Um Estudo Sobre a Densidade dos Conjuntos de Ideais Primos

Guilherme de Souza Monteiro

17 de setembro de 2018

UNIVERSIDADE FEDERAL DE MINAS GERAIS

Um Estudo Sobre a Densidade dos Conjuntos de Ideais Primos

Guilherme de Souza Monteiro

Orientação:
André Gimenez Bueno
Ana Cristina Vieira

Dissertação submetida à banca examinadora, designada pelo Programa de Pós-Graduação em Matemática da UFMG, como requisito parcial para a obtenção do título de mestre em Matemática.

Belo Horizonte
17 de setembro de 2018

Agradecimentos

"Boas vibrações pra vocês
Que me ajudam a seguir meu caminho
Obrigado aos amigos da terra e do céu
Ninguém faz nada sozinho."

Fábio Júnior

Como nas palavras de Fábio Júnior, "ninguém faz nada sozinho". Assim, este trabalho nunca poderia ter sido realizado não fosse o apoio e auxílio de tantas pessoas que passaram pela minha jornada.

Uma seção de agradecimentos é sempre uma parte complicada de escrever. Penso que todas as pessoas que conheci, as que gosto e as que não gosto, contribuíram de alguma forma para quem sou hoje. Portanto, sou grato a todas as pessoas que já passaram por minha vida. Sem vocês tudo poderia ter sido diferente.

Entretanto, como é de praxe, algumas pessoas merecem uma citação especial. Se você está procurando seu nome aqui e ele não está, desculpe-me por ter esquecido de você. Minha memória é realmente fraca.

Gostaria de agradecer primeiramente à minha família. Meus pais Ailton e Disa, que sempre me apoiaram e me incentivaram nessa jornada, meus irmãos Diego e Fábio, aqueles com quem posso contar para tudo nessa vida, e aos meus avós Luiz, Maria de Lourdes, José Ramos e Valdice por todo o amor e carinho que recebi.

Em segundo lugar, agradeço a três amigos que têm sido meus pilares na faculdade, que estão sempre dispostos a me ouvir e me ajudar. Camila Moura, Vinícius Furtado e Patrícia Botelho, obrigado por serem exatamente

quem vocês são.

Agradeço aos meus amigos de morada, que me fizeram me sentir em casa em todos esses anos que aqui estive, em especial ao Rodrigo Marques, Hene Saud, Luiz Filipe e Francisco, com quem dividi o apartamento nesses últimos tempos.

Ainda no âmbito de morada, agradeço àquelas pessoas que me ofereceram abrigo quando precisei, fosse esse abrigo, físico, emocional ou alimentício (este último sendo extremamente importante). Aqui devo destacar a Gabriela Silva, Ingrid Muniz, Alessandra Cordeiro, Deise de Souza, Raquel Mary, Natane Cardoso, Josiana Antônia, Lyandra Maciel, Cecilia Nascimento, Karla Coelly, Hyrra Iglesias, Carla Oliveira, Beatriz Couto, Dani Oliveira, Maralice Oliveira, Caroline Garonce, Adriana Saraiva, Rubens Geraldo, Robson, Teily Teles, Josenice, Édila, Ricardo, Jéssica e Glaucilene.

Deixo um agradecimento especial a uma pessoa que dedicou um tempo considerável dentre suas prioridades para me acompanhar, principalmente durante meu segundo ano de mestrado, e a me distrair nesse tempo. Teresinha Gouvêa, espero poder lhe retribuir quando estiver no meu lugar e desejo muito sucesso em sua vida. Aproveito esse parágrafo para agradecer uma pessoa a quem não tive oportunidade de agradecer pessoalmente. Embora tenhamos convivido por pouco tempo, sou grato por ter me ajudado a não pirar quando me deparei com o Exame de Qualificação, a primeira prova em minha vida que fiquei realmente aterrorizado de ter que fazer.

Agradeço aos meus colegas de faculdade que compartilharam essa jornada comigo e com quem pude dividir ótimas experiências, em especial ao Leonardo Trindade, Erick Oliveira, Marina Barbosa, Natália Barreto, João Cilia, Camila Amorim e Pollyana Reis.

Não poderia deixar de agradecer a todos os professores que contribuíram para o meu crescimento, em especial ao Matthew Joseph Perlmutter, André Gimenez Bueno, Ana Cristina Vieira, Luiz Gustavo Perona e Carolina Silva Rezende. Ao professor Flaviano Bahia, deixo um agradecimento póstumo por ter me instigado a descobrir esse maravilhoso mundo dos números primos.

Deixo ainda um breve agradecimento a uma pessoa que surgiu recentemente em minha vida, mas que fez questão de tomar bastante espaço nela me apoiando e incentivando em diversos momentos. Agradeço por ter tido a oportunidade de te conhecer, Anne Melo.

Para finalizar, quero agradecer ao Sírius e à Celeste. Eu não seria eu mesmo sem eles.

Obrigado!

Resumo

Nesta dissertação, nosso foco foi desenvolver importantes teoremas sobre a densidade de conjuntos de ideais primos com o objetivo de estabelecer ferramentas que podem ser úteis para o estudo do conjunto dos primos gêmeos, o qual sempre fora o meu foco principal dentro da matemática. Embora este fosse o objetivo a longo prazo, não pretendemos tratar neste texto da aplicação dessas ferramentas no problema específico, deixando isso para um trabalho posterior.

No capítulo (1) estruturamos alguns conceitos gerais de Teoria dos Números, Álgebra e Análise que serão utilizados no decorrer do texto. Evitamos nos demorar neste capítulo tendo em vista que alguns (ou vários) destes conceitos podem já ser conhecidos do leitor.

No capítulo (2) desenvolvemos a teoria de números p-ádicos e a ideia de completamentos de corpos através de valorações. Embora fosse suficiente para as demonstrações aqui apresentadas que definíssemos diretamente o conceito de valorações, os números p-ádicos apresentam relevância histórica no desenvolvimento da teoria de valorações. Além disso, acreditamos que a beleza dos números p-ádicos já é justificativa suficiente para sua adição ao texto.

No capítulo (3) começamos a trabalhar com nosso primeiro teorema de densidade. Aqui construímos a noção de caracteres para grupos abelianos finitos, L-séries e finalmente o próprio Teorema das Progressões Aritméticas.

No capítulo (4) estudamos a função zeta de Dedekind para, posteriormente, desenvolvermos o Teorema da Densidade de Dirichlet.

No capítulo (5), o último capítulo, chegamos ao Teorema da Densidade de Tchebotarëv. Após sua demonstração, revisamos algumas aplicações importantes.

A maior parte destes resultados pode ser encontrada em [7].

Abstract

In this dissertation, our focus was to develop important theorems about the density of sets of prime ideals with the purpose of establishing tools that can be useful for the study of the set of the twin primes, which has always been my main focus in mathematics. Although it is a long-term goal, we do not intend to treat in this text the application of these tools in the specific problem, leaving it to a later work.
In the first chapter, we have structured some general concepts of Number Theory, Algebra and Analysis that will be used throughout the text. We avoid spending a lot of time on these issues, as some of these concepts may already be known to the reader.
In second chapter we worked on the theory of p-adic numbers as well as the idea of completion of fields through valuations. It is sufficient for the statements presented here that we directly define the concept of valuations, but the p-adic figures present historical relevance in the development of valuation theory, so that we believe that the beauty of the p-adic numbers is a sufficient justification for its addition to the text.
In the third chapter, we start working on our first density theorem. Here we constructed the notion of characters for finite abelian groups, L-series, and finally the Arithmetic Progression Theorem itself.
In the fourth chapter, we studied the Dedekind zeta function to later develops the Dirichlet's Density Theorem.
In the last chapter, we arrived at the Tchebotarëv's Density Theorem. After its demonstration, we reviewed some important applications of it.
Most of these results can be found in [7].

Sumário

Prefácio

Tudo começou em uma tarde de um sábado ensolarado. Em uma sala de aula diferenciada, mas à qual eu já estava acostumado, fui apresentado à beleza dos números primos e aos seus mistérios. A obsessão por uma regularidade em sua distribuição tomaria conta de meus pensamentos por semanas.
Em meio a toneladas de folhas preenchidas por crivos de primalidade eu tentava enxergar o problema de uma perspectiva por vezes mais panorâmica, por vezes mais minimalista. Não me importava a eficiência de meus métodos, apenas a diversão de mergulhar naquele mundo maravilhoso e procurar por suas respostas.
Foi então que esbarrei em um fato que me faria esquecer todo o resto. Na época eu as chamava de *simetrias*. Existiam certos números compostos que pareciam criar eixos de simetria na distribuição dos primos. Comecei a estudar à fundo essas simetrias, convicto de que elas me mostrariam a regularidade que tanto busquei.
Posteriormente, percebi que essas simetrias já deveriam ser conhecidas, e busquei me informar sobre elas. Descobri então que no centro da maior parte de minhas simetrias figurava um conceito batizado de *primos gêmeos*. Dois números primos cuja média aritmética era exatamente o centro de minha simetria. Mais uma vez, mudei o foco de meus estudos.
Porém, por mais que pesquisasse, minhas fontes eram limitadas e pouco consegui descobrir sobre os primos gêmeos. Existia portanto um caminho a trilhar. Assim, decidi ingressar em um curso de matemática e procurar contatos que pudessem me fornecer material de estudo sobre o assunto.
Durante os primeiros semestres avancei muito no problema, pelo menos em minha visão. Me divertia construindo um crivo particular, específico para a obtenção de pares de primos gêmeos. Mas conforme os semestres passavam me sobrava cada vez menos tempo para lidar com o problema.
Após um longo tempo afastado, tive a oportunidade de cursar a disciplina de Teoria dos Números e percebi que estava na hora de voltar à ativa. Dessa vez, porém, precisava de uma orientação para guiar meus passos. Foi então que procurei aquele que havia ministrado as aulas de Teoria dos Números,

André Gimenez, para me orientar.
Neste momento estava também próximo de meu ingresso no Mestrado, e dentre as possibilidades indicadas por ele, percebemos que a teoria de densidade de primos poderia ser a mais indicada para meu estudo. Ela se encaixava com a forma por mim utilizada para atacar o problema.
Desse modo, o trabalho que aqui apresento é apenas um caminho para um objetivo que ainda não alcancei. Enquanto estudava essas ferramentas, não tive tempo de aplicá-las ao problema real. Mas também tive a oportunidade de conhecer outros campos da Teoria de Números que igualmente me fascinaram.
Talvez eu nunca chegue à resolver esse problema que me acompanhou por tantos anos, e que permanece em aberto para toda a comunidade matemática. Talvez eu tenha crescido e esse nem seja mais o meu objetivo nessa vida. Mas independente de tudo isso, convido você leitor a conhecer um pouco mais disso que tanto me fascinou nestes últimos anos.
Portanto, recolha as velas, prepare os remos e boa sorte em sua leitura.

Capítulo 1

Considerações Iniciais

1.1 Extensões de Corpos

Sejam K e L corpos tais que $K \subseteq L$. Denotamos por L/K a extensão definida por esses corpos.

Definição 1.1. *Um* ***corpo numérico algébrico*** *(ou, simplesmente,* ***corpo numérico****) é uma extensão de corpo de grau finito do corpo dos números racionais $\mathbb{Q}$. Aqui a sua dimensão como espaço vetorial sobre $\mathbb{Q}$ é chamada simplesmente de grau.*

Definição 1.2. *Uma extensão algébrica L/K é dita* ***normal*** *se $\alpha \in L$ implica que todas as raízes do polinômio minimal de α sobre K pertencem a L.*

Definição 1.3. *Dizemos que uma extensão algébrica L/K é* ***separável*** *se para todo $\alpha \in L$, o polinômio minimal de α sobre K é separável (i.e., sua derivada formal é não nula).*

Definição 1.4. *Uma extensão algébrica L/K é dita uma* ***extensão Galoisiana*** *se é uma extensão normal e separável.*

Definição 1.5. *Seja L/K uma extensão de corpos. Um automorfismo de L/K é definido como isomorfismo $\alpha : L \to L$ tal que $\alpha(x) = x$ para cada $x \in K$. O conjunto de todos os automorfismos de L/K forma um grupo denotado por* $\mathrm{Aut}(L/K)$.

Definição 1.6. *Se L/K é uma extensão Galoisiana, então* $\mathrm{Aut}(L/K)$ *é chamado de* ***Grupo de Galois de*** *L/K, e o denotaremos por* $\mathrm{Gal}(L/K)$.

Definição 1.7. *O* ***traço*** *e a* ***norma*** *de um elemento $x \in L$ em L/K são definidos como sendo o traço e o determinante, respectivamente, do endomorfismo*

$$T_x : L \to L, \quad T_x(\alpha) = x\alpha,$$

do K-espaço vetorial L:

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x), \quad N_{L/K}(x) = \det(T_x).$$

1.2 Anéis e Corpos

Definição 1.8. *Seja $A \subseteq B$ uma extensão de anéis comutativos. Um elemento $b \in B$ é dito um* ***inteiro*** *(ou* ***integral****) sobre A se satisfaz uma equação mônica*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad n \geq 1,$$

com coeficientes $a_i \in A$. O anel B é chamado ***inteiro*** *(ou* ***integral****) sobre A se todos os elementos $b \in B$ são inteiros sobre A.*

Definição 1.9. *Dado um corpo numérico K, o* ***anel de inteiros*** *de K é o anel de todos os elementos inteiros sobre $\mathbb{Z}$ contidos em K. Denotaremos esse anel por $\mathcal{O}_K$.*

Definição 1.10. *Seja R um anel comutativo de característica prima p. O Endomorfismo de Frobenius é definido por*

$$F(r) = r^p$$

para todo $r \in R$.

À respeito da multiplicação de R, temos

$$F(rs) = (rs)^p = r^p s^p = F(r)F(s).$$

Por outro lado, devido à característica de R ser p, temos também que

$$F(r+s) = (r+s)^p = r^p + s^p = F(r) + F(s).$$

Isto mostra que F é um homomorfismo de anéis.

1.3 Módulos e Ideais

Definição 1.11. *Dado um anel $(R, +, \cdot)$, seja $(R, +)$ seu grupo aditivo. Um subconjunto $\mathfrak{a}$ é chamado* ***ideal*** *de R se satisfaz*

1. *$(\mathfrak{a}, +)$ é um subgrupo de $(R, +)$;*
2. *$\forall x \in \mathfrak{a}, \forall r \in R$: $x \cdot r, r \cdot x \in \mathfrak{a}$.*

Podemos definir a soma e o produto de dois ideais como segue.

Definição 1.12. *Sejam $\mathfrak{a}$ e $\mathfrak{b}$ ideais de um anel R. Definimos*

$$\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

e

$$\mathfrak{a}\mathfrak{b} := \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a},\, b_i \in \mathfrak{b},\, n \in \mathbb{N} \right\}$$

Definição 1.13. *Um* ***domínio de integridade*** *é um anel comutativo não nulo em que o produto de dois elementos não nulos é um elemento não nulo.*

Definição 1.14. *Seja $A \subseteq B$ uma extensão de anéis comutativos. Seja $A' = \{x \in B \mid x \text{ é inteiro sobre } A\}$. Dizemos que A' é o* ***fecho inteiro*** *(ou* ***fecho integral****) de A em B.*

Definição 1.15. *Um* ***domínio integralmente fechado*** *é um domínio de integridade cujo fecho inteiro no seu corpo de frações é ele mesmo.*

Definição 1.16. *Um* ***ideal principal*** *é um ideal que pode ser gerado por um único elemento. Seja $\mathfrak{a}$ um ideal principal gerado pelo elemento a. Escrevemos então $(a) := \mathfrak{a}$.*

Definição 1.17. *Um* ***domínio de ideais principais*** *é um domínio de integridade em que todo ideal é principal.*

Definição 1.18. *Um ideal próprio $\mathfrak{p}$ é chamado um* ***ideal primo*** *se para quaisquer $a, b \in R$, se $(a)(b) \subseteq \mathfrak{p}$, então $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.*

Definição 1.19. *Um ideal próprio $\mathfrak{p}$ é chamado um* ***ideal completamente primo*** *se para quaisquer $a, b \in R$, se $ab \in \mathfrak{p}$, então $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.*

Proposição 1.20. *Todo ideal completamente primo é um ideal primo.*

A recíproca não é sempre verdadeira.

Exemplo 1.1. *O ideal* 0 *no anel das matrizes* $n \times n$ *sobre um corpo* K *é um ideal primo, mas não é um ideal completamente primo.*

Proposição 1.21. *Seja* R *um anel comutativo. Então todo ideal primo de* R *é um ideal completamente primo.*

Definição 1.22. *Um* ***anel comutativo Noetheriano*** *(ou simplesmente* ***anel Noetheriano****) é um anel comutativo que satisfaz a condição de cadeias ascendentes para ideais, isto é, dada qualquer cadeia de ideais*

$$\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_{k-1} \subseteq \mathfrak{a}_k \subseteq \mathfrak{a}_{k+1} \subseteq \cdots$$

existe $n \in \mathbb{N}$ *tal que*

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots .$$

Observação 1. *Embora utilizemos neste texto o termo anel Noetheriano para anéis comutativos Noetherianos, podemos definir um anel Noetheriano não-comutativo de forma semelhante, à partir das cadeias ascendentes de ideais à direita e ideais à esquerda, os quais não foram definidos aqui.*

Definição 1.23. *Um* ***domínio de Dedekind*** *é um domínio integralmente fechado, Noetheriano em que cada ideal primo não nulo é um ideal maximal.*

Teorema 1.24. *Seja* K *um corpo numérico e* $\mathcal{O}_K$ *o anel de inteiros de* K*.* $\mathcal{O}_K$ *é um domínio de Dedekind.*

Demonstração. [7] Teorema (3.1), capítulo I. □

Durante o resto do capítulo, $\mathcal{O}$ será um domínio de Dedekind.

Lema 1.25. *Para cada ideal* $\mathfrak{a} \neq 0$ *de* $\mathcal{O}$ *existem ideais primos não nulos* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ *tais que*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Demonstração. Suponha que o conjunto $\mathfrak{M}$ dos ideais que não satisfazem essa condição é não vazio. Como $\mathcal{O}$ é Noetheriano, toda cadeia ascendente de ideais se torna estacionária. Desse modo $\mathfrak{M}$ é indutivamente ordenada com respeito a inclusão e portanto admite um elemento maximal $\mathfrak{a}$. Este não pode ser um ideal primo, então existem elementos $b_1, b_2 \in \mathcal{O}$ tais que $b_1 b_2 \in \mathfrak{a}$, mas $b_1, b_2 \notin \mathfrak{a}$. Tome $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$, $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$. Então $\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$, e $\mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a}$. Pela maximalidade de $\mathfrak{a}$, tanto $\mathfrak{a}_1$ quanto $\mathfrak{a}_2$ contém um produto de ideais primos, e o produto desses produtos está contido em $\mathfrak{a}$, o que é uma contradição. □

Lema 1.26. *Seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}$, K o corpo de frações de $\mathcal{O}$ e defina*

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

Temos então que $\mathfrak{a}\mathfrak{p}^{-1} := \{\sum_i a_i x_i \mid a_i \in \mathfrak{a},\, x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a}$, para cada ideal $\mathfrak{a} \neq 0$.

