UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Luís Filipe Vital de França

Inteiros p-ádicos e Extensões Ciclotômicas

Manaus – AM
2025

Luís Filipe Vital de França

Inteiros p-ádicos e Extensões Ciclotômicas

Dissertação de Mestrado apresentada como pré-requisito de conclusão do curso de Mestrado em Matemática na Universidade Federal do Amazonas – Campus Manaus – para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Elkin Oveimar Quintero Vanegas

Manaus – AM
2025

Ficha Catalográfica

Elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

F814i França, Luís Filipe Vital de
Inteiros p-ádicos e extensões ciclotômicas / Luís Filipe Vital de França. - 2025.
52 f. : il., p&b. ; 31 cm.

Orientador(a): Elkin Oveimar Quintero Vanegas.
Dissertação (mestrado) - Universidade Federal do Amazonas, Programa de Pós-Graduação em Matemática, Manaus, 2025.

1. Grupos de Galois. 2. Grupos profinitos. 3. Números p-ádicos. 4. Extensões ciclotômicas. I. Vanegas, Elkin Oveimar Quintero. II. Universidade Federal do Amazonas. Programa de Pós-Graduação em Matemática. III. Título

---

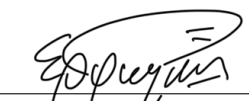
Luís Filipe Vital de França

Inteiros p-ádicos e Extensões Ciclotômicas

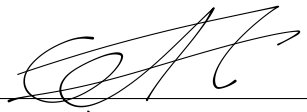
Dissertação de Mestrado apresentada como pré-requisito de conclusão do curso de Mestrado em Matemática na Universidade Federal do Amazonas – Campus Manaus – para obtenção do título de Mestre em Matemática.

Data de Aprovação: 13 de março de 2025

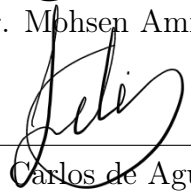
BANCA AVALIADORA



Prof. Dr. Elkin Oveimar Quintero Vanegas – UFAM



Prof. Dr. Mohsen Amiri – UFAM



Prof. Dr. Jean Carlos de Aguiar Lelis – UFPA

Agradecimentos

Agradeço inicialmente aos meus pais, Hélio Vital e Karem Fabíola, e aos meus irmãos, Rafael Vital e Leandro Alves, por todo o apoio e companheirismo que têm me proporcionado ao longo da minha vida.

Agradeço ao meu orientador, professor Elkin Vanegas, pela paciência e dedicação demonstradas ao longo da elaboração desta dissertação.

Agradeço aos professores Jean Lelis e Mohsen Amiri por aceitarem fazer parte da banca examinadora e por todas as sugestões feitas para aprimorar este trabalho.

Agradeço a todos os amigos que estiveram comigo durante o mestrado, em especial Oscar Blanco, Matheus Chaves, Alejandro Rodriguez, Ana Carolina Oliveira, Lílian Laís, Edwin Mateus, Paola Escobar e Vinícius Rosário. A amizade de vocês tornou esta jornada mais leve e significativa.

Agradeço ao Departamento de Matemática pela oportunidade de aprendizado e à CAPES pelo apoio financeiro.

Agradeço a todos que me ajudaram de forma direta ou indireta durante o mestrado.

"Kwaliteit zonder resultaat is zinloos. Resultaat zonder kwaliteit is saai."
Johan Cruijff

Resumo

Começaremos este trabalho com um Capítulo de preliminares, onde abordamos conceitos introdutórios de topologia geral e teoria de Galois. No Capítulo 2, estudaremos com mais detalhes os grupos de Galois. Vamos introduzir a topologia de Krull, uma topologia que torna qualquer grupo de Galois num grupo topológico. No Capítulo 3, vamos apresentar os conceitos de limite inverso e grupos profinitos e mostrar que todo grupo de Galois é um exemplo de grupo profinito. No Capítulo 4, vamos construir e estudar as principais propriedades do corpo $\mathbb{Q}_p$ dos números p-ádicos. Introduzimos outras métricas no conjunto dos números racionais e obtemos $\mathbb{Q}_p$ através do completamento feito com sequências de Cauchy. Por fim, no Capitulo 5, vamos estudar extensões ciclotômicas e mostrar que certas extensões ciclotômicas infinitas de $\mathbb{Q}$ estão intimamente relacionadas com o grupo multiplicativo das unidade p-ádicas.

Palavras-chave: grupos de Galois; grupos profinitos; números p-ádicos; extensões ciclotômicas.

Abstract

We'll begin this work with a preliminary Chapter, where we'll cover introductory concepts of general topology and Galois theory. In Chapter 2, we are going to study Galois groups in more detail. We'll introduce the Krull topology, a topology that makes any Galois group a topological group. In Chapter 3, we'll introduce the concepts of inverse limits and profinite groups and show that every Galois group is an example of a profinite group. In Chapter 4, we are going to construct and study the main properties of the field $\mathbb{Q}_p$ of p-adic numbers. We introduce other metrics on the set of rational numbers and obtain $\mathbb{Q}_p$ through completion using Cauchy sequences. Finally, in Chapter 5, we'll study cyclotomic extensions and show that certain infinite cyclotomic extensions of $\mathbb{Q}$ are closely related to the multiplicative group of p-adic units.

Keywords: Galois groups; profinite groups; p-adic numbers; cyclotomic extensions.

Sumário

Introdução

Durante a década de 1950, a teoria de corpos ciclotômicos foi bastante estudada pelo matemático Kenkichi Iwasawa. Nesse período, Iwasawa escreveu uma ótima sequência de artigos investigando torres de corpos ciclotômicos. Neste trabalho, buscamos detalhar alguns dos resultados presentes nas duas primeiras seções do artigo [Iwa59b].

No Capítulo 1, apresentamos alguns conceitos de topologia geral e teoria de Galois que são utilizados com frequência ao longo do trabalho. No Capítulo 2, estudamos com mais detalhes os grupos de Galois. Introduzimos a topologia de Krull e mostramos que, com essa topologia, um grupo de Galois é um grupo topológico localmente compacto.

No Capítulo 3, definimos e estudamos grupos profinitos. A principal finalidade desse Capítulo é estabelecer as bases necessárias para a compreensão de um resultado citado na seção 2 de [Iwa59b] e que está presente no Capítulo 5.

Para entender esse resultado, foi também necessário estudar os números p-ádicos, de modo que estes vieram a se tornar o principal tema deste trabalho. Façamos aqui uma breve contextualização histórica. Em 1850, o matemático alemão Ernst Kummer introduziu os números p-ádicos, porém Kurt Hensel foi o primeiro a desenvolver uma teoria para os números p-ádicos no interior de uma teoria algébrica dos números em termos de séries de potências e construiu o corpo dos números p-ádicos. Algum tempo depois, os números p-ádicos foram generalizados por intermédio de uma teoria das valorizações estudada por Jozsef Kurschak em 1913, por Hermann Minkowski e outros matemáticos ilustres, por exemplo, Jean-Pierre Serre.

O Capítulo 4 é onde construímos e estudamos o corpo $\mathbb{Q}_p$ dos números p-ádicos. Para construir este corpo, primeiramente definimos uma norma diferente no conjunto dos números racionais. Para cada primo p, existe uma norma $|\ |_p$ que é definida da seguinte forma:

$$|x|_p = \begin{cases} \dfrac{1}{p^{\mathrm{ord}_p x}}, & \text{se } x \neq 0 \\ 0, & \text{se } x = 0. \end{cases}$$

onde $\mathrm{ord}_p x$ é o que chamamos de ordinal p-ádico de x, objeto que também será definido no Capítulo 4.

Quando empregamos a norma $|\ |_p$, podemos encontrar propriedades inesperadas que contrariam nossa percepção geométrica intuitiva. Nesse sentido, podemos observar e verificar que todos os triângulos em $\mathbb{Q}$, com a métrica p-ádica, são isósceles e o comprimento da base não excede o comprimento dos lados. Como também, dada uma bola aberta ou fechada, todo ponto na bola é em centro.

A norma $|\ |_p$ induz uma métrica em $\mathbb{Q}$, de modo que podemos definir e estudar sequências de Cauchy com essa nova métrica. Assim como no caso do corpo dos números reais, obtemos o corpo $\mathbb{Q}_p$ através do completamento feito com essas sequências. Por

definição, $\mathbb{Q}_p$ é o conjunto das classes de equivalência de sequências de Cauchy. Após finalizada a construção do corpo dos números p-ádicos, vamos mostrar que se a é uma classe de equivalência em $\mathbb{Q}_p$, então a pode ser representada por uma "soma infinita" na base p. E esta soma infinita é chamada de expansão p-ádica de a.

