ um sistema completo de representantes das classes laterais a esquerda de G sobre $G_{\mathfrak{P}}$ e denote $W_{\mathfrak{p}}$ o conjunto dos ideais primos de L sobre $\mathfrak{p}$ e considere a aplicação

$$\{\sigma_1, \ldots, \sigma_r\} \longrightarrow W_{\mathfrak{P}}, \quad \sigma_i \longmapsto \sigma_i\mathfrak{P}.$$

Note que esta função é injetiva, pois se $\sigma_i\mathfrak{P} = \sigma_j\mathfrak{P}$, então $\sigma_i\sigma_j^{-1} \in G_{\mathfrak{P}}$, logo $i = j$. É também sobrejetiva, pois como a ação é transitiva, dado $\mathfrak{P}'$ ideal primo de L sobre $\mathfrak{p}$, existe $\sigma \in G$ tal que $\sigma\mathfrak{P} = \mathfrak{P}'$ e temos $\sigma \sim \sigma_i$ para algum i, logo $\sigma_i\mathfrak{P} = \sigma\mathfrak{P} = \mathfrak{P}'$.

(ii) $G_{\mathfrak{P}} = 1 \iff (G : G_{\mathfrak{P}}) = |G| = [L : K] \iff$ existem $[L : K]$ ideais de L sobre $\mathfrak{p} \iff \mathfrak{p}$ se decompõe totalmente.

(iii) $G_{\mathfrak{P}} = G \iff (G : G_{\mathfrak{P}}) = 1 \iff$ existe um único ideal de L sobre $\mathfrak{p} \iff \mathfrak{p}$ não se decompõe.

(iv) Dados $\sigma, \tau \in G$, temos que $\tau \in G_{\sigma\mathfrak{P}} \Leftrightarrow \tau\sigma\mathfrak{P} = \sigma\mathfrak{P} \Leftrightarrow \sigma^{-1}\tau\sigma\mathfrak{P} = \mathfrak{P} \Leftrightarrow \sigma^{-1}\tau\sigma \in G_{\mathfrak{P}} \Leftrightarrow \tau \in \sigma G_{\mathfrak{P}}\sigma^{-1}$. □

O grupo de decomposição também nos permite compreender a ramificação de ideais primos em extensões separáveis não necessariamente galoisianas. Para isso, primeiro relembramos que se U, V são subgrupos de um grupo G, então podemos definir uma relação de equivalência $\sim$ em G definida da seguinte maneira: dados $\sigma, \sigma' \in G$, dizemos que

$$\sigma \sim \sigma' \iff \exists u \in U, v \in V \text{ tais que } \sigma' = u\sigma v.$$

Note que a classe de equivalência de σ é

$$U\sigma V = \{u\sigma v \mid u \ \in U, v \in V\}$$

e chamamos as classes de equivalências de classes laterais duplas módulo U, V e denotamos o conjunto quociente por $U\backslash G/V$.

Proposição 15. *Seja $L|K$ uma extensão separável arbitrária mergulhada em uma extensão galoisiana $N|K$ com grupo de galois G e denote $H = G(N|L)$. Seja $\mathfrak{p}$ um ideal primo de K e fixe $\mathfrak{P}$ um ideal primo de N sobre $\mathfrak{p}$. Se σ percorre um sistema completo de representantes das classes laterais duplas $H\backslash G/G_{\mathfrak{P}}$, então $(\sigma\mathfrak{P}) \cap L$ percorre os diferentes ideais primos de de L sobre $\mathfrak{p}$, cada um exatamente uma vez.*

Demonstração. Denote por $P_{\mathfrak{p}}$ o conjunto dos ideais primos de L sobre $\mathfrak{p}$ e considere a função

$$H\backslash G/G_{\mathfrak{P}} \longrightarrow P_{\mathfrak{p}}, \quad H\sigma G_{\mathfrak{P}} \longmapsto (\sigma\mathfrak{P}) \cap L$$

que provaremos se tratar de uma bijeção bem definida. Com efeito, para a boa definição, se $\tau = h\sigma g$, com $h \in H, g \in G_{\mathfrak{P}}$, então

$$\sigma^{-1}h^{-1}\tau = g \in G_{\mathfrak{P}} \Rightarrow \sigma^{-1}h^{-1}\tau\mathfrak{P} = \mathfrak{P} \Rightarrow h^{-1}\tau\mathfrak{P} = \sigma\mathfrak{P} \Rightarrow (\sigma\mathfrak{P}) \cap L = (\tau\mathfrak{P}) \cap L,$$

onde a última igualdade segue do fato de que $h^{-1} \in H = G(N|L)$. Para a sobrejetividade, dado um ideal primo $\mathfrak{q}$ de L sobre $\mathfrak{p}$, considere um ideal primo $\mathfrak{P}'$ de N sobre $\mathfrak{q}$ e $\sigma \in G$ tal que $\sigma\mathfrak{P} = \mathfrak{P}'$, então

$$(\sigma\mathfrak{P}) \cap L = \mathfrak{P}' \cap L = \mathfrak{q}.$$

Agora para a injetividade, se $\sigma, \tau \in G$ são tais que $(\sigma\mathfrak{P}) \cap L = (\tau\mathfrak{P}) \cap L$, então $\sigma\mathfrak{P}$ e $\tau\mathfrak{P}$ são ideais primos de N sobre um mesmo ideal primo de L, então $\exists h \in H$ tal que $h\sigma\mathfrak{P} = \tau\mathfrak{P}$, logo

$$\tau^{-1}h\sigma\mathfrak{P} = \mathfrak{P} \Rightarrow \tau^{-1}h\sigma = g \in G_{\mathfrak{P}} \Rightarrow \tau = h\sigma g^{-1} \in H\sigma G_{\mathfrak{P}} \Rightarrow H\tau G_{\mathfrak{P}} = H\sigma G_{\mathfrak{P}}.$$

□

Proposição 16. *Numa extensão galoisiana $L|K$, com grupo de Galois G, se considerarmos a decomposição de um ideal primo $\mathfrak{p}$ de K,*

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

ocorre o fenômeno de todos esses índices de ramificação serem iguais entre si

$$e_1 = \cdots = e_r = e.$$

Assim como todos os respectivos graus de inércia serem iguais entre si

$$f_1 = \cdots = f_r = f$$

e escrevemos

$$\mathfrak{p}\mathcal{O} = \left(\prod_{\sigma} \sigma\mathfrak{P}\right)^e,$$

onde σ percorre um sistema completo de representantes de $G/G_{\mathfrak{P}}$ e $\mathfrak{P}$ é um primo qualquer acima de $\mathfrak{p}$ escolhido.

Demonstração. Escreva $\mathfrak{P} = \mathfrak{P}_1$. Para cada i, existe $\sigma_i \in G$ tal que $\sigma_i\mathfrak{P} = \mathfrak{P}_i$ e um isomorfismo $\sigma_i : \mathcal{O} \longrightarrow \mathcal{O}$, que induz um isomorfismo

$$\mathcal{O}/\mathfrak{P} \longrightarrow \mathcal{O}/\sigma_i\mathfrak{P}, \quad a \ mod \ \mathfrak{P} \longmapsto \sigma_i a \ mod \ \sigma_i\mathfrak{P}$$

e obtemos que $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}], i = 1, \ldots, r$. Além disso, perceba que $\sigma_i(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$, logo

$$\mathfrak{P}^v | \mathfrak{p}\mathcal{O} \Leftrightarrow \sigma_i(\mathfrak{P}^v) | \sigma_i(\mathfrak{p}\mathcal{O}) \Leftrightarrow \mathfrak{P}_i^v | \mathfrak{p}\mathcal{O}$$

e assim, $e_i = e_1, i, \ \forall i$ □

Proposição 17. *Seja $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$ o ideal primo de $Z_{\mathfrak{P}}$ abaixo de $\mathfrak{P}$. Então temos que*

(i) $\mathfrak{P}_Z$ não se decompõe em L, ou seja, $\mathfrak{P}$ é o único ideal primo de L sobre $\mathfrak{P}_Z$;

(ii) $e(\mathfrak{P}|\mathfrak{P}_Z) = e(\mathfrak{P}|\mathfrak{p})$ e $f(\mathfrak{P}|\mathfrak{P}_Z) = f(\mathfrak{P}|\mathfrak{p})$;

(iii) $e(\mathfrak{P}_Z|\mathfrak{p}) = f(\mathfrak{P}_Z|\mathfrak{p}) = 1$.

Demonstração. Ver proposição 9.3 do capítulo 1 de Neukirch (1999).

□

Agora perceba que para cada $\sigma \in G_{\mathfrak{P}}$, temos que $\sigma\mathcal{O} = \mathcal{O}$ e $\sigma\mathfrak{P} = \mathfrak{P}$, logo temos um automorfismo induzido

$$\overline{\sigma} : G_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}}, \quad a \ mod \ \mathfrak{P} \longmapsto \sigma a \ mod \ \mathfrak{P}.$$

Denotando $\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$ e $\kappa(\mathfrak{p}) = \mathcal{o}/\mathfrak{p}$, temos a seguinte proposição.

Proposição 18. *A extensão $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ é normal e o homomorfismo*

$$G_{\mathfrak{P}} \longrightarrow G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})), \quad \sigma \longmapsto \overline{\sigma}$$

é sobrejetivo. Além disso, se $\mathfrak{P}$ é não ramificado e a extensão de corpos de resíduos $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ é separável, então se trata de um isomorfismo.

Demonstração. Ver as proposições 9.4 e 9.6 do capítulo 1 de Neukirch (1999).

□

Definição 11. *O núcleo $I_{\mathfrak{P}|\mathfrak{p}} = I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}|\mathfrak{p}}$ do homomorfismo*

$$G_{\mathfrak{P}} \longrightarrow G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$$

é chamado de grupo de inércia de $\mathfrak{P}$ sobre K. O corpo fixado

$$T_{\mathfrak{P}|\mathfrak{p}} = T_{\mathfrak{P}} = \{x \in L | \sigma x = x, \forall \sigma \in I_{\mathfrak{P}}\}$$

é chamado de corpo de inércia de $\mathfrak{P}$ sobre K.

Temos a torre de corpos

$$K \subseteq Z_{\mathfrak{P}} \subseteq T_{\mathfrak{P}} \subseteq L$$

e a sequência exata

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \longrightarrow G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) \longrightarrow 1.$$

Proposição 19. *$Z_{\mathfrak{P}}$ é a maior subextensão de $L|K$ em que $\mathfrak{p}$ se decompõe totalmente, ou equivalentemente, $Z_{\mathfrak{P}}$ é a maior subextensão de $L|K$ em que o índice de ramificação e o grau de inércia de $\mathfrak{p}$ são ambos iguais a 1.*

Demonstração. Sabemos que $e(\mathfrak{P}_Z|\mathfrak{p}) = e(\mathfrak{P}_Z|\mathfrak{p}) = 1$, logo $\mathfrak{p}$ se decompõe totalmente em $Z_{\mathfrak{P}}$. Agora suponha que tenhamos uma subextensão $K'|K$ de $L|K$ em que $\mathfrak{p}$ se decompõe totalmente e denote $\mathfrak{p}' = \mathfrak{P} \cap K'$, logo temos $G_{\mathfrak{P}|\mathfrak{p}'} = G_{\mathfrak{P}|\mathfrak{p}} \cap G(L|K')$ e $I_{\mathfrak{P}|\mathfrak{p}'} = I_{\mathfrak{P}|\mathfrak{p}} \cap G(L|K')$ e temos o seguinte diagrama de corpos

$$\begin{array}{ccccccc} L & \text{———} & T_{\mathfrak{P}|\mathfrak{p}'} & \text{———} & Z_{\mathfrak{P}|\mathfrak{p}'} & \text{———} & K' \\ & \diagdown & | & & | & & | \\ & & T_{\mathfrak{P}|\mathfrak{p}} & \text{———} & Z_{\mathfrak{P}|\mathfrak{p}} & \text{———} & K. \end{array}$$

Como $\mathfrak{p}$ se decompõe totalmente em K' e a extensão $K'|K$ é separável, então da identidade fundamental segue que $e_{\mathfrak{p}'|\mathfrak{p}} = f_{\mathfrak{p}'|\mathfrak{p}} = 1$ e assim temos que $e_{\mathfrak{P}|\mathfrak{p}'} = e_{\mathfrak{P}|\mathfrak{p}}$ e $f_{\mathfrak{P}|\mathfrak{p}'} = f_{\mathfrak{P}|\mathfrak{p}}$. Da identidade fundamental também é fácil ver que

$$[L : T_{\mathfrak{P}|\mathfrak{p}'}] = e(\mathfrak{P}|\mathfrak{p}'), \qquad [T_{\mathfrak{P}|\mathfrak{p}'} : Z_{\mathfrak{P}|\mathfrak{p}'}] = f(\mathfrak{P}|\mathfrak{p}'),$$

e analogamente,

$$[L : T_{\mathfrak{P}|\mathfrak{p}}] = e(\mathfrak{P}|\mathfrak{p}), \qquad [T_{\mathfrak{P}|\mathfrak{p}} : Z_{\mathfrak{P}|\mathfrak{p}}] = f(\mathfrak{P}|\mathfrak{p}).$$

Portanto,

$$[L : T_{\mathfrak{P}|\mathfrak{p}'}] = [L : T_{\mathfrak{P}|\mathfrak{p}}], \qquad [T_{\mathfrak{P}|\mathfrak{p}'} : \ Z_{\mathfrak{P}|\mathfrak{p}'}] = [T_{\mathfrak{P}|\mathfrak{p}} : Z_{\mathfrak{P}|\mathfrak{p}}]$$

Da identidade do lado esquerdo segue que $T_{\mathfrak{P}|\mathfrak{p}} = T_{\mathfrak{P}|\mathfrak{p}'}$ e assim da identidade do lado direito juntamente com o fato de que $Z_{\mathfrak{P}|\mathfrak{p}} \subseteq Z_{\mathfrak{P}|\mathfrak{p}'}$, concluímos que $Z_{\mathfrak{P}|\mathfrak{p}} = Z_{\mathfrak{P}|\mathfrak{p}'}$. Concluímos que

$$G_{\mathfrak{P}|\mathfrak{p}} \cap G(L|K') = G_{\mathfrak{P}|\mathfrak{p}'} = G_{\mathfrak{P}|\mathfrak{p}} \Rightarrow G_{\mathfrak{P}|\mathfrak{p}} \subseteq G(L|K') \Rightarrow K' \subseteq Z_{\mathfrak{P}|\mathfrak{p}}.$$

□

2.3 TEORIA DE MINKOWSKI

Dado um corpo de números K com $[K : \mathbb{Q}] = n$, na Teoria de Minkowski, se mergulha K num espaço vetorial real de dimensão n. Seguimos a abordagem de Neukirch (1999) de fazer esse mergulho no que chamamos de espaço de Minkowski, onde está definido um produto interno, e assim, uma medida de Haar e uma noção de volume e buscamos utilizar essas noções geométricas e suas propriedades para deduzir propriedas algébricas do corpo de números, como por exemplo, a estrutura do grupo de unidades $\mathcal{O}_K^*$. Existem outras abordagens equivalentes um pouco menos abstratas, como a feita por Stewart e Tall (2016), de mergulhar K diretamente em

$$\mathbb{L}^{rs} = \mathbb{R}^r \times \mathbb{C}^s$$

onde r é a quantidade de mergulhos reais de K e s é o a quantidade de merulhos complexos não reais de K, e utilizar as propriedades geométricas da medida de Lebesgue em $\mathbb{L}^{rs}$.

2.3.1 Reticulados, espaço de Minkowski e o Teorema de Minkowski

Definição 12. *Seja V um espaço vetorial de dimensão n sobre $\mathbb{R}$. Um reticulado em V é um subgrupo da forma*

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

em que os vetores $v_1, \ldots, v_m$ são linearmente independentes sobre $\mathbb{R}$ (em particular $m \leq n$). Note que Γ é um grupo abeliano livre de rank m. A m-upla $(v_1, \ldots, v_m)$ é chamada de uma base e o conjunto

$$\Phi = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

é um domínio fundamental do reticulado. O reticulado é dito completo se $m = n$.

Proposição 20. *Um subgrupo $\Gamma \subseteq V$ é um reticulado se e somente se é discreto.*

Demonstração. Ver proposição 4.2 do capítulo 1 de Neukirch (1999).

□

Proposição 21. *Um reticulado Γ em V é completo se e somente se existe um subconjunto limitado $M \subseteq V$ tal que a coleção das translações $M + \gamma, \gamma \in \Gamma$ cobre todo o espaço V.*

Demonstração. Ver lema 4.3 do capítulo 1 de Neukirch (1999).

□

Seja V um espaço vetorial euclidiano, ou seja, um $\mathbb{R}$-espaço vetorial de dimensão finita n munido de um produto interno $\langle\ ,\ \rangle$. Então esse produto interno induz uma medida de Haar e temos assim a noção de volume em V de tal forma que um cubo gerado por uma base ortonormal $e_1, \ldots, e_n$ tem volume 1 e de forma mais geral, um paralelepípedo gerado por n vetores linearmente independentes $v_1, \ldots, v_n$

$$\Phi = \{x_1v_1 + \cdots x_nv_n \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\}$$

tem volume $vol(\Phi) = |detA|$ onde A é uma matriz de mudança de base de $v_1, \ldots v_n$ para $e_1, \ldots, e_n$. Escrevendo $v_i = \sum_k a_{ik}e_k$, segue que

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

e portanto, temos o invariante

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

Definição 13. *Se Γ é um reticulado gerado pelos vetores $v_1, \ldots, v_n$ de domínio fundamental Φ definimos o volume de Γ como o volume de um domínio fundamental*

$$vol(\Gamma) = vol(\Phi)$$

e este valor independe da escolha da base pois se tomarmos uma outra base, a matriz mudança de base tem entradas inteiras e portanto possui determinante ± 1.

Definição 14. *Dizemso que um subconjunto X de V é*

(i) centralmente simétrico se $\forall x \in V, x \in X \Rightarrow -x \in X$;

(ii) convexo se $\forall x, y \in X$, temos que $\{ty + (1-t)x \mid 0 \leq t \leq 1\} \subseteq X$.

Proposição 22 (Minkowski)**.** *Seja Γ um reticulado completo num espaço vetorial euclidiano V e seja X um subconjunto de V centralmente simétrico e convexo. Suponha que*

$$vol(X) > 2^n vol(\Gamma).$$

Então X contém pelo menos um ponto do reticulado $\gamma \in \Gamma$.

Demonstração. Afirmamos que existem dois pontos distintos do reticulado $\gamma_1, \gamma_2 \in \Gamma$ tais que

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset.$$

Com efeito, suponha por absurdo que todos os conjuntos da forma $\frac{1}{2}X + \gamma$, com $\gamma \in \Gamma$ sejam dois a dois disjuntos, então o mesmo vale para $\Phi \cap (\frac{1}{2}X + \gamma)$, onde Φ é um domínio fundamental de Γ. Sendo assim, teríamos que

$$vol(\Phi) \geq \sum_{\gamma \in \Gamma} vol(\Phi \cap (\frac{1}{2}X + \gamma)) = \sum_{\gamma \in \Gamma} vol((\Phi - \gamma) \cap \frac{1}{2}X) = vol(\frac{1}{2}X) = \frac{1}{2^n} vol(X)$$

o que é um absurdo.

Sendo assim, escolha $\gamma_1, \gamma_2 \in \Gamma$ tais que

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset,$$

então

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2, \ x_1, x_2 \in X$$

e obtemos

$$\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1 \in X \cap \Gamma \setminus \{0\}.$$

□

Vamos considerar o mapa canônico

$$j : K \longrightarrow K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}, \qquad a \longmapsto ja = (\tau a)_{\tau},$$

que resulta dos n mergulhos complexos $\tau : K \longrightarrow \mathbb{C}$. Agora vamos focar no $\mathbb{R}$-espaço vetorial

$$K_{\mathbb{R}} = \left[\prod_{\tau} \mathbb{C}\right]^{+} = \left\{(z_{\tau})_{\tau} \in K_{\mathbb{C}} \mid z_{\overline{\tau}} = \overline{z}_{\tau}\right\},$$

que chamamos **espaço de Minkowski** e note que $j(K) \subseteq K_{\mathbb{R}}$. Vamos denotar

$$\rho_1, \dots \rho_r : K \longrightarrow \mathbb{R}$$

os mergulhos reais e

$$\sigma_1, \overline{\sigma}_1, \cdots, \sigma_s, \overline{\sigma}_s : K \longrightarrow \mathbb{C}$$

os mergulhos complexos. Logo $n = r + 2s$. Escolhemos para cada par de mergulhos complexos conjugados um dos mergulhos, fazemos σ percorrer esses mergulhos escolhidos e fazemos ρ percorrer os mergulhos reais, então podemos perceber que

$$K_{\mathbb{R}} = \left\{(z)_{\tau} \in \prod_{\tau} \mathbb{C} \mid z_{\rho} \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z}_{\sigma}\right\}.$$

Proposição 23. *Temos o seguinte isomorfismo*

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

dado por $(z_{\tau}) \mapsto (x_{\tau})$*, onde*

$$x_{\rho} = z_{\rho}, \ x_{\sigma} = Re(z_{\sigma}), \ x_{\overline{\sigma}} = Im(z_{\sigma}).$$

Este isomorfismo transforma o produto interno canônico $\langle\ ,\ \rangle$ *de de* $K_{\mathbb{R}}$ *no seguinte produto interno*

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

onde $\alpha_{\tau} = 1$ *se* τ *é real e* $\alpha_{\tau} = 2$ *se* τ *é complexo. Ou seja*

$$\langle f(x), f(y)\rangle_{\textit{euclidiano}} = \sum_{\tau} \alpha_{\tau} x_{\tau} y_{\tau}.$$

Demonstração. Ver proposição 5.1 do capítulo 1 de Neukirch (1999).

□

É fácil ver que o produto interno definido acima transfere a medida canônica de $K_{\mathbb{R}}$ para $\mathbb{R}^{r+2s}$ de tal forma que

$$vol_{canônico}(X) = 2^{s} vol_{Lebesgue}(f(X)).$$

Proposição 24. *Se $\mathfrak{a} \neq 0$ é um ideal de $\mathcal{O}_K$, então $\Gamma = j\mathfrak{a}$ é um reticulado completo em $K_{\mathbb{R}}$. Seu domínio fundamental tem volume*

$$vol(\Gamma) = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}).$$

Demonstração. Ver proposição 5.2 do capítulo 1 de Neukirch (1999).

□

Proposição 25. *Seja $\mathfrak{a} \neq 0$ um ideal integral de K e sejam $c_\tau > 0$ constantes reais positivas para cada $\tau \in Hom(K, \mathbb{C})$ tais que $c_\tau = c_{\overline{\tau}}$ e*

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

Então existe $a \in \mathfrak{a}, a \neq 0$ tal que

$$|\tau a| < c_\tau, \ \forall \tau \in Hom(K, \mathbb{C}).$$

Demonstração. Ver teorema 5.3 do capítulo 1 de Neukirch (1999).

□

O grupo multiplicativo $K_{\mathbb{C}}^*$ admite o homomorfismo $N : K_{\mathbb{C}}^* \longrightarrow \mathbb{C}^*$ dado pelo produto das coordenadas e em $\prod_\tau \mathbb{R}$ podemos definir a aplicação $Tr : \prod_\tau \mathbb{R} \longrightarrow \mathbb{R}$ dada pela soma das coordenadas. A aplicação $l : \mathbb{C}^* \longrightarrow \mathbb{R}, \quad z \longmapsto log|z|$ induz um homomorfismo sobrejetivo

$$l : K_{\mathbb{R}} \longrightarrow \prod_\tau \mathbb{R}.$$

Obtemos o diagrama comutativo

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* & \xrightarrow{l} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle N_{L|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{C}^* & \xrightarrow{l} & \mathbb{R} \end{array},$$

que induz o seguinte diagrama comutativo

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & [\prod_\tau \mathbb{R}]^+ \\ \downarrow{\scriptstyle N_{L|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R} \end{array},$$

onde o $\mathbb{R}$-espaço vetorial $[\prod_\tau \mathbb{R}]^+$ é obtido da seguinte forma. Separe como anteriormente os mergulhos $\tau : K \longrightarrow \mathbb{C}$ entre os mergulhos reais $\rho_1, \ldots, \rho_r$ e os pares de mergulhos complexos conjugados $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s$, então

$$\left[\prod_\tau \mathbb{R}\right]^+ = \prod_\rho \mathbb{R} \times \prod_\sigma [\mathbb{R} \times \mathbb{R}]^+,$$

onde $[\mathbb{R} \times \mathbb{R}]^+ = \{(x, x) \mid x \in \mathbb{R}\}$ e identificamos este conjunto com $\mathbb{R}$ através do mapa $(x, x) \mapsto 2x$. Desta forma obtemos um ismorfismo

$$\left[\prod_\tau \mathbb{R}\right]^+ \simeq \mathbb{R}^{r+s}$$

e assim temos o homomorfismo

$$l : K_{\mathbb{R}}^* \longrightarrow \mathbb{R}^{r+s}$$

dado por

$$l(x) = (log|x_{\rho_1}|, \ldots, log|x_{\rho_r}|, log|x_{\sigma_1}|^2, \ldots, log|x_{\sigma_s}|^2).$$

Agora definimos os grupos

$$S = \{y \in K_{\mathbb{R}}^* \mid N(y) = \pm 1\},$$

$$H = \left\{x \in \left[\prod_\tau \mathbb{R}\right]^+ \mid Tr(x) = 0\right\}.$$

Temos então os homomorfismos

$$\mathcal{O}_K^* \xrightarrow{j} S \xrightarrow{l} H$$

e sua composição $\lambda := l \circ j : \mathcal{O}_K^* \longrightarrow H$, cuja imagem será denotada por Γ.

2.3.2 Número de Classe

Como aplicação da teoria de Minkowski vamos provar a finitude do número de classe h_K de um corpo de números K.

Definição 15. *Considere um corpo de números K. Dado um ideal não nulo $\mathfrak{a}$ de $\mathcal{O}_K$, definimos sua norma absoluta como*

$$\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$$

e sabemos que este índice é finito pela proposição 4. No caso de um ideal principal (α) de $\mathcal{O}_K$, tomando $w_1, \ldots, w_n$ uma $\mathbb{Z}$-base de $\mathcal{O}_K$, então $\alpha w_1, \ldots \alpha w_n$ é uma $\mathbb{Z}$-base de (α). Escrevendo

$$\alpha w_i = \sum_{j=1}^{n} a_{ij} w_j, \quad j = 1, \ldots, n,$$

pelo que vimos ao final do capítulo sobre números algébricos, sabemos que $|det(A)| = (\mathcal{O}_K : (\alpha))$ e por definição de norma de um elemento, temos que $|det(A)| = N_{K|\mathbb{Q}}(\alpha)$, portanto

$$\mathfrak{N}((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|,$$

ou seja, a norma absoluta generaliza para ideais a noção de norma de um elemento.

Proposição 26. *Se $\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$ é a fatoração prima de um ideal não nulo $\mathfrak{a} \neq 0$, então temos que*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{v_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{v_r}.$$

Demonstração. Ver proposição 6.1 do capítulo 1 de Neukirch (1999).

□

Dessa proposição segue a multiplicatividade da norma absoluta, ou seja, se $\mathfrak{a}$ e $\mathfrak{b}$ são dois ideais não nulos de $\mathcal{O}_K$, então

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

Além disso, a norma absoluta pode ser estendida naturalmente para um homomorfismo

$$\mathfrak{N} : J_K \longrightarrow \mathbb{R}_+^*$$

definido nos ideais fracionários $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}}, v_\mathfrak{p} \in \mathbb{Z}$.

Lema 3. *Para cada ideal não nulo $\mathfrak{a}$ de $\mathcal{O}_K$ existe um elemento não nulo $a \in \mathfrak{a}$ tal que*

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

Demonstração. Ver lema 6.2 do capítulo 1 de Neukirch (1999).

□

Teorema 4. *O grupo de classes de ideais $Cl_K = J_K/P_K$ é finito. Sua ordem*

$$h_K = (J_K : P_K)$$

é chamada de número de classe de K.