Demonstração. Seja $a \in \mathfrak{p}$, $a \neq 0$, e $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$, com r menor possível. Então um dos $\mathfrak{p}_i$, digamos $\mathfrak{p}_1$, está contido em $\mathfrak{p}$, e então $\mathfrak{p}_1 = \mathfrak{p}$ pois $\mathfrak{p}_1$ é um ideal maximal. (De fato, se nenhum dos $\mathfrak{p}_i$ estiver contido em $\mathfrak{p}$, então para cada i existirá um $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ tal que $a_1 \cdots a_r \in \mathfrak{p}$. Mas $\mathfrak{p}$ é primo.) Como $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$, existe $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tal que $b \notin a\mathcal{O}$, isto é, $a^{-1}b \notin \mathcal{O}$. Por outro lado temos que $b\mathfrak{p} \subseteq (a)$, isto é, $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$, e então $a^{-1}b \in \mathfrak{p}^{-1}$. Segue então que $\mathfrak{p}^{-1} \neq \mathcal{O}$.
Agora seja $\mathfrak{a} \neq 0$ um ideal de $\mathcal{O}$ e $\alpha_1, \ldots, \alpha_n$ um sistema de geradores. Vamos assumir que $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Então para cada $x \in \mathfrak{p}^{-1}$,

$$x\alpha_i = \sum_j a_{ij}\alpha_j, \quad a_{ij} \in \mathcal{O}.$$

Escrevendo A para a matriz $(x\delta_{ij} - a_{ij})$ nós obtemos que $A(\alpha_1, \ldots, \alpha_n)^t = 0$. Podemos mostrar que o determinante $d = \det(A)$ satisfaz $d\alpha_1 = \cdots = d\alpha_n = 0$ e portanto $d = 0$. Segue então que x é inteiro sobre $\mathcal{O}$, sendo um zero do polinômio mônico $f(X) = \det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$. Portanto $x \in \mathcal{O}$. Isso implica que $\mathfrak{p}^{-1} = \mathcal{O}$, uma contradição. □

Teorema 1.27. *Cada 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 $\mathcal{O}$ que é única à menos da ordem dos fatores.

Demonstração. I. **Existência da fatoração em ideais primos.** Seja $\mathfrak{M}$ o conjunto de todos os ideais diferentes de (0) e (1) que não admitem uma decomposição em ideais primos. Se $\mathfrak{M}$ é não vazio, então nós argumentamos como no lema (1.25) e obtemos que existe um elemento maximal $\mathfrak{a}$ em $\mathfrak{M}$. Ele está contido em um ideal maximal $\mathfrak{p}$, e a inclusão $\mathcal{O} \subseteq \mathfrak{p}^{-1}$ nos dá

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

Pelo lema (1.26), temos $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ e $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. Como $\mathfrak{p}$ é um ideal maximal, segue que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Em vista da maximalidade de $\mathfrak{a}$ em $\mathfrak{M}$ e como $\mathfrak{a} \neq \mathfrak{p}$, isto é, $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$, o ideal $\mathfrak{a}\mathfrak{p}^{-1}$ admite uma decomposição em ideais primos $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, e então $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$, uma contradição.

II. **Unicidade da fatoração em ideais primos.** Para um ideal primo $\mathfrak{p}$ temos: $\mathfrak{ab} \subseteq \mathfrak{p} \implies \mathfrak{a} \subseteq \mathfrak{p}$ ou $\mathfrak{b} \subseteq \mathfrak{p}$, isto é, $\mathfrak{p}|\mathfrak{ab} \implies \mathfrak{p}|\mathfrak{a}$ ou $\mathfrak{p}|\mathfrak{b}$. Sejam

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s$$

duas fatorações em ideais primos de $\mathfrak{a}$. Então $\mathfrak{p}_1$ divide um fator $\mathfrak{q}_i$, digamos $\mathfrak{q}_1$, e sendo maximal temos $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplicamos por $\mathfrak{p}^{-1}$ e obtemos, em vista de que $\mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$, que

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

Continuando indutivamente, vemos que $r = s$ e, possivelmente depois de uma renumeração, $\mathfrak{p}_i = \mathfrak{q}_i$ para todo $i = 1, \ldots, r$.

□

Agrupando as ocorrências do mesmo ideal primo na fatoração em ideais primos de um ideal $\mathfrak{a} \neq 0$ de $\mathcal{O}$ ganhamos uma representação

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1}\cdots\mathfrak{p}_r^{\nu_r}$$

Para um produto $\mathfrak{a} = \mathfrak{a}_1\cdots\mathfrak{a}_n$ de ideais relativamente primos $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, temos um análogo do bem conhecido "Teorema Chinês dos Restos" da teoria dos números elementar. Podemos formular esse resultado para um anel arbitrário considerando que

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

De fato, como $\mathfrak{a}_i|\mathfrak{a}$, $i = 1, \ldots, n$, nós temos por um lado que $\mathfrak{a} \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$, e para $a \in \bigcap_i \mathfrak{a}_i$ nós obtemos que $\mathfrak{a}_i|(a)$, e sendo os fatores relativamente primos, obtemos que $\mathfrak{a} = \mathfrak{a}_1\cdots\mathfrak{a}_n|(a)$, isto é, $a \in \mathfrak{a}$.

Teorema 1.28. ***Teorema Chinês dos Restos.*** *Sejam $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideais em um anel R tais que $\mathfrak{a}_i + \mathfrak{a}_j = R$ para $i \neq j$. Então, se $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i$, temos*

$$R/\mathfrak{a} \cong \bigoplus_{i=1}^{n} R/\mathfrak{a}_i.$$

Demonstração. O homomorfismo canônico

$$R \longrightarrow \bigoplus_{i=1}^{n} R/\mathfrak{a}_i, \quad a \longmapsto \bigoplus_{i=1}^{n} a \bmod \mathfrak{a}_i,$$

tem núcleo $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$. Portanto é suficiente mostrar que ele é sobrejetivo. Para isso, seja $x_i \bmod \mathfrak{a}_i \in R/\mathfrak{a}_i$, $i = 1, \ldots, n$ dados. Se $n = 2$, podemos

escrever $1 = a_1 + a_2$, $a_i \in \mathfrak{a}_i$, e colocando $x = x_2a_1 + x_1a_2$ nós obtemos que $x \equiv x_i \bmod \mathfrak{a}_i$, $i = 1, 2$.
Se $n > 2$ nós podemos encontrar como antes um elemento $y_1 \in R$ tal que

$$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \bigcap_{i=2}^{n} \mathfrak{a}_i,$$

e, pelo mesmo processo, elementos $y_2, \ldots, y_n$ tais que

$$y_i \equiv 1 \bmod \mathfrak{a}_i, \quad y_i \equiv 0 \bmod \mathfrak{a}_j \quad \text{para } i \neq j.$$

Colocando $x = x_1y_1 + \cdots + x_ny_n$ nós obtemos que $x \equiv x_i \bmod \mathfrak{a}_i$, $i = 1, \ldots, n$.
Isto prova a sobrejetividade. □

Seja $\mathcal{O}_K$ o anel de inteiros de um corpo algébrico K e $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$. Para uma extensão L/K nós podemos considerar também $\mathcal{O}_L$ o anel de inteiros de L e o ideal $\mathfrak{p} \cdot \mathcal{O}_L$ de $\mathcal{O}_L$. Este pode ou não ser primo, mas assumindo que $[L : K]$ é finito temos a seguinte fatoração de ideais primos

$$\mathfrak{p} \cdot \mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k},$$

onde os $\mathfrak{p}_i$ são ideais primos distintos de $\mathcal{O}_L$.

Definição 1.29. *É dito que* $\mathfrak{p}$ ***se ramifica*** *em L se $e_i > 1$ para algum i. Se para todo i temos $e_i = 1$, dizemos que* $\mathfrak{p}$ ***não se ramifica***.

Exemplo 1.2. *Considere o conjunto dos inteiros Gaussianos*

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

onde $i^2 = -1$. Como os inteiros Gaussianos são fechados para a adição e a multiplicação, eles formam um anel comutativo, que é um subanel do corpo dos números complexos $\mathbb{C}$.
As unidades do anel de inteiros Gaussianos são 1, -1, i e $-i$ (segue imediatamente utilizando a norma da definição (1.7)).
Os elementos primos de $\mathbb{Z}[i]$ são conhecidos como ***primos Gaussianos***.
Dado um número primo $p \in \mathbb{Z}$, gostaríamos de analisar o que acontece com $p \in \mathbb{Z}[i]$. Temos três casos possíveis:

1. *Se $p \equiv 3 \bmod 4$, então ele é um primo Gaussiano. Nesse caso dizemos que p é* ***inerte*** *nos inteiros Gaussianos, e p não se ramifica.*

2. *Se $p \equiv 1 \bmod 4$, então ele é um produto de um primo Gaussiano pelo seu conjugado, os quais não são associados (nenhum dos dois pode ser escrito como o produto do outro por uma unidade). Dizemos que p é um* ***primo decomponível*** *nos inteiros Gaussianos, e p não se ramifica.*

3. *Se $p = 2$, temos $2 = (1+i)(1-i) = i(1-i)^2$. Dizemos nesse caso que p se ramifica.*

Observação 2 ([7], capítulo 1)**.** *Todo ideal primo em $\mathbb{Z}[i]$ contém um primo usual de $\mathbb{Z}$, e acima de cada primo de $\mathbb{Z}$ há ao menos um primo gaussiano. Dessa forma, para analisar os primos de $\mathbb{Z}[i]$ basta olhar como se decompõem os primos usuais nos gaussianos.*

Definição 1.30. *Um **anel de valoração discreta** é um domínio de ideais principais $\mathcal{O}$ com um único ideal maximal $\mathfrak{p} \neq 0$.*

Exemplo 1.3. *O anel*

$$\mathbb{Z}_{(p)} := \left\{ \frac{g}{h} \mid g, h \in \mathbb{Z}, p \nmid h \right\}$$

é um anel de valoração discreta com o único ideal maximal (p)

Exemplo 1.4 ([1], teorema 9.3)**.** *A localização de um anel de inteiros algébricos em qualquer primo não nulo é sempre um anel de valoração discreta.*

O ideal maximal é da forma $\mathfrak{p} = (\pi) = \pi\mathcal{O}$, para algum elemento primo π.

Definição 1.31. *Seja R um anel comutativo e 1_R sua identidade multiplicativa. Um R-módulo M consiste de um grupo abeliano $(M, +)$ e uma operação $\cdot : R \times M \to M$ tal que para todo $r, s \in R$ e $x, y \in M$, temos:*

1. $r \cdot (x + y) = r \cdot x + r \cdot y$;
2. $(r + s) \cdot x = r \cdot x + s \cdot x$;
3. $(rs) \cdot x = r \cdot (s \cdot x)$;
4. $1_R \cdot x = x$.

Definição 1.32. *Seja $\mathcal{O}$ um domínio de Dedekind e K seu corpo de frações. Um **ideal fracionário** de K é um $\mathcal{O}$-submódulo finitamente gerado $\mathfrak{a}$ de K.*

Por exemplo, um elemento $a \in K^*$ define o "ideal principal" fracionário $(a) = a\mathcal{O}$. Obviamente, como $\mathcal{O}$ é Noetheriano, um $\mathcal{O}$-submódulo $\mathfrak{a} \neq 0$ de K é um ideal fracionário se e somente se existe $c \in \mathcal{O}$, $c \neq 0$, tal que $c\mathfrak{a} \subseteq \mathcal{O}$ é um ideal do anel $\mathcal{O}$. Ideais fracionários são multiplicados da mesma forma que ideais em $\mathcal{O}$. Por distinção podemos chamar os ideais anteriormente definidos (definição (1.11)) de **ideais inteiros** de K.

Proposição 1.33. *Os ideais fracionários de um domínio de Dedekind formam um grupo abeliano, o* ***grupo ideal*** J_K *de* K*. O elemento identidade 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. Temos claramente associatividade, comutatividade e $\mathfrak{a}(1) = \mathfrak{a}$. Para um ideal primo $\mathfrak{p}$, o lema (1.26) diz que $\mathfrak{p} \subsetneqq \mathfrak{p}\mathfrak{p}^{-1}$ e, portanto, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ pois $\mathfrak{p}$ é maximal. Consequentemente, se $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ é um ideal inteiro, então $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$ é um inverso. $\mathfrak{b}\mathfrak{a} = \mathcal{O}$ implica que $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Por outro lado, se $x\mathfrak{a} \subseteq \mathcal{O}$, então $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, então $x \in \mathfrak{b}$ pois $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Portanto temos $\mathfrak{b} = \mathfrak{a}^{-1}$.
Finalmente, se $\mathfrak{a}$ é um ideal fracionário arbitrário e $c \in \mathcal{O}$, $c \neq 0$, é tal que $c\mathfrak{a} \subseteq \mathcal{O}$, então $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ é o inverso de $c\mathfrak{a}$, então $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

Corolário 1.33.1. *Todo ideal fracionário* $\mathfrak{a}$ *admite uma única representação como um produto*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$$

com $\nu_\mathfrak{p} \in \mathbb{Z}$ *e* $\nu_\mathfrak{p} = 0$ *para quase todo* $\mathfrak{p}$ *(ou seja, pode ser escrito como um produto finito de ideais primos). Em outras palavras,* J_K *é o grupo livre abeliano no conjunto de ideais primos não nulos* $\mathfrak{p}$ *de* $\mathcal{O}$*.*

Demonstração. Cada ideal fracionário $\mathfrak{a}$ é um quociente $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ de dois ideais inteiros $\mathfrak{b}$ e $\mathfrak{c}$, que pelo teorema (1.27) tem uma decomposição prima. Assim sendo $\mathfrak{a}$ tem uma decomposição prima do tipo apresentada no corolário. Pelo teorema (1.27), ela é única se $\mathfrak{a}$ é inteiro, e portanto também será em geral. □

Definição 1.34. *Os ideais principais fracionários* $(a) = a\mathcal{O}$*,* $a \in K^*$*, formam um subgrupo do grupo de ideais* J_K*, que denotaremos por* P_K*. O grupo quociente*

$$Cl_K = J_K/P_K$$

é chamado de ***grupo de classes ideal****, ou* ***grupo de classes****, de* K*.*

Definição 1.35. *Dado um ideal* $\mathfrak{a} \neq 0$ *do anel* $\mathcal{O}_K$ *nós denotaremos por* ***norma absoluta*** *o índice finito*

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

Proposição 1.36. *Se* $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ *é a fatoração prima de um ideal* $\mathfrak{a} \neq 0$*, então temos*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}.$$

Demonstração. Pelo teorema chinês dos restos (1.28), temos

$$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r}.$$

Nós podemos então novamente nos concentrar no caso em que $\mathfrak{a}$ é uma potência prima $\mathfrak{p}^\nu$.
Na cadeia

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^\nu$$

temos que $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ devido a fatoração prima ser única, e cada quociente $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ é um $\mathcal{O}_K/\mathfrak{p}$-espaço vetorial de dimensão 1. De fato, se $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ e $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$, então $\mathfrak{p}^i \supseteq \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}$ e consequentemente $\mathfrak{p}^i = \mathfrak{b}$, pois do contrário $\mathfrak{b}' = \mathfrak{b}\mathfrak{p}^{-i}$ seria um divisor próprio de $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$. Assim $\overline{a} \equiv a \bmod \mathfrak{p}^{i+1}$ é uma base do $\mathcal{O}_K/\mathfrak{p}$-espaço vetorial $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Então nós temos $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{p}$ e portanto

$$\mathfrak{N}(\mathfrak{p}^\nu) = [\mathcal{O}_K : \mathfrak{p}^\nu] = [\mathcal{O}_K : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu] = \mathfrak{N}(\mathfrak{p})^\nu.$$

□

A proposição imediatamente implica a multiplicatividade

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

da norma absoluta. Esta pode ser estendida para um homomorfismo

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

definido em todos os ideais fracionários $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$.

Teorema 1.37. *O grupo de classes ideal $Cl_K = J_K/P_K$ é finito. Sua ordem*

$$h_K = [J_K : P_K]$$

é chamada de ***número de classe*** *de K.*

Demonstração. [7], Teorema 6.3. □

Dado um ideal $\mathfrak{m}$, seja $J_K^\mathfrak{m}$ o grupo de todos os ideais fracionários relativamente primos com $\mathfrak{m}$, e seja $P_K^\mathfrak{m}$ o grupo de todos os ideais principais $(a) \in P_K$ tais que

$$a \equiv 1 \bmod \mathfrak{m} \quad \text{e} \quad a \text{ é totalmente positivo.}$$

A última condição significa que, para toda imersão real $K \to \mathbb{R}$, a acaba por ser positivo. A congruência $a \equiv 1 \bmod \mathfrak{m}$ significa que a é o quociente b/c de dois inteiros relativamente primos a $\mathfrak{m}$ tais que $b \equiv c \bmod \mathfrak{m}$.

Definição 1.38. *Definimos*

$$Cl_K^\mathfrak{m} = J_K^\mathfrak{m}/P_K^\mathfrak{m}.$$

1.4 Séries e Funções

Definição 1.39. *Dados um conjunto S e funções $f_n : S \to \mathbb{C}$, a série*

$$\sum_{n=0}^{\infty} f_n(x)$$

é chamada ***normalmente convergente*** *se a série das normas uniformes (norma do supremo) dos termos da série converge. Isto é,*

$$\sum_{n=0}^{\infty} ||f_n|| := \sum_{n=0}^{\infty} \sup_S |f_n(x)| < \infty.$$

Definição 1.40. *Neste trabalho a denotaremos o* ***logaritmo neperiano*** *por* $\ln x$.

Capítulo 2

Números p-ádicos

2.1 Motivação e Definição

Os números p-ádicos foram primeiramente descritos por **Kurt Hensel** (1861 - 1941) em 1897 [4], embora, em retrospecto, alguns dos trabalhos anteriores de **Ernst Kummer** (1810 - 1893) possam ser interpretados como uma utilização implícita dos números p-ádicos [2].
A forma de começar a pensar nos números p-ádicos de Hensel baseava-se em se perguntar o que aconteceria se víssemos os números $f \in \mathbb{Z}$, em analogia aos polinômios $f(z) \in \mathbb{C}[z]$, como funções no espaço X dos números primos em $\mathbb{Z}$, associando a eles seus "valores" no ponto $p \in X$, isto é, o elemento

$$f(p) := f \bmod p$$

no corpo de resíduo de classe $\kappa(p) = \mathbb{Z}/p\mathbb{Z}$.
A partir desse ponto de vista, podemos aprofundar ainda mais a questão. Poderíamos também tentar definir as derivadas superiores de f? No caso dos polinômios $f(z) \in \mathbb{C}[z]$, as derivadas superiores no ponto $z = a$ são dadas pelos coeficientes da expansão

$$f(z) = a_0 + a_1(z-a) + \cdots + a_n(z-a)^n,$$

e mais geralmente, para funções racionais $f(z) = \frac{g(z)}{h(z)} \in \mathbb{C}(z)$, com $g, h \in \mathbb{C}[z]$, eles são definidos pela expansão de Taylor

$$f(z) = \sum_{v=0}^{\infty} a_v(z-a)^v,$$

desde que não haja um polo em $z = a$, isto é, enquanto $(z-a) \nmid h(z)$.
De fato, essa expansão também pode ser escrita relativa a um número primo

p em $\mathbb{Z}$ para qualquer racional $f \in \mathbb{Q}$ que pertença ao anel local

$$\mathbb{Z}_{(p)} = \left\{ \frac{g}{h} \mid g, h \in \mathbb{Z}, p \nmid h \right\}.$$

Assim, começamos a nos guiar à noção de números p-ádicos. Primeiro, todo inteiro positivo $f \in \mathbb{N}$ admite uma expansão p-ádica

$$f = a_0 + a_1 p + \cdots + a_n p^n,$$

com coeficientes a_i em $\{0, 1, \ldots p-1\}$, isto é, em um sistema fixado de representantes do "corpo de valores" $\kappa(p) = \mathbb{F}_p$. Esta representação é claramente única. Pode ser computada explicitamente dividindo-se sucessivamente por p, formando o seguinte sistema de equações:

$$\begin{aligned} f &= a_0 + p f_1, \\ f_1 &= a_1 + p f_2, \\ &\vdots \\ f_{n-1} &= a_{n-1} + p f_n, \\ f_n &= a_n. \end{aligned}$$

Aqui $a_i \in \{0, 1, \ldots p-1\}$ denota o representante de $f_i \bmod p \in \mathbb{Z}/p\mathbb{Z}$. Em casos concretos, podemos escrever o número f simplesmente como a sequência dos dígitos $a_0, a_1 a_2 \ldots a_n$, por exemplo

$$\begin{aligned} 839 &= 1,110001011 && (2\text{-ádico}) \\ 839 &= 2,001101 && (3\text{-ádico}) \\ 839 &= 4,2311 && (5\text{-ádico}) \end{aligned}$$

Logo que tentamos escrever expansões p-ádicas também para inteiros negativos, bem como para frações, somos forçados a permitir o uso de séries infinitas

$$\sum_{v=0}^{\infty} a_v p^v = a_0 + a_1 p + a_2 p^2 + \cdots.$$

Exemplo 2.1. *Vamos verificar a expansão 2-ádica de -1.*

$$-1 = 1 + 2(-1)$$

Notamos aqui que ao realizar as divisões sucessivas, encontraremos $f_i = -1$, para todo i. Desse modo teremos

$$-1 = \sum_{v=0}^{\infty} 2^v \quad \textit{(2-ádico)}.$$

Vamos entender essa notação primeiro no sentido puramente formal, isto é, $\sum_{v=0}^{\infty} a_v p^v$ simplesmente representa a sequência de somas parciais

$$s_n = \sum_{v=0}^{n-1} a_v p^v, \qquad\qquad n = 1, 2, \ldots$$

A expansão p-ádica de um número arbitrário $f \in \mathbb{Z}_{(p)}$ resulta da seguinte proposição sobre as classes de resíduos em $\mathbb{Z}/p^n\mathbb{Z}$.