Finalmente, o Capítulo 5 aborda as extensões ciclotômicas. Se F é um corpo arbitrário e ω é uma raiz da unidade qualquer, então $F(\omega)$ é um corpo ciclotômico. A primeira seção trás algumas propriedades de extensões ciclotômicas de um corpo base arbitrário. Em seguida, serão apresentados resutados sobre extensões ciclotômicas de $\mathbb{Q}$. Veremos que se K é um corpo de decomposição de $x^n - 1$ sobre $\mathbb{Q}$, então

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Por fim, vamos construir uma torre infinita de corpos ciclotômicos e ver a sua relação com o grupo multiplicativo das unidades p-ádicas.

Capítulo 1

Preliminares

Neste Capítulo, vamos abordar, de forma sucinta, alguns conceitos de topologia e teoria de Galois que serão utilizados ao longo da dissertação. Caso o leitor já esteja familiarizado com esses assuntos, pode ir direto para o Capítulo 2.

1.1 Topologia

Nesta seção, veremos alguns conceitos de topologia que serão utilizados nos Capítulos seguintes. Caso o leitor queira se aprofundar no assunto, ver [Mun14] e [Wil12].

Definição 1.1.1. *Uma topologia em um conjunto X é uma coleção $\mathcal{T}$ de subconjuntos de X com as seguintes propriedades:*

(1) *$\emptyset$ e X estão em $\mathcal{T}$.*

(2) *A união de elementos de qualquer subcoleção de $\mathcal{T}$ está em $\mathcal{T}$.*

(3) *A interseção de elementos de qualquer subcoleção finita de $\mathcal{T}$ está em $\mathcal{T}$.*

Um conjunto X para o qual uma topologia $\mathcal{T}$ foi especificada é chamado de espaço topológico.

Em termos práticos, um espaço topológico é um par ordenado $(X, \mathcal{T})$ formado por um conjunto X e uma topologia $\mathcal{T}$ em X, mas vamos representar o espaço apenas por X quando não houver dúvida sobre qual a topologia em questão.

Se X é um espaço topológico com topologia $\mathcal{T}$, dizemos que um subconjunto U de X é um *conjunto aberto* de X se U pertence à coleção $\mathcal{T}$. Usando essa terminologia, podemos dizer que um espaço topológico é um conjunto X junto com uma coleção de subconjuntos de X, denominados *conjuntos abertos*, tal que $\emptyset$ e X são ambos abertos, e tal que uniões arbitrárias e interseções finitas de conjuntos abertos são abertos.

Definição 1.1.2. *Se X é um conjunto, uma base para uma topologia em X é uma coleção $\mathcal{B}$ de subconjuntos de X (chamados elementos da base) tal que*

(1) *Para cada $x \in X$, existe pelo menos um $B \in \mathcal{B}$ tal que $x \in B$.*

(2) *Se x pertence à interseção de dois elementos da base B_1 e B_2, então existe um elemento da base B_3 tal que $x \in B_3 \subset B_1 \cap B_2$.*

Se $\mathcal{B}$ satisfaz essas duas condições, então definimos a *topologia* $\mathcal{T}$ *gerada por* $\mathcal{B}$ da seguinte forma: dizemos que um subconjunto U de X é aberto em X (isto é, um elemento de $\mathcal{T}$) se para cada $x \in U$, existe um elemento da base $B \in \mathcal{B}$ tal que $x \in B$ e $B \subset U$. Notemos que cada elemento da base é ele próprio um elemento de $\mathcal{T}$.

Na referência [Mun14], o leitor pode verificar que a coleção $\mathcal{T}$ é de fato uma topologia em X. Agora vejamos um Lema que mostra outra maneira de descrever a topologia gerada por uma base.

Lema 1.1.3. *Sejam X um conjunto e $\mathcal{B}$ uma base para uma topologia $\mathcal{T}$ em X. Então $\mathcal{T}$ é igual à coleção de todas as uniões de elementos de $\mathcal{B}$.*

Demonstração: Dada uma coleção de elementos de $\mathcal{B}$, eles também são elementos de $\mathcal{T}$. Visto que $\mathcal{T}$ é uma topologia, a união deles está em $\mathcal{T}$. Reciprocamente, dado $U \in \mathcal{T}$, escolhamos para cada $x \in U$ um elemento B_x de $\mathcal{B}$ tal que $x \in B_x \subset U$. Então $U = \bigcup_{x \in U} B_x$, logo U é igual à união de elementos de $\mathcal{B}$. □

Definição 1.1.4. *Se X é um espaço topológico e $x \in X$, uma vizinhança de x é um conjunto U que contém um conjunto aberto V contendo x. A coleção $\mathcal{U}_x$ de todas as vizinhanças de x é o sistema de vizinhanças de x.*

Definição 1.1.5. *Uma base de vizinhanças (ou um sistema fundamental de vizinahças) de x num espaço topológico X é uma subcoleção $\mathcal{B}_x$ do sistema de vizinhanças $\mathcal{U}_x$, tendo a propriedade de que cada $U \in \mathcal{U}_x$ contém algum $V \in \mathcal{B}_x$. Isto é, $\mathcal{U}_x$ pode ser determinado por $\mathcal{B}_x$ da seguinte forma:*

$$\mathcal{U}_x = \{U \subset X \mid V \subset U \text{ para algum } V \in \mathcal{B}_x\}.$$

Uma vez escolhida uma base de vizinhanças de x (existem muitas para escolher, todas produzindo o mesmo sistema de vizinhanças de x), seus elementos são chamados vizinhanças básicas.

Se X e Y são espaços topológicos, existe uma maneira padrão de definir uma topologia no produto cartesiano $X \times Y$. Consideraremos essa topologia agora e estudaremos algumas de suas propriedades.

Definição 1.1.6. *Sejam X e Y espaços topológicos. A topologia produto em $X \times Y$ é a topologia que tem como base a coleção $\mathcal{B}$ de todos os conjuntos da forma $U \times V$, onde U é um subconjunto aberto de X e V é um subconjunto aberto de Y.*

Vamos verificar que $\mathcal{B}$ é uma base. A primeira condição é trivial, visto que $X \times Y$ é ele próprio um elemento da base. A segunda condição também é fácil, pois a interseção de dois quaisquer elementos da base $U_1 \times V_1$ e $U_2 \times V_2$ é outro elemento da base. Tem-se

$$(U_1 \times V_1) \cap (U_2 \times V_2) = (U_1 \cap U_2) \times (V_1 \cap V_2),$$

e o último conjunto é um elemento da base pois $U_1 \cap U_2$ e $V_1 \cap V_2$ são abertos em X e Y, respectivamente.

Sempre que introduzimos um novo conceito, é apropriado tentar relacioná-lo com os conceitos que foram introduzidos anteriormente. No caso em questão, o que se pode dizer se as topologias em X e Y são geradas por bases? A resposta é a seguinte:

Teorema 1.1.7. *Se $\mathcal{B}$ é uma base para a topologia de X e $\mathcal{C}$ é uma base para a topologia de Y, então a coleção*

$$\mathcal{D} = \{B \times C \mid B \in \mathcal{B} \text{ and } C \in \mathcal{C}\}$$

é uma base para a topologia de $X \times Y$.

Demonstração: [Mun14, Teorema 15.1]

Definição 1.1.8. *Dizemos que um subconjunto A de um espaço topológico X é fechado se, e somente se, o conjunto $X - A$ é aberto.*

Teorema 1.1.9. *Seja X um espaço topológico. Então, as seguintes condições são satisfeitas:*

(a) *$\emptyset$ e X são conjuntos fechados.*

(b) *Interseções arbitrárias de conjuntos fechados são conjuntos fechados.*

(c) *Uniões finitas de conjuntos fechados são conjuntos fechados.*

Demonstração: (a) $\emptyset$ e X são fechados porque são os complementares dos conjuntos abertos X e $\emptyset$, respectivamente.

(b) Dada uma coleção de conjuntos fechados $\{A_\alpha\}_{\alpha \in J}$, aplicamos a lei de De Morgan,

$$X - \bigcap_{\alpha \in J} A_\alpha = \bigcup_{\alpha \in J} (X - A_\alpha).$$

Como os conjuntos $X - A_\alpha$ são abertos por definição, o lado direito da equação representa uma união arbitrária de conjuntos abertos, e portanto é aberto. Logo, $\bigcap A_\alpha$ é fechado.