Demonstração. Se $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_K$ e $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, então $\mathcal{O}_K/\mathfrak{p}$ é uma extensão finita do corpo $\mathbb{Z}/p\mathbb{Z}$ e denotando o grau dessa extensão por f, temos que

$$\mathfrak{N}(\mathfrak{p}) = \left|\frac{\mathcal{O}_K}{\mathfrak{p}}\right| = \left|\frac{\mathbb{Z}}{p\mathbb{Z}}\right|^f = p^f.$$

Dado um número primo $p \in \mathbb{Z}$, existe uma quantidade finita de primos $\mathfrak{p}$ de $\mathcal{O}_K$ sobre p, logo existe uma quantidade finita de ideais primos de $\mathcal{O}_K$ cuja norma é limitada por uma cota superior fixada. Como todo ideal admite uma decomposição $\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$, com $v_i > 0$, então dada uma cota superior $M > 0$, existe uma quantidade finita de ideais $\mathfrak{a}$ de $\mathcal{O}_K$ satisfazendo $\mathfrak{N}(\mathfrak{a}) \leq M$.

Para concluirmos a finitude do número de classe, basta provarmos que dada uma classe de ideal $[\mathfrak{a}] \in Cl_K$, ela contém um ideal integral $\mathfrak{a}_l$ satisfazendo

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

Com efeito, escolha um representante $\mathfrak{a}$ arbitrário da classe e um elemento $\gamma \in \mathcal{O}_K \setminus \{0\}$ tal que $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Então pelo lema anterior, existe um elemento não nulo $\alpha \in \mathfrak{b}$ tal que $|N_{K|\mathbb{Q}}(\alpha)| \leq M\mathfrak{N}(\mathfrak{b})$, então tomando $\mathfrak{a}_l = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$ e $\mathfrak{a}_l$ é um ideal integral de tal forma que

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

□

2.3.3 Teorema das unidades de Dirichlet

Agora vamos utilizar a teoria de Minkowski para caracterizar o grupo de unidades $\mathcal{O}_K^*$ do anel de inteiros de um corpo de números K.

Lema 4. *Denote $\mu(K)$ o grupo das raízes da unidade de K. Então a sequência*

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

é exata.

Demonstração. Ver proposição 7.1 do capítulo 1 de Neukirch (1999).

□

Lema 5. *A menos de multiplicação por unidades, existe uma quantidade finita de elementos $\alpha \in \mathcal{O}_K$ com uma norma dada fixada $N_{K|\mathbb{Q}}(\alpha) = a$.*

Demonstração. Ver lema 7.2 do capítulo 1 de Neukirch (1999).

□

Proposição 27. *O grupo Γ é um reticulado completo no espaço vetorial H de dimensão $r+s-1$ e portanto é isomorfo a $\mathbb{Z}^{r+s-1}$.*

Demonstração. Vamos primeiro provar que $\Gamma = \lambda(\mathcal{O}_K^*)$ é um reticulado em H, ou seja, um subgrupo discreto de H. Sabemos que a aplicação $\lambda : \mathcal{O}_K^* \longrightarrow H$ é obtida restringindo a aplicação

$$K^* \xrightarrow{j} \prod_\tau \mathbb{C} \xrightarrow{l} \prod_\tau \mathbb{R},$$

então basta mostrarmos que para cada $c > 0$, o conjunto $X_c = \{(x_\tau) \in \prod_\tau \mathbb{R} \ |x_\tau| \leq c\}$ contém uma quantidade finita de pontos de $\Gamma = l(j\mathcal{O}_K^*)$. Note que

$$l^{-1}(X_c) = \left\{(z_\tau) \in \prod_\tau \mathbb{C}^* \mid e^{-c} \leq |z_\tau| \leq e^c\right\}$$

é um subconjunto limitado de $\prod_\tau \mathbb{C}$, logo $\#(l^{-1}(X_c) \cap j\mathcal{O}_K^*) < \infty$ pois $j\mathcal{O}_K$ é reticulado em $[\prod_\tau \mathbb{C}]^+$. Portanto, $\#(X_c \cap \Gamma) \leq \#(l^{-1}(X_c) \cap j\mathcal{O}_K^*) < \infty$.

Agora provaremos que Γ é reticulado completo em H. Para isso, primeiramente considere constantes reais positivas c_τ para cada $\tau \in Hom(K, \mathbb{C})$ satisfazendo $c_\tau = c_{\overline{\tau}}$

$$C = \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

e

$$X = \{(z_\tau) \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}.$$

Dado $y = (y_\tau) \in S$, temos que

$$Xy = \{(z_\tau) \in K_\mathbb{R} \mid |z_\tau| < c'_\tau\}$$

onde $c'_\tau = c_\tau |y_\tau|$ e $c_\tau = c_{\overline{\tau}}$. Note que $\prod_\tau c'_\tau = \prod_\tau c_\tau \prod_\tau |y_\tau| = C$, portanto, por 25, existe $a \in \mathcal{O}_K \setminus \{0\}$ tal que $ja = (\tau a) \in Xy$. Agora tome $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K \setminus \{0\}$ tais que todo $a \in \mathcal{O}_K$ com $0 < |N_{K|\mathbb{Q}}| \leq C$ é elemento associado a algum α_i. Defina o conjunto

$$T = S \cap \bigcup_{i=1}^N X(j\alpha_i)^{-1}.$$

Afirmamos que

(i) T é conjunto limitado em S e existe $\delta > 0$ tal que $\|x\| > \delta, \forall x \in T$;

(ii) $S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} Tj\varepsilon$.

(i) T é limitado pois é união finita de subconjuntos limitados de S já que X é limitado e como $\prod_\tau |x_\tau| = 1, \forall (x_\tau) \in T$, não existem pontos de X arbitrariamente próximos da origem. Para provarmos (ii), tome $y \in S$, então pelo que expusemos, sabemos que existe $a \in \mathcal{O}_K \setminus \{0\}$ tal que $ja \in Xy^{-1}$, ou seja, $ja = xy^{-1}$ par algum $x \in X$. Sendo assim,

$$|N_{K|\mathbb{Q}}(a)| = |N(xy^{-1})| = |N(x)| < \prod_\tau c_\tau = C.$$

Portanto, $\alpha_i = \varepsilon a$ para certo $i \{1, \ldots, N\}$ e $\varepsilon \in \mathcal{O}_K^*$. Disto, segue que

$$y = xja^{-1} = xj\alpha_i^{-1}j\varepsilon.$$

Como $y, j\varepsilon \in S$, então $xj\alpha_i^{-1} \in S \cap Xj\alpha_i^{-1} \subseteq T$, portanto $y \in Tj\varepsilon$.

Provado isso, temos que

$$H = l(S) = \bigcup_{\gamma \in \Gamma} (M + \gamma)$$

onde $M = l(T)$ é subconjunto limitado de H e concluímos que Γ é reticulado completo em H por 21.

□

Teorema 5 (Teorema das unidades de Dirichlet)**.** *O grupo de unidades $\mathcal{O}_K^*$ é produto direto do grupo finito cíclico $\mu(K)$ e um grupo abeliano livre de rank $r + s - 1$.*

Demonstração. Pelo lema 4 temos a sequência exata

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

e pela proposição anterior Γ é um grupo abeliano livre de rank $t = r + s - 1$. Seja $v_1, \ldots, v_t$ uma $\mathbb{Z}$-base de Γ, $\varepsilon_1, \ldots, \varepsilon_t \in \mathcal{O}_K^*$ pré-imagens dos v_i e $A \subseteq \mathcal{O}_K^*$ o subgrupo gerado pelos ε_i. Então A é mapeado isomorficamente em Γ por λ, ou seja, $\mu(K) \cap A = \{1\}$ e portanto $\mathcal{O}_K^* \times A$. □

3 CORPOS COM VALOR ABSOLUTO

O matemático alemão Kurt Hensel (1861-1941) percebeu a analogia entre $\mathbb{Z}$, juntamente com seu corpo de frações $\mathbb{Q}$ e o anel de polinômios $\mathbb{C}[X]$ juntamente com seu corpo de frações $\mathbb{C}(X)$. Nos inteiros, temos a fatoração única em fatores irredutíveis p (números primos) e para polinômios temos a fatoração única em fatores irredutíveis $X-\alpha$ mas no caso dos polinômios temos a propriedade adicional que dado $f(X) \in \mathbb{C}(X)$ e $\alpha \in \mathbb{C}$, podemos fazer a expansão de Laurent de $f(X)$

$$f(X) = \sum_{i \geq n_0} a_i (X-\alpha)^i$$

para algum $n_0 \in \mathbb{Z}$. Esse tipo de expansão nos permite compreender o comportamento local de $f(X)$ em $X = \alpha$. Então a ideia seria encontrar também uma forma de poder representar qualquer número racional como uma série de potências p-ésimas. A primeira condição para isso seria utilizarmos em $\mathbb{Q}$ um valor absoluto apropriado, pois o valor absoluto usual falharia para isso. Para mais detalhes sobre a motivação da definição dos números p-ádicos e para conhecer alguns resultados que não serão abordados neste trabalho, uma boa leitura inicial é Gouvea (2003).

3.1 VALOR ABSOLUTO E COMPLETAMENTO

Definição 16. *Um **valor absoluto** em um corpo K é uma função*

$$|\ |: K \longrightarrow \mathbb{R}$$

satisfazendo as seguintes propriedades:

(i) $|x| \geq 0,$ *e* $|x| = 0 \Longleftrightarrow x = 0$*;*

(ii) $|xy| = |x||y|$*;*

(iii) $|x+y| \leq |x| + |y|$.

E vamos sempre supor que $|\ |$ não é o trivial, ou seja, não é tal que $|x| = 1, \forall x \neq 0$. Definimos a distância entre 2 pontos $x, y \in K$ por

$$d(x,y) = |x-y|.$$

Isso torna K um espaço métrico e portanto um espaço topológico.

Definição 17. *Dois valores absolutos em K são equivalentes se induzem a mesma topologia em K.*

Proposição 28. *Sejam $|\ |_1$ e $|\ |_2$ valores absolutos num corpo K. São equivalentes as seguintes afirmações:*

(i) *$|\ |_1$ e $|\ |_2$ são valores absolutos equivalentes;*

(ii) *Para cada $x \in K$, temos que $|x|_1 < 1 \iff |x|_2 < 1$;*

(iii) *Existe um número real $s > 0$ tal que*

$$|x|_1 = |x|_2^s, \ \forall x \in K.$$

Demonstração. Ver proposição 3.3 do capítulo 2 de Neukirch (1999).

□

Proposição 29 (Teorema de Aproximação)**.** *Sejam $|\ |_1, \ldots, |\ |_n$ valores absolutos num corpo K dois a dois não equivalentes e sejam $a_1, \ldots, a_n \in K$. Então para cada $\varepsilon > 0$, existe um $x \in K$ tal que*

$$|x - a_i|_i < \varepsilon, \ \text{para } i = 1, \ldots, n.$$

Demonstração. Ver proposição 3.4 do capítulo 2 de Neukirch (1999).

□

Definição 18. *Seja $(K, |\ |)$ um corpo com valor absoluto. O valor absoluto é chamado não arquimediano se a imagem do homomorfismo canônico $\mathbb{Z} \longrightarrow K$ é limitada. Caso contrário, é chamado de arquimediano.*

Proposição 30. *Um valor absoluto $|\ |$ num corpo K é não arquimediano se, se somente se vale a desigualdade triangular forte, ou seja,*

$$|x + y| \leq max\left\{|x|, |y|\right\}, \ \forall x, y \in K.$$

Demonstração. Ver a proposição 3.6 do capítulo 1 de Neukirch (1999).

□

Proposição 31. *Seja K um corpo com valor absoluto não arquimediano $|\ |$, Se $x, y \in K$ e $|x| \neq |y|$, então*

$$|x + y| = max\left\{|x|, |y|\right\}.$$

Demonstração. Ver proposição 2.2.3 de Gouvea (2003).

□

Definição 19. *Uma valoração exponencial num corpo K é uma função*

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}$$

satisfazendo

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

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

Desconsideramos o caso trivial em que $v(K) = \{0, \infty\}$. É fácil ver que se q é um número real fixado e maior que 1, então

$$|x| = q^{-v(x)}$$

define um valor absoluto em K não arquimediano. Reciprocamente se tivermos um valor absoluto não arquimediano definido em K e q é um número real fixado maior que 1, então

$$v(x) = -log_q|x|$$

define uma valoração exponencial em K. Dizemos que duas valorações exponenciais v_1, v_2 são equivalentes, se $v_1 = sv_2$ para algum $s > 0$.

Proposição 32. *Se K é um corpo com valor absoluto $|\ |$ não arquimediano e v é uma valoração exponencial associada a este valor absoluto, então o subconjunto*

$$\mathcal{o} = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$$

é um anel local, chamado anel de valoração. Seu grupo de unidades é

$$\mathcal{o}^* = \{x \in K : v(x) = 0\} = \{x \in K : |x| = 1\}$$

e o único ideal maximal

$$\mathfrak{p} = \{x \in K : v(x) > 0\} = \{x \in K : |x| < 1\}.$$

Tais conjuntos são invariantes se trocarmos $|\ |$ por um valor absoluto equivalente ou trocarmos v por uma valoração exponencial equivalente.

Demonstração. Ver proposição 3.8 do capítulo 2 de Neukirch (1999).

. □

Uma valoração exponencial é dita **discreta** se admite um menor valor positivo s. Neste caso temos que

$$v(K^*) = s\mathbb{Z}.$$

É dita **normalizada** se $s = 1$. Note que podemos sempre passar de uma valoração discreta para uma normalizada dividindo por s sem mudar os invariantes $\mathcal{o}, \mathcal{o}^*, \mathfrak{p}$. Feito isso, um elemento

$$\pi \in \mathcal{o} \text{ tal que } v(\pi) = 1$$

é dito **primo** e é fácil perceber que todo elemento $x \in K^*$ admite uma única representação

$$x = u\pi^m,$$

com $m \in \mathbb{Z}$ e $u \in \mathcal{o}^*$ e neste caso, claramente $m = v(x)$.

Proposição 33. *Se v é uma valoração exponencial discreta em K, então*

$$\mathcal{o} = \{x \in K : v(x) \geq 0\}$$

é um domínio de ideais principais. Se v é normalizada, então os ideais não nulos de $\mathcal{o}$ são

$$\mathfrak{p}^n = \pi^n\mathcal{o} = \{x \in K : v(x) \geq n\}\,,\ n \geq 0,$$

onde π é um elemento primo. Ademais, temos o seguinte isomorfismo de $\mathcal{o}$-módulos:

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \simeq \mathcal{o}/\mathfrak{p}.$$

Demonstração. Ver proposição 3.9 do capítulo 2 de Neukirch (1999).

□

Proposição 34. *Num corpo K de valoração discreta valem também as seguintes propriedades:*

(i) A cadeia

$$\mathcal{o} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \cdots$$

formada pelos ideais de $\mathcal{o}$ formam uma base de vizinhanças abertas de $0 \in K$;

(ii) Definimos $U^{(n)} = 1 + \mathfrak{p}^n$*, o* n*-ésimo grupo das unidades superiores e em especial chamamos* $U^{(1)}$ *de grupo das unidades principais. A cadeia descendente*

$$\mathcal{o}^* = U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \cdots$$

forma uma base de vizinhanças abertas de $1 \in K^*$*;*

(iii) Para $n \geq 1$*, temos isomorfismos canônicos* $\mathcal{o}^*/U^{(n)} \simeq (\mathcal{o}/\mathfrak{p}^n)^*$ *e* $U^{(n)}/U^{((n+1)} \simeq \mathcal{o}/\mathfrak{p}$*.*

Demonstração. Ver proposição 3.10 do capítulo 2 de Neukirch (1999).

□

Definição 20. *Um corpo com valor absoluto* $(K, |\ |)$ *é completo se toda sequência de Cauchy em* K *é convergente em* K*.*

Definição 21. *Sejam* $(K, |\ |), (\hat{K}, |\ |_c)$ *corpos com valores absolutos tais que* $K \subseteq \hat{K}$ *e* $|\ |_c$ *é extensão de* $|\ |$ *e* K *é denso em* $\hat{K}$*. Neste caso dizemos que* $(\hat{K}, |\ |_c)$ *é um completamento de* $(K, |\ |)$*.*

Lema 6. *Se* $(\hat{K}, |\ |_1)$ *e* $(\tilde{K}, |\ |_2)$ *são completamentos de* $(K, |\ |)$*, então existe um* K *- isomorfismo*

$$\sigma : \hat{K} \longrightarrow \tilde{K} \text{ tal que } |a|_1 = |\sigma a|_2, \forall a \in \hat{K}.$$

Demonstração. Ver capítulo 3.2 de Gouvea (2003).

□

Seja $(K, |\ |)$ um corpo com valor absoluto. Denotamos por $\mathcal{C}$ o conjunto das sequências de Cauchy de elementos de K. É fácil verificar que $\mathcal{C}$ é um anel comutativo com unidade. Definimos o subconjunto $\mathcal{N} \subset \mathcal{C}$ como

$$\mathcal{N} = \{(x_n) \text{ sequência em } K : \ x_n \longrightarrow 0\},$$

que é claramente um ideal do anel $\mathcal{C}$.

Lema 7. $\mathcal{N}$ *é um ideal maximal de* $\mathcal{C}$ *e definimos o corpo* $\hat{K} = \mathcal{C}/\mathcal{N}$*.*

Demonstração. Ver capítulo 3.2 de Gouvea (2003).

□

Note que temos o mergulho $K \hookrightarrow \hat{K}$, que leva $x \in K$ na classe de equivalência da sequência constante (x). Portanto, daqui em diante estaremos fazendo a identificação $K \subseteq \hat{K}$.

Definição 22. *Seja $x \in \hat{K}$ e (x_n) uma sequência de Cauchy representando x. Definimos*

$$|x| = \lim_{x\to\infty} |x_n|.$$

Note que $||x_n| - |x_m|| \leq |x_n - x_m|$, então $(|x_n|)$ é sequência de Cauchy em $\mathbb{R}$, logo converge para um certo número real que denotaremos por $|x|$. Se (y_n) é outra sequência de Cauchy representando x, note que

$$||x_n| - |y_n|| \leq |x_n - x_y| \longrightarrow 0, \text{ pois } \ (x_n) - (y_n) \in \mathcal{N}.$$

Portanto, $|y_n| \longrightarrow |x|$. Sendo assim, a definição é consistente. Perceba também que isso define uma função em $\hat{K}$ que quando restrita a K é o valor absoluto.

Proposição 35. *A função $|\ | : \hat{K} \longrightarrow \mathbb{R}$ que acabamos de definir é um valor absoluto em $\hat{K}$.*

Demonstração. Ver capítulo 3.2 de Gouvea (2003).

□

Proposição 36. *K é denso em $\hat{K}$.*

Demonstração. Ver capítulo 3.2 de Gouvea (2003).

□

Concluimos então que $(\hat{K}, |\ |)$ é um completamento de $(K, |\ |)$. Note que se o valor absoluto do corpo inicial é (não) arquimediano, então o completamento também é.

Seja K um corpo com valor absoluto não arquimediano, com valoração $v(\ ) = -log_q|\ |$ associada e $\hat{K}$ seu completamento. Então $\hat{v}(\ ) = \log_q|\ |$ é uma valoração associada ao valor absoluto de $\hat{K}$ que estende v. Se $a \in \hat{K}^*$, tome uma sequência (a_n) em K convergindo para a, logo $\exists n_0 \in \mathbb{N}$ tal que se $n \geq n_0$, então $\hat{v}(a_n - a) > \hat{v}(a)$, então

$$v(a_n) = \hat{v}(a_n - a + a) = min\{\hat{v}(a_n - a), \hat{v}(a)\} = \hat{v}(a),$$

logo

$$\hat{v}(a) = \lim_{n\to\infty} v(a_n) = v(a_{n_0})$$

e assim $v(K^*) = \hat{v}(\hat{K}^*)$. Portanto, se v for discreta então $\hat{v}$ também é discreta e se v for discreta e normalizada então $\hat{v}$ é discreta e normalizada.

Proposição 37. *Se $\mathcal{o} \subseteq K$ e $\hat{\mathcal{o}} \subseteq \hat{K}$ são os aneis de valoração de v e $\hat{v}$, respectivamente, e $\mathfrak{p}$, $\hat{\mathfrak{p}}$ são seus respetivos ideais maximais, então*

$$\hat{\mathcal{o}}/\hat{\mathfrak{p}} \simeq \mathcal{o}/\mathfrak{p},$$

e se v for discreta então

$$\hat{\mathcal{o}}/\hat{\mathfrak{p}}^n \simeq \mathcal{o}/\mathfrak{p}^n \ \forall n \geq 1.$$

Demonstração. Ver a proposição 4.3 do capítulo 2 de Neukirch (1999).

□

Proposição 38. *Seja $R \subseteq \mathcal{o}$ um sistema completo de representantes para $\kappa = \mathcal{o}/\mathfrak{p}$ tal que $0 \in R$ e seja $\pi \in \mathcal{o}$ um elemento primo. Então vale*

(i) Se $u \in \hat{\mathcal{o}}$, existem únicos $a_0, a_1, \cdots \in R$ tais que para cada $n \in \mathbb{N}$,

$$u \equiv a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \ mod\ \hat{\mathfrak{p}}^n$$

ademais, se $u \in \hat{\mathcal{o}}^*$, temos que $a_0 \neq 0$;

(ii) Se $x \in \hat{K}^*$, então x admite uma única representação como série de potências convergente

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$$

com $a_i \in R, a_0 \neq 0, m \in \mathbb{Z}$.

Demonstração. Ver proposição 4.4 do capítulo 2 de Neukirch (1999).

□

Seja K um corpo completo com respeito a uma valoração discreta, seja $\mathcal{o}$ seu anel de valoração e $\mathfrak{p}$ seu ideal maximal. Para cada $n \geq 1$, temos os homomorfismos canônicos

$$\mathcal{o} \longrightarrow \mathcal{o}/\mathfrak{p}^n$$

e

$$\mathcal{o}/\mathfrak{p} \xleftarrow{\lambda_1} \mathcal{o}/\mathfrak{p}^2 \xleftarrow{\lambda_2} \mathcal{o}/\mathfrak{p}^3 \xleftarrow{\lambda_3} \cdots$$

Isso nos dá um homomorfismo

$$\mathcal{o} \longrightarrow \varprojlim_n \mathcal{o}/\mathfrak{p}^n$$

de $\mathcal{O}$ no limite projetivo

$$\varprojlim_n \mathcal{O}/\mathfrak{p}^n = \left\{(x_n) \in \prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n : \lambda_n(x_{n+1}) = x_n\right\} \subseteq \prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n.$$

Considerando cada $\mathcal{O}/\mathfrak{p}^n$ com a topologia discreta, temos que $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$ é um anel topológico e portanto o limite projetivo também é.

Proposição 39. *O homomorfismo canônico*

$$\mathcal{O} \longrightarrow \varprojlim_n \mathcal{O}/\mathfrak{p}^n$$

é um isomorfismo e também um homeomorfismo.

Demonstração. Ver proposição 4.5 do capítulo 2 de Neukirch (1999).

□

Proposição 40. $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$ *é um subconjunto fechado de* $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$.

Demonstração. Ver o parágrafo 2 do capítulo 2 de Neukirch (1999).

□

Definição 23. *Um corpo com valor absoluto K é dito* ***corpo local*** *se é completo, a valoração é discreta e seu corpo de resíduos é um conjunto finito.*

Definição 24. *Um espaço topológico Hausdorff X é dito localmente compacto se cada ponto $x \in X$ possui uma vizinhança compacta.*

Proposição 41. *Todo corpo local K é localmente compacto e seu anel de valoração $\mathcal{O}$ é compacto.*

Demonstração. Ver proposição 5.1 do capítulo 2 de Neukirch (1999).

□

Definição 25. *Seja K um corpo completo com respeito a um valor absoluto não arquimediano $|\ |$ e $\mathcal{O}$ o anel de valoração correspondente com ideal maximal $\mathfrak{p}$ e corpo de resíduos $\kappa = \mathcal{O}/\mathfrak{p}$. Um polinômio*

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathcal{O}[X]$$

é dito primitivo se $f(X) \not\equiv 0 \ mod\ \mathfrak{p}$, ou seja, se

$$|f| = max\,\{|a_0|, \ldots, |a_n|\} = 1.$$

Teorema 6 (Lema de Hensel)**.** *Se um polinômio primitivo $f(X) \in \mathcal{o}[X]$ admite uma fatoração módulo $\mathfrak{p}$ dada por*

$$f(X) \equiv \overline{g}(X)\overline{h}(X) \ mod \ \mathfrak{p},$$

com $\overline{g}, \overline{h} \in \kappa[X]$ relativamente primos, então $f(X)$ admite fatoração

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

com $g, h \in \mathcal{o}[X]$ e $grau(g) = grau(\overline{g})$ e

$$g(X) \equiv \overline{g}(X) \ mod \ \mathfrak{p} \text{ e } h(X) \equiv \overline{h}(X) \ mod \ \mathfrak{p}.$$

Demonstração. Seja $d = grau(f), m = grau(\overline{g})$, logo $d-m \geq grau(\overline{h})$. Sejam $g_0, h_0 \in \mathcal{o}[X]$ tais que $g_0 \equiv \overline{g} \ mod \ \mathfrak{p}, h_0 \equiv \overline{h} \ mod \ \mathfrak{p}$ e $grau(g_0) = m, grau(h_0) \leq d - m$. Como $\overline{g}$ e $\overline{h}$ são primos entre si, existem polinômios $a(X), b(X) \in \mathcal{o}[X]$ tais que $ag_0 + bh_0 \equiv 1 \ mod \ \mathfrak{p}$. Entre os coeficientes de $f - g_0h_0$ e $ag_0 + bh_0 - 1 \in \mathfrak{p}[X]$, escolha um de maior valor absoluto e denote π.

Para cada $n \in \mathbb{N}$, vamos construir polinômios $p_1, \ldots, p_{n-1} \in \mathcal{o}[X]$ de grau $< m$ e polinômios $q_1, \ldots, q_{n-1} \in \mathcal{o}[X]$ de grau $\leq d - m$ tais que se definimos

$$g_{n-1} = g_0 + p_1\pi + \cdots + p_{n-1}\pi^{n-1},$$
$$h_{n-1} = h_0 + q_1\pi \cdots + q_{n-1}\pi^{n-1},$$

então

$$f \equiv g_{n-1}h_{n-1} \ mod \ \pi^n.$$

Fazendo $n \longrightarrow \infty$, temos que

$$g = g_0 + p_1\pi + p_2\pi^2 + \cdots \ \in \mathcal{o}[X],$$
$$h = h_0 + q_1\pi + q_2\pi^2 + \cdots \ \in \mathcal{o}[X],$$

e $f = gh$.

Primeiramente note que para o caso $n = 1$, já temos resolvido pela escolha de π e suponha que já construimos todos os polinômios envolvidos satisfazendo as propriedades necessárias para um certo $n \geq 1$. Queremos encontrar $p_n, q_n \in \mathcal{o}[X]$ tais que se

$$g_n = g_{n-1} + p_n\pi^n, \ h_n = h_{n-1} + q_n\pi^n,$$

então

$$f - g_nh_n \equiv \ 0 \ mod \ \pi^{n+1},$$

e como

$$f-(g_{n-1}+p_n\pi^n)(h_{n-1}+q_n\pi^n)=f-g_{n-1}h_{n-1}-g_{n-1}q_n\pi^n-h_{n-1}p_n\pi^n-p_nq_n\pi^{2n},$$

segue que

$$f-g_{n-1}h_{n-1}\equiv(g_{n-1}q_n+h_{n-1}p_n)\pi^n\ mod\ \pi^{n+1}.$$

Denotando $f_n=\pi^{-n}(f-g_{n-1}h_{n-1})\in\mathcal{o}[X]$, precisamos então encontrar polinômios p_n,q_n de graus $<m$ e $\leq d-m$, respectivamente, tais que

$$f_n\equiv g_{n-1}q_n+h_{n-1}p_n\equiv g_0q_n+h_0p_n\ mod\ \pi.$$

Vamos agora construir tais polinômios. Como $g_0\equiv\overline{g}\ mod\ \mathfrak{p}$ e $grau(g_0)=grau(\overline{g})$ o coeficiente líder de g_0 é uma unidade em $\mathcal{o}$, logo podemos efetuar a divisão euclidiana por g_0, em particular, podemos escrever

$$b(X)f_n(X)=q(X)g_0(X)+p_n(X),$$

com $grau(p_n)<grau(g_0)=m$. Denote $r(x)=p_n(X)$ e defina $q_n(X)$ como o polinômio obtido a partir de af_n+h_0q omitindo os coeficientes divisíveis por π. Lembrando que o valor absoluto de π é maior ou igual que o valor absoluto de cada um dos coeficientes de ag_0+bh_0-1, logo

$$g_0q_n+h_0p_n\equiv g_0(af_n+h_0q)+h_0p_n\equiv(ag_0+bh_0)f_n\equiv f_n\ mod\ \pi.$$

Por fim, note também que $grau(q_n)\leq d-m$, pois caso contrário, $grau(g_0q_n)>d$ e este polinômio tem coeficiente líder não divisível por π e $grau(h_0p_n)<(d-m)+m=d$ mas $grau(f_n)\leq d$ e teríamos uma contradição com a equivalência que acabamos de demonstrar.