Proposição 2.1. *A classe de resíduos* $a \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ *pode ser unicamente representada na forma*

$$a \equiv a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \bmod p^n$$

onde $0 \leq a_i < p$ *para* $i = 0, \cdots, n-1$.

Demonstração: (Indução sobre n.) A proposição é clara para $n = 1$. Assumamos que a afirmação está demonstrada para $n - 1$. Teremos então a representação única

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-2} p^{n-2} + g p^{n-1},$$

para algum inteiro g. Se $g \equiv a_{n-1} \bmod p$ tal que $0 \leq a_{n-1} < p$, então a_{n-1} é unicamente determinado por a, e a congruência da proposição segue. □

Definição 2.2. *Dado um número primo* p *fixado, dizemos que um* ***inteiro*** p***-ádico*** *é uma série infinita formal*

$$a_0 + a_1 p + a_2 p^2 + \cdots,$$

onde $0 \leq a_i < p$, *para todo* $i = 0, 1, 2, \ldots$ *O conjunto de todos os inteiros* p*-ádicos é denotado por* $\mathbb{Z}_p$.

Todo inteiro f e, mais geralmente, todo número racional $f \in \mathbb{Z}_{(p)}$ tal que seu denominador não é divisível por p, define uma sequência de classes de resíduos

$$\overline{s}_n = f \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n = 1, 2, \ldots,$$

para a qual nós encontramos, pela proposição anterior,

$$\begin{aligned}
&\overline{s}_1 = a_0 \bmod p, \\
&\overline{s}_2 = a_0 + a_1 p \bmod p^2, \\
&\overline{s}_3 = a_0 + a_1 p + a_2 p^2 \bmod p^3, \quad \text{etc.},
\end{aligned}$$

com coeficientes unicamente determinados $a_0, a_1, a_2, \cdots \in \{0, 1, \ldots, p-1\}$ que mantêm seu significado de uma linha para a outra. A sequencia de números

$$s_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}, \quad n = 1, 2, \ldots,$$

define um inteiro p-ádico

$$\sum_{v=0}^{\infty} a_v p^v \in \mathbb{Z}_p,$$

que chamaremos de **expansão p-ádica** de f.

Em analogia às séries de Laurent $f(z) = \sum_{v=-m}^{\infty} a_v (z-a)^v$, nós agora podemos estender o domínio dos inteiros p-ádicos nesta série formal

$$\sum_{v=-m}^{\infty} a_v p^v = a_{-m} p^{-m} + \cdots + a_{-1} p^{-1} + a_0 + a_1 p + \cdots,$$

onde $m \in \mathbb{Z}$ e $0 \leq a_v < p$. Chamaremos tais séries simplesmente de **números p-ádicos** e escreveremos $\mathbb{Q}_p$ para o conjunto de todos os números p-ádicos. Se $f \in \mathbb{Q}$ é um número racional, podemos escrever

$$f = \frac{g}{h} p^{-m} \quad \text{onde } g, h \in \mathbb{Z}, \quad (gh, p) = 1,$$

e se

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

é a expansão p-ádica de $\frac{g}{h}$, então nós relacionamos a f o número p-ádico

$$a_0 p^{-m} + a_1 p^{-m+1} + \cdots + a_m + a_{m+1} p + \cdots \in \mathbb{Q}_p$$

como sua expansão p-ádica.
Desse modo nós obtemos um mapa canônico

$$\mathbb{Q} \longrightarrow \mathbb{Q}_p,$$

que leva $\mathbb{Z}$ em $\mathbb{Z}_p$ e é injetivo. Se $a, b \in \mathbb{Z}$ têm a mesma expansão p-ádica, então $a - b$ é divisível por p^n para qualquer n, e portanto $a = b$. Com isso identificamos $\mathbb{Q}$ com sua imagem em $\mathbb{Q}_p$, então podemos escrever $\mathbb{Q} \subseteq \mathbb{Q}_p$ e $\mathbb{Z} \subseteq \mathbb{Z}_p$. Assim, para todo número racional $f \in \mathbb{Q}$, nós obtemos uma identidade

$$f = \sum_{v=-m}^{\infty} a_v p^v.$$

Exemplo 2.2. *Vamos analisar a expansão* 3*-ádica de* $\frac{2}{15}$*. Podemos escrever*

$$\frac{2}{15} = \frac{2}{5} \cdot 3^{-1}$$

Portanto precisamos achar a expansão 3*-ádica de* $\frac{2}{5}$*.*

$$\begin{aligned}
\frac{2}{5} &= 3 \cdot \left(-\frac{1}{5}\right) + 1 \\
-\frac{1}{5} &= 3 \cdot \left(-\frac{2}{5}\right) + 1 \\
-\frac{2}{5} &= 3 \cdot \left(-\frac{4}{5}\right) + 2 \\
-\frac{4}{5} &= 3 \cdot \left(-\frac{3}{5}\right) + 1 \\
-\frac{3}{5} &= 3 \cdot \left(-\frac{1}{5}\right) + 0
\end{aligned}$$

Assim, a expansão 3*-ádica de* $\frac{2}{5}$ *será*

$$1 + 1 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3 + 0 \cdot 3^4 + 1 \cdot 3^5 + 2 \cdot 3^6 + \cdots$$

E portanto a expansão 3*-ádica de* $\frac{2}{15}$ *será*

$$1 \cdot 3^{-1} + 1 + 2 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4 + 2 \cdot 3^5 + \cdots$$

Podemos definir uma adição e multiplicação dos números p-ádicos que torna $\mathbb{Z}_p$ um anel e $\mathbb{Q}_p$ um corpo de frações. No entanto, a abordagem direta dessas definições resulta em algumas complicações. Elas desaparecem uma vez que nós usamos outra representação dos números p-ádicos $f = \sum_{v=0}^{\infty} a_v p^v$, os vendo não como sequências de somas de inteiros

$$s_n = \sum_{v=0}^{n-1} a_v p^v \in \mathbb{Z},$$

mas como sequências de classes de resíduos

$$\overline{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

Os termos dessa sequência pertencem a diferentes anéis $\mathbb{Z}/p^n\mathbb{Z}$, mas eles estão relacionados pelas projeções canônicas

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\lambda_3} \cdots$$

e nós encontramos

$$\lambda_n(\overline{s}_{n+1}) = \overline{s}_n.$$

No produto direto

$$\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n\in\mathbb{N}} \mid x_n \in \mathbb{Z}/p^n\mathbb{Z}\},$$

nós agora consideramos o conjunto de todos os elementos $(x_n)_{n\in\mathbb{N}}$ com a propriedade

$$\lambda_n(x_{n+1}) = x_n \quad \forall n \in \mathbb{N}.$$

Este conjunto é chamado de **limite projetivo** dos anéis $\mathbb{Z}/p^n\mathbb{Z}$ e é denotado por $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. Em outras palavras, nós temos

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid \lambda_n(x_{n+1}) = x_n,\ n = 1, 2, \cdots \right\}.$$

A representação modificada dos números p-ádicos apresentada acima segue da seguinte proposição.

Proposição 2.3. *Associando a cada inteiro p-ádico*

$$f = \sum_{v=0}^{\infty} a_v p^v$$

a sequência $(\overline{s}_n)_{n\in\mathbb{N}}$ das classes de resíduos

$$\overline{s}_n = \sum_{v=0}^{n-1} a_v p^v \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z},$$

produzimos uma bijeção

$$\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

A demonstração é uma consequência direta da proposição (2.1). O limite projetivo $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ oferece a vantagem de ser claramente um anel. De

fato, ele é um subanel do produto direto $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ onde adição e multiplicação são definidos componente a componente. Nós identificamos $\mathbb{Z}_p$ com $\varprojlim \ \mathbb{Z}/p^n\mathbb{Z}$ e obtemos o **anel dos inteiros p-ádicos** $\mathbb{Z}_p$.
Como todo elemento $f \in \mathbb{Q}_p$ admite uma representação

$$f = p^{-m}g$$

com $g \in \mathbb{Z}_p$, adição e multiplicação estendem de $\mathbb{Z}_p$ para $\mathbb{Q}_p$ e $\mathbb{Q}_p$ vem a ser o corpo de frações de $\mathbb{Z}_p$.
Em $\mathbb{Z}_p$, nós encontramos os inteiros racionais $a \in \mathbb{Z}$ que são determinados pelas congruências

$$a \equiv a_o + a_1 p + \cdots + a_{n-1}p^{n-1} \bmod p^n,$$

$0 \leq a_i < p$. Fazendo a identificação

$$\mathbb{Z}_p = \varprojlim_n \ \mathbb{Z}/p^n\mathbb{Z}$$

o subconjunto $\mathbb{Z}$ é levado para o conjunto de tuplas

$$(a \bmod p, \ \ a \bmod p^2, \ \ a \bmod p^3, \dots) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

e assim é visto como um subanel de $\mathbb{Z}_p$. Nós obtemos $\mathbb{Q}$ como um subcorpo do corpo $\mathbb{Q}_p$ de números p-ádicos da mesma forma.

Apesar de suas origens nas ideias da teoria de funções, as aplicações dos números p-ádicos se estendem naturalmente para o cerne da aritmética através das **equações Diofantinas**. Uma tal equação

$$F(x_1, \dots, x_n) = 0$$

é dada pelo polinômio $F \in \mathbb{Z}[x_1, \dots, x_n]$, e a questão gira em torno de saber se ela admite soluções nos inteiros. Este problema pode ser facilitado considerando, no lugar da equação, todas as congruências

$$F(x_1, \dots, x_n) \equiv 0 \bmod m.$$

Pelo Teorema Chinês dos Restos, é suficiente considerar as congruências

$$F(x_1, \dots, x_n) \equiv 0 \bmod p^v$$

percorrendo todas as potências de primos. A esperança é obter assim informações sobre a equação original. Essa abundância de congruências pode agora ser sintetizada novamente em uma única equação através dos números p-ádicos. De fato, temos a seguinte proposição.

Proposição 2.4. *Seja $F(x_1, \ldots, x_n)$ um polinômio com coeficientes inteiros, e fixe p um número primo. A congruência*

$$F(x_1, \ldots, x_n) \equiv 0 \bmod p^v$$

tem solução para $v \geq 1$ arbitrário se e somente se a equação

$$F(x_1, \ldots, x_n) = 0$$

tem solução nos inteiros p-ádicos.

Demonstração. Como estabelecido acima, nós vemos o anel $\mathbb{Z}_p$ como o limite projetivo

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subseteq \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}.$$

Visto sobre o anel à direita, a equação $F = 0$ se divide em componentes sobre os anéis individuais $\mathbb{Z}/p^v\mathbb{Z}$, nomeadamente, as congruências

$$F(x_1, \ldots, x_n) \equiv 0 \bmod p^v.$$

Agora, se

$$(x_1, \ldots, x_n) = (x_1^{(v)}, \ldots, x_n^{(v)})_{v\in\mathbb{N}} \in \mathbb{Z}_p^n,$$

com $(x_i^{(v)})_{v\in\mathbb{N}} \in \mathbb{Z}_p = \varprojlim_v \mathbb{Z}/p^v\mathbb{Z}$, é uma solução p-ádica da equação $F(x_1, \ldots, x_n) = 0$, então as congruências são resolvidas por

$$F(x_1^{(v)}, \ldots, x_n^{(v)}) \equiv 0 \bmod p^v, \quad v = 1, 2, \ldots$$

Por outro lado, seja uma solução $(x_1^{(v)}, \ldots, x_n^{(v)})$ da congruência

$$F(x_1, \ldots, x_n) \equiv 0 \bmod p^v$$

dada para cada $v \geq 1$. Se os elementos $(x_i^{(v)})_{v\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^v\mathbb{Z}$ já estão em $\varprojlim \mathbb{Z}/p^v\mathbb{Z}$, para todo $i = 1, \ldots, n$, então nós temos uma solução p-ádica da equação $F = 0$. Mas este não é o caso automaticamente. Portanto, nós extraímos uma subsequência da sequência $(x_1^{(v)}, \ldots, x_n^{(v)})$ que satisfaz nossas necessidades. Para simplificar a notação, vamos escrever $x_v = (x_1^{(v)}, \ldots, x_n^{(v)})$. No que se segue, veremos (x_v) como uma sequência em $\mathbb{Z}^n$. Como $(\mathbb{Z}/p\mathbb{Z})^n$ é finito, existem infinitos termos x_v que são congruentes módulo p ao mesmo elemento $y_1 \in (\mathbb{Z}/p\mathbb{Z})^n$. Consequentemente nós podemos escolher uma subsequência $\{x_v^{(1)}\}$ de $\{x_v\}$ tal que

$$x_v^{(1)} \equiv y_1 \bmod p \quad \text{e} \quad F\left(x_v^{(1)}\right) \equiv 0 \bmod p.$$

Da mesma forma, podemos extrair de $\{x_v^{(1)}\}$ uma subsequência $\{x_v^{(2)}\}$ tal que

$$x_v^{(2)} \equiv y_2 \bmod p^2 \quad \text{e} \quad F\left(x_v^{(2)}\right) \equiv 0 \bmod p^2.$$

onde $y_2 \in (\mathbb{Z}/p^2\mathbb{Z})^n$ claramente satisfaz $y_2 \equiv y_1 \bmod p$. Continuando nesse caminho, nós obtemos para cada $k \geq 1$ uma subsequência $\{x_v^{(k)}\}$ de $\{x_v^{(k-1)}\}$ cujos termos satisfazem as congruências

$$x_v^{(k)} \equiv y_k \bmod p^k \quad \text{e} \quad F\left(x_v^{(k)}\right) \equiv 0 \bmod p^k$$

para algum $y_k \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^n$ tal que

$$y_k \equiv y_{k-1} \bmod p^{k-1}.$$

Os y_k definem uma n-upla ordenada de inteiros p-ádicos $y = (y_k)_{k\in\mathbb{N}} \in (\varprojlim_k \mathbb{Z}/p^k\mathbb{Z})^n = (\mathbb{Z}_p)^n$ satisfazendo

$$F(y_k) \equiv 0 \bmod p^k$$

para todo $k \geq 1$. Em outras palavras, $F(y) = 0$. □

2.2 O Valor Absoluto p-ádico

A representação de um inteiro p-ádico

$$a_0 + a_1 p + a_2 p^2 + \cdots, \quad 0 \leq a_i < p, \tag{2.1}$$

lembra muito a representação em frações decimais

$$a_0 + a_1\left(\frac{1}{10}\right) + a_2\left(\frac{1}{10}\right)^2 + \cdots, \quad 0 \leq a_i < 10,$$

de um número real entre 0 e 10. Mas ela não converge como as frações decimais. Não obstante, o corpo $\mathbb{Q}_p$ de números p-ádicos pode ser construído à partir do corpo $\mathbb{Q}$ da mesma maneira que o corpo dos números reais $\mathbb{R}$. A chave para isso é substituir o valor absoluto ordinário por um novo valor absoluto "p-ádico" $|\ |_p$ com relação à qual a série (2.1) converge para que os números p-ádicos apareçam da maneira usual como limites de sequências de Cauchy de números racionais. Essa abordagem foi proposta pelo matemático Húngaro *J. Kürschák* [5]. O valor absoluto p-ádico $|\ |_p$ é definido como segue.

Seja $a = \frac{b}{c}$, $b, c \in \mathbb{Z}$ um número racional não nulo. Nós extraímos de b e de c a maior potência possível do número primo p,

$$a = p^m \frac{b'}{c'}, \quad (b'c', p) = 1, \tag{2.2}$$

e definimos

$$|a|_p = \frac{1}{p^m}$$

Portanto o valor absoluto p-ádico não mede o tamanho de um número $a \in \mathbb{N}$. Em vez disso, ele fica menor se o número é divisível por uma grande potência de p. Isso é baseado na ideia de que um inteiro tem que ser 0 se ele é infinitamente divisível por p. Em particular, os termos de uma série p-ádica $a_0 + a_1 p + a_2 p^2 + \cdots$ formam uma sequência convergindo para 0 com respeito a $|\ |_p$.

O expoente m na representação (2.2) do número a é denotado por $v_p(a)$, e definimos formalmente $v_p(0) = \infty$. Isto nos dá a função

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\},$$

que satisfaz as seguintes propriedades

1. $v_p(a) = \infty \iff a = 0$;
2. $v_p(ab) = v_p(a) + v_p(b)$;
3. $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$.

Onde $x + \infty = \infty$, $\infty + \infty = \infty$ e $\infty > x$, para todo $x \in \mathbb{Z}$. A função v_p é chamada de **valoração exponencial p-ádica** de $\mathbb{Q}$. O valor absoluto p-ádico é dado por

$$|\ |_p : \mathbb{Q} \longrightarrow \mathbb{R}, \quad a \longmapsto |a|_p = p^{-v_p(a)}.$$

Em vista das propriedades citadas acima, estarão satisfeitas as condições de uma *norma* em $\mathbb{Q}$:

1. $|a|_p = 0 \iff a = 0$;
2. $|ab|_p = |a|_p |b|_p$;
3. $|a + b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$.

À partir de agora, iremos denotar a norma usual $|\ |$ por $|\ |_\infty$. Em conjunto com os valores absolutos $|\ |_p$, ela satisfaz a importante **fórmula do produto:**

Proposição 2.5. *Para todo número racional $a \neq 0$, temos*

$$\prod_p |a|_p = 1,$$

onde p percorre todos os números primos, bem como o símbolo ∞.