(c) De modo semelhante, se A_i é fechado para $i = 1, \ldots, n$, consideramos a equação

$$X - \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} (X - A_i).$$

O conjunto no lado direito dessa equação é uma interseção finita de conjuntos abertos e, portanto, é aberto. Assim, $\bigcup A_i$ é fechado. □

Definição 1.1.10. *Sejam X e Y espaços topológicos. Dizemos que uma função $f : X \longrightarrow Y$ é contínua quando, para cada subconjunto aberto V de Y, o conjunto $f^{-1}(V)$ é um subconjunto aberto de X.*

Teorema 1.1.11. *Sejam X e Y espaços topológicos, e seja $f : X \longrightarrow Y$ uma função. Então as seguintes condições são equivalentes:*

(a) *f é contínua*

(b) *Para cada $x \in X$ e cada conjunto aberto V contendo $f(x)$, existe um conjunto aberto U contendo x tal que $f(U) \subset V$.*

Se a condição (2) vale para o ponto x de X, dizemos que f é contínua no ponto x.

Demonstração: [Mun14, Teorema 18.1]

Definição 1.1.12. *Sejam X e Y espaços topológicos. Uma função $f : X \longrightarrow Y$ é um homeomorfismo se, e somente se, f é uma bijeção contínua e f^{-1} também é contínua.*

Definição 1.1.13. *Sejam J um conjunto de íncides, $\{A_\alpha\}_{\alpha\in J}$ uma família indexada de conjuntos e $X = \bigcup_{\alpha\in J} A_\alpha$. O produto cartesiano dessa família indexada, denotado por*

$$\prod_{\alpha\in J} A_\alpha,$$

é definido como o conjunto de todas as J-uplas $(x_\alpha)_{\alpha\in J}$ de elementos de X tais que $x_\alpha \in A_\alpha$ para cada $\alpha \in J$. Ou seja, é o conjunto de todas as funções

$$\mathbf{x} : J \to \bigcup_{\alpha\in J} A_\alpha$$

tais que $\mathbf{x}(\alpha) \in A_\alpha$ para cada $\alpha \in J$.

Nas próximas duas definições, apresentaremos duas topologias que podem ser definidas em um produto cartesiano de espaços topológicos.

Definição 1.1.14. *Seja $\{X_\alpha\}_{\alpha\in J}$ uma família indexada de espaços topológicos. Vamos tomar como uma base para uma topologia no espaço produto*

$$\prod_{\alpha\in J} X_\alpha$$

a coleção de todos os conjuntos da forma

$$\prod_{\alpha\in J} U_\alpha,$$

onde U_α é aberto em X_α, para cada $\alpha \in J$. A topologia gerada por essa base é chamada de box topologia.

Essa coleção satisfaz a primeira condição para uma base porque $\prod X_\alpha$ é ele próprio um elemento da base; e satisfaz a segunda condição porque a interseção de dois elementos da base é outro elemento da base:

$$\left(\prod_{\alpha\in J} U_\alpha\right) \cap \left(\prod_{\alpha\in J} V_\alpha\right) = \prod_{\alpha\in J} (U_\alpha \cap V_\alpha).$$

Definição 1.1.15. *A topologia produto em $\prod X_\alpha$ é obtida tomando como base a coleção de todos os conjuntos da forma $\prod U_\alpha$, onde*

(1) *U_α é aberto em X_α, para cada $\alpha \in J$.*

(2) *U_α é igual a X_α, exceto para um número finito de valores de α.*

Notemos que, para produtos finitos $\prod_{\alpha=1}^{n} X_\alpha$, a topologia produto e a box topologia são precisamente as mesmas. Para produtos arbitrários $\prod X_\alpha$, a topologia produto é a usual. Isso se deve ao fato de que muitos dos teoremas importantes sobre produtos finitos também serão válidos para produtos arbitrários se utilizarmos a topologia produto, mas não se utilizarmos a box topologia.

Definição 1.1.16. *Dizemos que uma coleção $\mathcal{A}$ de subconjuntos de um espaço X é uma cobertura de X se a união dos elementos de $\mathcal{A}$ é igual a X. A coleção $\mathcal{A}$ é chamada uma cobertura aberta de X se seus elementos são subconjuntos abertos de X.*

Definição 1.1.17. *Um espaço X é dito ser compacto se toda cobertura aberta $\mathcal{A}$ de X contém uma subcoleção finita que também cobre X.*

Exemplo 1.1.18. *A reta real $\mathbb{R}$ não é compacta, pois a cobertura de $\mathbb{R}$ por intervalos abertos*

$$\mathcal{A} = \{(n, n+1) \mid n \in \mathbb{Z}\}$$

não contém subcoleção finita que cubra $\mathbb{R}$.

Exemplo 1.1.19. *O seguinte subespaço de $\mathbb{R}$ é compacto:*

$$X = \{0\} \cup \{1/n \mid n \in \mathbb{Z}_+\}.$$

Dada uma cobertura aberta $\mathcal{A}$ de X, existe um elemento $U \in \mathcal{A}$ que contém 0. O conjunto U contém todos os pontos $1/n$, exceto uma quantidade finita deles. Escolha, para cada ponto de X que não está em U, um elemento de $\mathcal{A}$ que o contenha. A coleção formada por esses elementos de $\mathcal{A}$, junto com o elemento U, é uma subcoleção finita de $\mathcal{A}$ que cobre X.

Vamos finalizar essa seção com as definições de espaço Hausdorff e espaço totalmente desconexo, conceitos que serão utilizados no decorrer da dissertação.

Definição 1.1.20. *Um espaço topológico X é chamado um espaço Hausdorff se, e somente se, para cada par x, y de pontos distintos de X, existem conjuntos abertos disjuntos U e V em X tais que $x \in U$ e $y \in V$.*

Definição 1.1.21. *Seja X um espaço topológico.*

(1) *Uma cisão de X é um par U, V de subconjuntos abertos disjuntos de X cuja união é X.*

(2) *O espaço X é conexo se a única cisão de X é a trivial ($X = X \cup \emptyset$).*

(3) *O espaço X é totalmente desconexo se seus únicos subespaços conexos forem conjuntos de um ponto.*

1.2 Teoria de Galois

A chave para estudar extensões de corpos é associar a cada extensão um certo grupo, chamado de *grupo de Galois*. As propriedades do grupo de Galois e os teoremas da teoria de grupos podem então ser usados para estabelecer fatos importantes sobre a extensão de corpos. Nesta seção, definimos o grupo de Galois e desenvolvemos suas propriedades básicas. Ao longo desta seção, F é um corpo.

Definição 1.2.1. *Seja K uma extensão de um corpo F. Um F-automorfismo de K é um isomorfismo $\sigma : K \to K$ que fixa F elemento a elemento (isto é, $\sigma(c) = c$ para todo $c \in F$). O conjunto de todos os F-automorfismos de K é denotado por $\mathrm{Gal}(K/F)$ e é chamado de grupo de Galois de K sobre F.*

O uso da palavra "grupo" na definição é justificado pelo seguinte Lema:

Lema 1.2.2. *Se K é uma extensão de F, então* $\mathrm{Gal}(K/F)$ *é um grupo sob a operação de composição de funções.*

Demonstração: [Hun14, Teorema 12.1].

Seja K uma extensão de um corpo F. Um corpo E tal que $F \subseteq E \subseteq K$ é chamado de *corpo intermediário* da extensão. Nesse caso, podemos considerar K como uma extensão de E. O grupo de Galois $\mathrm{Gal}(K/E)$ consiste em todos os automorfismos de K que fixam E elemento a elemento. Todo tal automorfismo automaticamente fixa cada elemento de F, pois $F \subseteq E$. Assim, todo automorfismo em $\mathrm{Gal}(K/E)$ pertence a $\mathrm{Gal}(K/F)$, ou seja:

Se E é um corpo intermediário, $\mathrm{Gal}(K/E)$ é um subgrupo de $\mathrm{Gal}(K/F)$.

Temos então uma maneira natural de associar um subgrupo do grupo de Galois a cada corpo intermediário da extensão. Por outro lado, se H for um subgrupo do grupo de Galois, podemos associar um corpo intermediário a H usando o seguinte Teorema.

Teorema 1.2.3. *Seja K uma extensão de F. Se H é um subgrupo de* $\mathrm{Gal}(K/F)$*, seja*

$$E_H = \{k \in K \mid \sigma(k) = k \text{ para todo } \sigma \in H\}.$$

Então E_H é um corpo intermediário da extensão. O corpo E_H é chamado de corpo fixado do subgrupo H.