□

Corolário 3. *Seja K um corpo completo com respeito a um valor absoluto não arquimediano $|\ |$. Se $f(X)=a_0+a_1X+\cdots+a_nX^n\in K[X]$ é um polinômio irredutível com $a_0a_n\neq0$, então*

$$|f|=max\,\{|\,a_0|,|a_n|\}.$$

Em particular, se $a_n=1$ e $a_0\in\mathcal{o}$, então $f\in\mathcal{o}[X]$.

Demonstração. Ver corolário 4.7 do capítulo 2 de Neukirch (1999).

□

Proposição 42. *Seja K um corpo completo com respeito a um valor absoluto $|\ |$ e $L|K$ extensão algébrica. Então $|\ |$ pode ser estendido de uma única maneira para L. Ademais, se a extensão tem grau finito, $[L:K]=n$, então L é completo e vale*

$$|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|},\ \forall \alpha \in L.$$

Demonstração. Ver teorema 4.8 do capítulo 2 de Neukirch (1999).

□

Corolário 4. *Se $L|K$ é uma extensão finita de corpos com valor absoluto então o anel de valoração $\mathcal{O}$ de L é o fecho integral de o (anel de valoração de K) em L.*

Demonstração. Denote $|\ |$ o valor absoluto de K e $n=[L:K]$. Dado $\alpha \in L$, como

$$|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|},\ \forall \alpha \in L,$$

segue que

$$\mathcal{O} = \left\{\alpha \in L \mid N_{L|K}(\alpha) \in o\right\}.$$

Se $x \in L$ é integral sobre o, pelo que estudamos na seção de extensões integrais do capítulo 2, sabemos que $N_{L|K}(x) \in o$. Agora se $x \in \mathcal{O}$, considere

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X],$$

o polinômio mínimo de x sobre K, logo $N_{L|K}(x) = \pm a_0^m \in o$ e $|a_0| \leq 1$. Portanto $f(X) \in o[X]$ pelo corolário 3, ou seja, x é integral sobre o. □

3.2 p-ÁDICOS

Definição 26. *Fixado um número primo $p \in \mathbb{Z}$, a valoração p-ádica é a função*

$$v_p : \mathbb{Z} \longrightarrow \mathbb{R} \cup \{\infty\}$$

definida por: $v_p(0)=\infty$ e se $n \neq 0$, considere sua fatoração em potência de primos

$$n = \pm p_1^{e_1} \cdots p_l^{e_l}.$$

Se p não aparece na fatoração de n, definimos $v_p(n)=0$. Se aparece, com $p=p_j$, definimos $v_p(n)=e_j$.

Note que se $n \neq 0$, $v_p(n)$ é o único inteiro não negativo satisfazendo

$$n = p^{v_p(n)}n' \text{ com } p \nmid n'.$$

Estendemos v_p para os racionais como $v_p(a/b) = v_p(a) - v_p(b)$ e é fácil verificar que essa definição é consistente, ou seja

$$\frac{a}{b} = \frac{c}{d} \Rightarrow v_p(a) - v_p(b) = v_p(c) - v_p(d),$$

e temos que se $x = a/b \in \mathbb{Q}^*$, então $v_p(x)$ é o único número inteiro que satisfaz

$$x = p^{v_p(x)}\frac{a}{b} \text{ com } p \nmid ab.$$

Proposição 43. *Seja $p \in \mathbb{Z}$ um número primo. Então v_p é uma valoração exponencial em $\mathbb{Q}$, ou seja, para todos $x, y \in \mathbb{Q}$,*

(i) $v_p(x) = \infty \iff x = 0$;

(ii) $v_p(xy) = v_p(x) + v_p(y)$;

(iii) $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$.

Ademais, $v_p(\mathbb{Q}) = \mathbb{Z}$, ou seja, v_p é discreta e normalizada.

Demonstração. Ver lema 2.1.3 de Gouvea (2003).

□

Definição 27. *Para cada $x \in \mathbb{Q}$, definimos o valor absoluto p-ádico de x como*

$$|x|_p = p^{-v_p(x)}.$$

Note que a função $|\ |_p : \mathbb{Q} \longrightarrow \mathbb{R}$ é um valor absoluto não arquimediano.

Definição 28. *Denotamos $|\ |_\infty$ o valor absoluto euclidiano usual de $\mathbb{Q}$.*

Teorema 7. *Todo valor absoluto em $\mathbb{Q}$ é equivalente a um dos $|\ |_p$ ou $|\ |_\infty$.*

Demonstração. Caso 1: Seja $\|\ \|$ um valor absoluto não arquimediano em $\mathbb{Q}$. Então $\|n\| = \|1 + \cdots + 1\| \leq \|1\| = 1$, e como estamos trabalhando com um valor absoluto não trivial, existe um número primo p com $\|p\| < 1$. Note agora que o conjunto

$$I = \{a \in \mathbb{Z} : \|a\| < 1\}$$

é um ideal de $\mathbb{Z}$ satisfazendo $p\mathbb{Z} \subseteq I \neq \mathbb{Z}$ mas como $p\mathbb{Z}$ é ideal maximal, segue que $I = p\mathbb{Z}$. Agora seja $a \in \mathbb{Z}$ e escreva $a = bp^m$ com $p \nmid b$, logo $b \in I$, logo $\|b\| = 1$ e portanto

$$\|a\| = \|p^m\| = |a|_p^s,$$

com $s = \frac{-log\|p\|}{logp}$. Portanto, $\|\ \|$ é equivalente a $|\ |_p$.

Caso 2: Seja $\|\ \|$ um valor absoluto arquimediano em $\mathbb{Q}$, logo existe um menor inteiro positivo n_0 com $\|n_0\| > 1$. Escrevendo

$$\|n_0\| = n_0^{\alpha}, \text{ com } \alpha = \frac{log\|n_0\|}{log\ n_0}.$$

Afirmamos que $\|x\| = |x|^{\alpha}, \forall x \in \mathbb{Q}$ e para isso ser verdade, basta verificarmos para os inteiros positivos. Seja n inteiro positivo e escreva

$$n = a_0 + a_1 n_0 + \cdots + a_k n_0^k,$$

com $a_i \in \{0, 1, \ldots, n_0 - 1\}$ e $a_k \neq 0$, logo $k = \left\lfloor \frac{log\ n}{log\ n_0} \right\rfloor$ e $\|a_i\| \leq 1$. Segue que

$$\|n\| \leq \sum_{i=0}^{k} \|a_i\| \|n_0\|^i \leq \sum_{i=0}^{k} n_0^{i\alpha} = n_0^{k\alpha} \sum_{i=0}^{k} \frac{1}{n_0^{i\alpha}} \leq n_0^{k\alpha} \sum_{i=0}^{\infty} \frac{1}{n_0^{i\alpha}} \leq n^{\alpha} \frac{n_0^{\alpha}}{n_0^{\alpha} - 1}.$$

Substituindo n por n^r, tomando a raiz r - ésima dos dois lados da desigualdade acima e fazendo $r \longrightarrow \infty$, concluimos que $\|n\| \leq n^{\alpha}$. Agora provaremos a desigualdade inversa. Note que

$$\begin{aligned} \|n\| &\geq \|n_0^{k+1}\| - \|n_0^{k+1} - n\| \geq n_0^{(k+1)\alpha} - \left(n_0^{k+1} - n\right)^{\alpha} \geq n_0^{(k+1)\alpha} - \left(n_0^{k+1} - n_0^k\right)^{\alpha} \\ &= n_0^{(k+1)\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right) > n^{\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right) \end{aligned}$$

Substituindo n por n^r, tomando a raiz r - ésima dos dois lados da desigualdade acima e fazendo $r \longrightarrow \infty$, concluimos que $\|n\| \geq n^{\alpha}$.

□

Observação: Da demonstração, percebe-se que se $\|\ \|$ é um valor absoluto arquimediano em $\mathbb{Q}$, então $\|\ \| = |\ |^s$, com $s \in (0, 1]$, onde $|\ |$ é o valor absoluto usual.

Definição 29. *Definimos o corpo $\mathbb{Q}_p$ dos números p-ádicos como o completamento de $\mathbb{Q}$ com respeito ao valor absoluto p-ádico e denotamos seu anel de valoração por $\mathbb{Z}_p$.*

Proposição 44. *$\mathbb{Q}_p$ é corpo local, e em particular, é localmente compacto.*

Demonstração. Por construção $\mathbb{Q}_p$ é completo e $v_p(\mathbb{Q}_p) = v_p(\mathbb{Q}) = \mathbb{Z}$. E pelo corolário 3.3.6 de Gouvea (2003), temos o isomorfismo $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

□

Definição 30. *As extensões finitas $K|\mathbb{Q}_p$ são chamados de corpos de números $\mathfrak{p}$-ádicos.*

Proposição 45. *Seja K um corpo de números $\mathfrak{p}$-ádico, $e = v_K(p)$ e $n > \frac{e}{p-1}$. Então as séries de potências*

$$exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \quad e \quad \log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

são isomorfismos (e homeomorfismos), um inverso do outro.

$$\mathfrak{p}_K^n \underset{log}{\overset{exp}{\rightleftarrows}} U_K^{(n)}$$

Demonstração. Ver proposição 5.5 do capítulo 2 de Neukirch (1999). □

3.3 CLASSIFICAÇÃO DE CORPOS LOCALMENTE COMPACTOS

Teorema 8 (Ostrowski)**.** *Se $(K, \| \|)$ é um corpo com valor absoluto arquimediano e completo então existe um isomorfismo σ de K em $\mathbb{R}$ ou $\mathbb{C}$ satisfazendo*

$$\|a\| = |\sigma a|^s, \forall a \in K,$$

para algum $s \in (0, 1]$ fixado, com $|\ |$ o valor absoluto usual de $\mathbb{R}$ ou $\mathbb{C}$. Em particular, σ também é homeomorfismo.

Demonstração. Primeiramente note que se existir tal isomorfismo, segue de 28 que será também um homeomorfismo entre K com a topologia induzida por $|\ |$ e $\mathbb{R}$ ou $\mathbb{C}$ com a topologia euclidiana.

Como $char(K) = 0$, pois $|\ |$ é arquimediano, segue que $\mathbb{Q} \hookrightarrow K$, e seja $\mathbb{Q}_K$ a imagem de $\mathbb{Q}$ por tal mergulho e $\sigma : \mathbb{Q}_K \to \mathbb{Q}$ o isomorfismo inverso. Para cada $a \in \mathbb{Q}_K$, considere $\|\sigma a\|' = \|a\|$ e note que isso define um valor absoluto arquimediano em $\mathbb{Q}$, logo por 28 e 7, $\exists s \in (0, 1]$ tal que $\|\sigma a\|' = |\sigma a|^s,\ \forall a \in \mathbb{Q}_K$, com $|\ |$ o valor absoluto usual de $\mathbb{Q}$. Como K é completo, é fácil ver que é possível estendermos para um isomorfismo $\sigma : \overline{\mathbb{Q}_K} \to \mathbb{R}$ com $\|a\| = |\sigma a|^s, \forall a \in \overline{\mathbb{Q}_K}$.

Afirmamos que $\forall \xi \in K, \exists p(x) \in \overline{\mathbb{Q}_K}[X]$ com $grau(p(X)) \leq 2$ tal que $p(\xi) = 0$. Se isto for verdade, então K é extensão algébrica de $\overline{\mathbb{Q}_K}$ e $[K : \overline{\mathbb{Q}_K}] \leq 2$. Logo,

Caso 1: Se $[K : \overline{\mathbb{Q}_K}] = 1$, então $\overline{\mathbb{Q}_K} = K$ e terminamos.

Caso 2: Se $[K : \overline{\mathbb{Q}_K}] = 2$, como $\overline{\mathbb{Q}_K} \simeq \mathbb{R}$, então $\exists i \in K \setminus \overline{\mathbb{Q}_K}$ raiz de $X^2 + 1 \in \overline{\mathbb{Q}_K}[x]$, logo $K = \overline{\mathbb{Q}_K}[i]$. Assim, estendemos $\sigma : K \longrightarrow \mathbb{C}$, por $\sigma(a + ib) = \sigma(a) + i\sigma(b)$ e é fácil verificar que σ é isomorfismo. De (42) segue que

$$\begin{aligned} |\sigma(a+ib)|^s = |\sigma(a) + i\sigma(b)|^s = |\sigma(a)^2 + \sigma(b)^2|^{\frac{s}{2}} = |\sigma(a^2+b^2)|^{\frac{s}{2}} \\ = \|a^2 + b^2\|^{\frac{1}{2}} = \|a + ib\|. \end{aligned}$$

Vamos agora provar a afirmação. Pelo que já mostramos até agora, podemos considerar $\mathbb{R} \subseteq K$ e este mergulho é algébrico e topológico. Considere então a função contínua $f : \mathbb{C} \longrightarrow \mathbb{R}$ definida por

$$f(z) = |\xi^2 - (z + \overline{z})\xi + z\overline{z}|$$

e note que $z + \overline{z}, z\overline{z} \in \mathbb{R} \subset K$. Como $\lim_{z\to\infty} f(z) = \infty, f(z)$ alcança um valor mínimo m. Desta forma, conjunto

$$S = \{z \in \mathbb{C} : f(z) = m\}$$

é não vazio, limitado e fechado, logo compacto e portanto e existe $z_0 \in S$ tal que $|z_0| \geq |z|, \forall z \in S$. Basta então mostrar que $m = 0$, pois assim teremos que

$$\xi^2 - (z_0 + \overline{z_0})\xi + z_0\overline{z_0} = 0.$$

Suponha por contradição que $m > 0$ e considere o polinômio real

$$g(x) = x^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0} + \varepsilon$$

com $0 < \varepsilon < m$ e raízes $z_1, \overline{z_1}, \in \mathbb{C}$. Temos que $z_1\overline{z_1} = z_0\overline{z_0} + \varepsilon$, logo $|z_1| > |z_0|$, logo

$$f(z_1) > m.$$

Fixado $n \in \mathbb{N}$, considere o polinômio real

$$G(x) = (g(x) - \varepsilon)^n - (-\varepsilon)^n = \prod_{j=1}^{2n}(x - \alpha_j) = \prod_{j=1}^{2n}(x - \overline{\alpha_j})$$

de raízes $\alpha_1, \ldots \alpha_{2n} \in \mathbb{C}$. Segue que $G(z_1) = 0$ e sem perda de generalidade podemos supor que $z_1 = \alpha_1$. Substituindo $\xi \in K$ no polinômio

$$G(x)^2 = \prod_{j=1}^{2n}(x^2 - (\alpha_j + \overline{\alpha_j})x + \alpha_j\overline{\alpha_j}),$$

obtemos

$$|G(\xi)|^2 = \prod_{j=1}^{2n} f(\alpha_j) \geq f(\alpha_1)m^{2n-1}.$$

Dessa desigualdade acima e do seguinte fato

$$|G(\xi)| \leq |\xi^2 - (z_0 + \overline{z_0})\xi + z_0\overline{z_0}|^n + |-\varepsilon|^n = f(z_0)^n + \varepsilon^n = m^n + \varepsilon^n,$$

segue que

$$f(\alpha_1)m^{2n-1} \leq (m^n + \varepsilon^n)^2,$$

logo

$$\frac{f(\alpha_1)}{m} \leq \left(1 + \left(\frac{\varepsilon}{m}\right)^n\right)^2.$$

Fazendo $n \to \infty$, concluimos que $f(\alpha_1) \leq m$, o que é absurdo. □

Lema 8. *Seja K completo com respeito ao valor absoluto $|\ |$ e V um espaço vetorial normado n-dimensional sobre K. Então para toda base $v_1, \ldots, v_n$ de V, a norma do máximo*

$$\|x_1v_1 + \cdots x_nv_n\| = max\,\{|x_1|, \ldots, |x_n|\}$$

é equivalente a norma dada em V. Em particular, V é completo e o isomorfismo

$$K^n \longrightarrow V,\ (x_1, \ldots, x_n) \longmapsto x_1v_1 + \cdots x_nv_n$$

é um homeomorfismo.

Demonstração. Ver proposição 4.9 do capítulo 2 de Neukirch (1999).

□

Lema 9. *Seja K completo com respeito ao valor absoluto $|\ |$ e V espaço vetorial normado sobre K. Se W é subespaço de V com dimensão finita então W é fechado em V.*

Demonstração. Seja (w_m) sequência de vetores em W convergindo para um vetor $v \in V$, então (w_m) é sequência de Cauchy em W, mas pelo lema anterior, W é completo, logo $w_m \longrightarrow w \in W$, logo $v = w \in W$. □

Lema 10. *Se V espaço vetorial sobre $\mathbb{Q}_p$, normado e localmente compacto. Então $dim(V) < \infty$.*

Demonstração. Seja C uma vizinhança compacta da origem então pC é também vizinhança compacta da origem. Como

$$C \subseteq \bigcup_{v \in V} v + pC$$

e C é compacto, existe um conjunto finito de vetores S tal que $C \subseteq S + pC$. Se W é o subespaço vetorial de dimensão finita gerado por S, segue $C \subseteq W + pC$ e por indução sobre n, que $\forall n \in \mathbb{N}$

$$C \subseteq W + p^n C.$$

Note agora que se U é uma vizinhança da origem, como a multiplicação por escalar é contínua, existe U_0 vizinhança aberta da origem e existe $\delta > 0$ tal que se $\alpha \in \mathbb{Q}_p$ é tal que $|\alpha|_p < \delta$ então $\alpha U_0 \subseteq U$. Perceba que

$$B = \bigcup_{|\alpha|_p < \delta} \alpha U_0$$

é uma vizinhança aberta da origem, contida em U e balanceada, ou seja, se $|\beta|_p \leq 1$, então $\beta B \subseteq B$. Note que para cada $x \in C, \exists n \in \mathbb{N}$ tal que $p^n x \in B$, logo $x \in p^{-n} B$ e

$$C \subseteq \bigcup_{n=1}^{\infty} p^{-n} B.$$

Como C é compacto, existem $n_1 < \ldots < n_l$ tais que

$$C \subseteq \bigcup_{j=1}^{l} p^{-n_j} B$$

Como $\forall j$, temos que

$$n_l \geq n_j, \Rightarrow |p^{n_l}|_p \leq |p^{n_j}|_p \Rightarrow |p^{n_l - n_j}|_p \leq 1 \Rightarrow p^{n_l - n_j} B \subseteq B \Rightarrow p^{-n_j} B \subseteq p^{-n_l} B,$$

então

$$C \subseteq p^{-n_l} B \subseteq p^{-n_l} U \Rightarrow p^{n_l} C \subseteq U.$$

Portanto

$$C \subseteq W + U$$

para toda vizinhança U da origem. Se para cada $x \in C$, escrevemos $x = w_u + y_u$, com $w_u \in W$ e $y_u \in U$, como $y_u \longrightarrow 0$ (convergência de redes), segue que $w_u \longrightarrow x$ pois V é Hausdorff, logo $x \in \overline{W}$. Como por (9), W é fechado, concluimos que $C \subseteq W$. Mas C é vizinhança da origem, logo se $x \in V$, $\exists n \in \mathbb{N}$ tal que $p^n x \in C$, logo $x \in p^{-n} C \subseteq p^{-n} W = W$. Portanto, $V = W$. □

Lema 11. *Se $(K, |\ |)$ é um corpo com valor absoluto localmente compacto, então é completo.*

Demonstração. Seja $\hat{K}$ o completamento de K e $\overline{K}$ o fecho topológico de K em $\hat{K}$. Se provarmos que $K = \overline{K}$, segue que K é completo.

Primeiramente provaremos que K é aberto em $\overline{K}$. Seja $x \in K$ e U vizinhança aberta de x em K cujo fecho topológico em K, que denotamos por C, é compacto e escrevemos $U = V \cap K$, com V vizinhança aberta de x em $\overline{K}$. Como C é compacto e $\overline{K}$ é Hausdorff então C é fechado em $\overline{K}$, logo $V \setminus C$ é aberto em $\overline{K}$ mas $(V \setminus C) \cap K = \emptyset$ pois $V \cap K = U \subseteq C$. Portanto, $V \setminus C = \emptyset$, logo $x \in V \subseteq C \subseteq K$ e concluimos que K é aberto em $\overline{K}$.

Agora suponha por absurdo que $\overline{K} \setminus K \neq \emptyset$, tome $y \in \overline{K} \setminus K$ e note que yK é vizinhança aberta de y em $\overline{K}$ contida em $\overline{K} \setminus K$ pois se existisse $x \in yK \cap K$, escrevendo $x = yk$, com $k \in K$, teríamos $y = xk^{-1} \in K$, o que é absurdo. Portanto, K é fechado em $\overline{K}$, logo é fechado em $\hat{K}$ e assim temos que $\overline{K} = K$. □

Teorema 9. *Se $(K, |\ |)$ é corpo com valor absoluto localmente compacto e de característica 0, então existe um isomorfismo, que também é homeomorfismo, entre*

(i) $\mathbb{R}$ ou $\mathbb{C}$, se $(K, |\ |)$ é arquimediano;

(ii) Uma extensão finita de $\mathbb{Q}_p$, para algum primo p, se $(K, |\ |)$ é não arquimediano.

Demonstração. Da Análise, sabemos que $\mathbb{R}$ e $\mathbb{C}$ são corpos localmente compactos. Agora se $K|\mathbb{Q}_p$ é extensão finita de grau n, de (8), segue que existe um isomorfismo linear, que também é homeomorfismo entre K e $\mathbb{Q}_p^n$ e já que $\mathbb{Q}_p$ é localmente compacto, segue que K é localmente compacto.

Agora seja $(K, |\ |)$ como no enunciado. Se o valor absoluto é arquimediano, por Ostrowski (8), temos o caso (i). Se o valor absoluto é não arquimediano, como $char(K) > 0$, temos que $\mathbb{Q} \subseteq K$ e como o valor absoluto é não arquimediano, sua restrição é equivalente a um valor absoluto p-ádico por 7. Como K é completo, segue da unicidade do completamento (6) que o fecho topológico de $\mathbb{Q}$ em K é $\mathbb{Q}_p \subseteq K$. Concluímos então por (10), que K é extensão finita de $\mathbb{Q}_p$. □

Observação 1. *É possível mostrar que se $(K, |\ |)$ é um corpo de característica p com valor absoluto localmente compacto, então existe um isomorfismo, que também é homeomorfismo, entre K e uma extensão finita de $\mathbb{F}_p((t))$. Uma demonstração desse fato pode ser encontrada em Weil (1982).*

3.4 EXTENSÕES DE VALORIZAÇÕES

Por ora vamos fixar um corpo K henseliano com respeito a uma valoração não arquimediana v ou $|\ |$, ou seja, um corpo no qual vale o lema de Hensel. Vamos denotar o anel de valoração, o ideal maximal e o corpo de resíduos, respectivamente, por $\mathcal{o}, \mathfrak{p}, \kappa$. Se $L|K$ é uma extensão algébrica finita de grau n, sabemos que v se estende unicamente para uma valoração w em L tal que

$$w(\alpha) = \frac{1}{n} v(N_{L|K}(\alpha))$$

e os invariantes correspondentes de L denotamos por $\mathcal{O}, \mathfrak{B}, \lambda$. Temos as inclusões

$$v(K^*) \subseteq w(L^*) \ e \ \kappa \subseteq \lambda.$$

O índice

$$e(w|v) = (w(L^*) : v(K^*))$$

é chamado de índice de ramificação da extensão $L|K$ e o grau

$$f(w|v) = [\lambda : \kappa]$$

é chamado de grau de inércia. Se v, e portanto w é discreta e se $\mathcal{o}, \mathfrak{p}, \pi$, respectivamente $\mathcal{O}, \mathfrak{B}, \Pi$ são o anel de valoração, o ideal maximal e o elemento primo de K e L respectivamente, então

$$e = (w(\Pi)\mathbb{Z} : v(\pi)\mathbb{Z})$$

e $v(\pi) = ew(\Pi)$. Logo, $\pi = \varepsilon \Pi^e$ para alguma unidade $\varepsilon \in \mathcal{o}^*$, portanto

$$\mathfrak{p}\mathcal{O} = \mathfrak{B}^e,$$

e o conceito de índice de ramificação coincide com o que definimos para ideais primos.

Teorema 10. *Temos que* $[L : K] \geq e(w|v)f(w|v)$ *e a identidade fundamental*

$$[L : K] = e(w|v)f(w|v)$$

se v é discreta e $L|K$ separável.

Demonstração. Seja $w_1, \ldots, w_f \in \mathcal{o}$ tal que $\overline{w}_1, \ldots, \overline{w}_f \in \lambda$ são LI sobre κ e $\pi_0, \ldots, \pi_{e-1} \in L^*$ tais que $w(\pi_0), \ldots, w(\pi_{e-1})$ representam e classes laterais distintas em $w(L^*)/v(K^*)$. Note que

$$f \leq f(w|v), \qquad e \leq e(w|v)$$

e a princípio não sabemos se do lado direito das desigualdades temos números finitos. Afirmamos que os elementos

$$w_j\pi_i,\ j=1,\dots,f,\ i=0,\dots,e-1$$

são LI sobre K. Provado isso, teremos a finitude de $e(w|v)$ e $f(w|v)$ e a desigualdade desejada.

Suponha por absurdo que os elementos são LD, então existem $a_{ij}\in K$ não todos nulos tais que

$$\sum_{i=0}^{e-1}\sum_{j=1}^{f}a_{ij}w_j\pi_i=0.$$

Denote $s_i=\sum_{j=1}^{f}a_{ij}w_j$. Então para cada i tal que exista um j com $a_{ij}\neq 0$, temos que

(i) $s_i\neq 0$;

(ii) $w(s_i)\in v(K^*)$.

De fato, fixado i, denote por a_{iv} o coeficiente de menor valor e teremos a seguinte combinação linear com coeficientes em $\mathcal{o}\subseteq K$

$$\frac{s_i}{a_{iv}}=\sum_{j=1}^{f}\frac{a_{ij}}{a_{iv}}w_j,$$

com um dos coeficientes sendo igual a 1, logo $s_i/a_{iv}\not\equiv 0\ mod\ \mathfrak{B}$, ou seja, s_i/a_{iv} é unidade, devido a independência linear dos $\overline{w}_1,\dots,\overline{w}_f\in\lambda$ sobre κ. Sendo assim, $s_i\neq 0$ e $w(s_i)=v(a_{iv})\in v(K^*)$.

Como $\sum_{i=0}^{e-1}s_i\pi_i=0$, existem dois termos não nulos no somatório com a mesma valoração, pois caso contrário teríamos $w(0)=\min\{w(s_i\pi_i)\}$. Digamos que $w(s_i\pi_i)=w(s_j\pi_j)$ com $i\neq j$, então

$$w(\pi_i)-w(\pi_j)=w(s_j)-w(s_i)\in v(K^*),$$

o que é absurdo.

Agora supondo que v é discreta, provaremos que os elementos $w_j\pi_i$ formam uma base integral de $\mathcal{O}$ sobre $\mathcal{o}$, em particular é uma base para $L|K$ e disso segue a igualdade fundamental. Considere então o $\mathcal{o}$-módulo

$$M=\sum_{i=0}^{e-1}\sum_{j=1}^{f}\mathcal{o}w_j\pi_i,$$

com $\pi_i=\Pi^i$, onde Π é um elemento primo de $\mathcal{O}$. Afirmamos que $M=\mathcal{O}$. Para isso, denote

$$N=\sum_{j=1}^{f}\mathcal{o}w_j\pi_i$$

logo $M = N+\Pi N+\cdots+\Pi^{e-1}N$ e dado $\alpha \in \mathcal{O}$, temos que $\alpha \equiv a_1w_1+\cdots a_fw_f \; mod\, \Pi\mathcal{O}, a_i \in \mathcal{o}$ e disso segue que

$$\mathcal{O} = N + \Pi\mathcal{O}.$$

Logo

$$\mathcal{O} = N + \Pi(N + \Pi\mathcal{O}) = \cdots = N + \Pi N + \cdots + \Pi^{e-1}N + \Pi^e\mathcal{O},$$

portanto $\mathcal{O} = M+\mathfrak{B}^e = M+\mathfrak{p}\mathcal{O}$. Como $L|K$ é separável, então $\mathcal{O}$ é um $\mathcal{o}$-módulo finitamente gerado e concluímos pelo lema de Nakayama que $\mathcal{O} = M$. □

Definição 31. *Uma extensão finita $L|K$ é dita não ramificada se a extensão $\lambda|\kappa$ de seus corpos de resíduo for separável e se*

$$[L : K] = [\lambda : \kappa].$$

Uma extensão algébrica arbitrária $L|K$ é dita não ramificada se for a união de subextensões finitas não ramificadas.