Demonstração. Na fatoração prima

$$a = \pm \prod_{p \neq \infty} p^{v_p}$$

de a, o expoente v_p de p é precisamente a valoração exponencial $v_p(a)$ e o sinal é igual a $\frac{a}{|a|_\infty}$. A equação se torna então

$$a = \frac{a}{|a|_\infty} \prod_{p \neq \infty} \frac{1}{|a|_p} = a \prod_p \frac{1}{|a|_p},$$

O que prova que $\prod_p |a|_p = 1$. □

A notação $|\ |_\infty$ para o valor absoluto ordinário é motivada pela analogia do corpo de números racionais $\mathbb{Q}$ com o corpo de funções racionais $k(t)$ sobre um corpo finito k, com o qual começamos nossas considerações. No lugar de $\mathbb{Z}$, nós temos dentro de $k(t)$ o anel de polinômios $k[t]$, cujos ideais primos $\mathfrak{p} \neq 0$ são dados pelos polinômios mônicos irredutíveis $p(t) \in k[t]$. Para cada $\mathfrak{p}$, nós definimos um valor absoluto

$$|\ |_\mathfrak{p} : k(t) \longrightarrow \mathbb{R}$$

como segue. Seja $f(t) = \frac{g(t)}{h(t)}$, $g(t), h(t) \in k[t]$ uma função racional não nula. Nós extraímos de $g(t)$ e de $h(t)$ a maior potência possível do polinômio irredutível $p(t)$,

$$f(t) = p(t)^m \frac{\overline{g}(t)}{\overline{h}(t)}, \quad (\overline{g}\overline{h}, p) = 1,$$

e definimos

$$v_\mathfrak{p}(f) = m, \quad |f|_\mathfrak{p} = q_\mathfrak{p}^{-v_\mathfrak{p}(f)},$$

onde $q_\mathfrak{p} = q^{d_\mathfrak{p}}$, com $d_\mathfrak{p}$ sendo o grau do corpo de resíduos de classe de $\mathfrak{p}$ sobre k e q um número real fixado > 1. Além disso nós definimos $v_\mathfrak{p}(0) = \infty$ e $|0|_\mathfrak{p} = 0$, e obtemos para $v_\mathfrak{p}$ e para $|\ |_\mathfrak{p}$ as mesmas propriedades obtidas para v_p e $|\ |_p$. No caso $\mathfrak{p} = (t - a)$ para $a \in k$, a valoração $v_\mathfrak{p}(f)$ é claramente a ordem do zero, respectivamente polo, da função $f = f(t)$ em $t = a$.
Mas para o corpo de funções $k(t)$, existe mais uma valoração exponencial

$$v_\infty : k(t) \longrightarrow \mathbb{Z} \cup \{\infty\},$$

nomeadamente

$$v_\infty(f) = \deg(h) - \deg(g),$$

onde $f = \frac{g}{h} \neq 0$, $g, h \in k[t]$. Esta descreve a ordem do zero, respectivamente polo, da função $f(t)$ no ponto no infinito ∞, isto é, a ordem do zero, respectivamente polo, da função $f(1/t)$ no ponto $t = 0$. Está associada ao ideal primo $\mathfrak{p} = (1/t)$ do anel $k[1/t] \subseteq k(t)$ da mesma forma que as valorações exponenciais $v_\mathfrak{p}$ estão associadas aos ideais primos $\mathfrak{p}$ de $k[t]$. Colocando

$$|f|_\infty = q^{-v_\infty(f)},$$

a fatoração única em $k(t)$ nos fornece, como na proposição (2.5), a fórmula

$$\prod_\mathfrak{p} |f|_\mathfrak{p} = 1,$$

onde $\mathfrak{p}$ varia sobre os ideais primos de $k[t]$ bem como o símbolo ∞, que agora denota o ponto no infinito.
Em vista da fórmula do produto da proposição (2.5), a consideração acima mostra que o valor absoluto ordinário $|\ |$ de $\mathbb{Q}$ deve ser pensado como associado a um ponto virtual no infinito. Este ponto de vista justifica a notação $|\ |_\infty$. A diferença decisiva entre o valor absoluto $|\ |_\infty$ de $\mathbb{Q}$ e o valor absoluto $|\ |_\infty$ de $k(t)$ é, no entanto, que o primeiro não é derivado de nenhuma valoração exponencial $v_\mathfrak{p}$ anexada a um ideal primo.

Tendo introduzido o valor absoluto p-ádico no corpo $\mathbb{Q}$, daremos agora uma nova definição do corpo $\mathbb{Q}_p$ de números p-ádicos, imitando a construção do corpo dos números reais. Nós verificaremos posteriormente que essa construção analítica concorda com a definição de Hensel, vista na seção (2.1).

Uma **sequência de Cauchy** com respeito a $|\ |_p$ é, por definição, uma sequência $\{x_n\}$ de números racionais tais que para todo $\epsilon > 0$, existe um inteiro positivo n_0 satisfazendo

$$|x_n - x_m|_p < \epsilon, \quad \forall n, m \geq n_0.$$

Exemplo 2.3. *Para um primo p, toda série formal*

$$\sum_{v=0}^{\infty} a_v p^v, \quad 0 \leq a_v < p,$$

proporciona uma sequência de Cauchy através das somas parciais

$$x_n = \sum_{v=0}^{n-1} a_v p^v,$$

pois para $n > m$ temos

$$|x_n - x_m|_p = |\sum_{v=m}^{n-1} a_v p^v|_p \leq \max_{m \leq v < n} \{|a_v p^v|_p\} \leq \frac{1}{p^m}.$$

Uma sequência $\{x_n\}$ em $\mathbb{Q}$ é chamada **sequência nula** com respeito a $|\ |_p$ se $|x_n|_p$ é uma sequência convergindo para 0 no sentido usual.

Exemplo 2.4. $1, p, p^2, p^3, \ldots$ *é uma sequência nula.*

As sequências de Cauchy formam um anel R, as sequências nulas formam um ideal maximal $\mathfrak{m}$, e nós definimos novamente o corpo dos números p-ádicos como sendo o corpo de resíduos de classe

$$\mathbb{Q}_p := R/\mathfrak{m}.$$

Nós mergulhamos $\mathbb{Q}$ em $\mathbb{Q}_p$ associando a cada elemento $a \in \mathbb{Q}$ a classe de resíduos da sequência constante $(a, a, a, \ldots)$. O valor absoluto $|\ |_p$ sobre $\mathbb{Q}$ é estendido para $\mathbb{Q}_p$ dando ao elemento $x = \{x_n\} \bmod \mathfrak{m} \in R/\mathfrak{m}$ o valor absoluto

$$|x|_p := \lim_{n \to \infty} |x_n|_p \in \mathbb{R}.$$

O limite existe porque $\{|x_n|_p\}$ é uma sequência de Cauchy em $\mathbb{R}$, e isso é independente da escolha da sequência $\{x_n\}$ dentro de sua classe $\bmod \mathfrak{m}$ pois qualquer sequência nula p-ádica $\{y_n\} \in \mathfrak{m}$ obviamente satisfaz $\lim_{n\to\infty} |y_n|_p = 0$.

A valoração exponencial p-ádica v_p sobre $\mathbb{Q}$ estende para uma valoração exponencial

$$v_p : \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

De fato, se $x \in \mathbb{Q}_p$ é a classe da sequência de Cauchy $\{x_n\}$ onde $x_n \neq 0$, então

$$v_p(x_n) = -\ln_p |x_n|_p$$

ou diverge para ∞ ou é uma sequência de Cauchy em $\mathbb{Z}$ que eventualmente precisa se tornar constante para um n suficientemente grande pois $\mathbb{Z}$ é discreto. Colocamos

$$v_p(x) = \lim_{n \to \infty} v_p(x_n) = v_p(x_n) \quad \text{para } n \geq n_0.$$

Novamente nós encontramos para todo $x \in \mathbb{Q}_p$ que

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

Como para o corpo dos números reais, podemos provar a seguinte proposição.

Proposição 2.6. *O corpo $\mathbb{Q}_p$ de números p-ádicos é completo com respeito ao valor absoluto $|\ |_p$, isto é, toda sequência de Cauchy em $\mathbb{Q}_p$ converge com respeito a $|\ |_p$.*

Bem como para o corpo $\mathbb{R}$, nós então obtemos para cada número primo p um novo corpo $\mathbb{Q}_p$ satisfazendo as mesmas propriedades, de modo que $\mathbb{Q}$ dá origem a uma família de corpos

$$\mathbb{Q}_2,\ \mathbb{Q}_3,\ \mathbb{Q}_5,\ \mathbb{Q}_7,\ \mathbb{Q}_{11},\ldots,\ \mathbb{Q}_\infty = \mathbb{R}.$$

Uma importante propriedade especial dos valores absolutos p-ádicos $|\ |_p$ está no fato de que eles não só satisfazem a desigualdade triangular usual, mas também a versão mais forte

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

Isso produz a seguinte proposição, que nos dá uma nova definição para os inteiros p-ádicos.

Proposição 2.7. *O conjunto*

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

é um subanel de $\mathbb{Q}_p$. Ele será o fecho com respeito a $|\ |_p$ do anel $\mathbb{Z}$ no corpo $\mathbb{Q}_p$.

Demonstração. O fato de que $\mathbb{Z}_p$ é fechado para adição e multiplicação segue de

$$|x+y|_p \leq \max\left\{|x|_p, |y|_p\right\} \quad \text{e} \quad |xy|_p = |x|_p|y|_p.$$

Se $\{x_n\}$ é uma sequência de Cauchy em $\mathbb{Z}$ e $x = \lim_{n\to\infty} x_n$, então $|x_n|_p \leq 1$ implica também que $|x|_p \leq 1$, consequentemente $x \in \mathbb{Z}_p$. Por outro lado, seja $x = \lim_{n\to\infty} x_n \in \mathbb{Z}_p$, para uma sequência de Cauchy $\{x_n\}$ em $\mathbb{Q}$. Nós vimos acima que $|x|_p = |x_n|_p \leq 1$ para $n \geq n_0$, isto é, $x_n = \frac{a_n}{b_n}$, com $a_n, b_n \in \mathbb{Z}$, $(b_n, p) = 1$. Escolhendo para cada $n \geq n_0$ uma solução $y_n \in \mathbb{Z}$ da congruência $b_n y_n \equiv a_n \bmod p^n$ obtemos $|x_n - y_n|_p \leq \frac{1}{p^n}$, e portanto $x = \lim_{n\to\infty} y_n$, então x pertence ao fecho de $\mathbb{Z}$. □

O grupo de unidades de $\mathbb{Z}_p$ é

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}.$$

Cada elemento $x \in \mathbb{Q}_p^*$ admite uma representação única

$$x = p^m u \quad \text{com } m \in \mathbb{Z} \text{ e } u \in \mathbb{Z}_p^*.$$

Pois se $v_p(x) = m \in \mathbb{Z}$, então $v_p(xp^{-m}) = 0$, consequentemente $|xp^{-m}|_p = 1$, isto é, $u = xp^{-m} \in \mathbb{Z}_p^*$. Além disso nós obtemos a próxima proposição.

Proposição 2.8. *Os ideais não-nulos do anel $\mathbb{Z}_p$ são os ideais principais*

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq n\},$$

com $n \geq 0$, e temos

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Demonstração. Sejam $\mathfrak{a} \neq (0)$ um ideal de $\mathbb{Z}_p$ e $x = p^m u$, $u \in \mathbb{Z}_p^*$, um elemento de $\mathfrak{a}$ com o menor m possível (como $|x|_p \leq 1$, temos $m \geq 0$). Então $\mathfrak{a} = p^m\mathbb{Z}_p$ pois $y = p^n u' \in \mathfrak{a}$, $u' \in \mathbb{Z}_p^*$, implica $n \geq m$, consequentemente $y = (p^{n-m}u')p^m \in p^m\mathbb{Z}_p$. O homomorfismo

$$\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p, \quad a \longmapsto a \bmod p^n\mathbb{Z}_p,$$

tem núcleo $p^n\mathbb{Z}$ e é sobrejetivo. De fato, para cada $x \in \mathbb{Z}_p$, pela proposição (2.7) existe um $a \in \mathbb{Z}$ tal que

$$|x - a|_p \leq \frac{1}{p^n},$$

isto é, $v_p(x-a) \geq n$, então $x-a \in p^n\mathbb{Z}_p$ e consequentemente $x \equiv a \bmod p^n\mathbb{Z}_p$. Então nós obtemos o isomorfismo

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

□

Agora estamos prontos para tentar estabelecer uma conexão com a definição de Hensel do anel $\mathbb{Z}_p$ e do corpo $\mathbb{Q}_p$.
Havíamos definido os inteiros p-ádicos como séries formais

$$\sum_{v=0}^{\infty} a_v p^v, \quad 0 \leq a_v < p,$$

que nós identificamos com as sequências

$$\overline{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n = 1, 2, \ldots,$$

onde s_n são as somas parciais

$$s_n = \sum_{v=0}^{n-1} a_v p^v.$$

Essas sequências constituíram o limite projetivo

$$\varprojlim_n \ \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid x_{n+1} \mapsto x_n \right\}.$$

Nós vimos os inteiros p-ádicos como elementos desse anel. Como

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z},$$

nós obtemos, para cada $n \geq 1$, um homomorfismo sobrejetivo

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}.$$

Está claro que a família desses homomorfismos produz um homomorfismo

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \ \mathbb{Z}/p^n\mathbb{Z}.$$

Iremos agora provar a possibilidade de identificar as duas definições dadas para $\mathbb{Z}_p$ (e também para $\mathbb{Q}_p$) através da seguinte proposição.

Proposição 2.9. *O homomorfismo*

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

é um isomorfismo.

Demonstração. Se $x \in \mathbb{Z}$ é mapeado para zero, então $x \in p^n\mathbb{Z}_p$ para todo $n \geq 1$, isto é, $|x|_p \leq \frac{1}{p^n}$ para todo $n \geq 1$, e assim $|x|_p = 0$, o que implica $x = 0$. Isso mostra a injetividade.
Um elemento de $\varprojlim_v \ \mathbb{Z}/p^v\mathbb{Z}$ é dado por uma sequência de somas parciais

$$s_n = \sum_{v=0}^{n-1} a_v p^v, \quad 0 \leq a_v < p.$$

Nós vimos acima que esta sequência é uma sequência de Cauchy em $\mathbb{Z}_p$, e então converge para um elemento

$$x = \sum_{v=0}^{\infty} a_v p^v \in \mathbb{Z}_p.$$

Como

$$x - s_n = \sum_{v=n}^{\infty} a_v p^v \in p^n\mathbb{Z}_p,$$

temos $x \equiv s_n \bmod p^n$ para todo n, isto é, x é mapeado para um elemento de $\varprojlim_v \ \mathbb{Z}/p^v\mathbb{Z}$ que é definido por uma dada sequência $(s_n)_{n\in\mathbb{N}}$. Isso mostra a sobrejetividade. □

Nós enfatizamos que os elementos no lado direito do isomorfismo

$$\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_v \mathbb{Z}/p^v\mathbb{Z}$$

são dados formalmente por sequências de somas parciais

$$s_n = \sum_{v=0}^{n-1} a_v p^v, \quad n = 1, 2, \ldots$$

No lado esquerdo, por outro lado, estas sequências convergem com respeito ao valor absoluto e produzem elementos de $\mathbb{Z}_p$ da maneira usual, como séries infinitas convergentes

$$x = \sum_{v=0}^{\infty} a_v p^v.$$

2.3 Valorações

O processo que realizamos na seção anterior com o corpo $\mathbb{Q}$ para obter os números p-ádicos pode ser generalizado para corpos arbitrários usando o conceito de valoração multiplicativa.

Definição 2.10. *Uma **valoração** de um corpo K é uma função*

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

satisfazendo as propriedades

1. $|x| \geq 0$, *e* $|x| = 0 \iff x = 0$,
2. $|xy| = |x||y|$,
3. $|x + y| \leq |x| + |y|$

Estrategicamente iremos excluir no que segue o caso onde $|\ |$ é a valoração trivial de K que satisfaz $|x| = 1$ para todo $x \neq 0$. Definindo a distância entre dois pontos $x, y \in K$ por

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

torna K um espaço métrico, e em particular um espaço topológico.

Definição 2.11. *Uma valoração $|\ |$ em um corpo K induz uma topologia em que a base de vizinhanças abertas de um $a \in K$ são as bolas*

$$B(a, d) = \{x \in K \mid |x - a| < d\}$$

para $d > 0$.

Definição 2.12. *Duas valorações de K são chamadas equivalentes se elas definem a mesma topologia em K.*

Proposição 2.13. *Duas valorações $|\ |_1$ e $|\ |_2$ em K são equivalentes se, e somente se existe um número real $s > 0$ tal que*

$$|x|_1 = |x|_2^s$$

para todo $x \in K$.

Demonstração. Se $|\ |_1 = |\ |_2^s$, com $s > 0$, então $|x-a|_1 < d \iff |x-a|_2^s < d \iff |x-a|_2 < d^{1/s}$ então $B_1(a,d) = B_2(a,d^{1/s})$. Portanto as bases de vizinhanças abertas de a para $|\ |_1$ e $|\ |_2$ são idênticas.
Para uma valoração arbitrária $|\ |$ em K, a desigualdade $|x| < 1$ é equivalente à condição de que $\{x^n\}_{n\in\mathbb{N}}$ converge para zero na topologia definida por $|\ |$. Assim sendo, se $|\ |_1$ e $|\ |_2$ são equivalentes, temos a implicação

$$|x|_1 < 1 \implies |x|_2 < 1. \tag{2.3}$$

Agora seja $y \in K$ um elemento fixado satisfazendo $|\ |_1 > 1$. Seja $x \in K$, $x \neq 0$. Então $|x|_1 = |y|_1^\alpha$ para algum $\alpha \in \mathbb{R}$. Seja m_i/n_i uma sequência de números racionais (com $n_1 > 0$) que converge para o α definido acima. Então nós temos $|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i}$, e consequentemente

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

de modo que $|x|_2 \leq |y|_2^{m_i/n_i}$, e portanto $|x|_2 \leq |y|_2^\alpha$. Usando uma sequência m_i/n_i que converge para α por baixo, a equação (2.3) nos mostra que $|x|_2 \geq |y|_2^\alpha$. Então nós temos $|x|_2 = |y|_2^\alpha$. Para todo $x \in K$, $x \neq 0$, nós obtemos

$$\frac{\ln|x|_1}{\ln|x|_2} = \frac{\ln|y|_1}{\ln|x|_2} =: s,$$

e consequentemente $|x|_1 = |x|_2^s$. Mas $|y|_1 > 1$ implica $|y|_2 > 1$, e portanto $s > 0$. □

A demonstração mostra que a equivalência de $|\ |_1$ e $|\ |_2$ também é equivalente à condição

$$|x|_1 < 1 \implies |x|_2 < 1.$$

Nós usaremos esse fato para provar o seguinte teorema de aproximação, que pode ser considerado uma variação do teorema Chinês dos restos.

Teorema 2.14 (Teorema de Aproximação)**.** *Sejam* $|\ |_1, \ldots, |\ |_n$ *valorações não equivalentes duas a duas do corpo* K *e sejam* $a_1, \ldots, a_n \in K$ *elementos dados. Então para cada* $\epsilon > 0$ *existe um* $x \in K$ *tal que*

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

Demonstração. Pela afirmação acima, como $|\ |_1$ e $|\ |_n$ não são equivalentes, existe $\alpha \in K$ tal que $|\alpha|_1 < 1$ e $|\alpha|_n \geq 1$. Pela mesma razão, existe $\beta \in K$ tal que $|\beta|_n < 1$ e $|\beta|_1 \geq 1$. Colocando $y = \beta/\alpha$, temos $|y|_1 > 1$ e $|y|_n < 1$. Nós agora provaremos por indução sobre n que existe $z \in K$ tal que

$$|z|_1 > 1 \quad \text{e} \quad |z|_j < 1 \quad \text{para } j = 2, \ldots, n.$$

Já demonstramos o caso $n = 2$. Assuma que nós encontramos $k \in K$ satisfazendo

$$|k|_1 > 1 \quad \text{e} \quad |k|_j < 1 \quad \text{para } j = 2, \ldots, n-1.$$

Se $|k|_n \leq 1$, então $z = k^m y$ satisfará nossa hipótese para m suficientemente grande. Se, no entanto, $|k|_n > 1$, a sequência $t_m = k^m/(1+k^m)$ irá convergir para 1 com respeito a $|\ |_1$ e $|\ |_n$, e para 0 com respeito a $|\ |_2, \ldots, |\ |_{n-1}$. Consequentemente, para m suficientemente grande, $z = t_m y$ irá satisfazer nossa hipótese.
A sequência $z^m/(1+z^m)$ converge para 1 com respeito a $|\ |_1$ e para 0 com respeito a $|\ |_2, \ldots, |\ |_n$. Para cada i nós podemos construir desse modo um z_i que é muito próximo de 1 com respeito a $|\ |_i$, e muito perto de 0 com respeito a $|\ |_j$ para $j \neq i$. O elemento

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

então satisfaz as exigências do Teorema de Aproximação. □

Definição 2.15. *A valoração* $|\ |$ *é chamada* ***não-arquimediana*** *se* $|n|$ *permanece limitado para todo* $n \in \mathbb{N}$*. Caso contrário* $|\ |$ *é chamada* ***arquimediana****.*