Demonstração: Se $c, d \in E_H$ e $\sigma \in H$, então

$$\sigma(c+d) = \sigma(c) + \sigma(d) = c + d \quad \text{e} \quad \sigma(cd) = \sigma(c)\sigma(d) = cd.$$

Portanto, E_H é fechado pela adição e multiplicação. Como $\sigma(0_F) = 0_F$ e $\sigma(1_F) = 1_F$ para todo automorfismo, 0_F e 1_F estão em E_H. Como σ é um homomorfismo, tem-se para todo $c \in E_H$ não nulo,

$$\sigma(-c) = -\sigma(c) = -c \quad \text{e} \quad \sigma(c^{-1}) = \sigma(c)^{-1} = c^{-1}.$$

Portanto, $-c \in E_H$ e $c^{-1} \in E_H$. Assim, E_H é um subcorpo de K.

Como H é um subgrupo de $\mathrm{Gal}(K/F)$, tem-se que $\sigma(c) = c$ para todo $c \in F$ e todo $\sigma \in H$. Logo, $F \subseteq E_H$. □

A ideia essencial da teoria de Galois é relacionar propriedades de uma extensão de corpos com propriedades de seu grupo de Galois. A chave para fazer isso é o Teorema Fundamental da Teoria de Galois.

Se K é uma extensão de F, sejam S o conjunto de todos os corpos intermediários dessa extensão e T o conjunto de todos os subgrupos do grupo de Galois $\mathrm{Gal}(K/F)$. Definimos uma função $\varphi : S \longrightarrow T$ da seguinte forma:

$$\begin{array}{rccc} \varphi: & S & \longrightarrow & T \\ & E & \longmapsto & \mathrm{Gal}(K/E) \end{array}$$

A função φ é chamada de correspondência de Galois. Notemos que K (considerado como subcorpo de si mesmo) corresponde ao subgrupo identidade de $\mathrm{Gal}(K/F)$, e o subcorpo F corresponde a todo o grupo $\mathrm{Gal}(K/F)$ (considerado como subgrupo de si mesmo). Vejamos agora que, sob hipóteses apropriadas, a correspondência de Galois é uma aplicação bijetiva do conjunto de corpos intermediários para o conjunto de subgrupos de $\mathrm{Gal}(K/F)$.

Teorema 1.2.4. *Seja K uma extensão finita de F. Se H é um subgrupo do grupo de Galois $\mathrm{Gal}(K/F)$ e E é o corpo fixado de H, então $H = \mathrm{Gal}(K/E)$ e $|H| = [K : E]$. Portanto, no caso de extensões finitas, a correspondência de Galois é sobrejetiva.*

Demonstração: [Hun14, Teorema 12.8].

Definição 1.2.5. *Se K é uma extensão normal e separável de um corpo F, dizemos que K é uma extensão galoisiana de F.*

Teorema 1.2.6. *Seja K uma extensão galoisiana de F e E um corpo intermediário. Então E é o corpo fixado do subgrupo $\mathrm{Gal}(K/E)$.*

Demonstração: [Hun14, Teorema 12.9].

Se E e L são corpos intermediários com $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/L)$, então o Teorema 1.2.6 mostra que tanto E quanto L são o corpo fixado do mesmo grupo e, portanto, $E = L$. Assim, a correspondência de Galois é injetiva para extensões galoisianas.

Teorema 1.2.7. (*Teorema Fundamental da Teoria de Galois*) *Se K é uma extensão galoisiana finita de F, então existe uma bijeção entre o conjunto S de todos os corpos intermediários da extensão e o conjunto T de todos os subgrupos do grupo de Galois $\mathrm{Gal}(K/F)$, onde cada corpo intermediário E é enviado ao subgrupo $\mathrm{Gal}(K/E)$. Além disso,*

$$[K : E] = |\mathrm{Gal}(K/E)| \ \text{ e } \ [E : F] = [\mathrm{Gal}(K/F) : \mathrm{Gal}(K/E)].$$

Demonstração: O Teorema 1.2.4 e as observações após o Teorema 1.2.6 provam a primeira afirmação. Cada corpo intermediário E é o corpo fixado de $\mathrm{Gal}(K/E)$ pelo Teorema 1.2.6. Consequentemente, $[K : E] = |\mathrm{Gal}(K/E)|$. Em particular, se $F = E$, então $[K : F] = |\mathrm{Gal}(K/F)|$. Portanto, pelo Teorema de Lagrange,

$$[K : E]\,[E : F] = [K : F] = |\mathrm{Gal}(K/F)| = |\mathrm{Gal}(K/E)|\,[\mathrm{Gal}(K/F) : \mathrm{Gal}(K/E)].$$

Dividindo o primeiro e o último termo desta equação por $[K : E] = |\mathrm{Gal}(K/E)|$, obtemos

$$[E : F] = [\mathrm{Gal}(K/F) : \mathrm{Gal}(K/E)]. \qquad \square$$

Quando K é uma extensão galoisiana infinita de F, a correspondência de Galois continua sendo injetiva, mas em alguns casos, pode não ser sobrejetiva. Para contornar esse problema, introduzimos uma topologia no grupo de Galois $\mathrm{Gal}(K/F)$, conhecida como Topologia de Krull. Veremos com mais detalhes no próximo Capítulo.

Capítulo 2

Grupos de Galois

Neste Capítulo, vamos abordar algumas propriedades do grupo de Galois de uma extensão arbitrária K/F.

2.1 Topologia de Krull

Nesta seção, veremos um pouco sobre a Topologia de Krull, uma topologia que torna qualquer grupo de Galois num grupo topológico.

Definição 2.1.1. *Dizemos que uma tripla $(G, \mathcal{T}, *)$ é um grupo topológico quando $(G, \mathcal{T})$ é um espaço topológico, $(G, *)$ é um grupo e as aplicações*

$$\eta : G \times G \longrightarrow G \qquad e \qquad \lambda : G \longrightarrow G$$

definidas por $\eta(x, y) = x * y$ e $\lambda(x) = x^{-1}$ são ambas contínuas.

Dada uma extensão galoisiana K/F, usaremos o símbolo $\mathcal{I}$ para denotar o conjunto de todas as extensões galoisianas finitas de F contidas em K. Isto é,

$$\mathcal{I} = \{E;\ F \leq E \leq K,\ [E : F] < \infty \text{ e } E/F \text{ é galoisiana}\}$$

Desta forma, podemos definir uma topologia em $\mathrm{Gal}(K/F)$, conhecida como *Topologia de Krull*.

Definição 2.1.2. *Definimos a Topologia de Krull em* $\mathrm{Gal}(K/F)$ *como a topologia gerada pelo conjunto* $\mathcal{B} = \{\sigma\mathrm{Gal}(K/E); \sigma \in \mathrm{Gal}(K/F) \ \text{ e } \ E \in \mathcal{I}\}$

Suponhamos que $E_1, E_2 \in \mathcal{I}$. Se as classes laterais $\sigma\mathrm{Gal}(K/E_1)$ e $\omega\mathrm{Gal}(K/E_2)$ possuem interseção não-vazia, então $\forall\ \alpha \in \sigma\mathrm{Gal}(K/E_1) \cap \omega\mathrm{Gal}(K/E_2)$, temos

$$\alpha \in \alpha\mathrm{Gal}(K/E_1E_2) \subset \sigma\mathrm{Gal}(K/E_1) \cap \omega\mathrm{Gal}(K/E_2),$$

onde E_1E_2 é o subcorpo de K gerado por E_1 e E_2, que também pertence ao conjunto $\mathcal{I}$. Portanto, os abertos da Topologia de Krull são precisamente as uniões das classes laterais da forma $\sigma\mathrm{Gal}(K/E)$ para subextensões galoisianas finitas E de K/F.