Proposição 46. *Se $L|K$ é uma extensão não ramificada, então $w(L^*) = v(K^*)$.*

Demonstração. Vamos primeiro provar o caso finito. Pela proposição anterior, temos que

$$[L : K] \geq (w(L^*) : v(K^*))[\lambda : \kappa] \Rightarrow (w(L^*) : v(K^*)) = 1 \Rightarrow w(L^*) = v(K^*).$$

Para o caso infinito escreva $L = \bigcup L_i$ com $L_i|K$ extensão finita não ramificada, logo

$$w(L^*) = \bigcup w(L_i^*) = \bigcup v(K^*) = v(K^*)$$

□

Proposição 47. *Seja $L|K$ e $K'|K$ duas extensões dentro de um fecho algébrico $\overline{K}|K$ e seja $L' = LK'$. Se $L|K$ é não ramificada $\Longrightarrow L'|K'$ então é não ramificada.*

Demonstração. Ver proposição 7.2 do capítulo 2 de Neukirch (1999).

□

Corolário 5. *Cada subextensão de uma extensão não ramificada é também não ramificada.*

Demonstração. Ver cororlário 7.3 do capítulo 2 de Neukirch (1999).

□

Proposição 48. *Se $\{L_i\}_{i\in I}$ é uma família de extensões não ramificadas de K e denotamos o compósito dos L_i por L, então $L|K$ é não ramificada.*

Demonstração. Vamos primeiro provar o caso de uma família finita de extensões finitas e para isso basta provar o caso para 2 extensões pois o caso para uma maior quantidade segue por indução. Dito isso, sejam $L|K$ e $L'|K$ extensões finitas não ramificadas, então $LL'|L'$ é não ramificada pela proposição anterior, logo $LL'|K$ é não ramificada, pois a propriedade de separabilidade dos corpos e dos corpos de resíduos é transitiva e o grau das extensões de corpos e dos corpos de resíduos é multiplicativa.

Para o caso geral, considere L, L_i como no enunciado e escreva $L_i = \bigcup_{j\in J(i)} L_{i,j}$, com $L_{i,j}|K$ extensão não ramificada finita. Então temos que

$$L = \bigcup_{\substack{n,m_1,\ldots,m_n\in\mathbb{N}\\ i_1,\ldots,i_n\in I}} \left(\prod_{j_{i_1}=1}^{m_1} L_{i_1,j_{i_1}} \cdots \prod_{j_{i_n}=1}^{m_n} L_{i_n,j_{i_n}} \right)$$

e o resultado segue do caso finito. □

Definição 32. *Seja $L|K$ uma extensão algébrica. Então o compósito $T|K$ de todas as subextensões não ramificadas é chamada de subextensão não ramificada maximal de $L|K$.*

Proposição 49. *O corpo de resíduos de T é o fecho separável λ_s de κ no corpo de resíduos λ de L.*

Demonstração. Ver proposição 7.5 de Neukirch (1999).

□

O compósito de todas as extensões não ramificadas de K dentro do fecho algébrico $\overline{K}$ de K é chamada de extensão não ramificada maximal $K_{nr}|K$ de K. Seu corpo de resíduos é o fecho separável $\overline{\kappa}_s|\kappa$. K_{nr} contém todas as raízes da unidade de ordem m não divisível pela característica de κ pois o polinômio $x^m - 1$ se decompõe sobre $\overline{\kappa}_s$ e portanto sobre K_{nr} pelo lema de Hensel. Se κ é corpo finito, então a extensão $K_{nr}|K$ é gerada por essas raízes da unidade pois elas geram $\overline{\kappa}_s|\kappa$.

Proposição 50. *Seja $(n,p) = 1$ e $x \in K^*$. Então $K(\sqrt[n]{x})|K$ é não ramificada se e somente se $x \in U_K^n$.*

Demonstração. Ver lema 5.6 do capítulo 3 de Neukirch (1986). □

Vimos que valorações Henselianas se estendem de maneira única para uma extensão algébrica e agora vamos estudar como uma valoração qualquer de um corpo K pode ser estendida para uma estensão algébrica $L|K$. Até o momento utilizamos letras v, w para nos referirmos a valorações não arquimedianas mas daqui pra frente se mostrará útil utilizarmos a mesma notação para nos referirmos a valorações arquimedianas, ou seja a valores absolutos arquimedianos. Para cada valoração v num corpo K, consideramos o completamento K_v e o fecho algébrico $\overline{K}_v$ de K_v. Denotamos a extensão canônica de v para K_v novamente por v e a única extensão desta para $\overline{K}_v$ por $\overline{v}$. Seja $L|K$ uma extensão algébrica e fixamos um K-mergulho

$$\tau : L \longrightarrow \overline{K}_v$$

então

$$w = \overline{v} \circ \tau$$

é uma valoração em L que estende v. Se $[L : K] < \infty$, denotamos por L_w o completamento de L, com respeito ao valor absoluto $|\ \ |_w$. Se $[L : K] = \infty$, denotamos $L_w = \bigcup_i L_{iw}$ a união dos completamentos L_{iw} de todas as extensões finitas $L_i|K$ de $L|K$. Em qualquer um dos casos chamamos L_w de localização de L com respeito a w. Note que o mapa $\tau : L \longrightarrow \overline{K}_v$ é contínuo com respeito a w e se estende de maneira única para L_w. No caso de dimensão finita, τ é dado pela expressão

$$x = w - \lim_{n\to\infty} x_n \quad \longmapsto \quad \tau x := \overline{v} - \lim_{n\to\infty} \tau x_n,$$

onde (x_n) é uma w-sequência de Cauchy em L. Consideramos o diagrama de corpos

$$\begin{array}{ccc} L & \text{———} & L_w \\ \Big| & & \Big| \\ K & \text{———} & K_v \end{array}$$

e a extensão canônica de w para L_w é precisamente a única extensão da valoração v de K_v para a extensão de corpos $L_w|K_v$ e no caso de dimensão finita temos

$$L_w = LK_v.$$

Definição 33. *Sejam $\tau, \tau' : L \longrightarrow \overline{K}_v$ K-mergulhos. Dizemos que eles são conjugados sobre K_v se existe $\sigma \in G(\overline{K}_v|K_v)$ tal que $\tau' = \sigma \circ \tau$.*

Proposição 51 (Teorema de Extensão)**.** *Seja $L|K$ uma extensão algébrica e v uma valoração sobre K. Então*

(i) Toda extensão w da valoração v pode ser escrita como $w = \overline{v} \circ \tau$ para algum K-mergulho $\tau : L \longrightarrow \overline{K}_v$;

(ii) Duas extensões $\overline{v} \circ \tau$ e $\overline{v} \circ \tau'$ são iguais se e somente se τ e τ' são conjugados sobre K_v.

Demonstração. Ver teorema 8.1 do capítulo 2 de Neukirch (1999).

□

Proposição 52. *Seja K um corpo com valoração v e $L = K(\alpha)$ uma extensão de K e denote $f(X) \in K[X]$ o polinômio mínimo de α sobre K. Então as diferentes valorações $w_1, \ldots, w_r$ que estendem v a L estão em correspondência $1-1$ com os fatores irredutíveis $f_1(X), \ldots, f_r(X) \in K_v[X]$ da fatoração*

$$f(X) = f_1(X)^{m_1} \cdots f_r(X)^{m_r}$$

de f sobre o completamento K_v.

A extensão w_i pode ser obtida explicitamente do fator f_i da seguinte manteira: seja $\alpha_i \in \overline{K}_v$ um zero de f_i e seja

$$\tau_i : L \longrightarrow \overline{K}_v, \quad \alpha \longmapsto \alpha_i$$

o K-mergulho de L em $\overline{K}_v$ correspondente. Então temos que

$$w_i = \overline{v} \circ \tau_i$$

e τ_i estende para um isomorfismo

$$\tau_i : L_{w_i} \longrightarrow K_v(\alpha_i)$$

do completamente L_{w_i} de L com respeito a w_i.

Demonstração. Ver proposição 8.2 do capítulo 2 de Neukirch (1999).

□

Seja $L|K$ uma extensão finita de corpos arbitrária. Escrevemos $w|v$ para indicar que w é uma valoração em L que estende a valoração v de K. A inclusão $L \hookrightarrow L_w$ induz um homomorfismo

$$L \otimes_K K_v \longrightarrow L_w, \quad a \otimes b \longmapsto ab$$

e a partir dele temos um homomorfismo canônico

$$\varphi : L \otimes_K K_v \longmapsto \prod_{w|v} L_w.$$

Proposição 53. *Se $L|K$ é separável, então $L \otimes_K K_v \simeq \prod_{w|v} L_w$.*

Demonstração. Ver proposição 8.3 do capítulo 2 de Neukirch (1999).

□

Corolário 6. *Se $L|K$ é separável, então temos que*

$$[L : K] = \sum_{w|v} [L_w : K_v].$$

Demonstração.

$$[L : K] = \dim_K(L) = \dim_{K_v}(L \otimes_K K_v) = \dim_{K_v}\left(\prod_{w|v} L_w\right) = \sum_{w|v} \dim_{K_v}(L_w) = \sum_{w|v} [L_w : K_v].$$

□

Se v é uma valoração não arquimediana e temos uma extensão $w|v$, assim como no caso henseliano, definimos o índice de ramificação

$$e_w = (w(L^*) : v(K^*))$$

e o grau de inércia

$$f_w = [\lambda_w : \kappa]$$

, onde λ_w e κ são os corpos de resíduo com respeito a w e a v respectivamente.

Proposição 54 (Identidade fundamental da teoria de valoração)**.** *Se v é uma valoração discreta e $L|K$ é uma extensão finita separável, então*

$$\sum_{w|v} e_w f_w = [L : K].$$

Demonstração. Pelo teorema 10, temos que $e_w f_w = [L_w : K_v]$ e o resultado segue do corolário anterior. □

E a partir dessa proposição podemos perceber a a conexão entre a teoria de ideais primos em domínios de Dedekind e a teoria de valoração. Com efeito, se $\mathcal{O}$ é um domínio de Dedekind com corpo de frações K e $\mathfrak{p}$ é um ideal primo, então temos a valoração $\mathfrak{p}$-ádica $v_\mathfrak{p}$ de K, definida para $a \neq 0$ como

$$v_\mathfrak{p}(a) = v_\mathfrak{p}, \quad \text{onde} \quad (a) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}}$$

e o anel de valoração de $v_\mathfrak{p}$ é a localização $\mathcal{O}_\mathfrak{p}$. Se $L|K$ é uma extensão finita e separável, sendo $\mathcal{O}$ o fecho integral de $\mathcal{O}$ em L, sabemos que $\mathcal{O}$ é um domínio de Dedekind então considere a fatoração em ideais primos

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

então as valorações $w_i = \frac{1}{e_i} v_{\mathfrak{B}_i}, i = 1, \ldots, r$ estendem $v = v_\mathfrak{p}$ a L e é fácil ver que o índice de ramificação e_i da teoria de ideais, é igual ao respectivo índice de ramificação da teoria de valoração e que o grau de inércia $f_i = [\mathcal{O}/\mathfrak{B}_i : \mathcal{O}/\mathfrak{p}]$ da teoria de ideais é igual ao respectivo grau de inércia da teoria de valoração. E das identidades fundamentais da teoria de ideais e da teoria de valoração, vemos que $w_1, \ldots, w_r$ são de fato todas as possíveis extensões de valoração de v para L e assim a identidade fundamental da teoria de ideais e da teoria de valoração coincidem neste caso. Outro resultado simples de provar é que se $\mathfrak{B}$ é um ideal primo de L sobre o ideal primo $\mathfrak{p}$ de K, então $\mathfrak{B}$ é um ideal não ramificado se e somente a extensão de corpos $L_\mathfrak{B}|K_\mathfrak{p}$ for não ramificada, onde $K_\mathfrak{p}$ denota o completamento de K com respeito a valoração $\mathfrak{p}$-ádica e $L_\mathfrak{B}$ denota o completamento de L com respeito a valoração $\mathfrak{B}$-ádica. Este tipo de conexão entre as diferentes teorias será amplamente explorada ao longo do próximo capítulo para o caso de corpos de inteiros.

Se $L|K$ for uma extensão Galoisiana, w for uma valoração em L que estende a valoração v de K e $\sigma \in G = G(L|K)$, então $w \circ \sigma$ também é uma valoração em L que estende v e disso deduzimos que G age à direita nas extensões $w|v$.

Proposição 55. *A ação de G no conjunto das extensões $w|v$ é transitiva.*

Demonstração. Ver proposição 9.1 do capítulo 2 de Neukirch (1999).

□

Definição 34. *O grupo de decomposição de uma extensão w de v para L é definido como*

$$G_w = G_w(L|K) = \{\sigma \in G(L|K) | w \circ \sigma = w\}.$$

Proposição 56.

$$G_w(L|K) \simeq G(L_w|K_v).$$

Demonstração. Ver proposição 9.6 do capítulo 2 de Neukirch (1999).

□

4 TEORIA DE CORPOS DE CLASSE E O PRINCÍPIO LOCAL-GLOBAL PARA QUÁDRICAS

A teoria de corpos de classe busca estudar as extensões abelianas $L|K$ de corpos de números e de corpos de números $\mathfrak{p}$-ádicos. Essas extensões podem ser classificadas por certos grupos $\mathcal{N}_L = N_{L|K}A_L$ associados ao corpo base. No caso $\mathfrak{p}$-ádico, A_K é o grupo multiplicativo K^* e no caso de corpos de números utilizamos uma generalização do grupo de classe de ideais. Isso nos permite estudar as extensões abelianas a partir das propriedades intrínsecas do corpo base K. No centro dessa teoria, temos um isomorfismo canônico

$$G(L|K) \simeq A_K/N_{L|K}A_L$$

conhecido como mapa de reciprocidade. Este mapa que ocorre tanto no caso "local" quanto no caso "global" pode ser abstraído de sua natureza concreta relacionada aos corpos e ser tratado de um ponto de vista mais abstrato, o que nos permite desenvolver a teoria de corpos de classe generalizada e a partir dela estudar a teoria de corpos de classe local e a teoria de corpos de classe global. Desenvolvemos essa teoria para provar o Teorema de Hasse-Minkowski, conhecido também como princípio local-global para quádricas que garante que uma quádrica

$$Q(X_1, \ldots, X_n) = \sum_{i,j} a_{ij}X_iX_j$$

com coeficientes num corpo de números K representa 0 se e somente se representa 0 localmente, ou seja, em cada completamento $K_\mathfrak{p}$. Os conceitos envolvidos no enunciado do teorema serão desenvolvidos ao longo deste capítulo.

4.1 TEORIA DE GALOIS INFINITA

Definição 35. *Seja $\Omega|k$ uma extensão de corpos Galoisiana, definimos a topologia de Krull sobre o grupo de Galois $G = G(\Omega|k)$ da seguinte forma: para cada $\sigma \in G$, tomamos as classes laterais a esquerda*

$$\sigma G(\Omega|K)$$

como uma base de vizinhanças de σ, onde $K|k$ percorre todas as subextensões Galoisianas finitas de $\Omega|k$. E desta forma é fácil verificar que G é um grupo topológico.

Proposição 57. *Se $\Omega|k$ é uma extensão Galoisiana (finita ou infinita), então $G = G(\Omega|k)$ é Hausdorff e compacto com respeito a topologia de Krull.*

Demonstração. Ver proposição 1.1 do capítulo 1 de Neukirch (1986).

□

Proposição 58. *Seja $\Omega|k$ uma extensão Galoisiana (finita ou infinita) e considere o mapa*

$$K \mapsto G(\Omega|K).$$

Então

(i) O mapa é uma correspondência 1-1 entre as subextensões $K|k$ de $\Omega|k$ e os subgrupos fechados de $G(\Omega|k)$;

(ii) Os subgrupos abertos de $G(\Omega|k)$ são fechados e correspondem as subextensões finitas de $\Omega|k$.

Demonstração. Ver teorema 1.2 do capítulo 1 de Neukirch (1986).

□

Definição 36. *Um grupo profinito é um grupo topológico G Hausdorff e compacto e que possui uma base de vizinhanças abertas de $1 \in G$ consistindo de subgrupos normais.*

Definição 37. *Seja I um conjunto não vazio e $\leq$ uma relação em I. Dizemos que $(I, \leq)$ é um conjunto dirigido se a relação $\leq$ for reflexiva, transitiva e para quaisquer $i, j \in I$, existir $k \in I$ tal que $i \leq k$ e $j \leq k$. Quando estiver claro qual a relação simplesmente escrevemos I em vez de $(I, \leq)$ para nos referirmos ao conjunto dirigido. Um sistema projetivo sobre I é uma família $\{X_i, f_{ij} \mid i, j \in I,\ i \leq j\}$ de espaços topológicos X_i e mapas contínuos*

$$f_{ij} : X_j \longrightarrow X_i$$

tais que $f_{ii} = id_{X_i}$ e

$$f_{ik} = f_{ij} \circ f_{jk}$$

sempre que $i \leq j \leq k$.

Definição 38. *O limite projetivo*

$$X = \varprojlim_{i \in I} X_i$$

do sistema projetivo $\{X_i, f_{ij}\}$ é definido como o subconjunto

$$X = \left\{ (x_i)_{i \in I} \in \prod_{i \in I} X_i \mid f_{ij}(x_j) = x_i \text{ sempre que } i \leq j \right\}$$

do conjunto $\prod_{i \in I} X_i$.

Proposição 59. *Se G é um grupo profinito e N percorre os subgrupos normais abertos de G, então temos topologicamente e algebricamente*

$$G \simeq \varprojlim_{N} G/N.$$

Inversamente, se $\{G_i, f_{ij}\}$ é um sistema projetivo de grupos finitos G_i, então

$$G = \varprojlim_{i} G_i$$

é um grupo profinito.

Demonstração. Ver proposição 2.2 do capítulo 1 de Neukirch (1986).

□

Definição 39. *Os anéis $\mathbb{Z}/n\mathbb{Z},\ n \in \mathbb{N}$ formam um sistema projetivo com respeito as projeções $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ para $m|n$ quando consideramos $\mathbb{N}$ como conjunto dirigido com a relação de divisibilidade. Então o limite projetivo*

$$\hat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$$

é chamado de anel dos inteiros profinitos, ou anel de Prüfer, que se relaciona com os p-ádicos a partir do isomorfismo canônico

$$\hat{\mathbb{Z}} \simeq \prod_{p} \mathbb{Z}_p.$$

4.2 COHOMOLOGIA DE GRUPOS

Definição 40. *Seja G um grupo. Um G-módulo é um grupo abeliano A sobre o qual G age. O submódulo fixado é o subgrupo*

$$A^G = \{a \in A \mid \sigma a = a,\ \forall \sigma \in G\}.$$

A é dito um G-módulo trivial se $A^G = A$. Se G é um grupo profinito, então dizemos que A é um G-módulo multiplicativo contínuo se

$$A = \bigcup_{U} A^U$$

onde U percorre os subgrupos normais abertos de G. Note que isso é equivalente a dizer que G age continuamente sobre A, ou seja, que se considerarmos A com a topologia discreta, então a aplicação

$$G \times A \longrightarrow A, \quad (\sigma, a) \longmapsto \sigma a$$

é contínua.

Definição 41. *Um G-homomorfismo entre dois G-módulos A e B é um homomorfismo de grupos $f : A \longrightarrow B$, satisfazendo*

$$f(\sigma a) = \sigma f(a),\ \forall \sigma \in G, \forall a \in A.$$

Definição 42. *Se G é um grupo finito, então cada G-módulo A contém o subgrupo das normas definido como*

$$N_G A = \left\{ N_G(a) = \sum_{\sigma \in G} \sigma a \mid a \in A \right\}.$$

Note que $N_G A < A^G$.

Definição 43. *O grupo residual das normas é o grupo quociente*

$$H^0(G, A) = A^G / N_G A.$$

Definição 44. *Um 1-cociclo de G em A é uma função $f : G \longrightarrow A$ tal que:*

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau),\ \forall \sigma, \tau \in G.$$

Os 1-cociclos formam um grupo abeliano denotado $Z^1(G, A)$. Para cada $a \in A$, definimos o 1-cobordo

$$f_a : G \longrightarrow A, f_a(\sigma) = \sigma a - a,$$

que é claramente um 1-cociclo pois

$$f_a(\sigma\tau) = (\sigma\tau)a - a = \sigma(\tau a - a) + \sigma a - a = f_a(\sigma) + \sigma f_a(\tau).$$

Os 1-cobordos formam um subgrupo de $Z^1(G, A)$ que denotamos $B^1(G, A)$. Definimos o primeiro grupo de cohomologia como:

$$H^1(G, A) = Z^1(G, A)/B^1(G, A).$$

Proposição 60. *Se temos uma sequência exata curta de G módulos*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

então temos induzida a sequência exata

$$0 \longrightarrow A^G \xrightarrow{i} B^G \xrightarrow{j} C^G \xrightarrow{\delta} H^1(G, A).$$

Demonstração. Ver proposição 3.1 do capítulo 1 de Neukirch (1986).

□

Proposição 61. *Se g é um subgrupo normal de G e A é um G-módulo, então temos a sequência exata*

$$0 \longrightarrow H^1(G/g, A^g) \longrightarrow H^1(G, A) \longrightarrow H^1(g, A).$$

Demonstração. Ver proposição 3.2 do capítulo 1 de Neukirch (1986).

□

Definição 45. *Sejam G um grupo, $g < G$ um subgrupo e B um g-módulo. O G-módulo induzido por B, denotado por $M_G^g(B)$ é o grupo abeliano*

$$M_G^g(B) = \{f : G \longrightarrow B : f(\tau x) = \tau f(x)\ \forall \tau \in g\}.$$

A ação de G em $M_G^g(B)$ é dada por $(\sigma f)(x) = f(x\sigma)$. Temos assim um g-homomorfismo canônico

$$\begin{aligned} \pi : M_G^g(B) &\longrightarrow B \\ f &\longrightarrow f(1), \end{aligned}$$

que mapeia o g-submódulo

$$B' = \{f \in M_G^g \mid f(x) = 0 \text{ para } x \notin g\}$$

isomorficamente em B. Identificamos B' com B. Se g tiver índicie finito sobre G, é fácil ver que

$$M_G^g(B) = \bigoplus_{\sigma \in G/g} \sigma B,$$

onde σ percorre um sistema completo de representantes a esquerda de G/g. Se $g = \{1\}$, então escrevemos $M_G(B)$ para denotar $M_G^g(B)$.

Proposição 62. *Sejam G um grupo finito, $g < G$ um subgrupo e B um g-módulo. Para $i = 0, 1$ temos um isomorfismo natural*

$$H^i(G, M_G^g(B)) \simeq H^i(g, B).$$

Demonstração. Ver proposição 3.3 do capítulo 1 de Neukirch (1986).

□

Definição 46. *Sejam $G = \langle\sigma\rangle$ um grupo cíclico finito e A um G-módulo. Definimos os seguintes G-submódulos de A:*

$$ {}_{N_G}A = \{a \in A | N_G(a) = 0\}, \quad I_G A = \{\sigma a - a | a \in A\}. $$

Claramente $I_G A <\ {}_{N_G}A$ e podemos definir

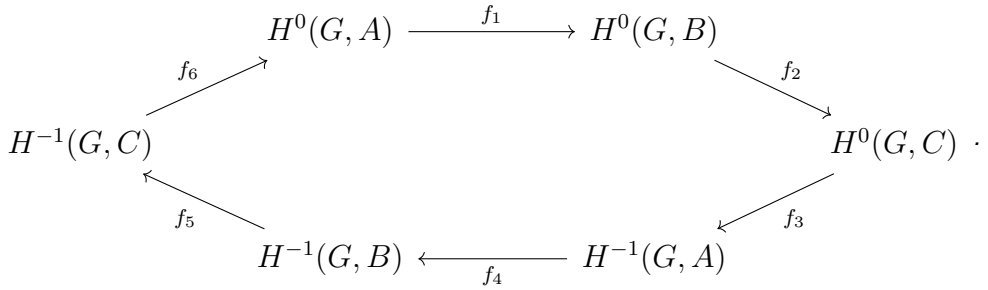
$$ H^{-1}(G, A) = {}_{N_G}A / I_G A. $$

Observação 2. *Em notação multiplicativa, definimos $a^{\sigma-1} = a^{\sigma}.a^{-1}$*

Proposição 63. *Dada uma sequência exata curta de G-módulos:*

$$ 0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0, $$

ela induz o seguinte hexágono exato:



Demonstração. Ver proposição 4.1 do capítulo 1 de Neukirch (1986).

□

Definição 47. *Sejam G um grupo finito cíclico e A um G-módulo, então o quociente de Herbrand de de A é definido como*

$$ h(G, A) = \frac{\#H^0(G, A)}{\#H^{-1}(G, A)} $$

se ambas cardinalidades forem finitas.

Proposição 64. *Se $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ é uma sequência exata de G-módulos, então*

$$ h(G, B) = h(G, A).h(G, C), $$

de modo que se quaisquer 2 dos quocientes forem finitos, então o terceiro também é finito e vale a igualdade acima.

Demonstração. Ver proposição 4.3 do capítulo 1 de Neukirch (1986).

□

Proposição 65. *Se A é um G-módulo finito, então $h(G, A) = 1$.*

Demonstração. Ver proposição 4.3 do capítulo 1 de Neukirch (1986).

□

Proposição 66. *Se G é um grupo finito cíclico, então $H^1(G, A) \simeq H^{-1}(G, A)$.*

Demonstração. Ver proposição 4.4 do capítulo 1 de Neukirch (1986).

□

Proposição 67 (Hilbert 90)**.** *Seja $L|K$ uma extensão de corpos finita e Galoisiana e seja $G = G(L|K)$. Então o grupo multiplicativo L^* é um G-módulo e temos*

$$H^1(G, L^*) = 1.$$

Em particular, se $G = \langle\sigma\rangle$ é cíclico, então todo elemento $a \in L^*$ cuja norma $N_{L|K}(a) = 1$ é da forma

$$a = \frac{\sigma b}{b},\ b \in L^*.$$

Demonstração. Ver proposição 5.1 do capítulo 1 de Neukirch (1986).

□

4.3 TEORIA DE CORPOS DE CLASSE GENERALIZADA

4.3.1 Teoria de Galois abstrata

Ao longo desta seção estaremos trabalhando com um grupo profinito G abstrato e buscaremos interpretar G formalmente como um grupo de Galois e aproveitar as noções e intuições da Teoria de Galois. Denotaremos os subgrupos fechados de G por G_K e chamaremos os índices K de corpos, nos referindo a K como o corpo fixado por G_K. O corpo k tal que $G_k = G$ será chamado de corpo base e denotaremos por $\overline{k}$ o corpo tal que $G_{\overline{k}} = 1$. Escrevemos formalmente $K \subseteq L$ ou $L|K$ se $G_L \subseteq G_K$ e nos referimos ao par $L|K$ como uma exntensão de corpos e dizemos que a extensão é finita se $(G_K : G_L) < \infty$ (ou seja, se G_L é aberto em G_K) e definimos

$$[L : K] = (G_K : G_L)$$

como o grau da extensão $L|K$. A extensão $L|K$ é dita Galoisiana ou normal se G_L é um subgrupo normal de G_K. Neste caso, definimos o grupo de Galois de $L|K$ como

$$G(L|K) = G_K/G_L.$$

Se $N \supseteq L \supseteq K$ são todas extensões Galoisianas, então definimos a restrição a L de um elemento $\sigma \in G(N|K)$ como

$$\sigma|_L = \sigma \ mod \ G(N|L) \in G(L|K).$$

A extensão $L|K$ é dita cíclica, abeliana, solúvel etc se o grupo de Galois $G(L|K)$ for cíclico, abeliano, solúvel etc. Para além disso, denotamos

$$K = \bigcap_i K_i$$

se G_K for gerado topologicamente pelos subgrupos G_{K_i} e

$$K = \prod_i K_i$$

se $G_K = \bigcap_i G_{K_i}$. Também definimos para cada $\sigma \in G$ o corpo L^σ com $G_{L^\sigma} = \sigma^{-1} G_L \sigma$.