Proposição 2.16. *A valoração* $|\ |$ *é não-arquimediana se e somente se ela satisfaz a* ***desigualdade triangular forte***

$$|x + y| \leq \max\{|x|, |y|\}$$

Demonstração. Se a desigualdade triangular forte vale, então temos

$$|n| = |1 + \cdots + 1| \leq 1.$$

Por outro lado, seja $|n| \leq N$ para todo $n \in \mathbb{N}$. Sejam $x, y \in K$ e suponha $|x| \geq |y|$. Então $|x|^v|y|^{n-v} \leq |x|^n$ para $v \geq 0$ e temos

$$|x+y|^n \leq \sum_{v=0}^{n} \left| \binom{n}{v} \right| |x|^v|y|^{n-v} \leq N(n+1)|x|^n,$$

consequentemente

$$|x+y| \leq N^{1/n}(1+n)^{1/n}|x| = N^{1/n}(1+n)^{1/n} \max\{|x|, |y|\},$$

e então $|x+y| \leq \max\{|x|, |y|\}$ colocando $n \to \infty$. □

Observação 3. *A desigualdade triangular forte imediatamente implica que*

$$|x| \neq |y| \implies |x+y| = \max\{|x|, |y|\}$$

Demonstração. Dados x e y tais que $|x| \neq |y|$, podemos supor sem perda de generalidade que $|x| \geq |y|$. Isso implica que $|x+y| \leq |x|$. Por outro lado, $|x| = |(x+y) - y| \leq \max\{|x+y|, |y|\}$. Agora, o valor de $\max\{|x+y|, |y|\}$ não pode ser y, pois isso implicaria $|x| \leq |y|$, o que contraria nossa hipótese inicial. Então $\max\{|x+y|, |y|\} = |x+y|$. Usando a primeira desigualdade temos $|x| \leq |x+y| \leq |x| \implies |x+y| = |x|$, como queríamos demonstrar. □

Podemos estender a valoração não-arquimediana $|\ |$ de K para uma valoração do corpo de funções $K(t)$ de uma maneira canônica colocando, para um polinômio $f(t) = a_0 + a_1 t + \cdots + a_n t^n$,

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

Proposição 2.17. *Cada valoração de $\mathbb{Q}$ é equivalente a uma das valorações $|\ |_p$ ou $|\ |_\infty$.*

Demonstração. Seja $\|\ \|$ uma valoração não-arquimediana de $\mathbb{Q}$. Então $\|n\| = \|1 + \cdots + 1\| \leq 1$, e existe um número primo p tal que $\|p\| < 1$ pois, do contrário, a fatoração prima única implicaria $\|x\| = 1$ para todo $x \in \mathbb{Q}^*$. O conjunto

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

é um ideal de $\mathbb{Z}$ satisfazendo $p\mathbb{Z} \subseteq \mathfrak{a} \neq \mathbb{Z}$, e como $p\mathbb{Z}$ é um ideal maximal, nós temos $\mathfrak{a} = p\mathbb{Z}$. Se $a \in \mathbb{Z}$ e $a = bp^m$ com $p \nmid b$, de modo que $b \notin \mathfrak{a}$, então $\|b\| = 1$ e consequentemente

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

onde $s = -\ln\|p\|/\ln p$. Assim $\|\ \|$ é equivalente a $|\ |_p$.
Agora seja $\|\ \|$ uma valoração arquimediana. Então temos, para dois números naturais arbitrários $n, m > 1$,

$$\|m\|^{1/\ln m} = \|n\|^{1/\ln n}. \tag{2.4}$$

De fato, podemos escrever

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

onde $a_i \in \{0, 1, \ldots, n-1\}$ e $n^r \leq m$. Consequentemente, observando que $r \leq \ln m/\ln n$ e $\|a_i\| = \|1 + \cdots + 1\| \leq a_i\|1\| \leq n$, obtemos a desigualdade

$$\|m\| \leq \sum_{i=0}^{r} \|a_i\| \cdot \|n\|^i \leq \sum_{i=0}^{r} \|a_i\| \cdot \|n\|^r \leq \left(1 + \frac{\ln m}{\ln n}\right) n \cdot \|n\|^{\ln m/\ln n}.$$

Tomando m^k no lugar de m, tirando as raízes k-ésimas nos dois lados e fazendo k tender para ∞, obtemos

$$\begin{aligned}
\|m^k\| &\leq \left(1 + \frac{\ln m^k}{\ln n}\right) n \cdot \|n\|^{\ln m^k/\ln n} \\
\|m\|^k &\leq \left(1 + k\frac{\ln m}{\ln n}\right) n \cdot \|n\|^{k(\ln m/\ln n)} \\
\lim_{k\to\infty} \sqrt[k]{\|m\|^k} &\leq \lim_{k\to\infty} \sqrt[k]{\left(1 + k\frac{\ln m}{\ln n}\right) n \cdot \|n\|^{k(\ln m/\ln n)}} \\
\|m\| &\leq \|n\|^{\ln m/\ln n} \\
\|m\|^{1/\ln m} &\leq \|n\|^{1/\ln n}
\end{aligned}$$

Trocando m e n conseguimos a igualdade (2.4). Tomando $c = \|n\|^{1/\ln n}$ temos $\|n\| = c^{\ln n}$, e colocar $c = e^s$ produz, para cada número racional positivo $x = a/b$,

$$\|x\| = e^{s\ln x} = |x|^s.$$

Portanto $\|\ \|$ é equivalente ao valor absoluto usual $|\ |$ sobre $\mathbb{Q}$. □

Seja $|\ |$ uma valoração não-arquimediana do corpo K. Fazendo

$$v(x) = -\ln|x| \quad \text{para } x \neq 0, \quad \text{e } v(0) = \infty,$$

nós obtemos uma função

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

satisfazendo as propriedades

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

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

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

onde nós fixamos as seguintes convenções acerca dos elementos $a \in \mathbb{R}$ e o símbolo ∞: $a < \infty$, $a + \infty = \infty$, $\infty + \infty = \infty$.
Uma função v sobre K com estas propriedades é chamada uma **valoração exponencial** de K. Nós excluiremos o caso da função trivial $v(x) = 0$ para $x \neq 0$, $v(0) = \infty$. Duas valorações exponenciais v_1 e v_2 de K são chamadas **equivalentes** se $v_1 = sv_2$, para algum número real $s > 0$. Para cada valoração exponencial v nós obtemos uma valoração no sentido da Definição (2.10) tomando

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

para algum número real $q > 1$ fixado. Para distinguir de v, vamos chamar $|\ |$ de uma **valoração multiplicativa** associada, ou **valor absoluto**. Substituindo v por uma valoração exponencial equivalente sv (isto é, substituindo q por $q' = q^s$) transforma $|\ |$ na valoração multiplicativa equivalente $|\ |^s$. As condições (i), (ii), (iii) implicam a seguinte proposição

Proposição 2.18. *O subconjunto*

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

é um anel com grupo de unidades

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

e o ideal maximal único

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

$\mathcal{O}$ é um domínio de integridade com corpo de frações K e tem a propriedade que, para cada $x \in K$, $x \in \mathcal{O}$ ou $x^{-1} \in \mathcal{O}$. Tal anel é chamado um **anel de valoração**. Seu único ideal maximal é $\mathfrak{p} = \{x \in \mathcal{O} \mid x^{-1} \notin \mathcal{O}\}$. O corpo $\mathcal{O}/\mathfrak{p}$ é chamado de **corpo de resíduos de classe** de $\mathcal{O}$. Um anel de valoração é sempre integralmente fechado. Pois se $x \in K$ é inteiro sobre $\mathcal{O}$, então existe uma equação

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

com $a_i \in \mathcal{O}$ e a hipótese $x \notin \mathcal{O}$, então $x^{-1} \in \mathcal{O}$, o que implica na contradição $x = -a_1 - a_2 x^{-1} - \cdots - a_n (x^{-1})^{n-1} \in \mathcal{O}$.

Uma valoração exponencial v é chamada **discreta** se admite um menor valor positivo s. Nesse caso, encontramos

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

Esta será chamada **normalizada** se $s = 1$. Dividindo por s nós sempre podemos passar para uma valoração normalizada sem mudar os invariantes $\mathcal{O}$, $\mathcal{O}^*$, $\mathfrak{p}$. Tendo feito isso, um elemento

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

é um **elemento primo**, e cada elemento $x \in K^*$ admite uma representação única

$$x = u\pi^m$$

com $m \in \mathbb{Z}$ e $u \in \mathcal{O}^*$. Pois se $v(x) = m$, então $v(x\pi^{-m}) = 0$, e consequentemente $u = x\pi^{-m} \in \mathcal{O}^*$.

Proposição 2.19. *Se v é uma valoração exponencial discreta de K, então*

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$$

é um domínio de ideais principais, e consequentemente um anel de valoração discreta.
Suponha que v é normalizado. Então os ideais não nulos de $\mathcal{O}$ são dados por

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

onde π é um elemento primo, isto é, $v(\pi) = 1$. Temos

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

enquanto $\mathcal{O}$-módulos.

Demonstração. Seja $\mathfrak{a}$ um ideal de $\mathcal{O}$ e $x \neq 0$ um elemento em $\mathfrak{a}$ com o menor valor $v(x) = n$ possível. Então $x = u\pi^n$, $u \in \mathcal{O}^*$, portanto $\pi^n\mathcal{O} \subseteq \mathfrak{a}$. Se $y = \epsilon\pi^m \in \mathfrak{a}$ é arbitrário com $\epsilon \in \mathcal{O}^*$, então $m = v(y) \geq n$, e consequentemente $y = (\epsilon\pi^{m-n})\pi^n \in \pi^n\mathcal{O}$, portanto $\mathfrak{a} = \pi^n\mathcal{O}$. O isomorfismo

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$$

resulta da correspondência $a\pi^n \mapsto a \bmod \mathfrak{p}$. □

Em um corpo K valorado discretamente a cadeia

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

consistindo dos ideais do anel de valoração $\mathcal{O}$ forma uma base de vizinhanças do elemento zero. De fato, se v é uma valoração exponencial normalizada e $|\ | = q^{-v}$ $(q > 1)$ uma valoração multiplicativa associada, então

$$\mathfrak{p}^n = \{x \in K \mid |x| < \frac{1}{q^{n-1}}\}.$$

Como uma base de vizinhanças do elemento 1 de K^*, nós obtemos da mesma forma a cadeia

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

de subgrupos

$$U^{(n)} = 1 + \mathfrak{p}^n = \{x \in K^* \mid |1 - x| < \frac{1}{q^{n-1}}\}, \quad n > 0,$$

de $\mathcal{O}^*$. (Observe que $1 + \mathfrak{p}^n$ é fechado para multiplicação e que, se $x \in U^{(n)}$, então também está x^{-1} pois $|1 - x^{-1}| = |x|^{-1}|x - 1| = |1 - x| < \frac{1}{q^{n-1}}$.)
$U^{(n)}$ é chamado de n-ésimo **grupo de unidades superiores** e $U^{(1)}$ de grupo de **unidades principais**. À respeito dos sucessivos quocientes da cadeia de grupos de unidades superiores, nós temos a seguinte proposição

Proposição 2.20. *$\mathcal{O}^*/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^*$ e $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}$ (isomorfos enquanto $\mathcal{O}$-módulos), para $n \geq 1$.*

Demonstração. O primeiro isomorfismo é induzido pelo homomorfismo canônico e obviamente sobrejetivo

$$\mathcal{O}^* \longrightarrow (\mathcal{O}/\mathfrak{p}^n)^*, \quad u \longmapsto u \bmod \mathfrak{p}^n,$$

cujo núcleo será $U^{(n)}$. O segundo homomorfismo é dado, uma vez que escolhemos um elemento primo π, pelo homomorfismo sobrejetivo

$$U^{(n)} = 1 + \pi^n\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}, \quad 1 + \pi^n a \longmapsto a \bmod \mathfrak{p},$$

cujo núcleo será $U^{(n+1)}$. □

Definição 2.21. *Um corpo valorado $(K, |\ \ |)$ é chamado **completo** se toda sequência de Cauchy $\{a_n\}_{n\in\mathbb{N}}$ em K converge para um elemento $a \in K$, isto é,*

$$\lim_{n\to\infty} |a_n - a| = 0.$$

Aqui, como usualmente, diremos que $\{a_n\}_{n\in\mathbb{N}}$ é uma **Sequência de Cauchy** se para todo $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que

$$|a_n - a_m| < \epsilon \quad \text{para todo} \quad n, m \geq N.$$

Para qualquer corpo valorado $(K, |\quad|)$ nós obtemos um corpo valorado completo $(\widehat{K}, |\quad|)$ pelo processo de **completamento**. Este completamento é obtido da mesma forma que o corpo de números reais é construído à partir do corpo de números racionais.
Pegue o anel R de todas as sequências de Cauchy de $(K, |\quad|)$, considere o ideal maximal $\mathfrak{m}$ de todas as sequências nulas com respeito a $|\quad|$, e defina

$$\widehat{K} = R/\mathfrak{m}.$$

Definição 2.22. *[3] Uma classe de equivalência de valorações $\mathfrak{p}$ em um corpo K é chamado de um **primo**, ou um **lugar** de K. Um primo é chamado **infinito** se ele contém uma valoração arquimediana. Caso contrário ele é chamado de primo **finito** de K. Como os completamentos de K com respeito a duas valorações equivalentes são isomorfos, podemos falar então sem ambiguidades sobre o único (a menos de isomorfismo) completamento de K com respeito ao primo $\mathfrak{p}$. Um primo infinito é chamado de **real** se o completamento de K com respeito a $\mathfrak{p}$ for o corpo dos números reais. Caso o completamento de K com respeito ao primo $\mathfrak{p}$ seja isomorfo ao corpo dos números complexos, denominamos tal primo de primo **complexo**.*

Capítulo 3

Teorema das Progressões Aritméticas

3.1 Caracteres de Grupos Abelianos Finitos

3.1.1 Dualidade

Seja G um grupo abeliano finito escrito multiplicativamente.

Definição 3.1. *Um **caracter multiplicativo** (ou simplesmente um **caracter**) de G é um homomorfismo de G no grupo multiplicativo $\mathbb{C}^*$.*
Os caracteres de G formam um grupo $\mathrm{Hom}(G, \mathbb{C}^*)$ que denotaremos por $\hat{G}$; este é chamado de dual de G.

Observação 4. *Embora os caracteres sejam definidos mais geralmente utilizando a teoria de representações, nos limitaremos neste texto aos caracteres multiplicativos definidos acima. Para um estudo mais aprofundado sobre representações e caracteres, recomendo consultar [9].*

Observação 5. *Suponha que G é cíclico de ordem n gerado por s. Se $\chi : G \to \mathbb{C}^*$ é um caracter de G, o elemento $w = \chi(s)$ satisfaz a relação $w^n = 1$, isto é, é uma n-ésima raiz da unidade. Por outro lado toda n-ésima raiz da unidade w define um caracter de G de modo que $s^a \to w^a$. Portanto nós vemos que o mapa $\chi \to \chi(s)$ é um isomorfismo de $\hat{G}$ no grupo μ_n das n-ésimas raízes da unidade. Em particular, $\hat{G}$ é cíclico de ordem n.*

Definição 3.2. *Um grupo abeliano $(G, \cdot)$ é divisível se, para todo inteiro positivo n e todo $g \in G$, existe $y \in G$ tal que $y^n = g$.*

Proposição 3.3. *Seja H um subgrupo de G. Todo caracter de H estende para um caracter de G.*

Demonstração. Nós usaremos indução sobre o índice $[G : H]$ de H em G. Se $[G : H] = 1$, então $H = G$ e não há nada para demonstrar. Por outro lado, seja x um elemento de G não contido em H, e seja $n > 1$ o menor inteiro tal que $x^n \in H$ (a existência de n deriva da finitude de G). Seja χ um caracter de H, e seja $t = \chi(x^n)$. Como $\mathbb{C}^*$ é um grupo divisível, podemos escolher um elemento $\omega \in \mathbb{C}^*$ tal que $\omega^n = t$. Seja H' o subgrupo de G gerado por H e x; todo elemento h' de H' pode ser escrito como $h' = hx^a$ com $a \in \mathbb{Z}$ e $h \in H$. Defina:

$$\chi'(h') = \chi(h)\omega^a.$$

É fácil verificar que esse número não depende da decomposição hx^a de h' e que $\chi' : H' \to \mathbb{C}^*$ é um caracter de H' estendendo χ. Como nós temos $[G : H'] < [G : H]$, a hipótese de indução nos permite estender χ' para um caracter de G. □

Proposição 3.4. *O grupo $\hat{G}$ é isomorfo a G. Em particular, $\hat{G}$ é um grupo abeliano finito da mesma ordem de G.*

Demonstração. [8] Capítulo 6, proposição 2. □

Se $x \in G$, a função $\chi \to \chi(x)$ é um caracter de $\hat{G}$. Nós obtemos então um homomorfismo $\epsilon : G \to \hat{\hat{G}}$.

Proposição 3.5. *O homomorfismo ϵ é um isomorfismo de G no seu bidual $\hat{\hat{G}}$.*

Demonstração. Como G e $\hat{\hat{G}}$ tem a mesma ordem, é suficiente provar que ϵ é injetiva, isto é, que se $x \neq 1 \in G$, então existe um caracter χ de G tal que $\chi(x) \neq 1$. Agora, seja H o subgrupo cíclico de G gerado por x. Pela observação (5) existe um caracter χ de H tal que $\chi(x) \neq 1$ e a proposição (3.3) mostra que χ estende para um caracter de G; daí o resultado desejado. □

Observação 6. *O mapa*

$$\begin{aligned} \chi : G &\to \mathbb{C} \\ x &\mapsto 1 \end{aligned}$$

é sempre um caracter de G. Denotamos este caracter por 1.

Proposição 3.6. *Seja $n = |G|$ e seja $\chi \in \hat{G}$.*

$$\sum_{x \in G} \chi(x) = \begin{cases} n, & \text{se } \chi = 1 \\ 0, & \text{se } \chi \neq 1. \end{cases}$$

Demonstração. A primeira fórmula é óbvia. Para provar a segunda, escolha $y \in G$ tal que $\chi(y) \neq 1$. Temos:

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x).$$

Segue então que:

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0.$$

Como $\chi(y) \neq 1$, isto implica que $\sum_{x \in G} \chi(x) = 0$. □

Corolário 3.6.1. *Seja $x \in G$. Então:*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n, & se\ x = 1 \\ 0, & se\ x \neq 1 \end{cases}$$

Demonstração. Isto segue diretamente da proposição (3.6) aplicada ao grupo dual $\hat{G}$. □

3.1.2 Caracteres Modulares

Seja $m \geq 1$ um inteiro. Nós denotamos por $G(m)$ o grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$ de elementos invertíveis do anel $\mathbb{Z}/m\mathbb{Z}$. Este é um grupo abeliano de ordem $\phi(m)$, onde ϕ é a função de Euler. Um elemento χ do dual de $G(m)$ é chamado um caracter módulo m; este pode ser visto como uma função, definida no conjunto dos inteiros primos com m, com valores em $\mathbb{C}^*$, e tal que $\chi(ab) = \chi(a)\chi(b)$. É conveniente estender como uma função em todo o $\mathbb{Z}$ definindo $\chi(a) = 0$ se a não é primo com m.

3.2 Séries de Dirichlet

Lema 3.7. *Seja U um aberto de $\mathbb{C}$ e seja f_n uma sequência de funções holomorfas em U que convergem uniformemente em todo o conjunto compacto para uma função f. Então f é holomorfa em U e as derivadas f_n' de f_n convergem uniformemente em todo subconjunto compacto para a derivada f' de f.*

Demonstração. Seja D um disco fechado contido em U e seja C a fronteira orientada da maneira usual. Pela fórmula de Cauchy, temos

$$f_n(z_0) = \frac{1}{2\pi i} \int_C \frac{f_n(z)}{z - z_0} dz$$

$\forall z_0$ no interior de D. Passando o limite, temos

$$f(z_0) = \frac{1}{2\pi i} \int_C \frac{f(z)}{z - z_0} dz,$$

que mostra que f é holomorfa no interior de D, e a primeira parte do lema segue. A segunda parte é demonstrada da mesma forma, utilizando a fórmula

$$f'(z_0) = \frac{1}{2\pi i} \int_C \frac{f(z)}{(z - z_0)^2} dz.$$

□

Lema 3.8 (Lema de Abel)**.** *Seja* (a_n) *e* (b_n) *duas sequências. Defina:*

$$A_{m,p} = \sum_{n=m}^{p} a_n, \qquad S_{m,m'} = \sum_{n=m}^{m'} a_n b_n.$$

Então temos

$$S_{m,m'} = A_{m,m'} b_{m'} + \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}).$$

Demonstração. Note inicialmente que

$$A_{m,n} - A_{m,n-1} = \sum_{i=m}^{n} a_i - \sum_{i=m}^{n-1} a_i = a_n.$$

Substituindo em $S_{m,m'}$ e rearranjando os termos, obtemos

$$\begin{aligned} S_{m,n'} &= \sum_{n=m}^{m'} (A_{m,n} - A_{m,n-1}) b_n \\ &= \sum_{n=m}^{m'} A_{m,n} b_n - \sum_{n=m}^{m'} A_{m,n-1} b_n \\ &= A_{m,m'} b_{m'} + \sum_{n=m}^{m'-1} A_{m,n} b_n - \sum_{n=m}^{m'-1} A_{m,n} b_{n+1} \\ &= A_{m,m'} b'_m + \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}). \end{aligned}$$

Como queríamos demonstrar. □

Lema 3.9. *Seja α, β dois números reais com $0 < \alpha < \beta$. Seja $z = x + iy$ com $x, y \in \mathbb{R}$ e $x > 0$. Então*

$$|e^{-\alpha z} - e^{-\beta z}| \leq \left|\frac{z}{x}\right| (e^{-\alpha x} - e^{-\beta x}).$$

Demonstração. Escrevemos

$$e^{-\alpha z} - e^{-\beta z} = -z \int_{\alpha}^{\beta} e^{-tz} dt.$$

Consequentemente, tomando valores absolutos, temos

$$|e^{-\alpha z} - e^{-\beta z}| \leq |z| \int_{\alpha}^{\beta} e^{-tx} dt = \frac{|z|}{x}(e^{-\alpha x} - e^{-\beta x}).$$

□

Seja (λ_n) uma sequência crescente de números reais tendendo para $+\infty$. Para simplificar, podemos supor que $\lambda_n \geq 0$.
Uma série de Dirichlet com expoentes (λ_n) é uma série da forma

$$\sum a_n e^{-\lambda_n z}.$$

Com $a_n, z \in \mathbb{C}$.