Teorema 2.1.3. *Seja* $\mathrm{Gal}(K/F)$ *uma extensão galoisiana (possivelmente infinita). A Topologia de Krull torna* $\mathrm{Gal}(K/F)$ *num grupo topológico.*

Demonstração: Precisamos mostrar que a operação do grupo e a aplicação que envia cada elemento para o seu inverso são ambas contínuas. Para isso, seja

$$\begin{array}{rccc} \eta: & \mathrm{Gal}(K/F)\times\mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Gal}(K/F) \\ & (\sigma,\omega) & \longmapsto & \sigma\omega \end{array}$$

a operação do grupo, e sejam $(\sigma,\omega)\in \mathrm{Gal}(K/F)\times\mathrm{Gal}(K/F)$ e $\sigma\omega$ sua imagem em $\mathrm{Gal}(K/F)$. Tomemos um conjunto aberto de $\mathcal{B}$ que contém $\sigma\omega$: $\sigma\omega\mathrm{Gal}(K/E)$. O conjunto $\sigma\mathrm{Gal}(K/E)\times\omega\mathrm{Gal}(K/E)$ é um aberto que contém (σ,ω): é o conjunto de todos os pares (f,g) tais que

$$f|_E \equiv \sigma|_E \quad \text{e} \quad g|_E \equiv \omega|_E$$

Então se $x\in E$, $g(x)=\omega(x)$, e este elemento pertence a E (pois E/F é galoisiana). Logo $f(g(x))=\sigma(\omega(x))$, o que implica $(f\circ g)(x)=(\sigma\circ\omega)(x)$ para todo $x\in E$, isto é, $fg|_E\equiv\sigma\omega|_E$. Portanto, $\eta(\sigma\mathrm{Gal}(K/E)\times\omega\mathrm{Gal}(K/E))\subset\sigma\omega\mathrm{Gal}(K/E)$, o que mostra que η é contínua em (σ,ω). Sendo (σ,ω) arbitrário, concluímos que a opereção do grupo é contínua.

Agora, vamos motrar que a aplicação

$$\begin{array}{rccc} \lambda: & \mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Gal}(K/F) \\ & \sigma & \longmapsto & \sigma^{-1} \end{array}$$

é contínua. Seja $\sigma\in\mathrm{Gal}(K/F)$ e $\sigma^{-1}\mathrm{Gal}(K/E)$ um aberto de $\mathcal{B}$ que contém σ^{-1}. Se $f\in\sigma\mathrm{Gal}(K/E)$, então $f|_E\equiv\sigma|_E$. Como E/F é galoisiana, f e σ são automorfismos de E e, portanto, a sua igualdade em E implica a igualdade dos seus inversos em E: $f^{-1}|_E\equiv\sigma^{-1}|_E$. Isso mostra que $f^{-1}\in\sigma^{-1}\mathrm{Gal}(K/E)$, logo λ é contínua em σ. Como σ é arbitrário, segue que λ é contínua em $\mathrm{Gal}(K/F)$. □

Se K/F é uma extensão galoisiana finita, então a Topologia de Krull em $\mathrm{Gal}(K/F)$ é a topologia discreta. De fato, para cada $\sigma\in\mathrm{Gal}(K/F)$, tem-se que $\{\sigma\}=\sigma\mathrm{Gal}(K/K)$ é um aberto de $\mathcal{B}$.

Teorema 2.1.4. $\mathrm{Gal}(K/F)$ *é um espaço topológico Hausdorff, compacto e totalmente desconexo.*

Uma demonstração desse Teorema pode ser encontrada em [Mor96, Teorema 17.6]. Desta forma, $\mathrm{Gal}(K/F)$ será sempre considerado um grupo topológico compacto com respeito a sua Topologia de Krull.

Definição 2.1.5. *Dizemos que um espaço topológico $(X,\mathcal{T})$ é localmente compacto se todo $x\in X$ admite uma base de vizinhanças formada por conjuntos compactos.*

Teorema 2.1.6. *Um espaço de Hausdorff $(X,\mathcal{T})$ é localmente compacto se, e somente se, todo $x\in X$ possui uma vizinhança compacta.*

Uma demonstração desse teorema pode ser encontrada em [Wil12]. Por um lado, esse resultado garante que todo espaço Hausdorff e compacto é localmente compacto. Então, pelo Teorema 2.1.4, o grupo de Galois $\mathrm{Gal}(K/F)$ é localmente compacto.

2.2 Subgrupos de Gal(K/F)

Nesta seção, veremos algumas propriedades dos subgrupos de Gal(K/F). Começaremos com um resultado muito útil, especialmente quando K/F é uma extensão infinita.

Teorema 2.2.1. *Se E é um corpo intermediário da extensão K/F,* Gal(K/E) *é um subgrupo fechado de* Gal(K/F).

Demonstração: Para provar que Gal(K/E) é fechado em Gal(K/F), vamos mostrar que o seu complementar é aberto. Se Gal(K/E) = Gal(K/F), não há o que provar. Então, suponhamos que $\sigma \in \text{Gal}(K/F) - \text{Gal}(K/E)$, o que significa que σ não atua como identidade em E: $\sigma(x) \neq x$ para algum $x \in E$.

Existe uma extensão galoisiana finita L/F contida em K que contém x. Então $\sigma\text{Gal}(K/L)$ é um aberto de $\mathcal{B}$ que contém σ e é disjunto de Gal(K/E). Para constatar isso, notemos que todos os elementos de $\sigma\text{Gal}(K/L)$ atuam em L da mesma forma que σ, o que significa que:

$$\omega(x) \neq x, \, \forall \, \omega \in \sigma\text{Gal}(K/L).$$

Por outro lado, todo elemento de Gal(K/E) fixa x, visto que $x \in E$. Com isso, concluímos que todo elemento de Gal(K/F) que não está em Gal(K/E) está contido em um aberto de $\mathcal{B}$ disjunto de Gal(K/E). Logo, o complementar de Gal(K/E) é aberto, como queríamos. □

O Teorema Fundamental da Teoria de Galois nos garante que existe uma bijeção entre os corpos intermediários de K/F e os subgrupos fechados de Gal(K/F), associando cada corpo intermediário E ao subgrupo Gal(K/E) (Quando K/F é uma extensão finita, todos os subgrupos de Gal(K/F) são fechados). Vejamos agora o caso em que E/F é também uma extensão galoisiana.

Teorema 2.2.2. *Seja E um corpo intermediário de K/F. Então E/F é uma extensão galoisiana se, e somente se,* Gal(K/E) *é normal em* Gal(K/F). *Quando isso ocorre, o grupo* Gal(E/F) *pode ser identificado canonicamente com o grupo quociente* Gal(K/F)/Gal(K/E).

Demonstração: Suponhamos que Gal(K/E) é um subgrupo normal de Gal(K/F). Seja $p(x)$ um polinômio irredutível em $F[x]$ com uma raiz $u \in E$. Devemos mostrar que cada raiz v de $p(x)$ também está em E. Pelo Teorema de Extensão de Isomorfismo, existe $\omega \in \text{Gal}(K/F)$ tal que $\omega(u) = v$. Se $\sigma \in \text{Gal}(K/E)$, então a normalidade implica $\sigma \circ \omega = \omega \circ \sigma_1$ para algum $\sigma_1 \in \text{Gal}(K/E)$. Como $u \in E$, temos:

$$\sigma(v) = \sigma(\omega(u)) = \omega(\sigma_1(u)) = \omega(u) = v$$

Portanto, v é fixado por todo elemento $\sigma \in \text{Gal}(K/E)$. Logo, $v \in E$.

Reciprocamente, suponhamos que E/F é galoisiana. A aplicação

$$\begin{array}{rccc} \theta: & \text{Gal}(K/F) & \longrightarrow & \text{Gal}(E/F) \\ & \sigma & \longmapsto & \sigma|_E \end{array}$$

é um homomorfismo de grupos. Se $\omega \in \mathrm{Gal}(E/F)$, então existe $\sigma \in \mathrm{Gal}(K/F)$ tal que $\sigma|_E = \omega$ (ver [Mor96, Proposição 3.28]). Logo, a aplicação é sobrejetiva. Além disso, temos que $Ker\ \theta = \mathrm{Gal}(K/E)$. Portanto, $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$ e, pelo Primeiro Teorema de Isomorfismo, temos

$$\frac{\mathrm{Gal}(K/F)}{\mathrm{Gal}(K/E)} \cong \mathrm{Gal}(E/F) \qquad \square$$

Se $\mathrm{Gal}(K/E)$ é um subgrupo normal e abeliano de $\mathrm{Gal}(K/F)$, então todo automorfismo interno $x \mapsto s^{-1}xs$ de $\mathrm{Gal}(K/F)$ induz um automorfismo $x \mapsto x\rho$ no subgrupo normal $\mathrm{Gal}(K/E)$ que depende apenas da classe lateral ρ de s módulo $\mathrm{Gal}(K/E)$. Vejamos agora porque isso ocorre.