Seja A um G módulo multiplicativo. Para cada corpo K, denotamos

$$A_K = A^{G_K} = \{a \in A \mid a^\sigma = a \ \forall \sigma \in G_K\}.$$

Se $L|K$ é uma extensão finita, então $A_K \subseteq A_L$ e temos o mapa norma

$$N_{L|K} : A_L \longrightarrow A_K, \quad N_{L|K}(a) = \prod_\sigma a^\sigma,$$

onde σ percorre um sistema completo de representantes de classes laterais a direita de G_K/G_L. Se $M \supseteq L \supseteq K$, então

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

Se $L|K$ for Galoisiana, então A_L é um $G(L|K)$ módulo e $A_K = A_L^{G(L|K)}$.

Ao longo desta subseção vamos supor que vale o seguinte **axioma**:

Para toda extensão cíclica $L|K$, temos que

$$H^{-1}(G(L|K), A_L) = 1$$

e vamos supor a existência de um G-homomorfismo sobrejetivo

$$\wp : A \longrightarrow A, \quad a \longmapsto a^\wp$$

com núcleo finito e cíclico $\mu_\wp$. A ordem $n = \#\mu_\wp$ é chamado de expoente do operador $\wp$. Vamos fixar um corpo K tal que $\mu_\wp \subseteq A_K$. Para cada subconjunto $B \subseteq A$, perceba que o grupo

$$H(B) = \{\sigma \in G_K | b^\sigma = b, \forall b \in B\}$$

é fechado em G, então denote por $K(B)$ seu corpo fixado. Se B é G_K-invariante, ou seja, $b^\sigma \in B, \forall b \in B, \forall \sigma \in G_K$, então $K(B)|K$ é claramente galoisiana. Uma extensão de Kummer (com respeito a $\wp$) é por definição uma extensão da forma

$$K(\wp^{-1}(\Delta))|K,$$

onde $\Delta \subseteq A_K$. Claramente uma extensão de Kummer $K(\wp^{-1}(\Delta))|K$ é sempre galoisiana e afirmamos que seu grupo de Galois é abeliano e tem expoente n, ou seja $\sigma^n = 1, \forall \sigma \in G(K(\wp^{-1}(\Delta))|K)$. Com efeito, note que para cada $a \in \Delta$, tomando $\alpha \in \wp^{-1}(a)$ podemos definir uma aplicação

$$G(K(\wp^{-1}(a)|K) \longrightarrow \quad \sigma \longmapsto \alpha^{\sigma-1}$$

e é fácil ver que se trata de um homomorfismo injetivo que não depende da escolha do $\alpha \in \wp^{-1}(a)$. Agora perceba que $L = \prod_{a\in\Delta} K(\wp^{-1}(a)|K)$ e o mapa de composição

$$G(L|K) \longrightarrow \prod_{a\in\Delta} G(K(\wp^{-1}(a)|K)) \longrightarrow \prod_{a\in\Delta} \mu_\wp$$

se trata de um homomorfismo injetivo. A proposição a seguir garante a recíproca, ou seja, que toda extensão abeliana $L|K$ de expoente n é uma extensão de Kummer (com respeito a $\wp$).

Proposição 68. *Se $L|K$ é uma extensão abeliana de expoente n, então*

$$L = K(\wp^{-1}(\Delta)), \quad \textit{com} \quad \Delta = A_L^\wp \cap A_K.$$

Demonstração. Primeiramente perceba que $\wp^{-1}(\Delta) \subseteq A_L$, pois se $x \in \wp^{-1}(\Delta)$, então existe $\alpha \in A_L$ tal que $x^\wp = \alpha^\wp = a \in A_K$, logo $x\alpha^{-1} = \xi \in \mu_\wp \subseteq A_K \subseteq A_L$, logo $x = \xi\alpha \in A_L$. Portanto, $K(\wp^{-1}(\Delta)) \subseteq L$, ou seja $G_L \subseteq H(\wp^{-1}(\Delta))$. Com efeito, se $\sigma \in G_L$, então $x^\sigma = x, \forall x \in A_L$, em particular, para todo $x \in \wp^{-1}(\Delta)$, logo $\sigma \in H(\wp^{-1}(\Delta))$.

Por outro lado, afirmamos que $L|K$ é o compósito de suas subextensões cíclicas finitas. Primeiramente provaremos que é o compósito de suas subextensões finitas: $L = \prod_{[M:K]<\infty} M$ ou seja

$$G_L = \bigcap_{(G_K:G_M)<\infty} G_M.$$

Isso é equivalente a provar que o mapa

$$G(L|K) \longrightarrow \prod_M G(M|K), \quad \sigma \longmapsto (\sigma|_M)$$

é injetivo e isso é verdade pois o núcleo desse mapa é

$$\bigcap_{(G_K:G_M)<\infty} G(L|M) = \bigcap_{(G_K:G_M)<\infty} \frac{G_M}{G_L} = 1,$$

pois $(G_M/G_L)_M$ é uma família de vizinhanças abertas do elemento neutro no grupo topológico hausdorff G_K/G_L.

Agora afirmamos que cada subextensão finita $M|K$ é o compósito de extensões cíclicas de K. Com efeito, como $G(M|K)$ é grupo abeliano finito, então é o produto de de grupos cíclicos e a partir disso é fácil ver que

$$\frac{G_K}{G_M} = \prod_{i=1}^{m} \frac{G_{K_i}}{G_M},$$

com $M|K_i,\ i = 1, \ldots, m$ extensões cíclicas, então tome

$$G_{C_i} = G_{K_1}.\cdots.G_{K_{i-1}}.G_M.G_{K_{i+1}}.\cdots G_{K_m},$$

logo

$$\bigcap_{i=1}^{m} \frac{G_{C_i}}{G_M} = 1 \Rightarrow \bigcap_{i=1}^{m} G_{C_j} = G_M \Rightarrow M = \prod_{i=1}^{m} C_i$$

e perceba que

$$\frac{G_K}{G_{C_i}} = \frac{G_{K_1}.\cdots.G_{K_{i-1}}.G_{K_i}.G_{K_{i+1}}.\cdots G_{K_m}}{G_{K_1}.\cdots.G_{K_{i-1}}.G_M.G_{K_{i+1}}.\cdots G_{K_m}} \simeq \frac{G_{K_i}}{G_M},$$

logo a extensão $C_i|K$ é cíclica.

Sendo assim, como $L|K$ é o compósito de suas subextensões cíclicas finitas, é suficiente mostrar que se $M|K$ é uma subextensão cíclica finita de $L|K$, então $M \subseteq K(\wp^{-1}(\Delta))$. Seja σ um gerador de $G(M|K)$ e ζ um gerador de $\mu_\wp$. Seja $d = [M : K], d' = n/d$ e $\xi = \zeta^{d'}$. Como $N_{M|K}(\xi) = \zeta^{dd'} = 1$, segue que $\xi = \alpha^{\sigma-1}$ para algum $\alpha \in A_M$. Assim $K \subseteq K(\alpha) \subseteq M$, ou seja $G_M \subseteq H(\alpha)$ e isso de fato é verdade pois $\alpha \in A_M$. Mas $\alpha^{\sigma^i} = \xi^i\alpha$, assim $\alpha^{\sigma^i} = \alpha$ é equivalente a $i \equiv 0\ mod\ d$, logo $H(\alpha)/G_M \subseteq G_K/G_M$ são ambos cíclicos e de ordem d, logo $K(\alpha) = M$. Mas $(\alpha^\wp)^{\sigma-1} = (\alpha^{\sigma-1})^\wp = \xi^\wp = 1$, então $a = \alpha^\wp \in A_K$. Portanto, $\alpha \in \wp^{-1}(\Delta)$, logo $M \subseteq K(\wp^{-1}(\Delta))$. □

E como o principal resultado da teoria geral de Kummer, temos a seguinte proposição.

Proposição 69. *A correspondência*

$$\Delta \longmapsto L = K(\wp^{-1}(\Delta))$$

é $1-1$ *entre os os grupos* Δ *tais que* $A_K^{\wp} \subseteq \Delta \subseteq A_K$ *e as extensões abelianas* $L|K$ *de expoente* n.

Se Δ *e* L *correspondem um ao outro, então* $A_L^{\wp} \cap A_K = \Delta$ *e temos um isomorfismo canônico*

$$\Delta/A_K^{\wp} \simeq Hom(G(L|K), \mu_{\wp}), \quad a \ mod \ A_K^{\wp} \longmapsto \chi_a,$$

onde o caráter $\chi_a : G(L|K) \longrightarrow \mu_{\wp}$ *é dado por* $\chi_a(\sigma) = \alpha^{\sigma-1}$, *para* $\alpha \in \wp^{-1}(a)$.

Demonstração. Ver teorema 3.3 do capítulo 4 de Neukirch (1999).

□

Observação 3. *Se* $L|K$ *é infinita, então* $G(L|K)$ *é munido da topologia de Krull e*

$$Hom(G(L|K), \mu_{\wp})$$

deve ser entendido como o grupo de todos os homomorfismo contínuos $\chi : G(L|K) \longrightarrow \mu_{\wp}$, *ou seja, o grupo de caráteres do grupo topológico* $G(L|K)$.

Observação 4. *O compósito de extensões de Kummer de expoente* n *é novamente uma extensão de Kummer de expoente* n *e toda extensão de Kummer está contida na extensão de Kummer maximal* $\hat{K} = K(\wp^{-1}(A_K))$ *de expoente* n, *e assim temos que*

$$Hom(G(\tilde{K}|K), \mu_n) \simeq \Delta/K^{*n}$$

e para o dual de Pontryagin temos

$$G(\hat{K}|K) = Hom(G(\hat{K}|K), \mathbb{Q}/\mathbb{Z}) = Hom(Hom(G(\hat{K}|K), \mu_{\wp}),$$

portanto

$$G(\hat{K}|K)^* \simeq A_K/A_K^{\wp}.$$

Corolário 7. *Seja* n *um número natural relativamente primo com a característica de um corpo* K *e suponha que* $\mu_n \subseteq K$. *então as extensões abelianas* $L|K$ *de expoente* n *correspondem* $1-1$ *aos subgrupos* $\Delta \subseteq K^*$ *que contém* K^{*n}, *através do mapa*

$$\Delta \longmapsto L = K(\sqrt[n]{\Delta})$$

e temos que

$$G(L|K) \simeq Hom(\Delta/K^{*n}, \mu_n).$$

Demonstração. Ver corolário 3.6 do capítulo 4 de Neukirch (1999). □

4.3.2 Teoria de valoração abstrata

No que segue, denotaremos sempre por K uma extensão finita do corpo base k e suporemos a existência de um homomorfismo sobrejetivo e contínuo

$$deg : G \longrightarrow \hat{\mathbb{Z}}.$$

Denotaremos o corpo fixado do núcleo desse mapa por $\tilde{k}$ então deg induz um isomorfismo (que é também homeomorfismo) $G(\tilde{k}|k) \simeq \hat{\mathbb{Z}}$. Para cada extensão finita $K|k$, definimos

$$\tilde{K} = K.\tilde{k} \quad e \quad f_K = [K \cap \tilde{k} : k].$$

Então o mapa deg induz um homomorfismo sobrejetivo e contínuo

$$deg_K = \frac{1}{f_K}\, deg : G_K \longrightarrow \hat{\mathbb{Z}}$$

e um isomorfismo (que também é homoeomorfismo) $deg_K : G(\tilde{K}|K) \xrightarrow{\sim} \hat{\mathbb{Z}}$.

Definição 48. *O elemento $\varphi_K \in G(\tilde{K}|K)$ com $deg(\varphi_K) = 1$ é chamado Frobenius sobre K. Note que ele gera topologicamente o grupo de Galois.*

Lema 12. *Se $L|K$ é uma subextensão finita de $\tilde{K}|K$, então $G(L|K) = \langle \varphi_K|_L \rangle$.*

Demonstração. Considere a aplicação de restrição

$$R : G(\tilde{K}|K) \longrightarrow G(L|K),$$

que é contínua e sobrejetiva. Como $\overline{\langle \varphi_K \rangle} = G(\tilde{K}|K)$, segue que

$$G(L|K) = R(G(\tilde{K}|K)) = R(\overline{\langle \varphi_K \rangle}) \subseteq \overline{R(\langle \varphi_K \rangle)} = \overline{\langle \varphi_K|_L \rangle} = \langle \varphi_K|_L \rangle,$$

onde a última igualdade segue do fato da topologia em $G(L|K)$ ser a discreta. □

Para cada extensão finita $L|K$, definimos

$$L^0 = L \cap \tilde{K}, \quad f_{L|K} = [L^0 : K] = \frac{f_L}{f_K}, \quad \varphi_{L^0|K} = \varphi_K|_{L^0}$$

e temos o seguinte diagrama comutativo

$$\begin{array}{ccc} G_L & \xrightarrow{deg_L} & \hat{\mathbb{Z}} \\ \downarrow & & \downarrow f_{L|K} \\ G_K & \xrightarrow{deg_K} & \hat{\mathbb{Z}} \end{array}.$$

Considere uma extensão $L|K$ Galoisiana finita e o seguinte diagrama de corpos

$$\begin{array}{ccccc} & & L & \text{——} & \tilde{L} \\ & & | & & | \\ K & \text{——} & L^0 & \text{——} & \tilde{K} \end{array},$$

em que $L^0 = L \cap \tilde{K}$ e $\tilde{L} = L.\tilde{K}$. Note também que o mapa $deg_K : G_K \longrightarrow \hat{\mathbb{Z}}$ induz um homomorfismo sobrejetivo contínuo

$$deg_K : G(\tilde{L}|K) \longrightarrow \hat{\mathbb{Z}},$$

e definimos o conjunto

$$\phi(\tilde{L}|K) = \left\{\tilde{\sigma} \in G(\tilde{L}|K) \mid deg_K(\tilde{\sigma}) \in \mathbb{N}\right\},$$

onde estamos considerando que $0 \notin \mathbb{N}$. Se $\tilde{\sigma} \in \phi(\tilde{L}|K)$ e $n = deg_K(\tilde{\sigma})$, então $\tilde{\sigma}|_{\tilde{K}} = \varphi_K^n$.

Proposição 70. *O mapa*

$$\phi(\tilde{L}|K) \longrightarrow G(L|K), \qquad \tilde{\sigma} \mapsto \tilde{\sigma}|_L$$

é sobrejetivo. Se $\sigma = \tilde{\sigma}|_L$, então dizemos que $\tilde{\sigma}$ é um levantamento de Frobenius de σ.

Demonstração. Se $\sigma \in G(L|K)$, então pelo lema 12, $\sigma|_{L^0} = \varphi^n_{L^0|K}$ para um certo $n > 0$. Seja $\tilde{\varphi}$ uma extensão de φ_K para $\tilde{L}$, ou seja, tome $\tilde{\varphi} \in G(\tilde{L}|K)$ tal que $\tilde{\varphi}|_{\tilde{K}} = \varphi_K$, então temos que

$$(\sigma\tilde{\varphi}^{-n})|_{L^0} = (\sigma|_{L^0})(\tilde{\varphi}^{-n}|_{L^0}) = (\sigma|_{L^0})(\tilde{\varphi}^{-n}|_{\tilde{K}})|_{L^0} = (\sigma|_{L^0})(\varphi_K^{-n})|_{L^0} = (\sigma|_{L^0})(\varphi^{-n}_{L^0|K}) = 1.$$

Sendo assim,

$$(\sigma\tilde{\varphi}^{-n})|_L \in G(L|L^0) \simeq G(\tilde{L}|\tilde{K}) \Rightarrow \exists \tau \in G(\tilde{L}|\tilde{K}) \text{ tal que } (\sigma\tilde{\varphi}^{-n})|_L = \tau|_L.$$

Portanto, $\tilde{\sigma} = \tau\tilde{\varphi}^n$ é um levantamento de Frobenius de σ com $\tilde{\sigma}|_{\tilde{K}} = \tilde{\varphi}^n|_{\tilde{K}} = \varphi_K^n$, logo $deg_K(\tilde{\sigma}) = n \in \mathbb{N}$. □

Definição 49. *Uma valoração Henseliana de A_K com respeito a deg é um homomorfismo*

$$v : A_k \longrightarrow \hat{\mathbb{Z}}$$

com as seguintes propriedades

(i) $v(A_K) = Z \supseteq \mathbb{Z}$ *e* $Z/nZ \simeq \mathbb{Z}/n\mathbb{Z}$ *para todo* $n \in \mathbb{N}$*;*

(ii) $v(N_{K|k}) = f_K Z$ *para todos os corpos* K*.*

Para cada corpo K, a valoração Henseliana $v : A_k \longrightarrow \hat{\mathbb{Z}}$ induz um homomorfismo

$$v_K = \frac{1}{f_K}\, v \circ N_{K|k} : A_K \longrightarrow \hat{\mathbb{Z}}$$

com imagem Z.

Proposição 71. *(i)* $v_K = v_{K^\sigma} \circ \sigma$ *para* $\sigma \in G$

(ii) Para cada extensão finita $L|K$, temos o seguinte diagrama comutativo

$$\begin{array}{ccc} A_L & \xrightarrow{v_L} & \hat{\mathbb{Z}} \\ {\scriptstyle N_{L|K}}\downarrow & & \downarrow{\scriptstyle f_{L|K}} \\ A_K & \xrightarrow{v_K} & \hat{\mathbb{Z}} \end{array}.$$

Demonstração. Ver proposição 1.5 do capítulo 2 de Neukirch (1986).

□

Definição 50. *Dizemos que $\pi_K \in A_K$ é um elemento primo se $v_K(\pi_K) = 1$. Também definimos*

$$U_K = \{u \in A_K | v_K(u) = 0\}.$$

Se $f_{L|K} = [L : K]$, ou seja, $L^0 = L$, então segue da proposição anterior que $v_L|_{A_K} = v_K$. Em particular, um elemento primo de A_K é também um elemento primo de A_L. Por outro lado, se $f_{L|K} = 1$, ou seja, $L^0 = K$ e π_L é um elemento primo de A_L, então $\pi_K = N_{L|K}(\pi_L)$ é um elemento primo de A_K.

No que segue vamos supor que A é um G-módulo que satisfaz o seguinte axioma:

Axioma de corpos de classe. *Para cada subextensão finita $L|K$ de $\tilde{K}|K$*

$$\#H^i(G(L|K), A_L) = \begin{cases} [L : K] & \text{se } i = 0; \\ 1 & \text{se } i = -1. \end{cases}$$

Proposição 72. *Se $L|K$ é uma subextensão finita de $\tilde{K}|K$, então*

$$\#H^i(G(L|K), U_L) = 0 \ \ \textit{se} \ \ i = 0, -1.$$

Demonstração. Ver proposição 2.2 do capítulo 2 de Neukirch (1986).

□

4.3.3 Mapa de reciprocidade

Definição 51. *Seja $L|K$ uma extensão Galoisiana finita. Definimos o mapa de reciprocidade*

$$r_{L|K} : G(L|K) \longrightarrow A_K/N_{L|K}A_L,$$

com

$$r_{L|K}(\sigma) := N_{\Sigma|K}(\pi_\Sigma) \ mod \ N_{L|K}A_L,$$

onde Σ é o corpo fixado de um levantamento de Frobenius $\tilde{\sigma} \in \phi(\tilde{L}|K)$ de $\sigma \in G(L|K)$ e $\pi_\Sigma \in A_\Sigma$ é um elemento primo.

Temos que mostrar a boa definição dessa função, ou seja, que dado $\sigma \in G(L|K)$, a imagem $r_{L|K}(\sigma)$ independe do levantamento $\tilde{\sigma}$ escolhido.

Lema 13. *Sejam $\tilde{\sigma}_1, \tilde{\sigma}_2, \tilde{\sigma}_3 \in \phi(\tilde{L}|K)$ tais que $\tilde{\sigma}_3 = \tilde{\sigma}_1.\tilde{\sigma}_2$. Se Σ_i é o corpo fixado de $\tilde{\sigma}_i$, ou seja, o corpo intermediário de $\tilde{L}|K$ fixado pelo grupo $\overline{\langle \sigma_i \rangle}$ e $\pi_i \in A_{\Sigma_i}$ é um elemento primo, $i = 1, 2, 3$, então*

$$N_{\Sigma_3|K}(\pi_{\pi_3}) \equiv N_{\Sigma_1|K}(\pi_{\pi_1}) \cdot N_{\Sigma_2|K}(\pi_2) \ mod \ N_{L|K}A_L.$$

Demonstração. Ver lema 2.4 do capítulo 2 de Neukirch (1986).

□

Proposição 73. *O mapa*

$$r_{L|K} : G(L|K) \longrightarrow A_K/N_{L|K}A_L$$

é um homomorfismo bem definido.

Demonstração. Sejam $\tilde{\sigma}, \tilde{\sigma}' \in \phi(\tilde{L}|K)$ dois levantamentos de Frobenius de σ. Seja Σ, Σ' os corpos fixados por $\tilde{\sigma}, \tilde{\sigma}'$ e sejam $\pi \in A_\Sigma$ e $\pi' \in A_{\Sigma'}$ elementos primos. Sem perda de

generalidade vamos supor que $m = deg_K(\tilde{\sigma}') - deg_K(\tilde{\sigma}) \geq 0$. Vamos provar primeiro que no caso $m = 0$, o mapa de reciprocidade está bem definido. Com efeito, temos que $\tilde{\sigma}'|_{\tilde{K}} = \tilde{\sigma}|_{\tilde{K}}$ e $\tilde{\sigma}'|_{\tilde{L}} = \tilde{\sigma}|_{\tilde{L}}$ e é fácil ver que a aplicação

$$G(\tilde{L}|K) \longrightarrow G(L|K) \times G(\tilde{K}|K), \quad \tau \longmapsto \tau|_L \times \tau|_{\tilde{K}}$$

se trata de um isomorfismo, logo $\tilde{\sigma}' = \tilde{\sigma}$ e $\pi' = \pi.u$, com $u \in U_\Sigma$. Então escolhemos uma subextensão galoisiana finita $M|K$ de $\tilde{L}|K$ contendo L e Σ. Como $H^0(G(M|\Sigma), U_M) = 1$, temos que $u = N_{M|\Sigma}(\tilde{u}), \tilde{u} \in U_M$, logo

$$N_{\Sigma|K}(\pi') = N_{\Sigma|K}(\pi)N_{M|K}(\tilde{u}) \equiv N_{\Sigma|K}(\pi) \ mod \ N_{L|K}A_L.$$

Logo $N_{M|K}(\tilde{u}) \in N_{M|K}A_M \subseteq N_{L|K}A_L$

Se $m > 0$, então $\tilde{\tau} = \tilde{\sigma}^{-1}.\tilde{\sigma}' \in G(\tilde{L}|K)$ é um levantamento de Frobenius de $1 \in G(L|K)$ com $deg_K(\tilde{\tau}) = m$. Se $M \supseteq L$ é o corpo fixado de $\tilde{\tau}$ e $\pi_M \in A_M$ é um elemento primo, então

$$N_{\Sigma'|K}(\pi') \equiv N_{\Sigma|K}(\pi).N_{M|K}(\pi_M) \equiv N_{\Sigma|K}(\pi) \ mod \ N_{L|K}A_L,$$

o que prova que $r_{L|K}(\sigma)$ independe da escolha do levantamento $\tilde{\sigma} \in \phi(\tilde{L}|K)$ e do elemento primo $\pi_\Sigma \in A_\Sigma$.

Por fim, o fato do mapa de reciprocidade ser um homomorfismo segue do lema anterior e do fato que se $\tilde{\sigma}_1, \tilde{\sigma}_2$ são levantamentos de Frobenius de $\sigma_1, \sigma_2 \in G(L|K)$, respectivamente, então $\tilde{\sigma}_3 = \tilde{\sigma}_1.\tilde{\sigma}_2$ é um levantamento de Frobenius de $\sigma_3 = \sigma_1.\sigma_2$.

□

Proposição 74. *Se $L|K$ é uma subextensão finita de $\tilde{K}|K$, então o mapa de reciprocidade*

$$r_{L|K}G(L|K) \longrightarrow A_K/N_{L \ vertK}A_L$$

é dado por

$$r_{L|K}(\varphi_{L|K}) = \pi_K \ mod \ N_{L|K}A_L$$

e é um isomorfismo.

Demonstração. Ver teorema 2.6 do capítulo 2 de Neukirch (1986).

□

Proposição 75. *Sejam $L|K$ e $L'|K'$ extensões galoisianas e sejam $K \subseteq K'$ e $L \subseteq L'$. Então o diagrama*

$$\begin{array}{ccc} G(L'|K') & \xrightarrow{r_{L'|K'}} & A_{K'}/N_{L'|K'}A_{L'} \\ \downarrow & & \downarrow N_{K'|K} \\ G(L|K) & \xrightarrow{r_{L|K}} & A_K/N_{L|K}A_L \end{array}$$

é comutativo, com a seta da esquerda sendo a restrição $\sigma' \mapsto \sigma'|_L$.

Demonstração. Ver proposição 2.7 do capítulo 2 de Neukirch (1986).

□

No que segue vamos supor que o G módulo A satisfaz o seguinte axioma.

Axioma de corpos de classe. *Para cada extensão finita cíclica* $L|K$

$$\#H^i(G(L|K), A_L) = \begin{cases} [L:K] & \text{se } i = 0; \\ 1 & \text{se } i = -1. \end{cases}$$

Chamamos de uma teoria de corpos de classe para um G módulo um par de homomorfismos

$$deg : G \longrightarrow \hat{\mathbb{Z}}, \qquad v : A_K \longrightarrow \hat{\mathbb{Z}},$$

onde deg é contínuo e sobrejetivo e v é uma valoração henseliana com respeito a deg.

Teorema 11. *Se* $L|K$ *é uma extensão Galoisiana finita, então*

$$r_{L|K} : G(L|K)^{ab} \longrightarrow K^*/N_{L|K}L^*$$

é um isomorfismo.

Demonstração. Se $M|K$ é uma subextensão galoisiana de $L|K$, então temos o seguinte diagrama comutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G(L|M) & \longrightarrow & G(L|K) & \longrightarrow & G(M|K) & \longrightarrow & 1 \\ & & \downarrow r_{L|M} & & \downarrow r_{L|K} & & \downarrow r_{M|K} & & \\ & & A_M/N_{L|M}A_L & \xrightarrow{N_{M|K}} & A_K/N_{L|K}A_L & \longrightarrow & A_K/N_{M|K}A_M & \longrightarrow & 1 \end{array},$$

que usaremos para reduzir a demonstração em três passos.

Passo 1: Sem perda de generalidade podemos supor que $G(L|K)$ é abeliano. Come efeito, se o teorema tiver sido provado para este caso, então tome $M = L^{ab}$ máxima subextensão abeliana de $L|K$, ou seja, $G(L|K)^{ab} = G(M|K)$ e o subgrupo de comutadores $G(L|M)$ de $G(L|K)$ é precisamente o núcleo do mapa $r_{L|K}$, logo $r_{L|K} : G(L|K)^{ab} \longrightarrow A_K/N_{L|K}A_L$ é injetivo. A sobrejetividade do mapa de reciprocidade então pode ser provada primeiramente

para extensões solúveis por indução no grau da extensão pois neste caso $M = L$ ou $[L : M] < [L : K]$ e se $r_{M|K}$ e $r_{L|M}$ são sobrejetivas, então $r_{L|K}$ também é.