A partir de agora, $\Re(z)$ denotará a parte real de um número complexo z e $\arg(z)$ denotará seu argumento.

Proposição 3.10. *Se a série $f(z) = \sum a_n e^{-\lambda_n z}$ converge para $z = z_0$, então converge uniformemente em todo domínio da forma $\Re(z - z_0) > 0$, $\arg(z - z_0) \leq \frac{\pi}{2}$.*

Demonstração. Depois de fazer uma translação em z, nós podemos supor que $z_0 = 0$. A hipótese então significa que a série $\sum a_n$ é convergente. Nós podemos provar que existe uma convergência uniforme em todo domínio da forma $\Re(z) > 0$, $\frac{|z|}{\Re(z)} \leq k$.
Seja $\epsilon > 0$. Como a série $\sum a_n$ converge, $\exists N \in \mathbb{N}$ tal que $\forall m, m' \geq N$, nós temos que $|A_{m,m'}| \leq \epsilon$.
Aplicando o Lema (3.8) com $b_n = e^{-\lambda_n z}$, nós obtemos

$$S_{m,m'} = A_{m,m'} e^{-\lambda_{m'} z} + \sum_{n=m}^{m'-1} A_{m,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}).$$

Colocando $z = x + iy$ e aplicando o Lema (3.9), nós encontramos

$$\begin{aligned} |S_{m,m'}| &\leq \epsilon \left(1 + \frac{|z|}{x}\right) \sum_{m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) \\ &\leq \epsilon(1 + k(e^{-\lambda_m x} - e^{-\lambda_{m'} x})) \\ &\leq \epsilon(1 + k). \end{aligned}$$

E a convergência uniforme é clara. □

Corolário 3.10.1. *Se f converge para $z = z_0$, então converge para $\Re(z) > \Re(z_0)$ e a função assim definida é holomorfa.*

Corolário 3.10.2. *O conjunto de convergência da série f contém um semiplano aberto maximal (chamado semiplano de convergência).*

Por abuso de linguagem, consideraremos $\emptyset$ e $\mathbb{C}$ como semiplanos abertos. Se o semiplano de convergência é dado por $\Re(z) > \rho$ nós dizemos que ρ é a abscissa de convergência da série considerada.
(Os casos $\emptyset$ e $\mathbb{C}$ correspondem respectivamente a $\rho = +\infty$ e $\rho = -\infty$).

Corolário 3.10.3. *$f(z)$ converge para $f(z_0)$ quando $z \to z_0$ no domínio $\Re(z - z_0) > 0$, $\arg(z - z_0) \leq \dfrac{\pi}{2}$.*

Corolário 3.10.4. *A função $f(z)$ será identicamente nula se, e somente se todos os coeficientes a_n são nulos.*

Proposição 3.11. *Seja $f = \sum a_n e^{-\lambda_n z}$ uma série de Dirichlet cujos coeficientes $a_n \geq 0$ são reais. Suponha que f converge para $\Re(z) > \rho$, com $\rho \in \mathbb{R}$, e que f pode ser estendida analiticamente para uma função holomorfa em uma vizinhança do ponto $z = \rho$. Então $\exists \epsilon > 0$ tal que f converge para $\Re(z) > \rho - \epsilon$.*
(Em outras palavras, o domínio de convergência de f é limitado por uma singularidade de f localizada no eixo real.)

Demonstração. Substituindo z por $z - \rho$, nós podemos assumir que $\rho = 0$. Como f é holomorfa para $\Re(z) > 0$ e em uma vizinhança de 0, ela é holomorfa em um disco $|z - 1| \leq 1 + \epsilon$, com $\epsilon > 0$. Em particular, sua série de Taylor converge no disco. Pelo Lema (3.7), a p-ésima derivada de f é dada por

$$f^{(p)}(z) = \sum_n a_n (-\lambda_n)^p e^{-\lambda_n z}$$

para $\Re(z) > 0$. Consequentemente

$$f^{(p)}(1) = (-1)^p \sum_n \lambda_n^p a_n e^{-\lambda_n}.$$

A série de Taylor em questão pode ser escrita

$$f(z) = \sum_{p=0}^{\infty} \frac{1}{p!}(z-1)^p f^{(p)}(1), \quad |z-1| \leq 1+\epsilon.$$

Em particular para $z = -\epsilon$, temos

$$f(-\epsilon) = \sum_{p=0}^{\infty} \frac{1}{p!}(1+\epsilon)^p (-1)^p f^{(p)}(1)$$

com a série sendo convergente.
Mas $(-1)^p f^{(p)}(1) = \sum_n \lambda_n^p a_n e^{-\lambda_n}$ é uma série convergente com termos positivos.
Consequentemente a série dupla com termos positivos

$$f(-\epsilon) = \sum_{p,n} a_n \frac{1}{p!}(1+\epsilon)^p \lambda_n^p e^{-\lambda_n}$$

converge. Rearranjando os termos, obtemos

$$\begin{aligned} f(-\epsilon) &= \sum_n a_n e^{-\lambda_n} \sum_{p=0}^{\infty} \frac{1}{p!}(1+\epsilon)^p \lambda_n^p \\ &= \sum_n a_n e^{-\lambda_n} e^{\lambda_n(1+\epsilon)} = \sum a_n e^{\lambda_n \epsilon} \end{aligned}$$

que mostra que a série de Dirichlet converge para $z = -\epsilon$, portanto também converge para $\Re(z) > -\epsilon$. □

Proposição 3.12. *Se as somas parciais $A_{m,p} = \sum_m^p a_n$ são limitadas, então converge para $\Re(s) > 0$.*

Demonstração. Assuma que $|A_{m,p}| \leq K$. Aplicando o Lema de Abel, encontramos

$$|S_{m,m'}| \leq K \left(\sum_{n=m}^{m'-1} \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| + \left| \frac{1}{m'^s} \right| \right).$$

Nós podemos supor que s é real (pela proposição (3.10)). Isso nos permite escrever a desigualdade na forma

$$|S_{m,m'}| \leq \frac{K}{m^s}.$$

E a convergência é clara. □

3.2.1 A Função Zeta de Riemann

Durante o resto deste capítulo, P irá denotar o conjunto dos números primos.

Definição 3.13. *Uma função $f : \mathbb{N} \to \mathbb{C}$ é chamada multiplicativa se $f(1) = 1$ e*

$$f(mn) = f(m)f(n)$$

para quaisquer n e m que são relativamente primos.

Lema 3.14. *Seja f uma função multiplicativa. A série de Dirichlet $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converge absolutamente para $\Re(s) > 1$ e essa soma no domínio é igual ao produto infinito convergente*

$$\prod_{p \in P} (1 + f(p)p^{-s} + \cdots + f(p^m)p^{-ms} + \dots).$$

Lema 3.15. *([8], capítulo 6, lema 5) Se f satisfaz $f(nn') = f(n)f(n')$, $\forall n, n' \in \mathbb{N}$, temos*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in P} \frac{1}{1 - \dfrac{f(p)}{p^s}}.$$

Definição 3.16. *Aplicando o Lema (3.15) para a $f = 1$, obtemos a função zeta*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in P} \frac{1}{1 - \dfrac{1}{p^s}}.$$

Esta fórmula fazendo sentido para $\Re(s) > 1$.

Proposição 3.17. *(a) A função zeta é holomorfa e $\zeta(s) \neq 0$ no semiplano $\Re(s) > 1$.*

(b) Temos $\zeta(s) = \dfrac{1}{s-1} + \phi(s)$, onde $\phi(s)$ é holomorfa para $\Re(s) > 0$.

Demonstração. A afirmação (a) é clara. Para (b) nós observamos que

$$\frac{1}{s-1} = \int_1^{\infty} t^{-s} dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s} dt.$$

Consequentemente, podemos escrever

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s} dt \right) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s}) dt.$$

Defina agora

$$\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s})dt, \quad \phi(s) = \sum_{n=1}^{\infty} \phi_n(s).$$

Temos que mostrar que $\phi(s)$ está definida e é holomorfa para $\Re(s) > 0$. Mas está claro que cada $\phi_n(s)$ tem essa propriedade, então é suficiente provar que a série $\sum \phi_n$ converge normalmente em todo compacto para $\Re(s) > 0$. Temos

$$|\phi_n(s)| \leq \sup_{n \leq t \leq n+1} |n^{-s} - t^{-s}|$$

Mas a derivada da função $n^{-s} - t^{-s}$ é a igual a $\dfrac{s}{t^{s+1}}$. Disso nós obtemos

$$|\phi_n(s)| \leq \frac{|s|}{n^{x+1}}$$

com $x = \Re(s)$. E a série $\sum \phi_n$ converge normalmente para $\Re(s) \geq \epsilon$, $\forall \epsilon > 0$. □

Corolário 3.17.1. *A função zeta tem um polo simples em $s = 1$*

Corolário 3.17.2. *Quando $s \to 1$, temos $\sum_p p^{-s} \sim \ln \dfrac{1}{(s-1)}$, e $\sum_{p,k\geq 2} \dfrac{1}{p^{ks}}$ continua limitado.*

Demonstração. Temos

$$\ln \zeta(s) = \sum_{\substack{p \in P \\ k \geq 1}} \frac{1}{kp^{ks}} = \sum_{p \in P} \frac{1}{p^s} + \psi(s)$$

com $\psi(s) = \sum_{p \in P} \sum_{k \geq 2} \left(\dfrac{1}{kp^{ks}} \right)$. A série ψ é majorada pela série

$$\sum \frac{1}{p^{ks}} = \sum \frac{1}{p^s(p^{s-1})} \leq \sum \frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1.$$

Isto implica que ψ é limitada, e como o corolário (3.17.1) mostra que $\ln \zeta(s) \sim \ln \dfrac{1}{s-1}$, o corolário (3.17.2) segue. □

3.2.2 A Função Gamma

Definição 3.18. *A **função gamma** é dada pela integral absolutamente convergente*

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}$$

definida para $\Re(s) > 0$

Essa função obedece as seguintes regras

Proposição 3.19. *(i) A função gamma é analítica e admite uma continuação meromorfa para todo o* $\mathbb{C}$.

(ii) É não nula e tem polos simples em $s = -n$, $n = 0, 1, 2 \ldots$, *com resíduos* $(-1)^n/n!$. *Não existem outros polos.*

(iii) Satisfaz as equações funcionais

1) $\Gamma(s+1) = s\Gamma(s)$,

2) $\Gamma(s)\Gamma(1-s) = \dfrac{\pi}{\sin(\pi s)}$,

3) $\Gamma(s)\Gamma(s+\frac{1}{2}) = \frac{s\sqrt{\pi}}{2^{2s}}\Gamma(2s)$, ***(fórmula de duplicação de Legendre)***

(iv) Tem valores especiais $\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(1) = 1$, $\Gamma(k+1) = k!$ $k = 0, 1, 2, \ldots$.

Para relacionar a função gamma com a função zeta, comece com a substituição $y \mapsto \pi n^2 y$, que nos dá a equação

$$\pi^{-s}\Gamma(s)\frac{1}{n^{2s}} = \int_0^\infty e^{-\pi n^2 y} y^s \frac{dy}{y}.$$

Agora somemos sobre todos os $n \in \mathbb{N}$ e obtenhamos

$$\pi^{-s}\Gamma(s)\zeta(2s) = \int_0^\infty \sum_{n=1}^\infty e^{-\pi n^2 y} y^s \frac{dy}{y}.$$

Observemos que é possível trocar o somatório e a integral pois

$$\begin{aligned}\sum_{n=1}^\infty \int_0^\infty |e^{-\pi n^2 y} y^s| \frac{dy}{y} &= \sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 y} y^{\Re(s)} \frac{dy}{y} \\ &= \pi^{-\Re(s)}\Gamma(\Re(s))\zeta(2\Re(s)) < \infty\end{aligned}$$

Agora a série sob a integral,

$$g(y) = \sum_{n=1}^{\infty} e^{-\pi n^2 y},$$

surge da **série theta de Jacobi** clássica

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z} = 1 + 2\sum_{n=1}^{\infty} e^{\pi i n^2 z},$$

isto é, temos $g(y) = \frac{1}{2}(\theta(iy) - 1)$. A função

$$Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$$

é chamada a **função zeta completada**. Nós obtemos a seguinte proposição.

Proposição 3.20. *A função zeta completada $Z(s)$ admite a representação integral*

$$Z(s) = \frac{1}{2}\int_0^{\infty} (\theta(iy) - 1)y^{s/2}\frac{dy}{y}.$$

A demonstração da equação funcional para a função $Z(s)$ é baseada no princípio geral apresentado à seguir. Para uma função continua $f : \mathbb{R}_+^* \to \mathbb{C}$ no grupo $\mathbb{R}_+^*$ de números reais positivos, definimos a **transformada de Mellin** sendo a integral imprópria

$$L(f, s) = \int_0^{\infty} (f(y) - f(\infty))y^s\frac{dy}{y},$$

fornecido o limite $f(\infty) = \lim_{y\to\infty} f(y)$ e a integral existe. O teorema seguinte é de fundamental importância também para aplicações futuras. Muitas vezes nos referimos a ele como **princípio de Mellin**.

Teorema 3.21. *Sejam $f, g : \mathbb{R}_+^* \to \mathbb{C}$ funções continuas tais que*

$$f(y) = a_0 + O(e^{-cy^\alpha}), \quad g(y) = b_0 + O(e^{-cy^\alpha}),$$

para $y \to \infty$, com constantes positivas c, α. Se essas funções satisfazem a equação

$$f\left(\frac{1}{y}\right) = Cy^k g(y),$$

para algum número real $k > 0$ e algum número complexo $C \neq 0$, então temos:

(i) As integrais $L(f,s)$ e $L(g,s)$ convergem absolutamente e uniformemente se s varia em um domínio compacto arbitrário contido em $\{s \in \mathbb{C} \mid \Re(s) > k\}$. Além disso elas são funções holomorfas em $\{s \in \mathbb{C} \mid \Re(s) > k\}$ e admitem continuações holomorfas para $\mathbb{C} \setminus \{0, k\}$.

(ii) Elas tem polos simples em $s = 0$ e $s = k$ com resíduos

$$\operatorname*{Res}_{s=0}(L(f,s)) = -a_0, \qquad \operatorname*{Res}_{s=k}(L(f,s)) = Cb_0,$$
$$\operatorname*{Res}_{s=0}(L(g,s)) = -b_0, \qquad \operatorname*{Res}_{s=k}(L(g,s)) = C^{-1}a_0,$$

respectivamente.

(iii) Elas satisfazem a equação funcional

$$L(f,s) = CL(g,k-s).$$

Observação 7. *O simbolo $\phi(y) = O(\psi(y))$ significa que temos $\phi(y) = c(y)\psi(y)$, para alguma função $c(y)$ que permanece limitada sob o limite em questão, no nosso caso, quando $y \to \infty$.*

Observação 8. *A condição (ii) diz que não existe polo caso $a_0 = 0$ ou $b_0 = 0$, respectivamente. Mas existe um polo, que é simples, se $a_0 \neq 0$ ou $b_0 \neq 0$, respectivamente.*

Demonstração. Se s varia sobre um subconjunto compacto de $\mathbb{C}$, então a função $e^{-cy^\alpha}y^\sigma$, $\sigma = \Re(s)$, é limitada para $y \geq 1$ por uma contante que é independente de σ. Assim sendo a condição $f(y) = a_0 + O(e^{-cy^\alpha})$ nos dá a seguinte limitante superior para a integral de Mellin $L(f,s)$.

$$|(f(y) - a_0)y^{s-1}| \leq Be^{-cy^\alpha}y^{\sigma+1}y^{-2} \leq B'\frac{1}{y^2},$$

para todo $y \geq 1$, com constantes B, B'. A integral $\int_1^\infty (f(y)-a_0)y^{s-1}dy$ portanto admite uma majoração convergente $\int_1^\infty \frac{B'}{y^2}dy$ que é independente de s. Converge, portanto, uniforme e absolutamente, para todo s no subconjunto compacto. O mesmo acontece para $\int_1^\infty (g(y) - b_0)y^{s-1}dy$.
Agora seja $\Re(s) > k$. Nós dividimos o intervalo de integração $(0,\infty)$ em $(0,1]$ e $(1,\infty)$ e escrevemos

$$L(f,s) = \int_1^\infty (f(y) - a_0)y^s\frac{dy}{y} + \int_0^\infty (f(y) - a_0)y^s\frac{dy}{y}.$$

Para a segunda integral, a substituição $y \mapsto 1/y$ e a equação $f(1/y) = Cy^k g(y)$ nos dá:

$$\begin{aligned}\int_0^1 (f(y) - a_0)y^s \frac{dy}{y} &= -a_0 \frac{y^s}{s}\Big|_0^1 + \int_1^\infty f\left(\frac{1}{y}\right) y^{-s} \frac{dy}{y} \\ &= -\frac{a_0}{s} + C\int_1^\infty (g(y) - b_0)y^{k-s-1}dy - \frac{Cb_0}{k-s}.\end{aligned}$$

Pelo que segue acima, ela também converge uniforme e absolutamente para $\Re(s) > k$. Nós assim obtemos

$$L(f, s) = -\frac{a_0}{s} + \frac{Cb_0}{s-k} + F(s)$$

onde

$$F(s) = \int_1^\infty [(f(y) - a_0)y^s + C(g(y) - b_0)y^{k-s}]\frac{dy}{y}.$$

Trocando f e g, vemos de $g(1/y) = C^{-1}y^k f(y)$ que:

$$L(g, s) = -\frac{b_0}{s} + \frac{C^{-1}a_0}{s-k} + G(s)$$

onde

$$G(s) = \int_1^\infty [(g(y) - b_0)y^s + C^{-1}(f(y) - a_0)y^{k-s}]\frac{dy}{y}.$$

As integrais $F(s)$ e $G(s)$ convergem absolutamente e localmente uniformes em todo o plano complexo, como vimos acima. Então elas representam funções holomorfas, e claramente temos $F(s) = CG(k-s)$. Portanto $L(f, s)$ e $L(g, s)$ tem continuações para todo o $\mathbb{C} \setminus \{0, k\}$ e temos $L(f, s) = CL(g, k-s)$. Isto encerra a demonstração do teorema. □

O resultado pode agora ser aplicado à integral da proposição (3.20) representando a função $Z(s)$.

3.2.3 As Funções L

Seja $m \geq 1$ um inteiro e seja χ um caracter módulo m. A função L correspondente é definida pela série de Dirichlet

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Note que, nesta soma, apenas os inteiros n que são primos com m dão uma contribuição não nula.