Seja

$$\begin{array}{rccc} \theta: & \mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Gal}(K/F) \\ & x & \longmapsto & s^{-1}xs \end{array}$$

um automorfismo interno de $\mathrm{Gal}(K/F)$. Se t é congruente a s módulo $\mathrm{Gal}(K/E)$, então $t = sh$, onde $h \in \mathrm{Gal}(K/E)$. Temos então outro automorfismo interno de $\mathrm{Gal}(K/F)$:

$$\begin{array}{rccc} \varphi: & \mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Gal}(K/F) \\ & x & \longmapsto & t^{-1}xt \end{array}$$

Se $x \in \mathrm{Gal}(K/E)$, então

$$\begin{aligned} \varphi(x) &= t^{-1}xt = (sh)^{-1}x(sh) \\ &= h^{-1}(s^{-1}xs)h \\ &= (s^{-1}xs)h^{-1}h && \text{pois } \mathrm{Gal}(K/E) \text{ é abeliano} \\ &= s^{-1}xs = \theta(x) \end{aligned}$$

Portanto, os automorfismos φ e θ são equivalentes em $\mathrm{Gal}(K/E)$. Logo, o automorfismo induzido depende apenas da classe lateral de s, como afirmado.

Assim sendo, podemos definir uma ação de $\mathrm{Gal}(E/F)$ em $\mathrm{Gal}(K/E)$. Como $\mathrm{Gal}(E/F)$ é isomorfo ao grupo quociente $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$, todo elemento de $\mathrm{Gal}(E/F)$ é identificado como uma classe lateral ρ módulo $\mathrm{Gal}(K/E)$. Definimos então

$$\begin{array}{rccc} \eta: & \mathrm{Gal}(K/E) \times \mathrm{Gal}(E/F) & \longrightarrow & \mathrm{Gal}(K/E) \\ & (x, \rho) & \longmapsto & s^{-1}xs \end{array}$$

onde s é um representante da classe lateral ρ módulo $\mathrm{Gal}(K/E)$. Nesse caso, dizemos então que $\mathrm{Gal}(K/E)$ é um $\mathrm{Gal}(E/F)$-grupo à direita em que $\mathrm{Gal}(E/F)$ age continuamente. [Iwa59b]

2.3 Caracteres de Gal(K/F) e Gal(K/E)

Nesta seção, veremos algumas propriedades do grupo de caracteres de $\mathrm{Gal}(K/F)$ e $\mathrm{Gal}(K/E)$. Começaremos abordando alguns conceitos sobre caracteres de grupos topológicos. Vamos utilizar o símbolo $\mathbb{S}^1$ para representar o grupo multiplicativo dos

números complexos com módulo igual a 1. Consideramos $\mathbb{S}^1$ um grupo topológico com a topologia induzida pelo plano complexo.

2.3.1 O grupo de caracteres de um grupo topológico

Definição 2.3.1. *Seja G um grupo arbitrário. Um homomorfismo $\chi : G \longrightarrow \mathbb{S}^1$ é chamado um caracter de G*

Todo grupo G possui pelo menos um caracter: a função que é identicamente 1 em G. Este é chamado o caracter *principal*, e será denotado por χ_1.

Lema 2.3.2. *Se a multiplicação de caracteres for definida pela relação*

$$(\chi_i\chi_j)(a) = \chi_i(a)\chi_j(a)$$

para cada $a \in G$, então o conjunto de caracteres de G forma um grupo abeliano. Vamos denotar esse grupo por G^*. O elemento identidade de G^* é o caracter principal χ_1. O inverso de χ_i é o recíproco $1/\chi_i = \overline{\chi_i}$.

A demonstração desse lema é feita através da verificação imediata dos axiomas de grupos e será omitida no texto.

Vejamos agora um exemplo que ilustra os caracteres de um grupo de ordem 6.

Exemplo 2.3.3. *Seja U_7 o grupo multiplicativo dos elementos invertíveis de $\mathbb{Z}/7\mathbb{Z}$. Ou seja, $U_7 = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$. Este grupo possui exatamente 6 caracteres, que estão ilustrados na tabela abaixo. Denotamos $\delta = e^{\pi i/3}$*

n	1	2	3	4	5	6
$\chi_1(n)$	1	1	1	1	1	1
$\chi_2(n)$	1	1	-1	1	-1	-1
$\chi_3(n)$	1	δ^2	$-\delta$	$-\delta$	δ^2	1
$\chi_4(n)$	1	δ^2	δ	$-\delta$	$-\delta^2$	-1
$\chi_5(n)$	1	$-\delta$	δ^2	δ^2	$-\delta$	1
$\chi_6(n)$	1	$-\delta$	$-\delta^2$	δ^2	δ	-1

Tabela 2.1: Caracteres de U_7

Este exemplo é um caso particular de um resultado que vale para qualquer grupo abeliano finito. Se G é um grupo abeliano finito de ordem n, então G possui exatamente n caracteres distintos. A demonstração desse resultado pode ser encontrada em [Apo13, Teorema 6.8].

Definição 2.3.4. *Seja G um grupo topológico. O grupo de todos os caracteres contínuos de G é chamado o grupo de caracteres de G (ou grupo dual de G). Este grupo será denotado por $\hat{G}$. Desta forma, tem-se $\hat{G} \leq G^*$.*

Dado um grupo topológico G, o grupo $\hat{G}$ será sempre considerado um grupo topológico com a topologia *compacto-aberto*. Vejamos agora alguns resultados que serão necessários nas subseções seguintes. Em todos os casos, G é um grupo topológico.

Ao leitor interessado, pode-se encontrar a demonstração dos Teoremas abaixo no Capítulo 6 de [Ros12].

Teorema 2.3.5. *Se G é um grupo abeliano localmente compacto, então $\hat{G}$ é um grupo abeliano localmente compacto.*

Teorema 2.3.6. *Seja G um grupo abeliano localmente compacto.*

(a) *Se G é compacto, então $\hat{G}$ é discreto*

(b) *Se G é discreto, então $\hat{G}$ é compacto*

Definição 2.3.7. *Seja G um grupo abeliano localmente compacto. Para um subconjunto não-vazio arbitrário H de G, seja H^0 o subconjunto de $\hat{G}$ formado por todos os χ tais que $\chi(H) = 1$. O conjunto H^0 chama-se o anulador de H em $\hat{G}$.*

Se H é um subconjunto não-vazio de G e H_1 é o menor subgrupo de G contendo H, então $H^0 = {H_1}^0$. Além disso, H^0 é um subgrupo de $\hat{G}$.

Teorema 2.3.8. *Sejam G um grupo abeliano localmente compacto e H um subgrupo fechado de G. O grupo de caracteres de H é isomorfo a $\hat{G}/H^0$.*

2.3.2 Caracteres de Gal(K/F)

Nesta subseção, vamos considerar o caso em que $\mathrm{Gal}(K/F)$ é um grupo abeliano. Vamos denotar o grupo de caracteres de $\mathrm{Gal}(K/F)$ por $\mathrm{A}(K/F)$.

Desta forma, como $\mathrm{Gal}(K/F)$ é abeliano, decorre dos Teoremas 2.3.5 e 2.3.6 que $\mathrm{A}(K/F)$ é um grupo abeliano discreto. Se E é um corpo intermediário da extensão K/F, então $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$. Assim sendo, seja $\mathrm{A}(E/F)$ o grupo de caracteres de $\mathrm{Gal}(E/F)$. O grupo $\mathrm{A}(E/F)$ pode ser mergulhado como um subgrupo de $\mathrm{A}(K/F)$. Vejamos agora porque isso ocorre.

Teorema 2.3.9. *Seja G um grupo abeliano localmente compacto com grupo de caracteres $\hat{G}$, e seja H um subgrupo fechado de G. Seja $\widehat{(G/H)}$ o grupo de caracteres do grupo G/H. O grupo $\widehat{(G/H)}$ é isomorfo ao grupo H^0.*

Demonstração: Seja

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & G/H \\ & x & \longmapsto & xH \end{array}$$

a projeção natural de G em G/H. Vamos mostrar que a aplicação

$$\begin{array}{rccc} \theta: & \widehat{(G/H)} & \longrightarrow & H^0 \\ & \psi & \longmapsto & \psi \circ \varphi \end{array}$$

é um isomorfismo. Como φ é um homomorfismo contínuo e $\varphi^{-1}(\{H\}) = H$, tem-se que $\psi \circ \varphi \in H^0, \ \ \forall\, \psi \in (\widehat{G/H})$. Se $\psi_i, \psi_j \in (\widehat{G/H})$, então $(\psi_i\psi_j) \circ \varphi = (\psi_i \circ \varphi)(\psi_j \circ \varphi)$, logo θ é um homomorfismo.