Para o caso geral, note primeiro que $a^{[L:K]} \equiv 1 \ mod \ N_{L|K}A_L$, logo para cada primo $p|[L : K]$, temos que

$$A_K/N_{L|K}A_L = \bigoplus_p (A_K/N_{L|K}A_L)_p,$$

onde $(A_K/N_{L|K}A_L)_p = \left\{a \ mod \ N_{L|K}A_L \mid a^{p^k} = 1 \ mod \ N_{L|K}A_L, \text{ para algum } k \geq 1\right\}$ e seja M o corpo fixado de um p-Sylow subgrupo de $G(L|K)$. Em geral $M|K$ não é galoisiana mas podemos ainda utilizar o lado esquerdo do digrama, no qual $r_{L|M}$ é sobrejetiva, então basta mostrarmos que a imagem de $N_{M|K}$ é $(A_K/N_{L|K}A_L)_p$, pois assim teremos que

$$(A_K/N_{L|K}A_L)_p \subseteq r_{L|K}(G(L|K)), \ \forall p \mid [L|K] \Rightarrow A_K/N_{L|K}A_L \subseteq r_{L|K}(G(L|K)).$$

Para isso, como a inclusão $A_K \subseteq A_M$ induz o homomorfismo $i : A_K/N_{L|K}A_L \longrightarrow A_K/N_{M|K}A_M$ e $N_{M|K} \circ i = [M : K]$. Como $([M : K], p) = 1$, segue que $(A_K/N_{L|K}A_L)_p \xrightarrow{[M:K]} (A_K/N_{L|K}A_L)_p$ é sobrejetivo, logo $(A_K/N_{L|K}A_L)_p$ é a imagem de $N_{M|K}$.

Passo 2: Podemos assumir sem perda de generaldiade que $L|K$ é cíclico. Com efeito, se a proposição valer para extensões cíclicas e $M|K$ percorrer as subextensões cíclicas de $L|K$, então o diagrama nos mostra que o núcleo de $r_{L|K}$ está contido no nucleo do mapa $G(L|K) \longrightarrow \prod_M G(M|K)$, que é injetivo se $L|K$ for abeliana, portanto $r_{L|K}$ é injetivo. Agora escolhendo uma subextensão cíclica apropria $M|K$ de $L|K$, a sobrejetividade do mapa de reciprocidade é provada por indução como no passo 1 no caso solúvel.

Passo 3: Seja $L|K$ cíclica, podemos supor também que $f_{L|K} = 1$. Com efeito, tome $M = L^0$, então $f_{L|M} = 1$ e $r_{M|K}$ é um isomorfismo. O mapa $N_{M|K}$ no diagrama acima é injetivo pois os grupos na sequência inferior tem cardinalidades $[L : M], [L : K], [M : K]$. Portanto, se $r_{L|M}$ é um isomorfismo, então $r_{L|K}$ também é.

Agora seja $L|K$ cíclica com $f_{L|K} = 1$ e seja σ um elemento gerador de $G(L|K)$ que veremos pelo isomorfismo $G(L|K) \simeq G(\tilde{L}|\tilde{K})$ como um elemento de $G(\tilde{L}|\tilde{K})$, então $\tilde{\sigma} = \sigma\varphi_L \in \phi(\tilde{L}|K)$ é um levantamento de Frobenius de σ com $deg_K(\tilde{\sigma}) = 1$. Sendo assim, para o corpo fixado $\Sigma|K$ temos que $f_{\Sigma|K} = 1$, ou seja $\Sigma \cap \tilde{K} = K$. Seja $M|K$ uma subextensão galoisiana finita de $\tilde{L}|K$ contendo Σ e L e denote $N = N_{M|M^0}$. Como $f_{\Sigma|K} = f_{L|K} = 1$, temos que $N|_{A_\Sigma} = N_{\Sigma|K}$ e $N|_{A_L} = N_{L|K}$. Para provar a injetividade do mapa de reciprocidade temos que mostrar que se $r_{L|K}(\sigma^k) = 1$, com $0 \leq k < n = [L : K]$, então $k = 0$. Tome $\pi_\Sigma \in A_\Sigma, \pi_L \in A_L$ elementos primos e como $\Sigma, L \subseteq M \subseteq \tilde{L} \subseteq \tilde{\Sigma}$, temos que π_Σ, π_L são

elementos primos de M também. Escrevendo $\pi_\Sigma^k = u.\pi_L^k, u \in U_M$, temos que

$$r_{L|K}(\sigma^k) \equiv N(\pi_\Sigma^k) \equiv N(u).N(\pi_L^k) \equiv N(u) \equiv 1 \; mod \; N_{L|K}A_L,$$

logo $N(u) = N(v)$ com $v \in U_L$, logo $N(u^{-1}v) = 1$ e segue que $u^{-1}v = a^{\sigma-1}, a \in A_M$ pelo Axioma de Corpos de Classe. Agora em A_M temos que

$$(\pi_L^k.v)^{\sigma-1} = (\pi_\Sigma^k u^{-1}v)^{\tilde{\sigma}-1} = (a^{\sigma-1})^{\tilde{\sigma-1}} = (a^{\tilde{\sigma}-1})^{\sigma-1,}$$

logo $x = \pi_L^k v.a^{1-\tilde{\sigma}} \in A_{M^0}$. Como $v_{M^0}(x) \in \hat{\mathbb{Z}}$ e $n.v_{M^0} = v_M(x) = k$, segue que $k = 0$. A sobrejetividade é concluída então pelo Axioma de Corpos de Classe. □

Definição 52. *Considere o mapa de reciprocidade $r_{L|K} : G(L|K)^{ab} \longrightarrow A_K/N_{L|K}A_L$ e a projeção $\pi : A_K \longrightarrow A_K/N_{L|K}$, então definimos o homomorfismo*

$$(\ , L|K) = r_{L|K}^{-1} \circ \pi : A_K \longrightarrow G(L|K)^{ab}$$

chamado de símbolo da norma residual de $L|K$.

Seja A um G módulo satisfazendo o axioma de corpos de classe e seja

$$deg : G \longrightarrow \hat{\mathbb{Z}}, \quad v : A_K \longrightarrow \hat{\mathbb{Z}}$$

uma teoria de corpos de classe. Para cada corpo K, definimos uma topologia em A_K da seguinte forma: para cada $a \in A_K$, tomamos as classes laterais $aN_{L|K}A_L$ como uma base de vizinhanças abertas de a, onde $L|K$ percorre todas as extensões Galoisianas finitas de K. Chamamos esta topologia de topologia da norma de A_K.

Proposição 76. *Valem as seguintes propriedades*

(i) Os sugrupos abertos de A_K são precisamente os subgrupos fechados de índice finito;

(ii) A valoração $v_K : A_K \longrightarrow \hat{\mathbb{Z}}$ é contínua;

(iii) Se $L|K$ é uma extensão finita, então $N_{L|K} : A_L \longrightarrow A_K$ é contínua;

(iv) A_K é Hausdorff se e somente se o grupo

$$A_K^0 = \bigcap_L N_{L|K}A_L$$

de normas universais for trivial.

Demonstração. Ver proposição 4.1 do capítulo 2 de Neukirch (1986).

□

Proposição 77. *O mapa*

$$L \longmapsto \mathcal{N}_L = N_{L|K}A_L$$

é uma correspondência biunívoca entre extensões abelianas finitas $L|K$ e os subgrupos abertos $\mathcal{N}$ de A_K. Além do mais,

- $L_1 \subseteq L_2 \Leftrightarrow \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}$;
- $\mathcal{N}_{L_1.L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$'
- $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}.\mathcal{N}_{L_2}$.

Demonstração. Se L_1 e L_2 são extensões abelianas finitas, então pela transitividade da norma temos que $\mathcal{N}_{L_1.L_2} \subseteq \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$. inversamente, se $a \in \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ então o elemento $(a, L_1.L_2|K) \in G(L_1.L_2|K)$ tem as projeções triviais $(a, L_i|K) = 1$ em $G(L_i|K), i = 1, 2$, logo $(a, L_1.L_2|K) = 1$, logo $a \in \mathcal{N}_{L_1.L_2}$. Portanto, temos que $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ e

$$\mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2} \Leftrightarrow \mathcal{N}_{L_1} \cap \mathcal{N}_{L_1} = \mathcal{N}_{L_1.L_2} \Leftrightarrow [L_1.L_2 : K] = [L_2 : K] \Leftrightarrow L_1 \subseteq L_2.$$

Isso implica que o mapa $L \mapsto \mathcal{N}_L$ é injetivo. Se $\mathcal{N}$ é um subgrupo aberto de A_K, então contém um grupo de norma $\mathcal{N}_L = N_{L|K}A_L$. Como $\mathcal{N}_L = \mathcal{N}_{L^{ab}}$, podemos supor que $L|K$ é abeliana. Agora $(\mathcal{N}, L|K) = G(L|L')$ com um corpo intermediário L' de $L|K$. Já que $\mathcal{N} \supseteq \mathcal{N}_L$, então $\mathcal{N}$ é pré-imagem de $G(L|L')$ pelo mapa de norma residual $(\ , L'|K) : A_K \to G(L'|K)$, logo $\mathcal{N} = \mathcal{N}_L$. Portanto, o mapa $L \mapsto \mathcal{N}_L$ é sobrejetivo.

Por fim, a identidade $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ é obtida da seguinte forma. Como $L_1 \cap L_2 \subseteq L_i$, segue que $\mathcal{N}_{L_1 \cap L_2} \supseteq \mathcal{N}_{L_i}, i = 1, 2$, logo $\mathcal{N}_{L_1 \cap L_2} \supseteq \mathcal{N}_{L_1}.\mathcal{N}_{L_2}$. Agora como $\mathcal{N}_{L_1}.\mathcal{N}_{L_2}$ é aberto em A_K, temos que $\mathcal{N}_{L_1}.\mathcal{N}_{L_2} = \mathcal{N}_L$ para alguma extensão abeliana finita $L|K$. De $\mathcal{N}_{L_i} \subseteq \mathcal{N}_L$, segue que $L \subseteq L_1 \cap L_2$, logo $\mathcal{N}_{L_1}.\mathcal{N}_{L_2} = \mathcal{N}_L \supseteq \mathcal{N}_{L_1 \cap L_2}$. □

Agora construída toda essa teoria de corpos de classe generalizada, vamos utilizar os conceitos e resultados que desenvolvemos para aplicar no estudo de corpos locais, e assim teremos a teoria de corpos de classe local com uma versão local do axioma de corpos de classe, e no estudo de corpos de números, e assim teremos a teoria de corpos de classe global e uma versão global do axioma de corpos de classe. Por fim, com todo esse fundamental teórico, seremos capazes de provar o Teorema de Hasse-Minkowski, também conhecido com princípio local-global para quádricas.

4.4 TEORIA DE CORPOS DE CLASSE LOCAL

Ao longo desta seção vamos trabalhar com corpos locais, como definimos em 23 e estaremos em especial interessados em corpos $\mathfrak{p}$-ádicos, ou seja, as extensões finitas de $\mathbb{Q}_p$. Utilizaremos a teoria abstrata que desenvolvemos na seção anterior, mas agora estaremos trabalhando com corpos "concretos" no sentido usual que estamos acostumados da álgebra. Seja k um corpo local, $\overline{k}$ seu fecho separável e $G = G(\overline{k}|k)$ seu grupo de Galois absoluto, que sabemos ser um grupo profinito com a topologia de Krull por 57, e sabemos que os subgrupos fechados de G são os subgupos da forma $G_K = G(K|k)$, onde $K|k$ é uma subextensão de $\overline{k}|k$ por 58, portanto podemos aplicar a teoria de galois abstrata e assim a teoria de corpos de classe abstrata, onde agora os "corpos abstratos", que eram meros índices, são corpos concretos no sentido da álgebra.

Considere $\tilde{k}|k$ a extensão não ramificada maximal de k, ou seja, o compósito de todas as extensões finitas não ramificadas. Sabemos que $\tilde{k}$ é gerado por todas as raízes da unidade de ordem prima com $p = char(\mathcal{O}_k/\mathfrak{p}_k)$. O grupo de Galois $G(\tilde{k}|k)$ é gerado topologicamente pelo automorfismo de Frobenius $\varphi_K \in G(\tilde{k}|k)$ que é definido por

$$a^{\varphi_k} \equiv a^{q_k} \ mod \ \mathfrak{p}_{\tilde{k}} \quad \forall a \in \mathcal{O}_{\tilde{k}}.$$

Se $L|k$ é uma subextensão finita de $\tilde{k}|k$, então o grupo de Galois $G(L|k)$ é cíclico e gerado por $\varphi_{L|k} = \varphi_k|_L$. Se $n = [L : k]$, então temos um isomorfismo canônico

$$G(L|k) \simeq \mathbb{Z}/n\mathbb{Z},$$

que envia $\varphi_{L|k}$ em $1 \ mod \ n\mathbb{Z}$. Passando para o limite projetivo, obtemos um isomorfismo topológico

$$G(\tilde{k}|k) \simeq \hat{\mathbb{Z}},$$

que manda φ_k em 1. Obtemos também um homomorfismo contínuo e sobrejetivo

$$deg : G \longrightarrow \hat{\mathbb{Z}}.$$

Se $K|k$ é uma extensão finita, então $f_K = f_{K|k} = [K \cap \tilde{k} : k]$ é o grau de inércia da extensão, que induz um homomorfismo contínuo sobrejetivo

$$deg_K = \frac{1}{f_K} \ deg : G_K \longrightarrow \hat{\mathbb{Z}},$$

que determina a extensão não ramificada maximal $\tilde{K} = K.\tilde{k}$ de K. O elemento $\varphi_K \in G(\tilde{K}|K)$ que é enviado em 1 pelo isomorfismo $G(\tilde{K}|K) \simeq \hat{\mathbb{Z}}$ é o automorfismo de Frobenius de $\tilde{K}|K$ já que $\varphi_K|_{\tilde{k}} = \varphi_k^{f_K}$ e

$$a^{\varphi_K} \equiv a^{\varphi_k^{f_K}} \equiv a^{q_k^{f_K}} \equiv a^{q_k} \ mod \ \mathfrak{p}_{\tilde{k}}$$

para todo $a \in \mathcal{O}_{\tilde{k}}$ logo para todo $a \in \mathcal{O}_{\tilde{k}}$ pois $\tilde{K} = K.\tilde{k}$. Nós consideramos o G-módulo $A = \overline{k}^*$. Se $K|k$ é uma extensão finita, então $A_K = K^*$. Consideramos também a valoração henseliana normalizada usual

$$v : k^* \longrightarrow \mathbb{Z} \subset \hat{\mathbb{Z}}$$

e note que ela também é henseliana com respeito a deg. Agora provaremos que A satisfaz o axioma da teoria de corpos de classe, então o par

$$deg : G \longrightarrow \hat{\mathbb{Z}} \qquad v : k^* \longrightarrow \hat{\mathbb{Z}}$$

é uma teoria de corpos de classe.

Teorema 12 (Axioma de corpos de classe local)**.** *Se $L|K$ é uma extensão finita cíclica de corpos locais, então*

$$\#H^i(G(L|K), L^*) = \begin{cases} [L:K] & \text{se } i = 0; \\ 1 & \text{se } i = -1. \end{cases}$$

Demonstração. Vamos apenas provar o caso em que $char(K) = 0$, que é o que de fato vamos precisar ao longo desse texto. Para o caso de característica positiva, pode ser consultado o livro de Artin e Tate (1967). Seja $G = G(L|K)$. Pelo teorema 90 de Hilbert, temos que $H^{-1}(G, L^*) = 1$, logo o quociente de Herbrand do G-módulo L^* é $h(G, L^*) = \#H^0(G, L^*)$. Agora considere a sequência exata de G-módulos

$$1 \longrightarrow U_L \longrightarrow L^* \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0$$

em que $\mathbb{Z}$ é visto como G-módulo trivial e U_L denota o grupo de unidades do anel de valoração de L. Então pela multiplicidade do quociente de Herbrand, segue que

$$h(G, L^*) = h(G, \mathbb{Z}).h(G, U_L) = [L:K].h(G, U_L).$$

Então basta provarmos que $h(G, U_L) = 1$. Seja $n > \frac{e}{p-1} = v_L(p)$, então pela proposição 45, $U_L^{(n)} \simeq \mathfrak{p}_L^n$ e como $U_L/U_L^{(n)}$ é finito, temos que

$$h(G, U_L) = h(G, U_L/U_L^{(n)}).h(G, U_L^{(n)}) = h(G, \mathfrak{p}_L^n).$$

Seja $\{\tau\alpha|\tau \in G\}$ uma base normal de $L|K$ e seja M o G-módulo

$$M = \bigoplus_{\tau\in G} \mathcal{o}_K \tau\alpha = \bigoplus_{\tau\in G} \tau B$$

onde $B = \mathcal{o}_K\alpha$, logo $M = M_G(B)$. Multiplicando α por uma potência de π_K apropriada se necessário, podemos supor sem perda de generalidade que M é um submódulo aberto de $\mathfrak{p}_L^n$, então segue que $\mathfrak{p}_L^n/M$ é finito, logo

$$h(G, U_L) = h(G, \mathfrak{p}_L^n) = h(G, \mathfrak{p}_L^n/M).h(G, M) = 1.$$

□

Sendo assim, temos a lei de reciprocidade local:

Proposição 78. *Para toda extensão Galoisiana $L|K$ de corpos locais, temos um isomorfismo canônico*

$$r_{L|K} : G(L|K)^{ab} \longrightarrow K^*/N_{L|K}L^*.$$

Proposição 79. *O mapa*

$$L \longmapsto \mathcal{N}_L = N_{L|K}L^*$$

é uma correspondência biunívoca entre extensões abelianas finitas L do corpo local K e os subgrupos $\mathcal{N}$ de K^* de índice finito. Além do mais,

- $L_1 \subseteq L_2 \Leftrightarrow \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}$;
- $\mathcal{N}_{L_1.L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$;
- $\mathcal{N}_{L_1\cap L_2} = \mathcal{N}_{L_1} \cdot \mathcal{N}_{L_2}$.

Demonstração. Ver teorema 3.1 do capítulo 3 de Neukirch (1986).

□

Proposição 80. *Se K contém as raízes m-ésimas da unidade e se $L = K(\sqrt[m]{K^*})$, então*

$$N_{L|K}L^* = K^{*m} \qquad e \qquad G(L|K) \simeq K^*/K^{*m}.$$

Demonstração. Ver teorema 3.2 do capítulo 3 de Neukirch (1986). □

4.5 TEORIA DE CORPOS DE CLASSE GLOBAL

Agora neste capítulo trabalharemos com corpos de números e provaremos que vale uma versão global do Axioma de Corpos de Classe e dele deduziremos um dos resultados centrais da teoria de corpos de classe, conhecido como Teorema da Norma de Hasse e o utilizaremos para provar o Teorema de Hasse-Minkowski, também conhecido como princípio local-global para quádricas.

Definição 53. *Um primo (ou place)* $\mathfrak{p}$ *de um corpo de números* K *é uma classe de equivalência de valorações equivalentes de* K*. As classes de equivalências não arquimedianas são chamadas de primos finitos e as classes de equivalência arquimedianas são chamadas de primos infinitos.*

Sabemos da teoria de extensão de valoração que cada primo infinito $\mathfrak{p}$ é obtido a partir de um $\mathbb{Q}$-mergulho $\tau : K \longrightarrow \mathbb{C}$ e temos os primos reais, induzidos por mergulhos reais $\tau : K \longrightarrow \mathbb{R}$ e os primos complexos, induzidos por pares de mergulhos complexos conjugados não reais $K \longrightarrow \mathbb{C}$ e é fácil ver que $\mathfrak{p}$ é real ou complexo se o completamento $K_{\mathfrak{p}}$ for isomorfo a $\mathbb{R}$ ou a $\mathbb{C}$ respectivamente. Para nos referirmos aos primos infinitos utilizamos a notação $\mathfrak{p} \mid \infty$ e para os primos finitos, a notação $\mathfrak{p} \nmid \infty$.

Se $L|K$ é uma extensão de corpos de números e denotamos os primos de L por $\mathfrak{P}$, então escrevemos $\mathfrak{P}|\mathfrak{p}$ para denotar que se tomarmos uma valoração na classe $\mathfrak{P}$ e restringirmos a K, obteremos uma valoração na classe $\mathfrak{p}$. Para o caso de um primo finito $\mathfrak{p}$, sabemos que existe um único número primo p tal que $\mathfrak{p}|p$, onde estamos denotando por p a classe das valorações em $\mathbb{Q}$ equivalentes a valoração p-ádica.

Para o caso de primos finitos, a letra $\mathfrak{p}$ tem múltiplos significados $\mathfrak{p}$: se refere a um ideal primo do anel de inteiros $\mathcal{O}_K$ do corpo de números K, ou ao ideal maximal associado a sua localização $(\mathcal{O}_K)_{\mathfrak{p}}$, ao ideal maximal do completamento de $\mathcal{O}_K$ com respeito a uma valoração do place $\mathfrak{p}$ e se refere a uma classe de equivalência de valorações equivalentes em $\mathfrak{p}$. E ao invés de causar confusão, quando nos acostumamos com essa sobreposição, isso nos ajuda a criar intuições sobre diversas conexões e equivalências existentes entre as teorias de ideais em domínios de Dedekind, que desenvolvemos no capítulo 1 e a teoria de corpos com valor absoluto, que desenvolvemos no capítulo 2. Em geral, dada uma uma valoração não arquimediana em K, sabemos que quando restrita $\mathbb{Q}$, temos uma valoração equivalente a p-ádica, então escrevemos a fatoração de p em ideais primos de K (mais precisamente de $\mathcal{O}_K$)

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

e as valorações $\mathfrak{p}_i$-ádicas, que denotamos $v_{\mathfrak{p}_i}, i = 1, \ldots, r$ são todas as extensões da valoração p-ádica para K, então v é equivalente a alguma valoração $\mathfrak{p}_i$-ádica, $i = 1, \ldots, r$ e denotando $\mathfrak{p} = \mathfrak{p}_i$, utilizamos o símbolo $\mathfrak{p}$ para nos referirmos tanto ao ideal primo em questão quanto a classe de equivalência de v e perceba que o ideal primo seria o mesmo se tomássemos uma outra valoração w mas na mesma classe de equivalência de v.

Definição 54. *Seja K um corpo de números. Se $\mathfrak{p}$ for um place infinito, vamos denotar $\mathcal{o}_\mathfrak{p} = K_\mathfrak{p}$. Se $\mathfrak{p}$ for um place finito, vamos denotar $\mathcal{o}_\mathfrak{p} = \mathcal{o}_{K_\mathfrak{p}}$, o anel de valoração do corpo $\mathfrak{p}$-ádico $K_\mathfrak{p}$ e sabemos pelo que estudamos no capítulo 3 que $K_\mathfrak{p}$ é uma extensão finita de $\mathbb{Q}_p$ e que $\mathcal{o}_\mathfrak{p}$ é o fecho integral de $\mathbb{Z}_p$ em $K_\mathfrak{p}$ onde p é o número primo sob $\mathfrak{p}$. Um **adele** α de K é uma família $(\alpha_\mathfrak{p})$ de elementos $\alpha \in K_\mathfrak{p}$, em que $\mathfrak{p}$ percorre todos os places de K e para quase todo $\mathfrak{p}$, temos que $\alpha_\mathfrak{p} \in \mathcal{o}_\mathfrak{p}$. Os adeles formam um anel denotado $\mathbb{A}_K$. Nesse anel, adição e multiplicação são definidas componente a componente.*

Seja S um conjunto finito de primos de K contendo $S_\infty = \{\mathfrak{p}|\infty\}$. Então

$$K^S = \{a \in K^* \mid v_\mathfrak{p}(a) = 0 \ \forall \mathfrak{p} \notin S\}$$

é chamado de grupo das S-unidades de K. Em particular, K^{S_∞} é o grupo das unidades do anel $\mathcal{O}_K$ de inteiros de K. Temos o teorema das unidades de Dirichlet generalizado.

Proposição 81 (Teorema das unidades de Dirichlet generalizado)**.** *O mapa*

$$l : K^S \longrightarrow \prod_{\mathfrak{p} \in S} \mathbb{R}, \quad l(x) = (\log|x|_\mathfrak{p})_{\mathfrak{p} \in S}$$

é um homomorfismo, cujo núcleo é $\mu(K)$ e cuja imagem é um reticulado completo no espaço vetorial de traço zero $H = \left\{(x_\mathfrak{p}) \in \prod_{\mathfrak{p} \in S} \mathbb{R} \mid \sum_{\mathfrak{p} \in S} x_\mathfrak{p} = 0\right\}$.

Demonstração. Ver a proposição 1.1 do capítulo 6 de Neukirch (1999).

□

Definição 55. *Um **idele** é uma unidade no anel dos adeles, ou seja, uma família $\alpha = (\alpha_\mathfrak{p})$ de elementos $\alpha_\mathfrak{p} \in K_\mathfrak{p}^*$, em que para quase todo $\mathfrak{p}$, temos que $\alpha_\mathfrak{p}$ é um elemento de $U_\mathfrak{p} = \mathcal{o}_\mathfrak{p}^*$, o grupo de unidades de $\mathcal{o}_\mathfrak{p}$. Os ideles formam portanto um grupo abeliano que denotaremos I_K.*

Definição 56. *Seja S um conjunto finito de primos do corpo K. O grupo*

$$I_K^S = \prod_{\mathfrak{p} \in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p} \notin S} U_\mathfrak{p} \subseteq \prod_{\mathfrak{p}} K_\mathfrak{p}^*$$

é chamado de grupo de S-ideles de K.

Note que o grupo de ideles é então a união

$$I_K = \bigcup_S I_K^S \subseteq \prod_{\mathfrak{p}} K_{\mathfrak{p}}^*,$$

onde S percorre todos os conjuntos finitos de primos de K. Agora perceba que a seguinte aplicação é um mergulho canônico de grupos multiplicativos

$$K^* \longrightarrow I_K, \quad x \longmapsto (x),$$

onde a componente $\mathfrak{p}$ do idele (x) é $x_{\mathfrak{p}} = x \in K_{\mathfrak{p}}^*$ e esta aplicação está bem definida pois para quase todo $\mathfrak{p}$, x é uma unidade em $K_{\mathfrak{p}}$, pois escrevendo a fatoração do ideal fracionário gerado por x em K, temos que $x\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ e temos que $v_{\mathfrak{p}}(x) = 0$ quase sempre. Daqui pra frente vamos então considerar K^* mergulhado em I_K e temos o grupo

$$K^S = K^* \cap I_K^S$$

das S-unidades de K.

Definição 57. *O grupo quociente*

$$C_K = I_K/K^*$$

é chamado de grupo de classe de ideles de K.

Temos assim a sequência exata curta

$$1 \longrightarrow K^* \longrightarrow I_K \longrightarrow C_K \longrightarrow 1.$$

Proposição 82. *Seja S_∞ o conjunto de todos os primos infinitos. Então*

$$I_K/I_K^{S_\infty} \simeq J_K \qquad I_K/I_K^{S_\infty}.K^* \simeq J_K/P_K,$$

onde J_K e P_K denotam o grupo dos ideais fracionários e o grupo dos ideais fracionários principais de K, respectivamente.

Demonstração. Ver proposição 2.3 do capítulo 4 de Neukirch (1986).

□

Proposição 83. *Seja $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ um sistema completo de representantes das classes de $C_K = J_K/P_K$ e considere o conjunto finito $P = \{\mathfrak{p} : \mathfrak{p}|\mathfrak{a}_i,$ para algum $i\}$. Se S for um conjunto finito de primos contendo P, assim como os primos infintos, então*

$$I_K = I_K^S.K^*$$

e portanto $C_K = I_K^S.K^*/K^*$.

Demonstração. Ver teorema 2.4 do capítulo 4 de Neukirch (1986).

□

Seja $L|K$ uma extensão finita de corpos de números. O grupo de ideles I_K de K está mergulhado no grupo de ideles I_L de L da seguinte maneira: para cada cada $\alpha = (\alpha_{\mathfrak{p}}) \in I_K$, associe o idele $\alpha' = (\alpha'_{\mathfrak{P}}) \in I_L$ cujas componentes são

$$\alpha'_{\mathfrak{P}} = \alpha_{\mathfrak{p}} \in K^*_{\mathfrak{p}} \subseteq L^*_{\mathfrak{P}} \quad \text{para} \quad \mathfrak{P}|\mathfrak{p}$$

e através deste mergulho $I_K \longrightarrow I_L$, vamos identificar $I_K \subseteq I_L$. Sendo assim, um idele $\alpha = (\alpha_{\mathfrak{P}}) \in I_L$ pertence ao subgrupo I_K precisamente quando

(i) $\alpha_{\mathfrak{P}} \in K_{\mathfrak{p}}$ com $\mathfrak{P}|\mathfrak{p}$ para cada primo $\mathfrak{P}$ de L;

(ii) Se $\mathfrak{P}$ e $\mathfrak{P}'$ são dois primos de L sobre um mesmo primo $\mathfrak{p}$ de K, então $\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{P}'} \in K^*_{\mathfrak{p}}$.