Proposição 3.22. *Para $\chi = 1$, temos*

$$L(s,1) = F(s)\zeta(s), \quad \text{com } F(s) = \prod_{\substack{p|m \\ p\in P}} (1 - p^{-s}).$$

Em particular $L(s,1)$ estende analiticamente para $\Re(s) > 0$ e tem um polo simples em $s = 1$.

Proposição 3.23. *Para $\chi \neq 1$ a série $L(s,\chi)$ converge (resp. converge absolutamente) no semiplano $\Re(s) > 0$ (resp. $\Re(s) > 1$); temos*

$$L(s,\chi) = \prod_{p\in P} \frac{1}{1 - \dfrac{\chi(p)}{p^s}} \quad \text{para } \Re(s) > 1.$$

Demonstração. A afirmação sobre $\Re(s) > 1$ segue dos Lemas (3.14) e (3.15). Resta mostrar a convergência da série para $\Re(s) > 0$. Usando a proposição (3.12), é suficiente ver que a soma, com $u \leq v$

$$A_{u,v} = \sum_{u}^{v} \chi(n)$$

é limitada. Pela proposição (3.6), nós temos

$$\sum_{u}^{u+m-1} \chi(n) = 0.$$

Consequentemente é suficiente majorar a soma $A_{u,v}$ para $v - u < m$. Temos

$$|A_{u,v}| \leq \phi(m).$$

A proposição então segue. □

Vamos definir uma função $\zeta_m(s)$ pela fórmula

$$\zeta_m(s) = \prod_{\chi\in\hat{G}(m)} L(s,\chi)$$

Proposição 3.24. *Temos*

$$\zeta_m(s) = \prod_{p\nmid m} \frac{1}{\left(1 - \dfrac{1}{p^{f(p)s}}\right)^{g(p)}}$$

onde $g(p) = \dfrac{\phi(m)}{f(p)}$. Esta é uma série de Dirichlet, com coeficiente inteiros positivos, convergindo no semiplano $\Re(s) > 1$.

Teorema 3.25. *(a) ζ_m tem um polo simples em $s = 1$.*

(b) $L(1, \chi) \neq 0$, $\forall \chi \neq 1$.

Demonstração. É fácil ver que $(b) \implies (a)$. De fato, se $L(1, \chi) \neq 0 \ \forall \chi \neq 1$, o fato de que $L(s, 1)$ tem um polo simples em $s = 1$ mostra que o mesmo é verdadeiro para ζ_m. Portanto, basta provar (b).
Suponha agora que $L(1, \chi) = 0$ para algum $\chi \neq 1$. Então a função ζ_m seria holomorfa em $s = 1$, assim como para todo s tal que $\Re(s) > 0$ (proposições (3.22) e (3.23)). Como é uma série de Dirichlet com coeficientes positivos, esta série convergiria para todo s no mesmo domínio (proposição (3.11)). Mas isso é um absurdo.
De fato, o p-ésimo fator de ζ_m é igual a

$$\frac{1}{(1 - p^{-f(p)s})^{g(p)}} = (1 + p^{-f(p)s} + p^{-2f(p)s} + \dots)$$

e domina a série

$$1 + p^{-\phi(m)s} + p^{-2\phi(m)s} + \dots$$

Isto segue do fato de que ζ_m tem todos os seus coeficientes maiores do que os da série

$$\sum_{(n,m)=1} n^{-\phi(m)s}.$$

Que diverge para $s = \dfrac{1}{\phi(m)}$. Isso conclui a prova. □

3.3 Teorema das Progressões Aritméticas

3.3.1 Densidade

Seja P o conjunto dos números primos. Nós vimos no corolário (3.17.2) que quando $s \to 1$, temos

$$\sum_{p \in P} \frac{1}{p^s} \sim \ln \frac{1}{s - 1}.$$

Seja $A \subset P$. Dizemos que A tem como densidade um número real k quando a razão

$$\frac{\left(\sum_{p \in A} \dfrac{1}{p^s} \right)}{\left(\ln \dfrac{1}{s - 1} \right)}$$

tende para k quando $s \to 1$. (Claramente, temos $0 \leq k \leq 1$).

3.3.2 Lemas

Seja χ um caracter de $G(m)$ (de acordo com a definição dada na seção (3.1.2)). Defina:

$$f_\chi(s) = \sum_{p\nmid m} \frac{\chi(p)}{p^s}.$$

Esta série será convergente para $s > 1$.

Lema 3.26. *Se $\chi = 1$, então $f_\chi \sim \ln\left(\frac{1}{s-1}\right)$ quando $s \to 1$.*

Demonstração. De fato, f_1 difere da série $\sum \frac{1}{p^s}$ apenas por um número finito de termos. □

Lema 3.27. *Se $\chi \neq 1$, f_χ continua limitada quando $s \to 1$.*

Demonstração. Nós usaremos o logaritmo da função $L(s,\chi)$. Para isso, precisaremos ser um pouco mais precisos.
$L(s,\chi)$ é definido pelo produto $\prod \frac{1}{(1-\chi(p)p^{-s})}$. Para $\Re(s) > 1$, cada fator é da forma $\frac{1}{(1-\alpha)}$ com $|\alpha| < 1$. Nós definimos $\ln\frac{1}{1-\alpha}$ como $\sum_{n=1}^{\infty}\frac{\alpha^n}{n}$ e definimos $\ln L(s,\chi)$ pela série (claramente convergente)

$$\begin{aligned}\ln L(s,\chi) &= \sum \ln \frac{1}{1-\chi(p)p^{-s}} \\ &= \sum_{p,n} \frac{\chi(p)^n}{np^{ns}}\end{aligned}$$

com $\Re(s) > 1$. Nós agora dividimos $\ln L(s,\chi)$ em duas partes

$$\ln L(s,\chi) = f_\chi(s) + F_\chi(s)$$

onde

$$F_\chi(s) = \sum_{p,n\geq 2} \frac{\chi(p)^n}{np^{ns}}.$$

O teorema (3.25), junto com o corolário (3.17.2) mostram que $L(s,\chi)$ e $F_\chi(s)$ continuam limitadas quando $s \to 1$.
Consequentemente, o mesmo acontece para $f_\chi(s)$, o que prova o lema. □

Sejam $m \geq 1$ e $a \geq 1$ tal que $(a, m) = 1$. Chame P_a o conjunto de números primos tais que $p \equiv a \ (mod\ m)$. Vamos definir

$$g_a(s) = \sum_{p \in P_a} \frac{1}{p^s}.$$

Lema 3.28. *Temos* $g_a(s) = \dfrac{1}{\phi(m)} \sum_{\chi \in \hat{G}(m)} \chi(a)^{-1} f_\chi(s)$.

Demonstração. A função $\sum \chi(a)^{-1} f_\chi(s)$ pode ser escrita, substituindo f_χ por sua definição

$$\sum_{p \nmid m} \frac{\left(\sum_{\chi \in \hat{G}(m)} \chi(a^{-1}) \chi(p) \right)}{p^s}.$$

Mas $\chi(a^{-1})\chi(p) = \chi(a^{-1}p)$. Pelo corolário (3.6.1) nós temos

$$\sum_{\chi \in \hat{G}(m)} \chi(a^{-1}p) = \begin{cases} \phi(m), & \text{se } a^{-1}p \equiv 1 \bmod m \\ 0, & \text{em outros casos.} \end{cases}$$

Consequentemente, nós encontramos a função $\phi(m) g_a(s)$. □

Teorema 3.29 (Teorema das Progressões Aritméticas)**.** *Sejam* $m \geq 1$ *e* $a \geq 1$ *tal que* $(a, m) = 1$. *O conjunto* P_a *de números primos tais que* $p \equiv a$ $(mod\ m)$ *tem densidade* $\dfrac{1}{\phi(m)}$.

Demonstração. O lema (3.26) mostra que $f_\chi(s) \sim \ln\left(\dfrac{1}{s-1}\right)$ para $\chi = 1$, e o lema (3.27) mostra que todos as outras f_χ continuam limitados. Usando o lema (3.28), vemos que $g_a(s) \sim \dfrac{1}{\phi(m)} \ln \dfrac{1}{s-1}$, e isso significa que a densidade de P_a é $\dfrac{1}{\phi(m)}$, como queríamos demonstrar. □

Corolário 3.29.1. *O conjunto* P_a *é infinito.*

Demonstração. É fácil ver que todo conjunto finito têm densidade 0. Portanto P_a será infinito. □

Capítulo 4

Teorema da Densidade de Dirichlet

4.1 A Função Zeta de Dedekind

A função zeta de Riemann $\zeta(s) = \sum_{k=1}^{\infty} k^{-s}$ está associada ao corpo $\mathbb{Q}$ de números racionais. Podemos generalizá-la para um corpo numérico arbitrário K de grau $n = [K : \mathbb{Q}]$.

Definição 4.1. *A **função zeta de Dedekind** do corpo numérico K é definida pela série*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s},$$

onde $\mathfrak{a}$ varia sobre todos os ideais inteiros de K, e $\mathfrak{N}(a)$ denota sua norma absoluta.

Proposição 4.2. *A série $\zeta_K(s)$ converge absolutamente e uniformemente no domínio $\Re(s) \geq 1 + \delta$ para todo $\delta > 0$, e temos*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}},$$

onde $\mathfrak{p}$ percorre todos os ideais primos de K.

Definição 4.3. *O **discriminante** de uma base $\alpha_1, \ldots, \alpha_n$ de uma extensão separável $L|K$ é definido por*

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

onde σ_i, $i = 1, \ldots, n$, varia sobre as K-imersões $L \to \overline{K}$.

No caso especial de uma base inteira $\omega_1, \ldots, \omega_n$ de $\mathcal{O}_K$ nós obtemos o **discriminante do corpo algébrico numérico** K,

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \ldots, \omega_n).$$

Para as funções zeta parciais

$$\zeta(\mathfrak{K}, s) = \sum_{\mathfrak{b} \in \mathfrak{K} \text{ inteiro}} \frac{1}{\mathfrak{N}(\mathfrak{b})^s},$$

obtemos o resultado a seguir, onde as notações d_K, R, w, e r significam, respectivamente, o discriminante, o regulador, o número de raízes da unidade, e o número de lugares infinitos.

Teorema 4.4. *A função*

$$Z(\mathfrak{K}, s) = Z_\infty(s)\zeta(\mathfrak{K}, s), \quad \Re(s) > 1,$$

$Z_\infty(s) = |d_K|^{s/2}\pi^{-ns/2}\Gamma_K(s/2)$, *admite uma continuação analítica para* $\mathbb{C} \setminus \{0, 1\}$ *e satisfaz a equação funcional*

$$Z(\mathfrak{K}, s) = Z(\mathfrak{K}', 1 - s),$$

onde as classes de ideais $\mathfrak{K}$ *e* $\mathfrak{K}'$ *correspondem uma à outra por* $\mathfrak{K}\mathfrak{K}' = [\mathfrak{d}]$. *Ela tem polos simples em* $s = 0$ *e* $s = 1$ *com resíduos*

$$-\frac{2^r}{w}R \quad e \quad \frac{2^r}{w}R, \text{ respectivamente.}$$

Esse teorema sobre as funções zeta parciais imediatamente implica um resultado análogo para a **função zeta completa** do corpo numérico K,

$$Z_K(s) = Z_\infty(s)\zeta_K(s) = \sum_{\mathfrak{K}} Z(\mathfrak{K}, s).$$

Corolário 4.4.1. *A função zeta completa* $Z_K(s)$ *admite uma continuação analítica para* $\mathbb{C} \setminus [0, 1]$ *e satisfaz a equação funcional*

$$Z_K(s) = Z_K(1 - s).$$

Apresentando polos simples em $s = 0$ *e* $s = 1$, *com resíduos*

$$-\frac{2^r hR}{w} \quad e \quad \frac{2^r hR}{w}, \text{ respectivamente,}$$

onde h *é o número de classe de* K.

O último resultado pode imediatamente ser generalizado como segue. Para cada caracter

$$\chi : J/P \longrightarrow \mathbb{C}^*$$

do grupo de classes ideal, podemos formar a função zeta

$$Z(\chi, s) = Z_\infty(s)\zeta(\chi, s),$$

onde

$$\zeta(\chi, s) = \sum_{\mathfrak{a} \text{ inteiro}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}$$

e $\chi(\mathfrak{a})$ denota o valor $\chi(\mathfrak{K})$ da classe $\mathfrak{K} = [\mathfrak{a}]$ de um ideal $\mathfrak{a}$. Então claramente

$$Z(\chi, s) = \sum_{\mathfrak{K}} \chi(\mathfrak{K}) Z(\mathfrak{K}, s),$$

e em vista de $\mathfrak{K}' = \mathfrak{K}^{-1}[\mathfrak{d}]$, nós obtemos do teorema (4.4) a equação funcional

$$Z(\chi, s) = \chi(\mathfrak{d}) Z(\overline{\chi}, 1 - s).$$

Se $\chi \neq 1$, então $Z(\chi, s)$ é holomorfa em todo $\mathbb{C}$, visto que $\sum_{\mathfrak{K}} \chi(\mathfrak{K}) = 0$. Concluímos agora com a função zeta de Dedekind original

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s}, \quad \Re(s) > 1.$$

O fator de Euler no infinito, $Z_\infty(s)$, é dado explicitamente como

$$Z_\infty(s) = |d_K|^{s/2} L_X(s) = |d_K|^{s/2} L_{\mathbb{R}}(s)^{r_1} L_{\mathbb{C}}(s)^{r_2},$$

onde r_1 e r_2 denotam o número de lugares reais e complexos, respectivamente.

Corolário 4.4.2. *(i) A função zeta de Dedekind $\zeta_K(s)$ tem uma continuação analítica para $\mathbb{C} \setminus \{1\}$.*

(ii) Em $s = 1$ tem um polo simples com resíduo

$$\kappa = \frac{2^{r_1}(2\pi)^{r_2}}{w|d_K|^{1/2}} hR.$$

Onde h denota o número de classe e $w = \#\mu(K)$ denota o número de raízes da unidade em K.

4.2 Densidade

Utilizando as L-séries, agora iremos conseguir generalizar o Teorema das Progressões Aritméticas para ideais primos.

Definição 4.5. *Seja M um conjunto de ideais primos de K. O limite*

$$d(M) = \lim_{s\to 1^+} \frac{\sum\limits_{\mathfrak{p}\in M} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum\limits_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{-s}},$$

quando existe, é chamado de ***densidade de Dirichlet*** *de M.*

Da expansão

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-\mathfrak{N}(\mathfrak{p})^{-s}}, \quad \Re(s) > 1,$$

obtemos que

$$\ln \zeta_K(s) = \sum_{\mathfrak{p},m} \frac{1}{m\mathfrak{N}(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}} + \sum_{\mathfrak{p},m\geq 2} \frac{1}{m\mathfrak{N}(\mathfrak{p})^{ms}}.$$

O último somatório define uma função analítica em $s = 1$. Nós escreveremos $f(s) \sim g(s)$ se $f(s) - g(s)$ é uma função analítica em $s = 1$. Então nós temos

$$\ln \zeta_K(s) \sim \sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}(p)^{s}} \sim \sum_{\deg(\mathfrak{p})=1} \frac{1}{\mathfrak{N}(p)^{s}},$$

pois a soma $\sum_{\deg(\mathfrak{p})\geq 2} \mathfrak{N}(\mathfrak{p})^{-s}$ tomada sobre todos os $\mathfrak{p}$ de grau ≥ 2 é analítica em $s = 1$. Além disso, por (4.4.2), temos $\zeta_K(s) \sim \frac{1}{s-1}$, e então

$$\sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}} \sim \ln \frac{1}{s-1}.$$

Portanto, podemos escrever a densidade de Dirichlet como

$$d(M) = \lim_{s\to 1^+} \frac{\sum\limits_{\mathfrak{p}\in M} \mathfrak{N}(\mathfrak{p})^{-s}}{\ln \frac{1}{s-1}}.$$

Como a soma $\sum \mathfrak{N}(\mathfrak{p})^{s-1}$ sobre todos os ideais primos de grau > 1 converge, a definição da densidade de Dirichlet apenas depende dos ideais primos de grau 1 em M. Adicionar ou omitir uma quantidade finita de ideais primos também

não muda nada em relação à existência ou mesmo ao valor da densidade de Dirichlet.
Frequentemente consideramos também a **densidade natural**

$$\delta(M) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in M \mid \mathfrak{N}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \mid \mathfrak{N}(\mathfrak{p}) \leq x\}}.$$

A existência de $\delta(M)$ implica na existência de $d(M)$, e nesse caso temos $\delta(M) = d(M)$. A recíproca não é sempre verdadeira.

Lema 4.6. *Seja χ um caracter não trivial de $J^{\mathfrak{m}}/P^{\mathfrak{m}}$. Então a L-série de Hecke*

$$L(\chi, s) = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}$$

($\chi(\mathfrak{p}) = 0$ para $\mathfrak{p}|\mathfrak{m}$) satisfaz

$$L(\chi, 1) \neq 0.$$

Teorema 4.7 (Teorema da Densidade de Dirichlet)**.** *Seja $\mathfrak{m}$ um módulo de K e $H^{\mathfrak{m}}$ um grupo ideal tal que $J^{\mathfrak{m}} \supseteq H^{\mathfrak{m}} \supseteq P^{\mathfrak{m}}$ com índice $h_{\mathfrak{m}} = [J^{\mathfrak{m}} : H^{\mathfrak{m}}]$. Para cada classe $\mathfrak{K} \in J^{\mathfrak{m}}/H^{\mathfrak{m}}$, o conjunto $P(\mathfrak{K})$ de ideais primos em $\mathfrak{K}$ tem densidade*

$$d(P(\mathfrak{K})) = \frac{1}{h_{\mathfrak{m}}}.$$

Demonstração. Exatamente como para a função zeta de Dedekind, nós obtemos para a L-série de Dirichlet que

$$\ln L(\chi, s) \sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s} = \sum_{\mathfrak{K}' \in J^{\mathfrak{m}}/P^{\mathfrak{m}}} \chi(\mathfrak{K}') \sum_{\mathfrak{p}\in\mathfrak{K}'} \frac{1}{\mathfrak{N}(\mathfrak{p})^s}.$$

Multiplicando por $\chi(\mathfrak{K}^{-1})$ e somando sobre todos os χ (irredutíveis) obtemos

$$\ln \zeta_K(s) + \sum_{\chi\neq 1} \chi(\mathfrak{K}^{-1}) \ln L(\chi, s) \sim \sum_{\mathfrak{K}' \in J^{\mathfrak{m}}/P^{\mathfrak{m}}} \sum_{\chi} \chi(\mathfrak{K}'\mathfrak{K}^{-1}) \sum_{\mathfrak{p}\in\mathfrak{K}'} \frac{1}{\mathfrak{N}(\mathfrak{p})^s}.$$

Como $L(\chi, 1) \neq 0$, $\ln L(\chi, s)$ é analítica em $s = 1$. Mas

$$\sum_{\chi} \chi(\mathfrak{K}'\mathfrak{K}^{-1}) = \begin{cases} 0, & \text{se } \mathfrak{K}' \neq \mathfrak{K} \\ h_{\mathfrak{m}}, & \text{se } \mathfrak{K}' = \mathfrak{K}. \end{cases}$$

Consequentemente nós obtemos

$$\ln \frac{1}{s-1} \sim \ln \zeta_K(s) \sim h_{\mathfrak{m}} \sum_{\mathfrak{p}\in\mathfrak{K}} \frac{1}{\mathfrak{N}(\mathfrak{p})^s},$$

e o teorema está demonstrado. □

O teorema nos mostra, em particular, que a densidade dos ideais primos em uma classe de $J^{\mathfrak{m}}/H^{\mathfrak{m}}$ é a mesma para cada classe, isto é, os ideais primos estão equidistribuidos ao longo das classes. No caso $K = \mathbb{Q}$, $\mathfrak{m} = (m)$, e $H^{\mathfrak{m}} = P^{\mathfrak{m}}$, temos $J^{\mathfrak{m}}/P^{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^*$, que corresponde ao teorema das progressões aritméticas visto no capítulo (3).