Agora, seja $\chi \in H^0$. Tem-se que χ é constante em cada classe lateral xH. Logo, a função ψ em G/H definida por $\psi(xH) = \chi(x)$ está bem definida, e é claramente um caracter de G/H. Vejamos agora que ψ é contínua em G/H. Dado $\varepsilon > 0$, existe uma vizinhança U de e em G tal que $|\chi(x) - 1| < \varepsilon$, $\forall\ x \in U$. O conjunto $V = \{xH; x \in U\}$ é uma vizinhança da identidade H em G/H em que $|\psi(xH) - 1| < \varepsilon$, $\forall\ xH \in V$. Consequentemente, ψ é contínua em H e, portanto, contínua em todo o G/H. Como $\chi = \psi \circ \varphi$, concluímos que a aplicação θ é sobrejetiva. É imediato que $Ker\ \theta = \psi_1$ (caracter principal de G/H). Portanto, θ é um isomorfismo, como queríamos demonstrar. □

Observação: Na demonstração do Teorema acima, a continuidade em H implica a continuidade em todo o G/H devido a um resultado sobre continuidade uniforme em grupos topológicos. Para mais detalhes, ver [Ros12, (5.40)].

Assim sendo, pelo Teorema acima, concluímos que o grupo de caracteres $\mathrm{A}(E/F)$ é isomorfo ao anulador de $\mathrm{Gal}(K/E)$ em $\mathrm{A}(K/F)$. Logo, $\mathrm{A}(E/F)$ pode ser mergulhado como um subgrupo de $\mathrm{A}(K/F)$, como afirmado anteriormente. Além disso, pelo Teorema 2.3.8, concluímos que $\mathrm{A}(K/E) \cong \mathrm{A}(K/F)/\mathrm{A}(E/F)$.

2.3.3 Caracteres de Gal(K/E)

Agora vamos considerar o caso em que $\mathrm{Gal}(K/E)$ é um subgrupo normal abeliano de $\mathrm{Gal}(K/F)$, mas $\mathrm{Gal}(K/F)$ não é necessariamente abeliano. Como vimos na seção 2.2, $\mathrm{Gal}(K/E)$ é um $\mathrm{Gal}(E/F)$-grupo abeliano. Podemos definir também uma ação de $\mathrm{Gal}(E/F)$ no grupo de caracteres $\mathrm{A}(K/E)$. Se $\rho \in \mathrm{Gal}(E/F)$ e $a = a(x) \in \mathrm{A}(K/E)$ $(x \in \mathrm{Gal}(E/F))$, definimos ρa em $\mathrm{A}(K/E)$ da seguinte forma:

$$\begin{array}{rccc} \eta: & \mathrm{Gal}(E/F) \times \mathrm{A}(K/E) & \longrightarrow & \mathrm{A}(K/E) \\ & (\rho, a) & \longmapsto & \rho a \end{array}$$

onde $(\rho a)(x) = a(x\rho) = a(s^{-1}xs)$ e s é um elemento de $\mathrm{Gal}(K/F)$ tal que ρ é a classe lateral de s módulo $\mathrm{Gal}(K/E)$. Desta forma, $\mathrm{A}(K/E)$ torna-se um $\mathrm{Gal}(E/F)$-grupo à esquerda discreto em que $\mathrm{Gal}(E/F)$ age continuamente.

Definição 2.3.10. *Sejam X e A grupos topológicos abelianos e seja G um grupo topológico que age continuamente em X e em A, de modo que X é um G-grupo à direita e A é um G-grupo à esquerda. Então um par ordenado (x, a) de X e A será chamado um G-emparelhamento se*

$$(x\rho, a) = (x, \rho a) \qquad\qquad x \in X,\ a \in A$$

para todo ρ em G. [Iwa59a].

De acordo com a definição acima, tem-se que

$$(x, a) = a(x) \qquad\qquad x \in \mathrm{Gal}(K/E),\ a \in \mathrm{A}(K/E)$$

define um $\mathrm{Gal}(E/F)$-emparelhamento entre $\mathrm{A}(K/E)$ e $\mathrm{Gal}(K/E)$.

Capítulo 3

Grupos Profinitos

Neste Capítulo, estudaremos o conceito e algumas propriedades dos Grupos Profinitos, que serão necessários para o entendimento de um resultado que será apresentado no Capítulo 5. Alguns resultados presentes neste Capítulo não se encontram demonstrados aqui, mas todas as demonstrações podem ser encontradas na referência [Zal00].

3.1 Limites Inversos ou Projetivos

Nesta seção, definimos o conceito de limite inverso (ou projetivo) e estabelecemos algumas de suas propriedades elementares. Vamos desenvolver o conceito e estabelecer essas propriedades nos casos de espaços topológicos ou grupos topológicos. No entanto, vale ressaltar que os conceitos e resultados obtidos aqui podem ser estendidos para outros objetos, como conjuntos, anéis (topológicos), módulos,... ou para categorias mais gerais.

Seja $I = (I, \preceq)$ um *conjunto dirigido parcialmente ordenado* ou *poset dirigido*, isto é, I é um conjunto com uma relação binária $\preceq$ satisfazendo as seguintes condições:

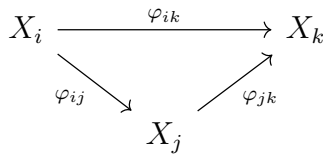
(a) $i \preceq i$, para $i \in I$;

(b) $i \preceq j$ e $j \preceq k$ implica $i \preceq k$, para $i, j, k \in I$;

(c) $i \preceq j$ e $j \preceq i$ implica $i = j$, para $i, j \in I$; and

(d) se $i, j \in I$, existe um $k \in I$ tal que $i, j \preceq k$.

Um *sistema inverso ou projetivo* de espaços topológicos (resp. grupos topológicos) sobre I consiste em uma coleção $\{X_i \mid i \in I\}$ de espaços topológicos (resp. grupos topológicos) indexados por I, e uma coleção de aplicações contínuas (resp. homomorfismos de grupos contínuos) $\varphi_{ij} : X_i \to X_j$, definidas sempre que $i \succeq j$, tal que os diagramas da forma



comutam sempre que estão definidos, isto é, sempre que $i, j, k \in I$ e $i \succeq j \succeq k$.

Além disso, assumimos que φ_{ii} é a aplicação identidade id_{X_i} em X_i. Denotamos tal sistema por $\{X_i, \varphi_{ij}, I\}$, ou por $\{X_i, \varphi_{ij}\}$ quando não há duvidas sobre o conjunto de índices I em questão. Se X é um espaço topológico fixado (resp. grupo topológico), denotamos por $\{X, \mathrm{id}\}$ o sistema inverso $\{X_i, \varphi_{ij}, I\}$, onde $X_i = X$ para todo $i \in I$, e φ_{ij} é a aplicação identidade $\mathrm{id} : X \to X$. Dizemos que $\{X, \mathrm{id}\}$ é o *sistema inverso constante* em X. Um sistema inverso $\{X_i, \varphi_{ij}, I\}$ é chamado um *sistema inverso sobrejetivo* se cada uma das aplicações φ_{ij} $(i \succeq j)$ é sobrejetiva.

Exemplo 3.1.1. *Sejam $I = \mathbb{N}$ e p um número primo. Para cada $i \in \mathbb{N}$, seja $\mathbb{Z}/p^i\mathbb{Z}$ o grupo aditivo dos inteiros* mod p^i. *Então, para cada $i \geq j$, definimos*

$$\begin{array}{rccc} \varphi_{ij}: & \mathbb{Z}/p^i\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^j\mathbb{Z} \\ & n + p^i\mathbb{Z} & \longmapsto & n + p^j\mathbb{Z} \end{array}$$

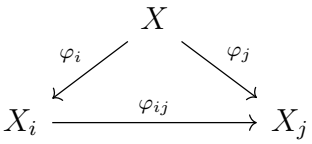
para cada $n \in \mathbb{Z}$. Vejamos que φ_{ij} está bem definida. Ora, φ_{ij} está bem definida se, e somente se, $p^i\mathbb{Z} \subseteq p^j\mathbb{Z}$. Dado $p^i \in p^i\mathbb{Z}$, temos que $p^i \in p^j\mathbb{Z}$ se, e somente se, $p^j | p^i$. Mas $p^j | p^i$ se, e somente se, $i \geq j$. Logo $p^i\mathbb{Z} \subseteq p^j\mathbb{Z}$ e, portanto, φ_{ij} está bem definida.

Segue que φ_{ii} é a aplicação identidade para todo $i \in I$, e se $i \geq j \geq k$, tem-se $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$. De fato, seja $n + p^i\mathbb{Z} \in \mathbb{Z}/p^i\mathbb{Z}$, então

$$(\varphi_{jk} \circ \varphi_{ij})(n + p^i\mathbb{Z}) = \varphi_{jk}(\varphi_{ij}(n + p^i\mathbb{Z})) = \varphi_{jk}(n + p^j\mathbb{Z}) = n + p^k\mathbb{Z} = \varphi_{ik}(n + p^i\mathbb{Z}).$$

Logo $\{\mathbb{Z}/p^i\mathbb{Z}, \varphi_{ij}, I\}$ é um sistema inverso de grupos finitos.