Um isomorfismo $\sigma : L \longrightarrow \sigma L$ induz um isomorfismo

$$\sigma : I_L \longrightarrow I_{\sigma L}$$

canonicamente da seguinte maneira: para cada primo $\mathfrak{P}$ de L, σ induz um isomorfismo $\sigma : L_{\mathfrak{P}} \longrightarrow (\sigma L)_{\sigma\mathfrak{P}}$. Então dado um idele $\alpha \in I_L$, as componentes de $\sigma\alpha \in I_{\sigma L}$ são dadas por

$$(\sigma\alpha)_{\sigma\mathfrak{P}} = \sigma\alpha_{\mathfrak{P}} \in (\sigma L)_{\sigma\mathfrak{P}}.$$

Se $L|K$ for galoisiana com grupo de Galois $G = G(L|K)$, então cada $\sigma \in G$ induz um automorfismo $\sigma : I_L \longrightarrow I_L$, logo I_L se torna um G-módulo.

Proposição 84. *Se $L|K$ é uma extensão Galoisiana com grupo de Galois G, então*

$$I_L^G = I_K.$$

Demonstração. Ver proposição 3.1 do capítulo 4 de Neukirch (1986).

□

Para uma extensão finita de corpos de números (não necessariamente galoisiana), definimos o mapa de norma

$$N_{L|K} : I_L \longrightarrow I_K$$

da seguinte maneira. Seja $M|K$ o fecho normal de $L|K$ e denote $G = G(M|K), H = G(M|L)$. Então I_L é o módulo fixado de I_M por H e

$$N_{L|K}(\alpha) = \prod_{\sigma} \sigma\alpha \quad \text{para } \alpha \in I_L$$

onde σ percorre um sistema completo de representantes de G/H. É fácil ver que $N_{L|K}(\alpha)$ independe da escolha dos representantes de G/H e para cada $\tau \in G$, temos que $\tau N_{L|K}(\alpha) = N_{L|K}(\alpha)$, logo de fato $N_{L|K}(\alpha)$ é um elemento de I_K.

Proposição 85. *Se $L|K$ é uma extensão finita e $\alpha \in I_L$, então as componentes locais de $N_{L|K}(\alpha) \in I_K$ são dadas por*

$$(N_{L|K}(\alpha))_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}).$$

Demonstração. Ver proposição 3.2 do capítulo 4 de Neukirch (1986).

□

Proposição 86. *Seja $L|K$ uma extensão Galoisiana de corpos de números com grupo de Galois G, seja*

$$I_L^{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}^*,$$

seja

$$U_L^{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}^*,$$

e seja

$$I_L^S = \prod_{\mathfrak{p}\in S} I_L^{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_L^{\mathfrak{p}}$$

com S um conjunto finito de primos de K. Então:

(i) $I_L^{\mathfrak{p}} = M_G^{G_{\mathfrak{P}}}(L_{\mathfrak{P}}^*)$ *e* $U_L^{\mathfrak{p}} = M_G^{G_{\mathfrak{P}}}(U_{\mathfrak{P}}^*)$ *onde $\mathfrak{P}$ é um primo de L sobre $\mathfrak{p}$ dado;*

(ii) Se S contém os places infinitos e os places que se ramificam, temos, para $i = 0, 1$

$$H^i(G, I_L^S) \simeq \bigoplus_{\mathfrak{p}\in S} H^i(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$$

e

$$H^i(G, I_L) \simeq \bigoplus_{\mathfrak{p}} H^i(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*),$$

onde para cada $\mathfrak{p}$, escolhemos um primo $\mathfrak{P}$ sobre ele.

Demonstração. Ver proposições 3.3 e 3.4 do capítulo 4 de Neukirch (1986).

□

A proposição anterior nos mostra que

$$I_K/N_{L|K}I_L \simeq \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}^*/N_{L_{\mathfrak{P}|K_{\mathfrak{p}}}} L_{\mathfrak{P}}^*,$$

onde $\mathfrak{P}$ é um primo de L sobre $\mathfrak{p}$. De tal forma que um idele $\alpha \in I_K$ é norma de um idele de L se e somente se cada componente local $\alpha_{\mathfrak{p}}$ for norma de um elemento de $L_{\mathfrak{P}}^*$, ou seja, um idele é globalmente uma norma se e somente se for uma norma localmente em todo place. Note também que do lado direito temos uma soma direta de uma quantidade infinita de grupos, então cada elemento da soma direta tem quase todas as suas componentes iguais a 1, ou seja se $\alpha \in I_K$ é um idele, então existe uma quantidade finita de primos $\mathfrak{p}$ para os quais a componente $\alpha_{\mathfrak{p}}$ não é uma norma da extensão $L_{\mathfrak{P}}|K_{\mathfrak{p}}$.

Proposição 87. *Se $L|K$ é uma extensão finita, então a injeção $I_K \hookrightarrow I_L$ induz uma injeção dos grupos de classes de ideles*

$$C_K \longrightarrow C_L, \quad \alpha K^* \longmapsto \alpha L^*.$$

Demonstração. Ver a proposição 3.6 do capítulo 4 de Neukirch (1986).

□

Proposição 88. *Se $L|K$ é uma extensão galoisiana e $G = G(L|K)$, então C_L é canonicamente um G-módulo e $C_L^G = C_K$.*

Demonstração. Ver proposição 3.7 do capítulo 4 de Neukirch (1986).

□

Se $L|K$ é uma extensão finita então o mapa de norma $N_{L|K} : I_L \longrightarrow I_K$ mapeia ideles principais $a \in L^*$ em ideles principais $N_{L|K}(a) \in K^*$. Então induz um homomorfismo

$$N_{L|K} : C_L \longrightarrow C_K, \quad \alpha.L^* \longmapsto N_{L|K}(\alpha).K^*.$$

Se $M \supseteq L \supseteq K$, então

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

Proposição 89. *Seja $L|K$ uma extensão cíclica de grau n com grupo de Galois $G = G(L|K)$. Então*

$$h(G, C_L) = \frac{\#H^0(G, C_L)}{\#H^1(G, C_L)} = n.$$

Em particular, $(C_K : N_{L|K}C_L) \geq n$.

Demonstração. Ver teorema 3.8 do capítulo 4 de Neukirch (1986).

□

Proposição 90. *Se $L|K$ é cíclica de ordem potência de primo $n = p^v$, então existem infinitos primos de K que não se decompõem em L.*

Demonstração. Suponha por absurdo que o conjunto S de primos que não se decompõe seja finito. Seja $M|K$ a única subextensão de $L|K$ de grau primo p. Para cada $\mathfrak{p} \notin S$, existe mais de um primo de L sobre $\mathfrak{p}$, logo o grupo de decomposição $G_\mathfrak{p}$ de $L|K$ é distinto de $G(L|K)$, logo $\#G_\mathfrak{p} \leq p^{v-1}$, logo $G_\mathfrak{p} \subseteq G(L|M)$. Disso segue que $\mathfrak{p}$ não se mantém primo em M, pois caso contrário, teríamos que $G_\mathfrak{p}$ seria o grupo de decomposição de $\mathfrak{p}$ na extensão $L|M$ e assim

$$(G(L|K) : G_\mathfrak{p}) = \text{quantidade de primos distintos de } L \text{ sobre } \mathfrak{p} = (G(L|M) : G_\mathfrak{p}),$$

logo $G(L|K) = G(L|M) \Rightarrow M = K$, o que é absurdo, e como $[M : K] = p$ é um número primo, segue que $\mathfrak{p}$ se decompõe totalmente sobre M. Agora afirmamos que $N_{M|K}C_M = C_K$ e assim teremos um absurdo.

Com efeito, seja $\alpha \in I_K$. Pelo teorema de aproximação, existe $a \in K^*$ tal que $\alpha_\mathfrak{p}a^{-1}$ está contido no subgrupo aberto $N_{M_\mathfrak{P}|K_\mathfrak{p}}M_\mathfrak{P}^*$ de $K_\mathfrak{p}^*, \forall \mathfrak{p} \in S$. Para $\mathfrak{p} \notin S, \alpha_\mathfrak{p}a^{-1}$ está automaticamente em $N_{M_\mathfrak{P}|K_\mathfrak{p}}M_\mathfrak{P}^*$ já que $M_\mathfrak{P} = K_\mathfrak{p}$, pois $G(M_\mathfrak{P}|K_\mathfrak{p})$ é o grupo de decomposição de $\mathfrak{p}$ sobre M e como $\mathfrak{p}$ se decompõe totalmente sobre M, segue que

$$[M : K] = \text{quantidade de primos distintos de } M \text{ sobre } \mathfrak{p} = \#G(M|K)/\#G(M_\mathfrak{P}|K_\mathfrak{p}),$$

logo $\#G(M_\mathfrak{P}|K_\mathfrak{p}) = 1$. Portanto, αa^{-1} é a norma de um idele β de M, ou seja, $\alpha = (N_{M|K}\beta).a \in N_{M|K}I_M.K^*$. Isso nos mostra que a classe de α está contida em $N_{M|K}C_M$, portanto, $C_K = N_{M|K}C_M$. □

4.5.1 Extensões de Kummer

Suponha fixado um corpo de números K que contém as raízes n-ésimas da unidade, onde n é uma potência de um primo fixado. Queremos calcular o grupo de norma $N_{L|K}C_L$ de uma extensão de Kummer $L|K$ com grupo de Galois

$$G(L|K) \simeq (\mathbb{Z}/n\mathbb{Z})^r.$$

Escolhemos um conjunto finito S de primos de K contendo os primos infinitos, o primo dividindo n e os primos que se ramificam em L tal que $I_K = I_K^S.K^*$ e denotamos $s = \#S$.

Proposição 91. *Temos que $s \geq r$ e existe um conjunto T de $s-r$ primos de K não contidos em S tais que*

$$L = K(\sqrt[n]{\Delta}),$$

onde Δ é o núcleo do mapa $K^S \longrightarrow \prod_{\mathfrak{p}\in T} K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*n}$.

Demonstração. Primeiramente provaremos que $L = K(\sqrt[n]{\Delta})$ com $\Delta = L^{*n} \cap K^S$. Sabemos que $L = K(\sqrt[n]{\Delta})$ com $D = L^{*n} \cap K^*$. Se $x \in D$, então $K_{\mathfrak{p}}(\sqrt[n]{x})|K_{\mathfrak{p}}$ é não ramificada $\forall \mathfrak{p} \notin S$, então podemos escrever $x = u_{\mathfrak{p}} y_{\mathfrak{p}}^n$ com $u_{\mathfrak{p}} \in U_{\mathfrak{p}}$ e $y_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$. Definindo $y_{\mathfrak{p}} = 1$ para $\mathfrak{p} \in S$, obtemos um idele $y = (y_{\mathfrak{p}})$ que pode ser escrito como $y = \alpha.z$, com $\alpha \in I_K^S$ e $z \in K^*$. Agora $x.z^{-n} = u_{\mathfrak{p}}.\alpha_{\mathfrak{p}}^n \in U_{\mathfrak{p}}, \forall \mathfrak{p} \notin S$, então $x.z^{-n} \in I_K^S \cap K^* = K^S$, logo $x.z^{-n} \in \Delta$. Isso prova que $D = \Delta.K^{*n}$, logo $L = K(\sqrt[n]{\Delta})$.

O corpo $N = K(\sqrt[n]{K^S})$ contém L pois $\Delta \subseteq K^S$. Pela teoria de Kummer, nós temos que

$$G(N|K) \simeq Hom(K^S/(K^S)^n, \mathbb{Z}/n\mathbb{Z}).$$

Pelo Teorema das Unidades de Dirichlet generalizado, existe um sugrupo R de K^S livremente gerado, de rank $s-1$ tal que $\mu(K) \times R$ e note que $\mu(K)$ é finito e portanto cíclico, pois todo elemento de $\mu(K)$ tem como polinômio mínimo um polinômio ciclotômico Φ_d de grau $d|n^r$, logo $\Phi_d|X^{n^r} - 1$, logo $\mu(K) \subseteq \mu_{n^r}$, que é um conjunto finito. Sendo assim,

$$\frac{K^S}{(K^S)^n} \simeq \frac{\mu(K) \times \mathbb{Z}^{s-1}}{\mu(K)^n \times (n\mathbb{Z})^{s-1}} \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^s,$$

ou seja, $K^S/(K^S)^n$ é um $\mathbb{Z}/n\mathbb{Z}$-módulo de rank s e portanto $G(N|K)$ também é. Como $G(N|K)/G(N|L) \simeq G(L|K) \simeq (\mathbb{Z}/n\mathbb{Z})^r$ é um $\mathbb{Z}/n\mathbb{Z}$-módulo livre de rank r afirmamos que $r \leq s$ e $G(N|L)$ é um $\mathbb{Z}/n\mathbb{Z}$-módulo livre de rank $s-r$. Com efeito, $G(N|K)$ e $G(L|K)$ são $\mathbb{Z}$-módulos finitamente gerado de rank s e r respectivamente, como $G(N|K)/G(N|L) \simeq G(L|K)$, logo $r \leq s$ e $G(N|L)$ é um $\mathbb{Z}$-módulo finitamente gerado de rank $s-r$ e a $\mathbb{Z}$-ação em $G(N|L)$ envolvida induz uma $(\mathbb{Z}/n\mathbb{Z})$-ação em $G(N|L)$ de forma que $G(N|L)$ é um $(\mathbb{Z}/n\mathbb{Z})$-módulo livre de rank $s-r$.

Seja $\sigma_1, \ldots \sigma_{s-r}$ uma $(\mathbb{Z}/n\mathbb{Z})$-base de $G(N|L)$ e seja N_i o corpo fixado por $\sigma_i, i = 1, \ldots, s-r$. Então $L = \bigcap_{i=1}^{s-r} N_i$. Para cada $i = 1, \ldots, s-r$, escolhemos um primo $\mathfrak{P}_i$ de N_i que não se decompõe em N tal que os primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-r}$ de K sob $\mathfrak{P}_1, \ldots \mathfrak{P}_{s-r}$ são dois a dois distintos e não estão em S. Perceba que isso é possível pois existem infinitos primos de K que não se decompõe em L. Afirmamos que o conjunto $T = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-r}\}$ satisfaz as propriedades desejadas.

Pra isso, primeiro mostraremos que N_i é o corpo de decomposição da extensão $N|K$ do único primo $\mathfrak{P}_i'$ de N sobre $\mathfrak{P}_i, i = 1, \ldots, s-r$. De fato, como $\mathfrak{P}_i$ não se decompõe em N, existe um único primo N sobre $\mathfrak{P}_i$, logo $\sigma_i\mathfrak{P}_i = \mathfrak{P}_i$, logo σ_i pertence ao grupo de decomposição $G(N|Z_i)$, logo $G(N|N_i) \subseteq G(N|Z_i)$. Por outro lado, $\mathfrak{p}_i$ é não ramificado em N, pois se $\mathfrak{Q}_i$ é um primo de N sobre $\mathfrak{p}_i$, então para cada $u \in K^S$, do capítulo sobre corpos com valor absoluto, sabemos que $K_{\mathfrak{p}_i}(\sqrt[n]{u})|K_{\mathfrak{p}_i}$ é não ramificado e $K_{\mathfrak{p}_i}(\sqrt[n]{u})$ é a localização de $K(\sqrt[n]{u})$ com respeito ao place de $K(\sqrt[n]{u})$ abaixo de $\mathfrak{Q}_i$, então o compósito das extensões $K_{\mathfrak{p}_i}(\sqrt[n]{u})|K_{\mathfrak{p}_i}$, sobre todos os $u \in K^S$, que é igual a $N_{\mathfrak{Q}_i}|K_{\mathfrak{p}}$ é não ramificado, logo todo primo $\mathfrak{Q}_i$ de N sobre $\mathfrak{p}_i$ é não ramificado, ou seja $\mathfrak{p}_i$ é não ramificado em N. Logo $\mathfrak{P}_i$ é não ramificado sobre N_i, logo temos o isomorfismo

$$G(N|Z_i) \simeq G(\kappa(\mathfrak{P}_i)|\kappa(\mathfrak{P}_i \cap Z_i))$$

e o grupo do lado direito é cíclico pois é o grupo de Galois de uma extensão finita do corpo finito $\mathbb{Z}/p_i\mathbb{Z}$, onde p_i é o número primo abaixo de $\mathfrak{P}_i$, logo $G(N|Z_i)$ é cíclico. Como $G(N|Z_i) \supseteq G(N|N_i)$, $\#G(N|N_i) = n$, então $n|\#G(N|Z_i)$ mas todo elemento de $G(N|K)$ tem ordem dividindo n, em particular o elemento gerador de $G(|Z_i)$, logo $n = \#G(N|Z_i)$, ou seja, $G(N|Z_i) = G(N|N_i)$. Portanto $N_i = Z_i$.

Para cada i, sabemos da proposição 19 que o corpo de decomposição N_i é maior subextensão de $N|K$ em que $\mathfrak{p}_i$ se decompõe totalmente e como $L = \bigcap_i^{s-r} N_i$, vemos que $L|K$ é a subextensão maximal de $N|K$ em que todos os primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-r}$ se decompõe totalmente. Portanto, se $x \in K^S$, temos que

$$x \in \Delta \Leftrightarrow K(\sqrt[n]{x}) \subseteq L \Leftrightarrow \mathfrak{p}_i, i = 1, \ldots, s-r, \text{ se decompõe totalmente em } K(\sqrt[n]{x}) \Leftrightarrow$$
$$e(K_{\mathfrak{p}_i}(\sqrt[n]{x})|K_{\mathfrak{p}_i}) = f(K_{\mathfrak{p}_i}(\sqrt[n]{x})|K_{\mathfrak{p}_i}) = 1, i = 1, \ldots, s-r, \Leftrightarrow [K_{\mathfrak{p}_i}(\sqrt[n]{x}) : K_{\mathfrak{p}_i}] = 1,$$
$$i = 1, \ldots, s-r \Leftrightarrow K_{\mathfrak{p}_i}(\sqrt[n]{x}) = K_{\mathfrak{p}_i}, i = 1, \ldots, s-r \Leftrightarrow x \in K_{\mathfrak{p}_i}^{*n}, i = 1, \ldots, s-r.$$

Portanto, Δ é o núcleo do mapa $K^S \longrightarrow \prod_{i=1}^{s-r} K_{\mathfrak{p}_i}^*/K_{\mathfrak{p}_i}^{*n}$. □

Proposição 92. *Seja T um conjunto de primos como na proposição anterior e seja $C_K(S,T) = I_K(S,T) \cdot K^*/K^*$, onde*

$$I_K(S,T) = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p} \in T} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S \cup T} U_{\mathfrak{p}}.$$

Se, em particular, $L|K$ for cíclica, então $N_{L|K}C_L = C_K(S,T)$.

4.5.2 Teorema da Norma de Hasse

Teorema 13 (Axioma de corpos de classe global)**.** *Sejam $L|K$ uma extensão cíclica de corpos de números. Então:*

$$\#H^i(G(L|K), C_L)) = \begin{cases} [L:K] & \text{se } i = 0; \\ 1 & \text{se } i = -1. \end{cases}$$

Demonstração. Temos que

$$[L:K] = h(G(L|K), C_L) = \frac{\#H^0((L|K), C_L))}{\#H^{-1}((L|K), C_L))},$$

então basta mostrarmos que $H^{-1}((L|K), C_L)) = H^1((L|K), C_L)) = 1$. Provaremos isso por indução no grau $n = [L:K]$ e denotaremos $H^1(L|K) = H^1(G(L|K), C_L)$. Seja $M|K$ uma subextensão de $L|K$ de grau primo p. Se $p < n$, então por hipótese de indução $H^1(M|K) = 1$ e $H^1(L|M) = 1$ e da sequência exata

$$H^1(M|K) \to H^1(L|K) \to H^1(L|M)$$

obtida de 61, segue que $H^1(L|K) = 1$. Se $p = n$, então denotamos $K' = K(\mu_p)$ e $L' = L(\mu_p)$ e temos que $L'|K'$ é extensão de Kummer cíclica, logo, por 92 $\#H^0(L'|K') = [L':K']$, ou seja, $H^1(L'|K') = 1$. Como $[K':K] \leq p-1 < p$, temos por hipótese de indução que $H^1(K'|K) = 1$, então da sequência exata

$$H^1(K'|K) \to H^1(L'|K) \to H^1(L'|K')$$

deduzimos que $H^1(L'|K) = 1$. Portanto, da sequência exata $1 \to H^1(L|K) \to H^1(L'|K)$, concluímos que $H^1(L|K) = 1$. □

Teorema 14 (Teorema da norma de Hasse)**.** *Seja $L|K$ uma extensão cíclica de corpos de números. A propriedade de um elemento $x \in K^*$ ser norma de um elemento de L é local, ou seja, é equivalente à propriedade de ser norma em qualquer completamento $L_{\mathfrak{P}}|K_{\mathfrak{p}}$.*

Demonstração. Seja $G = G(L|K)$ e $G_{\mathfrak{P}} = G(L_{\mathfrak{P}}|K_{\mathfrak{p}})$. A sequência exata de G-módulos $1 \to L^* \to I_L \to C_L \to 1$ induz, pela proposição 63, uma sequência exata

$$H^{-1}(G, C_L) \longrightarrow H^0(G, L^*) \longrightarrow H^0(G, I_L) \longrightarrow H^0(G, C_L).$$

Sabemos pelo axioma de corpos de classe global que $H^{-1}(G, C_L) = 1$ e sabemos por 86 que $H^0(G, I_L) = \bigoplus_{\mathfrak{p}} H^0(G_{\mathfrak{p}}, L^*_{\mathfrak{P}})$. Portanto, o homomorfismo

$$K^*/N_{L|K}L^* \longrightarrow \bigoplus_{\mathfrak{p}} K^*_{\mathfrak{p}}/N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}L^*_{\mathfrak{P}}$$

é injetivo, e isso prova a proposição. □

4.5.3 Princípio Local-Global para Quádricas

Por fim, vamos utilizar a teoria de corpos de classe desenvolvida até aqui, em especial o teorema da norma de Hasse, para enunciar e provar o Teorema de Hasse-Minkowski, conhecido também como princípio local-global para quádricas. Para não estender ainda mais o trabalho, não faremos uma exposição detalhada da teoria de formas quadráticas e nesse sentido recomendamos como referência introdutória o capítulo 4 de Serre (1973) e para um estudo mais sistemático e aprofundado, indicamos O'Meara (2000). Primeiramente precisaremos do seguinte lema técnico.

Lema 14. *Sejam K um corpo, $K(\sqrt{a})|K$ e $K(\sqrt{b})|K$ extensões quadráticas de K e $c \in K^*$. Suponha que $K(\sqrt{a}, \sqrt{b})$ é uma extensão própria de $K(\sqrt{ab})$. Então c é o produto de uma norma de $K(\sqrt{a})|K$ por uma norma de $K(\sqrt{b})|K$ se e somente se, c visto como um elemento de $K(\sqrt{ab})$ for uma norma da extensão $K(\sqrt{a}, \sqrt{b})|K(\sqrt{ab})$.*

Demonstração. Ver lema 2.5.1 de Gondim (2006).

□

Lema 15. *Sejam K um corpo de números e $\mathfrak{p}$ um place finito. Então $K^{*2}_{\mathfrak{p}}$ é aberto em $K^*_{\mathfrak{p}}$.*

Demonstração. Ver corolário 63:1.b de O'Meara (2000).

□

Definição 58. *Dizemos que uma forma quadrática $Q(X_1, \ldots, X_n) = \sum_{i,j} a_{ij}X_iX_j$ com coeficientes num corpo K de característica diferente de 2 representa 0 se a equação $Q(x_1, \ldots, x_n) = 0$ admite solução não trivial em K.*

Teorema 15 (Hasse-Minkowski)**.** *Seja K um corpo de números e $n \geq 2$. Considere uma quádrica*

$$Q(X_1, \ldots, X_n) = \sum_{i,j} a_{ij}X_iX_j$$

com coeficientes em K. Então Q representa 0 em K se e somente se Q representa 0 em $K_\mathfrak{p}$ para cada place $\mathfrak{p}$.

Demonstração. A ida é clara, então basta demonstrarmos a volta. A menos de mudança de variáveis, podemos supor que a forma quadrática é da forma $Q(X_1, \ldots, X_n) = \sum_i^n a_i X_i^2$. Para mais detalhes sobre essa mudança de variáveis e para uma introdução a teoria de formas quadráticas, ver o capítulo 4 de Serre (1973).

Caso $n = 2$: Sejam $a, b, c \in K^*$, então

$$ax^2 - by^2 = 0 \Leftrightarrow \sqrt{\frac{b}{a}} = \frac{x}{y} \in K^*.$$

Portanto, basta provar que se $d \in K^*$ é um quadrado em cada localização $K_\mathfrak{p}$, então é um quadrado em K, ou seja, que se a extensão $L = K(\sqrt{d})|K$ tem grau 2, então existe um uma localização $K_\mathfrak{p}$ em que d não é quadrado. Como a quantidade de places de K que se ramificam em L é finita, assim como a quantidade de places infinitos é finita, mas existe uma quantidade infinita de places de K que não se decompõe em L, então existe um place finito $\mathfrak{p}$ de L não ramificado que não se decompõe em L. Seja $\mathfrak{P}$ o único place L sobre $\mathfrak{p}$. Da identidade fundamental, temos que

$$[L : K] = e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p}) \Rightarrow 2 = 1.f(\mathfrak{P}|\mathfrak{p}) \Rightarrow f(\mathfrak{P}|\mathfrak{p}) = 2.$$

Como $\mathfrak{p}$ não se ramifica em L, segue que $[L_\mathfrak{P} = K_\mathfrak{p}] = f(\mathfrak{P}|\mathfrak{p}) = 2$. Portanto, d não é quadrado em $K_\mathfrak{p}$.

Caso $n = 3$: Sem perda de generalidade podemos supor $Q = X^2 - aY^2 - bZ^2$. A condição de de Q representar 0 é equivalente a b ser uma norma de um elemento da extensão $K(\sqrt{a})|K$. De fato, $b = N_{K(\sqrt{a})|K}(x + y\sqrt{a})$. Como a extensão $K(\sqrt{a})|K$ é cíclica, o resultado segue do teorema da norma de Hasse.

Caso $n = 4$: Sem perda de generalidade podemos supor $Q = X^2 + bY^2 - cZ^2 - acT^2$. Suponha que Q representa 0 em $K_\mathfrak{p}$, para cada place $\mathfrak{p}$. Primeiramente vamos supor que $[K(\sqrt{a}, \sqrt{b}) : K(\sqrt{ab})] = 2$. Temos duas possibilidades

(i) $[K_\mathfrak{p}(\sqrt{a}, \sqrt{b}) : K_\mathfrak{p}(\sqrt{ab})] = 2$, e assim

$$c = N_{K_\mathfrak{p}(\sqrt{b})|K_\mathfrak{p}}(x + y\sqrt{b}).N_{K_\mathfrak{p}(\sqrt{a})|K_\mathfrak{p}}\left(\frac{1}{z + t\sqrt{a}}\right)$$

ou seja, c é o produto da norma de um elemento da extensão $K_\mathfrak{p}(\sqrt{a})|K_\mathfrak{p}$ e a norma de um elemento da extensão $K_\mathfrak{p}(\sqrt{b})|K_\mathfrak{p}$, logo c é a norma de um elemento da extensão $K_\mathfrak{p}(\sqrt{a}, \sqrt{b})|K_\mathfrak{p}(\sqrt{ab})$, pelo lema 14;

(ii) $[K_\mathfrak{p}(\sqrt{a},\sqrt{b}) : K_\mathfrak{p}(\sqrt{ab})] = 1$, e assim é imediato que c é uma norma da extensão $K_\mathfrak{p}(\sqrt{a},\sqrt{b})|K_\mathfrak{p}(\sqrt{ab})$.

Como a extensão $K(\sqrt{a},\sqrt{b})|K(\sqrt{ab})$ é cílica, o resultado segue do teorema da norma de Hasse 14 e do lema 14.