Capítulo 5

Teorema da Densidade de Tchebotarëv

5.1 O Teorema

Seja

1. L/K uma extensão de corpos numéricos.
2. v_K uma valoração discreta normalizada por $v_K(K^*) = \mathbb{Z}$,
3. $\mathcal{O}_K = \{a \in K \mid v_K(a) \geq 0\}$ o anel de valoração,
4. $\mathfrak{p}_K = \{a \in K \mid v_K(a) > 0\}$ o ideal maximal de $\mathcal{O}_K$,
5. $U_K = \{a \in K^* \mid v_K(a) = 0\}$ o grupo unitário de $\mathcal{O}_K$,
6. $U_K^{(n)} = 1 + \mathfrak{p}_K^n$ o grupo de n-ésimas unidades superiores de $\mathcal{O}_K$, $n = 1, 2, \ldots$.

Observação 9. *Note que $\mathcal{O}_K$, $\mathfrak{p}_K$, U_K e $U_K^{(n)}$ dependem da valoração escolhida, uma vez que existem infinitas valorações não-equivalentes.*

Exemplo 5.1. *Para o caso $K = \mathbb{Q}$, veja a proposição (2.17).*

Definição 5.1. *Se $\mathfrak{P}$ é um ideal primo de $\mathcal{O}_L$, então o subgrupo*

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

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

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

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

Teorema 5.2. *Para todo subgrupo aberto $\mathcal{N}$ de índice finito em K^*, existe uma extensão abeliana L/K tal que $N_{L/K}L^* = \mathcal{N}$. Este é o* ***corpo de classe*** *de $\mathcal{N}$.*

Definição 5.3. *Seja L/K uma extensão abeliana finita, e n o menor número ≥ 0 tal que $U_K^{(n)} \subseteq N_{L/K}L^*$, onde definimos $U_K^{(0)} = U_K$. Então o ideal*

$$\mathfrak{f} = \mathfrak{p}_K^n$$

é chamado de ***condutor*** *de L/K.*

Exemplo 5.2. *Considere $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ onde d é um inteiro livre de quadrados. Então, ([6], exemplo 3.11)*

$$\mathfrak{f} = \begin{cases} \mathfrak{p}^{|d_{\mathbb{Q}(\sqrt{d})}|}, & \text{para } d > 0 \\ \mathfrak{p}^{\infty|d_{\mathbb{Q}(\sqrt{d})}|}, & \text{para } d < 0 \end{cases},$$

onde $d_{\mathbb{Q}(\sqrt{d})}$ é o discriminante de $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ e $\mathfrak{p} = \mathfrak{p}_{\mathbb{Q}(\sqrt{d})}$.

Teorema 5.4. *Se L/K é uma extensão Galoisiana de corpos numéricos, e $\mathfrak{P}$ um ideal primo que não se ramifica sobre K (i.e., $\mathfrak{p} = \mathfrak{P} \cap K$ não se ramifica em L), então existe um único automorfismo $\varphi_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ tal que*

$$\varphi_{\mathfrak{P}} a \equiv a^q \bmod \mathfrak{P}$$

para todo $a \in \mathcal{O}_L$, onde $q = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})]$. Este é chamado de Automorfismo de Frobenius. O grupo de decomposição $G_{\mathfrak{P}}$ é cíclico e $\varphi_{\mathfrak{P}}$ é um gerador de $G_{\mathfrak{P}}$.
Vamos denotar

$$\varphi_{\mathfrak{P}} =: \left(\frac{L/K}{\mathfrak{P}}\right).$$

Observação 10. *Vale observar aqui que, de acordo com nossa definição de ramificação (Definição (1.29)), ao escrever $\mathfrak{P} \cap K$ queremos dizer mais precisamente $\mathfrak{P} \cap \mathcal{O}_K$, ou seja, a interseção se dá com o anel de inteiros de K.*

Definição 5.5. *Para qualquer ideal $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$ de K, definimos*

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}}\right)^{\nu_{\mathfrak{p}}}$$

$\left(\frac{L/K}{\mathfrak{a}}\right)$ *é chamado de* ***símbolo de Artin****.*

Teorema 5.6. *Seja L/K uma extensão abeliana, e seja $\mathfrak{m}$ um módulo de definição para ela. Então o símbolo de Artin induz um homomorfismo sobrejetivo*

$$\left(\frac{L/K}{\phantom{\mathfrak{a}}}\right) : Cl_K^{\mathfrak{m}} \to G(L/K)$$

com núcleo $H^{\mathfrak{m}}/P_K^{\mathfrak{m}}$, onde $H^{\mathfrak{m}} = (N_{L/K}J_L^{\mathfrak{m}})P_K^{\mathfrak{m}}$, e nós temos um diagrama comutativo exato

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N_{L/K}C_L & \longrightarrow & C_K & \xrightarrow{(\ \ ,L/K)} & G(L/K) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H^{\mathfrak{m}}/P_K^{\mathfrak{m}} & \longrightarrow & Cl_K^{\mathfrak{m}} & \xrightarrow{\left(\frac{L/K}{\phantom{\mathfrak{a}}}\right)} & G(L/K) & \longrightarrow & 1 \end{array}$$

Demonstração. Demonstração em [7], capítulo VI, teorema (7.1). □

Corolário 5.6.1. *O símbolo de Artin $\left(\frac{L/K}{\mathfrak{a}}\right)$, para $\mathfrak{a} \in J_K^{\mathfrak{m}}$, só depende da classe de $\mathfrak{a}$ mod $P_K^{\mathfrak{m}}$. Ele define um isomorfismo*

$$\left(\frac{L/K}{\phantom{\mathfrak{a}}}\right) : J_K^{\mathfrak{m}}/H^{\mathfrak{m}} \xrightarrow{\sim} G(L/K)$$

Teorema 5.7 (Lei de Decomposição)**.** *Seja L/K uma extensão abeliana de grau n, e seja $\mathfrak{p}$ um ideal primo que não se ramifica. Seja $\mathfrak{m}$ um módulo de definição para L/K que não é divisível por $\mathfrak{p}$ (por instância o condutor), e seja $H^{\mathfrak{m}}$ o grupo ideal correspondente.*
Se f é a ordem de $\mathfrak{p}$ mod $H^{\mathfrak{m}}$ no grupo de classe $J_K^{\mathfrak{m}}/H^{\mathfrak{m}}$, isto é, o menor inteiro positivo tal que

$$\mathfrak{p}^f \in H^{\mathfrak{m}},$$

então $\mathfrak{p}$ decompõe em L em um produto

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

de $r = n/f$ primos distintos de grau f sobre $\mathfrak{p}$.

Demonstração. Seja $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ a decomposição prima de $\mathfrak{p}$ em L. Como $\mathfrak{p}$ não se ramifica, os $\mathfrak{P}_i$ são todos distintos e têm o mesmo grau f. Esse grau é a ordem do grupo de decomposição de $\mathfrak{P}_i$ sobre K, isto é, a ordem do automorfismo de Frobenius $\varphi_{\mathfrak{p}} = \left(\frac{L/K}{\mathfrak{p}}\right)$. Em vista do isomorfismo $J_K^{\mathfrak{m}}/H^{\mathfrak{m}} \cong G(L/K)$, está é também a ordem de $\mathfrak{p}$ mod $H^{\mathfrak{m}}$ em $J_K^{\mathfrak{m}}/H^{\mathfrak{m}}$. Isto finaliza a demonstração. □

O teorema mostra em particular que os ideais primos que fatoram completamente são precisamente aqueles contidos no grupo ideal $H^{\mathfrak{f}}$, se $\mathfrak{f}$ é o condutor de L/K.

Relacionando os ideais primos $\mathfrak{p}$ das classes de $J^{\mathfrak{m}}/P^{\mathfrak{m}}$, através do isomorfismo da teoria de corpos de classes $J^{\mathfrak{m}}/P^{\mathfrak{m}} \cong G(L/K)$, ao automorfismo de Frobenius $\varphi_{\mathfrak{p}} = \left(\dfrac{L/K}{\mathfrak{p}}\right)$, obtemos uma interpretação baseada na teoria de Galois do teorema da densidade de Dirichlet. Podemos agora deduzir um teorema de densidade mais geral para extensões Galoisianas mais gerais (não necessariamente abelianas).

Definição 5.8. *Para todo $\sigma \in \mathrm{Gal}(L/K)$, vamos considerar o conjunto*

$$P_{L/K}(\sigma)$$

de todos os ideais primos $\mathfrak{p}$ de K que não se ramificam tais que existe um ideal primo $\mathfrak{P}|\mathfrak{p}$ de L satisfazendo

$$\sigma = \left(\frac{L/K}{\mathfrak{P}}\right),$$

onde $\left(\dfrac{L/K}{\mathfrak{P}}\right)$ é o automorfismo de Frobenius $\varphi_{\mathfrak{P}}$ de $\mathfrak{P}$ sobre K.

Claramente, este conjunto depende apenas da classe de conjugação

$$\langle\sigma\rangle = \{\tau\sigma\tau^{-1} | \tau \in \mathrm{Gal}(L/K)\}$$

de σ e temos $P_{L/K}(\sigma) \cap P_{L/K}(\tau) = \emptyset$ se $\langle\sigma\rangle \neq \langle\tau\rangle$.

Teorema 5.9 (Tchebotarëv)**.** *Seja L/K uma extensão Galoisiana com grupo G. Então para todo $\sigma \in G$, o conjunto $P_{L/K}(\sigma)$ tem densidade, e esta é dada por*

$$d(P_{L/K}(\sigma)) = \frac{\#\langle\sigma\rangle}{\#G}.$$

Demonstração. Nós assumiremos inicialmente que G é gerado por σ. Seja $\mathfrak{m}$ o condutor de L/K. Então L/K é o corpo de classe de um grupo ideal $H^{\mathfrak{m}}$, $J^{\mathfrak{m}} \supseteq H^{\mathfrak{m}} \supseteq P^{\mathfrak{m}}$. Seja $\mathfrak{K} \in J^{\mathfrak{m}}/H^{\mathfrak{m}}$ a classe correspondente ao elemento σ pelo isomorfismo

$$J^{\mathfrak{m}}/H^{\mathfrak{m}} \xrightarrow{\sim} G, \quad \mathfrak{p} \longmapsto \left(\frac{L/K}{\mathfrak{p}}\right).$$

Então $P_{L/K}(\sigma)$ consiste precisamente dos ideais primos $\mathfrak{p}$ que estão na classe $\mathfrak{K}$. Pelo teorema da densidade de Dirichlet, nós concluímos que $P_{L/K}(\sigma)$ tem densidade

$$d(P_{L/K}(\sigma)) = \frac{1}{h_{\mathfrak{m}}} = \frac{1}{\#G} = \frac{\#\langle\sigma\rangle}{\#G}.$$

No caso geral, seja Σ o corpo fixo de σ. Se f é a ordem de σ, então, como acabamos de ver, $d(P_{L/\Sigma}(\sigma)) = \frac{1}{f}$. Seja $\overline{P}(\sigma)$ o conjunto dos ideais primos $\mathfrak{P}$ de L tais que $\mathfrak{P}|\mathfrak{p} \in P_{L/K}(\sigma)$ e $\left(\frac{L/K}{\mathfrak{P}}\right) = \sigma$. Então $\overline{P}(\sigma)$ corresponde bijetivamente ao conjunto $P'_{L/\Sigma}(\sigma)$ dos ideais primos $\mathfrak{q} \in P_{L/\Sigma}(\sigma)$ tais que $\Sigma_{\mathfrak{q}} = K_{\mathfrak{p}}$, $\mathfrak{q}|\mathfrak{p}$. Como os ideais primos restantes são ramificados ou têm grau > 1 sobre $\mathbb{Q}$, nós podemos omiti-los e obter

$$d(P'_{L/\Sigma}(\sigma)) = d(P_{L/\Sigma}(\sigma)) = \frac{1}{f}.$$

Agora nós consideramos o mapa sobrejetivo

$$\rho : P'_{L/\Sigma}(\sigma) \to P_{L/K}(\sigma), \quad \mathfrak{q} \mapsto \mathfrak{q} \cap K.$$

Como $P'_{L/\Sigma}(\sigma) \cong \overline{P}(\sigma)$, nós tomamos, para todo $\mathfrak{p} \in P_{L/K}(\sigma)$,

$$\rho^{-1}(\mathfrak{p}) \cong \left\{\mathfrak{P} \in \overline{P}(\sigma) \mid \mathfrak{P}|\mathfrak{p}\right\} \cong Z(\sigma)/(\sigma),$$

onde $Z(\sigma) = \{\tau \in G \mid \tau\sigma = \sigma\tau\}$ é o centralizador de σ. Então nós temos

$$d(P_{L/K}(\sigma)) = \frac{1}{[Z(\sigma) : (\sigma)]} d(P'_{L/\Sigma}(\sigma)) = \frac{f}{\#Z(\sigma)} \frac{1}{f} = \frac{\#\langle\sigma\rangle}{\#G}.$$

□

5.2 Aplicações do Teorema

O Teorema da Densidade de Tchebotarëv apresenta algumas consequências bastante interessantes.
Se S e T são dois conjuntos de primos, então escrevemos

$$S \;\dot{\subseteq}\; T$$

para indicar que S está contido em T até um número finito de elementos excepcionais. Além disso, escrevemos $S \doteq T$ se $S \;\dot{\subseteq}\; T$ e $T \;\dot{\subseteq}\; S$.
Seja L/K uma extensão finita de corpos algébricos numéricos. Nós denotamos por $P(L/K)$ o conjunto de todos os ideais primos não ramificados $\mathfrak{p}$ de

K que admitem em L um divisor primo $\mathfrak{P}$ de grau 1 sobre K. Então, se L/K é Galoisiana, $P(L/K)$ é justamente o conjunto de todos os ideais primos de K que decompõe completamente em L.

Lema 5.10. *Seja N/K uma extensão Galoisiana contendo L, e seja $G = \mathrm{Gal}(N/K)$, $H = \mathrm{Gal}(N/L)$. Então temos*

$$P(L/K) \doteq \dot{\bigcup_{\langle\sigma\rangle \cap H \neq \emptyset}} P_{N/K}(\sigma) \quad \textit{(união disjunta).}$$

Demonstração. Um ideal primo $\mathfrak{p}$ de K que não se ramifica em N encontra-se em $P(L/K)$ se, e somente se, a classe de conjugação $\langle\sigma\rangle$ de $\sigma = \left(\frac{N/K}{\mathfrak{P}}\right)$, para algum ideal primo $\mathfrak{P}|\mathfrak{p}$ de N, contém um elemento de H, isto é, se e somente se $\mathfrak{p} \in P_{N/K}(\sigma)$ para algum $\sigma \in G$ tal que $\langle\sigma\rangle \cap H \neq \emptyset$ □

Corolário 5.10.1. *Se L/K é uma extensão de grau n, então o conjunto $P(L/K)$ tem densidade $d(P(L/K)) \geq \frac{1}{n}$. Além disso, temos*

$$d(P(L/K)) = \frac{1}{n} \iff L/K \textit{ é Galoisiana.}$$

Demonstração. Seja N/K uma extensão Galoisiana contendo L, e seja $G = \mathrm{Gal}(N/K)$ e $H = \mathrm{Gal}(N/L)$. Pelo lema (5.10), temos

$$P(L/K) \doteq \dot{\bigcup_{\langle\sigma\rangle \cap H \neq \emptyset}} P_{N/K}(\sigma)$$

O teorema da densidade de Tchebotarëv então produz

$$d(P(L/K)) = \sum_{\langle\sigma\rangle \cap H \neq \emptyset} \frac{\#\langle\sigma\rangle}{\#G} = \frac{1}{\#G} \# \left(\dot{\bigcup_{\langle\sigma\rangle \cap H \neq \emptyset}} \langle\sigma\rangle \right).$$

Como $H \subseteq \dot{\bigcup}_{\langle\sigma\rangle \cap H \neq \emptyset} \langle\sigma\rangle$, segue que

$$d(P(L/K)) \geq \frac{\#H}{\#G} = \frac{1}{n}.$$

L/K é Galoisiana se e somente se H é um subgrupo normal de G, e este é o caso se e somente se $\langle\sigma\rangle \subseteq H$ sempre que $\langle\sigma\rangle \cap H \neq \emptyset$, e então isso acontece se e somente se $H = \dot{\bigcup}_{\langle\sigma\rangle \cap H \neq \emptyset} \langle\sigma\rangle$. Isto implica a segunda hipótese. □

Corolário 5.10.2. *Se quase todos os ideais primos decompõe completamente na extensão finita L/K, então $L = K$.*

Demonstração. Seja N/K o fecho normal de L/K, isto é, a menos extensão Galoisiana contendo L. Um ideal primo $\mathfrak{p}$ de K decompõe completamente em L se e somente se ele decompõe completamente em N/K (veja [7], capítulo I, §9, exercício 4). Sob a hipótese do corolário, temos

$$1 = d(P(L/K)) = d(P(N/K)) = \frac{1}{[N : K]},$$

então $[N : K] = 1$ e $N = L = K$. □

Corolário 5.10.3. *Uma extensão L/K é Galoisiana se e somente se todo ideal primo em $P(L/K)$ decompõe completamente em L.*

Demonstração. Seja N/K o fecho normal de L/K. Então $P(N/K)$ consiste precisamente dos ideais primos que decompõe completamente em L. Portanto se $P(N/K) = P(L/K)$, temos, pelo corolário (5.10.1),

$$\frac{1}{[N : K]} = d(P(N/K)) = d(P(L/K)) \geq \frac{1}{[L : K]},$$

isto é, $[N : K] \leq [L : K]$, então $L = N$ é Galoisiana. A outra implicação é trivial. □

Conclusão

Após o tempo utilizado para estudar estes resultados, compreendemos que a resposta para o problema da infinitude dos primos gêmeos pode, talvez, permear as ferramentas aqui apresentadas. O conceito de densidade e sua utilização para demonstrar a infinitude de conjuntos de números primos, como no corolário [3.29.1] do Teorema das Progressões Aritméticas, podem ser igualmente úteis em nossa questão.
Dado que o próximo passo seria estudar à fundo os avanços já realizados na demonstração de tal conjectura, encerro este trabalho deixando para o leitor uma breve apresentação do problema da Infinitude dos Primos Gêmeos.

Definição. *Um* ***par de primos gêmeos*** *é uma dupla ordenada* $(p, p+2)$ *em que* p *e* $p+2$ *são números primos.*

Exemplo. *As duplas à seguir são pares de primos gêmeos.*

$$(5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,42),\ (59,61).$$

Conjectura (Conjectura da Infinitude dos Primos Gêmeos)**.** *O conjunto* P_g *de todos os pares de primos gêmeos é infinito.*

Referências Bibliográficas

[1] Atiyah, M.; Macdonald, I. G. *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[2] Dedekind, R.; Weber, H. *Theory of Algebraic Functions of One Variable*, History of mathematics, **39**, American Mathematical Society, ISBN 978-0-8218-8330-3, 2012.
Tradução para o Inglês de *Theorie der algebraischen Functionen einer Veränderlichen* (1882) por John Stillwell.

[3] Ferreira, L. A. *Teoria de corpos de classe e aplicações* / Luan Alberto Ferreira; orientador Oziride Manzoli Neto. – São Carlos, 2012. Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2012.

[4] Hensel, K. *"Über eine neue Begründung der Theorie der algebraischen Zahlen", Jahresbericht der Deutschen Mathematiker-Vereinigung*, **6** (3): 83-88, 1997.

[5] Kürschák, J. *Über Limesbildung und allgemeine Körpertheorie*. Proceedings of the 5th International Congress of Mathematicians Cambridge 1912, vol. 1 (1913).

[6] Milne, J. *Class field theory*, (v4.02 ed.), (2013) [Online]. Disponível em: `https://www.jmilne.org/math/CourseNotes/cft.html`. [Acessado em 12 de Agosto de 2017, 12:01]

[7] Neukirch, J. *Algebraic Number Theory*, Berlin: Springer-Verlag, 1999.

[8] Serre, Jean-Pierre. *A course in arithmetic*, Graduate Texts in Mathematics, **7**, New York-Heidelberg-Berlin: Springer- Verlag, 1973.

[9] Serre, Jean-Pierre. *Linear Representations of Finite Groups*. Graduate Texts in Mathematics. **42**. Traduzido da segunda edição francesa por Leonard L. Scott. New York-Heidelberg: Springer-Verlag. 1977.