Agora suponha que $[K(\sqrt{a},\sqrt{b})|K(\sqrt{ab})] = 1$, então é fácil provar que $K(\sqrt{a}) = K(\sqrt{b})$, logo para cada place $\mathfrak{p}$, temos que $K_\mathfrak{p}(\sqrt{a}) = K_\mathfrak{p}(\sqrt{b})$ e assim

$$c = N_{K_\mathfrak{p}(\sqrt{a})|K_\mathfrak{p}}\left(\frac{x+y\sqrt{b}}{z+t\sqrt{a}}\right),$$

ou seja, c é a norma de um elemento na extensão $K_\mathfrak{p}(\sqrt{b})|K_\mathfrak{p}$ para cada place $\mathfrak{p}$, logo é norma na extensão $K(\sqrt{b})|K$, então a quádrica $X-bY^2-cZ^2$ representa 0 em K, logo Q representa 0 em K.

Caso $n \geq 5$: vamos proceder por indução no número de variáveis. Escreva $Q = aX_1^2 + bX_2^2 - \tilde{Q}$ e denote S e conjunto de places em que $\tilde{Q}$ não representa 0. Com efeito $\tilde{Q}$ tem pelo menos 3 variáveis, então basta mostrar que uma quádrica da forma $X^2 - bY^2 - cZ^2$ com $b, c \in K^*$ representa 0 em quase todo place e isso é de fato verdade, pois a quádrica $X^2 - bY^2 - cZ^2$ representa 0 em $K_\mathfrak{p}$ se e somente se $b \in N_{K_\mathfrak{p}(\sqrt{a})|K_\mathfrak{p}}K_\mathfrak{p}(\sqrt{a})^*$ e b de fato é uma norma quase sempre pois pelo teorema da norma de Hasse 14, a aplicação

$$K/N_{K(\sqrt{a})|K}K(\sqrt{a})^* \hookrightarrow \bigoplus_\mathfrak{p} K_\mathfrak{p}^*/N_{K_\mathfrak{p}(\sqrt{a})|K_\mathfrak{p}}K_\mathfrak{p}(\sqrt{a})^*$$

é injetiva. Nossa hipótese é de que Q representa 0 em $K_\mathfrak{p}$ para cada place $\mathfrak{p}$, portanto para cada $\mathfrak{p}$, existe um $c_\mathfrak{p} \in K_\mathfrak{p}^*$ tal que $aX_1^2 + bX_2^2$ e $\tilde{Q}$ o representam em $K_\mathfrak{p}$. Vamos chamar tais coordenadas $x_i(\mathfrak{p})$. Como K^{*2} é aberto e S é finito, existe $\varepsilon > 0$ tal que se $c \in K^*$ e $|c - c_\mathfrak{p}|_\mathfrak{p} < \varepsilon, \forall \mathfrak{p} \in S$, então $c/c_\mathfrak{p} \in K_\mathfrak{p}^{*2}, \forall \mathfrak{p} \in S$. Como $h(x_1,x_2) = ax_1^2 + bx_2^2$ é contínua em $K_\mathfrak{p}$ para cada $\mathfrak{p} \in S$, existe $\delta > 0$ tal que se $x_1, x_2 \in K$ satisfazem

$$\max\{|x_1 - x_1(\mathfrak{p})|,\ |x_2 - x_2(\mathfrak{p})|\} < \delta, \tag{4.1}$$

então $|h(x_1,x_2) - c_\mathfrak{p}| < \varepsilon, \forall \mathfrak{p} \in S$ mas pelo teorema de aproximação 29, podemos encontrar $x_1, x_2, \in K$ satisfazendo a condição (4.1) para cada $\mathfrak{p} \in S$ e denote $h(x_1,x_2) = c$.

Considere agora a forma quadrática $\overline{Q} = cY^2 - \tilde{Q}$. Ela representa 0 em $K_\mathfrak{p}, \forall \mathfrak{p} \notin S$ pois $\tilde{Q}$ representa 0 nesses corpos, por hipótese. Por outro lado, nossa construção nos mostra que a forma quadrática $\overline{Q}$ também representa 0 em $K_\mathfrak{p} \forall \mathfrak{p} \in S$, pois nesse caso, $c = c_\mathfrak{p} d_\mathfrak{p}^2$ e é suficiente tomar $y = 1/d_\mathfrak{p}$ e as coordenadas em $\tilde{Q}$ que a fazem representar $c_\mathfrak{p}$. Pela hipótese

indutiva, temos que a foram quadrática $\overline{Q}$ representa 0 em K. Se nesse caso, tivermos $y = 0$, então $\tilde{Q}$ representa 0 em K e assim Q também. Se ocorrer $y \neq 0$, então dividindo por y^2, percebemos que $\tilde{Q}$ e $aX_1^2 + aX_2^2$ representam o mesmo c em K e portanto sua diferença, Q, representa 0 em K. □

5 PROBLEMA DE FROBENIUS EM DOMÍNIOS COM VALOR ABSOLUTO

Sejam $k \geq 2$ e $a_1, \ldots, a_k, c \in \mathbb{Z}_{>0}$ com $mdc(a_1, \ldots, a_n) = 1$ e considere uma equação linear

$$a_1x_1 + \cdots + a_kx_k = c$$

em $x_1, \ldots, x_k \in \mathbb{Z}$. É possível provar que existe $c_0 \in \mathbb{Z}_{\geq 0}$ tal que para todo inteiro $c \geq c_0$, a equação acima admite solução não negativa, ou seja, com $x_i \geq 0, \forall i$. Um número positivo c para o qual a equação acima tem solução positiva é chamado de representável e algumas perguntas interessantes são:

- Quais são os números representáveis?
- Qual o menor número representável tal que todo número maior que ele é também representável? Chamamos este número de número de Frobenius $\gamma(a_1, \ldots, a_n)$.
- Quantas representações diferentes um número possui?

Estes questionamentos são chamados de problemas de Frobenius e vários resultados sobre eles podem ser encontrados em Alfonsín (2005). Outros autores propuseram formulações para os problemas de Frobenius em outros ambientes matemáticos como Johnson e Looper (2012) fizeram para domínios de integridade e Gondim e Rodriguez (2017) fizeram para polinômios. O que buscamos nesta parte do trabalho foi investigar estes tipos de questões em domínios com valor absoluto. Seja $(D, |\ |)$ um domínio de característica 0 com valor absoluto e $(K, |\ |)$ seu corpo de frações com o valor absoluto estendido de D, então a inclusão $D \subseteq K$ é um mergulho algébrico e topológico. Sejam $\hat{D} \subseteq \hat{K}$ os completamentos de $D \subseteq K$ com respeito a métrica induzida pelo valor absoluto $|\ |$, então temos o seguinte diagrama

$$\begin{array}{ccc} K & \hookrightarrow & \hat{K} \\ \uparrow & & \uparrow \\ D & \hookrightarrow & \hat{D} \end{array}$$

e vamos supor que $\hat{K}$ é localmente compacto. Já provamos em 9 que estes corpos podem ser classificados da seguinte forma:

Proposição 93. *Se $(K, |\ |)$ é corpo com valor absoluto localmente compacto e de característica 0, então existe um isomorfismo, que também é homeomorfismo, entre K e*

(i) $\mathbb{R}$ *ou* $\mathbb{C}$*, se* $(K, |\ |)$ *é arquimediano;*

(ii) Uma extensão finita de $\mathbb{Q}_p$*, para algum primo* p*, se* $(K, |\ |)$ *é não arquimediano.*

Então neste breve capítulo propomos formulações análogas aos problemas de Frobenius no caso arquimediano e no caso não arquimediano, assim como provamos certos resultados originais em cada um dos casos. Sobre esta parte do trabalho foi aceito um resumo para apresentação de pôster na I Semana de Encontros Aritméticos, entre os dias 24-26 de fevereiro de 2025 na UNESP Rio Preto.

5.1 O CASO ARQUIMEDIANO

Definição 59. *Um domínio ordenado é um domínio* D *com um subconjunto não vazio* $P \subseteq D$ *satisfazendo as seguintes propriedades:*

(i) $\forall a, b \in P, a + b \in P$*;*

(ii) $\forall a, b \in P, ab \in P$*;*

(iii) Para cada $a \in D$*, uma e apenas um dos casos ocorre:*

$$a \in P,\ a = 0,\ -a \in P$$

e dizemos que P *é um conjunto de elementos positivos.*

Exemplo: $D = \mathbb{R}$ e $P = \mathbb{R}_{>0}$.

Observação 5. *Note que um domínio ordenado* (D, P) *possui uma relação de ordem dada por* $y > x \iff y - x \in P$*.*

Observação 6. *Lembramos que todo domínio ordenado tem característica* 0*.*

Observação 7. *Se* (D, P) *é um domínio ordenado, então seu corpo de frações é naturalmente ordenado.*

Definição 60. *Um domínio ordenado* (D, P) *é dito arquimediano se a imagem* $\mathbb{Z} \hookrightarrow D$ *não tem cota superior. Neste caso identificamos a imagem de* $\mathbb{Z}$ *com os inteiros.*

Observação 8. *Note que este conceito não é exatamente o mesmo de valor absoluto arquimediano mas ele será útil devido o teorema de classificação de corpos localmente compactos e a relação ficará clara ao longo desta seção.*

Lema 16. *Seja (D, P) um domínio ordenado arquimediano. Dados $x, y \in D$ tais que $y - x > 1$, então existe $n \in \mathbb{Z}$ tal que $x < n < y$.*

Demonstração. Considere o seguinte subconjunto $S = \{n \in \mathbb{Z} : n > x\}$ que é não vazio pela hipótese de arquimedianidade e x é uma cota inferior de S, então existe um elemento minimal $n_0 \in S$. Nós temos que $n_0 < y$, pois caso contrário, $n_0 \geq y$ e assim $n_0 - x \geq y - x > 1$, o que implicaria $n_0 - 1 > x$, contradizendo a minimalidade de $n_0 \in S$. □

Lema 17. *Seja (D, P) um domínio ordenado arquimediano . Então, dados $a, b \in P$, para todo $f \in P \cap (a, b)$ tal que $f > ab$, existem $x, y \in P$ tais que*

$$ax + by = f.$$

Demonstração. Já que $f \in (a, b)$, existem $x_0, y_o \in D$ tais que $f = ax_0 + by_0$. Para todo $u \in D$ temos que $x = x_0 + bu$ e $y = y_0 - au$ também é solução da equação. Para que ocorra $x, y > 0$ é necessário que

$$\frac{-x_0}{b} < u < \frac{y_0}{a}.$$

A diferença

$$\frac{y_0}{a} - \frac{-x_0}{b} = \frac{ax_0 + by_0}{ab} = \frac{f}{ab} > 1$$

implica que existe $m \in \mathbb{Z}$ tais que

$$\frac{-x_0}{b} < m < \frac{y_0}{a}$$

e assim, basta tomar $x = x_0 + mb$, $y = y_0 - ma$. □

Proposição 94. *Seja (D, P) um domínio ordenado arquimediano. Então, dados $a_1, \ldots a_k \in P$, $(k \geq 3)$, para todo $f \in P \cap (a_1, \ldots, a_k)$ tal que $f > (k-1)a_1 \ldots a_{k-1}a_k^2$, existem $x_1, \ldots, x_k \in P$ tais que*

$$a_1x_1 + \cdots + a_kx_k = f.$$

Demonstração. Já que $f \in P \cap (a_1, \ldots, a_k)$, então existem $y_1, \ldots y_k \in D$ tais que

$$a_1y_1 + \cdots + a_ky_k = f.$$

Seja $A_i = \prod_{j \neq i} a_i$ para $i = 1, \ldots, k-1$. É fácil ver que para todos $u_1, \ldots, u_{k-1} \in D$ a k-upla

$$\begin{aligned} x_1 &= y_1 + A_1 u_1 \\ x_2 &= y_2 + A_2 u_2 \\ &\cdots \\ x_{n-1} &= y_{n-1} + A_{k-1} u_{k-1} \\ x_k &= y_k - A_k(u_1 + u_2 + \cdots + u_{k-1}) \end{aligned}$$

também representa uma solução da equação linear. Vamos nos restringir ao caso $u_i \in \mathbb{Z}$.

Afirmamos que pela propriedade arquimediana, podemos escolher $0 < x_i \leq A_i$ para $i = 1, \ldots, k-1$. De fato, para cada i, o conjunto $\{A_i u_i : u_i \in \mathbb{Z}\}$ é ilimitado, então seja n_i o menor inteiro tal que

$$n_i A_i \geq y_i.$$

Então $n_i A_i \geq y_i > (n_i - 1)A_i$, logo $A_i \geq y_i - (n_i - 1)A_i > 0$. Defina $u_i = -n_i + 1$ e $x_i = y_i + u_i A_i$ e a afirmação segue. Neste caso

$$0 < g := a_1 x_1 + a_2 x_2 + \cdots + a_{n-1} x_{n-1} \leq (n-1) a_1 \ldots a_k.$$

Perceba que $f \in P(g, a_k)$ e por hipótese $f > (n-1)a_1 \ldots a_{k-1} a_k^2 \geq g a_k$. Portanto, existem $v_0, w_0 \in P$ tais que $f = g v_0 + a_k w_0$, logo

$$f = a_1(x_1 v_0) + \cdots + a_{n-1}(x_{n-1} v_0) + a_k w_0$$

e $x_1 v_0, \ldots, x_{n-1} v_0, w_0 \in P$. □

Observação 9. *Problema de Frobenius em domínios arquimedianos. Considere novamente o diagrama*

$$\begin{array}{ccc} K & \hookrightarrow & \hat{K} \\ \uparrow & & \uparrow \\ D & \hookrightarrow & \hat{D} \end{array}$$

pelo Teorema de Classificação de corpos localmente compactos, $\hat{K}$ é ou $\mathbb{R}$ ou $\mathbb{C}$. Se supomos $\hat{K} = \mathbb{R}$, então $(D, D \cap \mathbb{R}_{>0})$ é um domínio ordenado e os resultados anteriores nos dão um Problema de Frobenius em D. Se supomos $\hat{K} = \mathbb{C}$, então D não tem uma noção consistente de positividade. Por outro lado, o problema de Frobenius pode ser enunciado nos números complexos através de outra abordagem, como fizeram Maier e Paschke (2011).

5.2 O CASO NÃO ARQUIMEDIANO

No caso não arquimediano, não temos uma noção precisa de positividade pois $\mathbb{Z}_p$ não é domínio ordenado. Mas neste caso podemos definir um conceito de pseudopositividade e assim enunciar um problema de Frobenius e estudá-lo.

Definição 61. *Seja $(D, |\ |)$ um domínio de característica 0 com valor absoluto. Dizemos que $P \subseteq D$ é um conjunto de elementos pseudopositivos se*

- $0 \in P$;
- $\forall a, b \in P, a + b \in P$ *e* $ab \in P$;
- P *é topologicamente fechado.*

Exemplo: $(\mathbb{Z}_p, |\ |_p)$ com $P = p\mathbb{Z}_p$.

O problema que precisamos estudar é o seguinte:

Problema 1. *Seja $k \geq 2$ um número inteiro. Dados $a_1, \ldots a_k, c \in P \subseteq D$, como se comportam as soluções pseudopositivas $x_1, \ldots, x_k \in P$ da equação*

$$a_1 x_1 + \cdots + a_k x_k = c\ ?$$

Novamente, de volta ao diagrama para o caso não arquimediano

$$\begin{array}{ccc} K & \hookrightarrow & \hat{K} \\ \uparrow & & \uparrow \\ D & \hookrightarrow & \hat{D} \end{array}$$

Pelo teorema de classificação, $\hat{K}$ é uma extensão finita de $\mathbb{Q}_p$ para algum número primo p e também temos que $\mathbb{Z}_p \subseteq \hat{D}$. Vamos denotar $\mathcal{O}$ o anel de valoração de $\hat{K}$, π seu elemento primo e v a valoração normalizada. Nós conseguimos estudar o problema de Frobenius no completamento $\hat{D}$ pois é possível calcular explicitamente o conjunto P usando o seguinte lema.

Lema 18. *Se $P \subseteq \mathcal{O}$ é um conjunto de elementos pseudopositivos, então $P = \pi^m \mathcal{O}$ onde $m = \min\{v(x) : x \in P\}$.*

Demonstração. Seja $\alpha \in P$, então perceba que $\alpha\mathcal{O} \subseteq P$ pois P é topologicamente fechado, é fechado sob adição e todo elemento de $\mathcal{O}$ pode ser escrito como $\sum_{l\geq 0} a_l\pi^l,\ 0 \leq a_l \leq p-1$. Como $\alpha\mathcal{O} = p^{v_p(\alpha)}\mathcal{O}$, obtemos

$$P = \bigcup_{\alpha\in P} \pi^{v_p(\alpha)}\mathcal{O} = \pi^{v_p(\alpha_0)}\mathcal{O},$$

onde $v(\alpha_0)$ é minimal. □

Portanto, estamos lidando com o seguinte problema: dados $a_1, \ldots, a_k, c \in \pi^m\mathcal{O}, k \geq 2,\ m > 0$, temos a equação

$$a_1x_1 + \cdots + a_kx_k = c$$

e queremos entender a existência e comportamento das soluções $x_1, \ldots, x_k \in \pi^m\mathcal{O} \setminus \{0\}$. Primeiramente, dividindo os coeficientes e o termo resultado por π^m e o resultado c da combinação linear ainda está em $\pi^m\mathcal{O}$ pois todos os x_is estão.

5.2.1 Equação linear com restrição em anel de valoração discreta

Vamos fixar um corpo K com característica 0 e discreto com valoração (normalizada) v. Seja $\mathcal{O}$ seu anel de valoração, $\mathfrak{p}$ seu único ideal maximal e π um elemento primo $(v(\pi) = 1)$.

Teorema 16. *Para cada $k, n \in \mathbb{Z}_{>0}$, dados $a_1, \ldots, a_k \in \mathcal{O} \setminus \{0\}$ e $c \in \mathfrak{p}^n \setminus \{0\}$, a equação*

$$a_1x_1 + \cdots + a_kx_k = c \tag{5.1}$$

tem solução em $x_1, \ldots, x_k \in \mathfrak{p}^n \setminus \{0\} \iff v(c) \geq \min_{1\leq i\leq k}\{v(a_i)\} + n$.

Demonstração. ($\Rightarrow$) Já que $x_1, \ldots, x_k \in \mathfrak{p}^n$, $a_1, \ldots, a_k \in \mathcal{O}$ e $c = \sum_{i=1}^k a_ix_i$, então

$$v(c) \geq \min_{1\leq i\leq k}\{v(a_ix_i)\} = \min_{1\leq i\leq k}\{v(a_i) + n\} = \min_{1\leq i\leq k}\{v(a_i)\} + n.$$

($\Leftarrow$) Quando $k = 1$, precisamos resolver a equação $a_1x = c$, supondo $a_1, c \in \mathcal{O} \setminus \{0\}$ e $v(c) \geq v(a_1) + n$, então $x = ca_1^{-1} \neq 0$ em K e $v(x) = v(c) - v(a_1) \geq n$, logo $x \in \mathfrak{p}^n \setminus \{0\}$. Agora suponha verdade para k e provaremos ser verdade o caso $k+1$. Temos a equação

$$a_1x_1 + \cdots + a_{k+1}x_{k+1} = c.$$

Seja $l = v(c)$ e sem perda de generalidade, podemos supor $v(a_{k+1}) = \max_{1\leq i\leq k+1}\{v(a_i)\}$.

Se $c \neq a_{k+1}\pi^l$, tome $x_{k+1} = \pi^l$, então $v(c - a_{k+1}\pi^l) \geq l \geq \min_{1\leq i\leq k}\{v(a_i)\} + n$ logo, pelo caso k, $\exists x_1, \ldots, x_k \in \mathfrak{p}^n \setminus \{0\}$ tais que

$$\sum_{i=1}^{k} a_i x_i = c - a_{k+1}\pi^l = c - a_{k+1}x_{k+1} \Rightarrow \sum_{i=1}^{k+1} a_i x_i = c.$$

Se $c = a_{k+1}\pi^l$, tome $x_{k+1} = 2\pi^l$ e segue analogamente. □

Em uma linguagem de Frobenius, dados $a_1, \ldots, a_k \in \mathcal{O} \setminus \{0\}$, dizemos que um elemento $c \in \mathfrak{p}^n \setminus \{0\}$ é representável se a equação (5.1) tem solução em $x_1, \ldots, x_k \in \mathfrak{p}^n \setminus \{0\}$. A menor valoração possível de um elemento representável é $\gamma(a_1, \ldots, a_n) = \min_{1 \leq i \leq k} \{v(a_i)\} + n$ e podemos dizer que este é um número de Frobenius. Além disso, cada elemento com uma valoração maior é representável e nenhum elemento com valoração menor é representável. Agora vamos provar alguns resultados sobre a infinitute de representações de um elemento representável fixado, de maneira análoga ao que foi feito por Gondim e Rodriguez (2017) para polinômios.

Proposição 95. *Seja $k \geq 2$ e $a_1, \ldots, a_k, c \in \mathcal{O} \setminus \{0\}$ tais que $v(a_1) \leq \cdots \leq v(a_k)$ e $c \in \mathfrak{p}^n \setminus \{0\}$. Dados inteiros $m_2, \ldots, m_k \geq v(c)+1$, então existem infinitas soluções $(x_1, x_2, \ldots, x_k)$ da equação*

$$a_1 x_1 + \cdots + a_k x_k = c$$

em $\mathfrak{p}^n \setminus \{0\}$ tais que

$$v(x_1) = v(c) - v(a_1),\ v(x_2) = m_2, \cdots, v(x_k) = m_k.$$

Demonstração. Se $k = 2$, há no máximo um $u \in \mathcal{O}^*$ tal que $c = a_2 u \pi^{m_2}$ mas $\mathcal{O}^*$ é um conjunto infinito, logo para cada cada $u \in \mathcal{O}^*$ com $c - a_2 u \pi^{m_2} \neq 0$, tome $x_{2,u} = u\pi^{m_2}$, assim

$$c - a_2 u \pi^{m_2} = \pi^{v(c)} u(c) - u\pi^{v(a_2)+m_2} u(a_2) = \pi^{v(c)}(u(c) - u\pi^{v(a_2)+m_2-v(c)} u(a_2))$$

com $u(c), u(a_2) \in \mathcal{O}^*$, então $v(c - a_2 t \pi^{m_2}) = v(c)$, assim, tomando $x_1 = a_1^{-1}(c - a_2 t \pi^{m_2})$, segue que $(x_1, x_{2,t})$ é solução da equação satisfazendo as condições apresentadas.

Agora suponha provado o caso k e iremos provar o caso $k+1$. Perceba que existe no máximo um $u \in \mathcal{O}^*$ tal que $c = a_{k+1} u \pi^{m_{k+1}}$ mas $\mathcal{O}^*$ é um conjunto infinito, logo para cada $u \in \mathcal{O}^*$ com $c - a_{k+1} u \pi^{m_{k+1}} \neq 0$, temos $v(c - a_{k+1} u \pi^{m_{k+1}}) = v(c)$, então tome $x_{k+1,u} = u\pi^{m_{k+1}}$ e por hipótese de indução segue que existem infinitas k-uplas $(x_1, \ldots, x_k)$ satisfazendo $v(x_1) = v(c) - v(a_1),\ v(x_2) = m_2, \cdots, v(x_k) = m_k$ e

$$\sum_{i=1}^{k} a_i x_i = c - a_{k+1} u \pi^{m_{k+1}} = c - a_{k+1} x_{k+1,u} \Rightarrow \left(\sum_{i=1}^{k} a_i x_i\right) + a_{k+1} x_{k+1,u} = c$$

□

Proposição 96. *Sejam* $a_1, \ldots, a_k \in \mathcal{O} \setminus \{0\}$ *e* $c \in \mathfrak{p}^n \setminus \{0\}$, *tais que* $v(a_1) \leq \cdots \leq v(a_k)$, $v(c) \geq v(a_1) + n$ *e fixado* $x_1 \in \mathfrak{p}^n \setminus \{0\}$, *tal que* $v(x_1) \neq v(c) - v(a_1)$, *temos*

(i) se $v(x_1) < v(c) - v(a_1)$, *então existem* $x_2, \ldots x_k \in \mathfrak{p}^n \setminus \{0\}$ *tais que*

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_kx_k = c$$

se e somente se $v(a_2) \leq v(x_1) + v(a_1) - n$. *Neste caso, fixados inteiros* $m_3, \ldots m_k \geq v(x_1)+v(a_1)+1$, *existem infinitas* $(k-1)$*-uplas* $(x_2, x_3, \ldots, x_k)$ *de elementos de* $\mathfrak{p}^n \setminus \{0\}$ *satisfazendo a equação acima tais que*

$$v(x_2) = v(x_1) + v(a_1) - v(a_2), v(x_3) = m_3, \ldots, v(x_k) = m_k;$$

(ii) Se $v(x_1) > v(c) - v(a_1)$, *então existem* $x_2, \ldots x_k \in \mathfrak{p}^n \setminus \{0\}$ *tais que*

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_kx_k = c$$

se e somente se $v(c) \geq v(a_2) + n$. *Neste caso, fixados inteiros* $m_3, \ldots m_k \geq v(c) + 1$, *existem infinitas* $(k-1)-$*uplas* $(x_2, x_3, \ldots, x_k)$ *de elementos de* $\mathfrak{p}^n \setminus \{0\}$ *satisfazendo a equação acima tais que*

$$v(x_2) = v(c) - v(a_2), v(x_3) = m_3, \ldots, v(x_k) = m_k.$$

Demonstração. (i) Fixado x_1 como no enunciado, perceba que $v(c - a_1x_1) = v(a_1) + v(x_1)$, logo, pelo teorema 16, a equação $\sum_{i=2}^{k} a_ix_i = c - a_1x_1$ tem solução em $\mathfrak{p}^n \setminus \{0\}$ se e somente se

$$v(a_1) + v(x_1) = v(c - a_1x_1) \geq v(a_2) + n.$$

Neste caso, fixados inteiros $m_3, \ldots, m_k \geq v(x_1)+v(a_1)+1$, a demonstração deste item segue da proposição anterior.

(ii) Fixado x_1 como no enunciado segue que $v(c - a_1x_1) = v(c))$ e pelo teorema 16, a equação $\sum_{i=2}^{k} a_ix_i = c - a_1x_1$ tem solução em $\mathfrak{p}^n \setminus \{0\}$ se e somente se

$$v(c) = v(c - a_1x_1) \geq v(a_2) + n.$$

Neste, caso a demonstração deste item também segue da proposição anterior. □

Corolário 8. *Na situação* (i) *da proposição acima, segue que* $v(a_2) < v(c) - n$.

Demonstração. Use as desigualdades $v(x_1) < v(c) - v(a_1)$ e $v(a_2) \leq v(x_1) + v(a_1) - n$. □

Corolário 9. *Na situação* (ii) *da proposição acima, segue que* $v(x_1) > v(a_2) + n - v(a_1)$.

Demonstração. Use as desigualdades $v(x_1) > v(c) - v(a_1)$ e $v(c) \geq v(a_2) + n$. □

REFERÊNCIAS

ALFONSíN, J. R. *The Diophantine Frobenius Problem*. Oxford: Oxford University Press, 2005.

ARTIN, E.; TATE, J. *Class field theory*. New York: Benjamin, 1967.

ASH, R. *Basic Abstract Algebra: For Graduate Students and Advanced Undergraduates*. New York: Dover Publications, 2006.

GONDIM, R. *Aritmética das curvas algébricas*. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2006.

GONDIM, R. C. R.; RODRIGUEZ, M. On a frobenius problem for polynomials. *Geombinatorics Quarterly*, v. 47, n. 5, p. 1427–1462, 2017.

GOUVEA, F. *p-adic Numbers: An Introduction*. New York: Springer, 2003.

JOHNSON, P.; LOOPER, N. Frobenius problems in integral domains. *Geombinatorics Quarterly*, XXII, n. 2, p. 71–86, 2012.

MAIER, K. D. P. J. C.; PASCHKE, J. Frobenius problems in the gaussian integers. *Geombinatorics Quarterly*, XX, n. 3, p. 93–109, 2011.

NEUKIRCH, J. *Class Field Theory*. New York: Springer, 1986.

NEUKIRCH, J. *Algebraic Number Theory*. New York: Springer, 1999.

O'MEARA, O. T. *Introduction to Quadratic Forms*. New York: Springer, 2000.

SERRE, J.-P. *A Course in Arithmetic*. New York: Springer, 1973.

STEWART, I.; TALL, D. *Algebraic Number Theory and Fermat's Last Theorem*. Florida: CRC Press, 2016.

WEIL, A. *Basic Number Theory*. New York: Springer, 1982.