Seja X um espaço topológico (resp. grupo topológico), $\{X_i, \varphi_{ij}, I\}$ um sistema inverso de espaços topológicos (resp. grupos topológicos) sobre um poset dirigido I, e seja $\varphi_i : X \to X_i$ uma aplicação contínua (resp. homomorfismo de grupos contínuo) para cada $i \in I$. Dizemos que essas aplicações φ_i são *compatíveis* se $\varphi_{ij} \circ \varphi_i = \varphi_j$ sempre que $j \preceq i$, isto é, se os seguintes diagramas comutam:

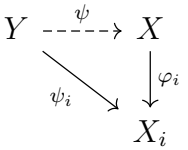


Com esses conceitos, podemos definir limite inverso.

Definição 3.1.2. *Um espaço topológico (resp. grupo topológico) X junto com aplicações contínuas compatíveis (resp. homomorfismos contínuos)*

$$\varphi_i : X \longrightarrow X_i \quad (i \in I)$$

é um limite inverso ou um limite projetivo do sistema inverso $\{X_i, \varphi_{ij}, I\}$ se a seguinte propriedade universal é satisfeita: sempre que Y for um espaço topológico (resp. grupo topológico) com aplicações contínuas compatíveis (resp. homomorfismos contínuos) $\psi_i : Y \to X_i$, existe uma única aplicação contínua (resp. homomorfismo contínuo) $\psi : Y \to X$ tal que para todo $i \in I$, o seguinte diagrama é comutativo:



Dizemos que ψ é "induzido" ou "determinado" pelos homomorfismos compatíveis ψ_i.

As aplicações $\varphi_i : X \to X_i$ são chamadas *projeções*. As projeções φ_i não são necessariamente sobrejetivas. Nós denotamos o limite inverso por (X, φ_i), ou muitas vezes apenas por X, por abuso de notação.

Se $\{X_i, I\}$ é uma coleção de espaços topológicos (resp. grupos topológicos) indexados por um conjunto I, o seu *produto direto* ou *produto cartesiano* é o espaço topológico (resp. grupo topológico) $\prod_{i \in I} X_i$, munido com a topologia produto. No caso de grupos topológicos, a operação do grupo é definida coordenada a coordenada.

Proposição 3.1.3. *Seja $\{X_i, \varphi_{ij}, I\}$ um sistema inverso de espaços topológicos (resp. grupos topológicos) sobre um poset dirigido I. Então*

(a) *Existe um limite inverso do sistema inverso $\{X_i, \varphi_{ij}, I\}$.*

(b) *Este limite é único no seguinte sentido. Se (X, φ_i) e (Y, ψ_i) são dois limites do mesmo sistema inverso $\{X_i, \varphi_{ij}, I\}$, então existe um único homeomorfismo (resp. isomorfismo topológico) $\varphi : X \to Y$ tal que $\psi_i \circ \varphi = \varphi_i$ para cada $i \in I$.*

Demonstração: (a) Seja $C = \prod_{i \in I} X_i$ e para cada $i \in I$, considere π_i a aplicação projeção de C em X_i. Definimos o seguinte conjunto

$$X = \{c \in C \mid (\varphi_{ij} \circ \pi_i)(c) = \pi_j(c), \text{ para todo } i, j, \text{ com } j \preceq i\}$$

e $\varphi_i = \pi_i \mid_X$, para cada i. Então (X, φ_i) é um limite inverso de $\{X_i, \varphi_{ij}, I\}$. De fato, X é um espaço topológico (resp. grupo topológico) com aplicações contínuas compatíveis (resp. homomorfismos contínuos) $\varphi_i : X \longrightarrow X_i$. Devemos mostrar que ele satisfaz a propriedade universal.

Seja Y um espaço topológico (resp. grupo topológico) com aplicações contínuas compatíveis (resp. homomorfismos contínuos) $\psi_i : Y \longrightarrow X_i$. O objetivo é mostrar que existe uma única aplicação contínua (resp. homomorfismo contínuo) $\psi : Y \longrightarrow X$ tal que $\varphi_i \circ \psi = \psi_i$, para cada i.

Seja $\overline{\psi} : Y \longrightarrow C$ a aplicação que leva cada $y \in Y$ em $(\psi_i(y)) \in C$. Então, para todo $y \in Y$,

$$(\pi_i \circ \overline{\psi})(y) = \pi_i(\overline{\psi}(y)) = \psi_i(y).$$

Logo, $\pi_i \circ \overline{\psi} = \psi_i$. Além disso, $\overline{\psi}$ é contínua, pois sua composição com cada aplicação projeção é contínua.

Como $\{\psi_i : Y \longrightarrow X_i\}$ é uma família compatível de aplicações contínuas, então sempre que $i \succeq j$, temos que $\psi_j = \varphi_{ij} \circ \psi_i$. Assim, se $i \succeq j$, então

$$\pi_j \circ \overline{\psi} = \psi_j = \varphi_{ij} \circ \psi_i = \varphi_{ij} \circ \pi_i \circ \overline{\psi}.$$

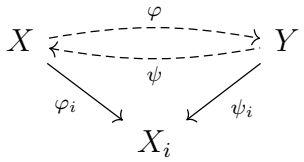
Logo, a imagem de $\overline{\psi}$ está contida em X. Agora defina $\psi : Y \longrightarrow X$ por

$$\psi(y) = \overline{\psi}(y), \text{ para cada } y.$$

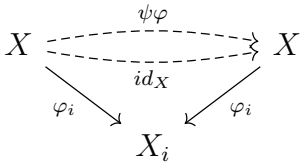
Temos que ψ é contínua e $\varphi_i \circ \psi = \psi_i$, para cada i.

Resta verificar a unicidade. Considere $\psi' : Y \longrightarrow X$ uma aplicação contínua satisfazendo $\varphi_i \circ \psi' = \psi_i$ para cada $i \in I$. Então para cada $y \in Y$ e $i \in I$, $\psi'(y) = \psi(y)$ em X_i. Logo $\psi' = \psi$. Portanto, (X, φ_i) é um limite inverso de $\{X_i, \varphi_{ij}, I\}$.

(b) Suponhamos que (X, φ_i) e (Y, ψ_i) são dois limites inversos do sistema inverso $\{X_i, \varphi_{ij}, I\}$. Como as aplicações $\psi_i : Y \longrightarrow X_i$ são compatíveis, a propriedade universal do limite inverso (X, φ_i) mostra que existe uma única aplicação contínua (resp. homomorfismo contínuo) $\psi : Y \longrightarrow X$ tal que $\varphi_i \circ \psi = \psi_i$ para todo $i \in I$. Analogamente, como as aplicações $\varphi_i : X \longrightarrow X_i$ são compatíveis e (Y, ψ_i) é um limite inverso, existe uma única aplicação contínua (resp. homomorfismo contínuo) $\varphi : X \longrightarrow Y$ tal que $\psi_i \circ \varphi = \varphi_i$ para todo $i \in I$.



Agora, observemos que



comuta para cada $i \in I$. Como, por definição, existe apenas uma aplicação satisfazendo essa propriedade, tem-se $\psi \circ \varphi = \mathrm{id}_X$. Analogamente, $\varphi \circ \psi = \mathrm{id}_Y$. Logo φ é um homeomorfismo (resp. isomorfismo topológico). □

Se $\{X_i, \varphi_{ij}, I\}$ é um sistema inverso, denotamos o seu limite inverso por $\varprojlim_{i \in I} X_i$, ou $\varprojlim_{i} X_i$, ou $\varprojlim_{I} X_i$, ou $\varprojlim X_i$, dependendo do contexto.

Proposição 3.1.4. *Seja $\{X_i, \varphi_{ij}\}$ um sistema inverso de espaços topológicos não-vazios compactos e Hausdorff X_i sobre um conjunto dirigido I. Então*

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

é não-vazio. Em particular, o limite inverso de um sistema inverso de conjuntos finitos não-vazios é não-vazio.

Agora vamos enunciar uma definição e um resultado que serão necessários nas próximas seções.

Definição 3.1.5. *Um espaço topológico X que surge como limite inverso*

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

de espaços finitos X_i munidos com a topologia discreta é chamado um espaço profinito.

Teorema 3.1.6. *Seja X um espaço topológico. Então as seguintes condiçoes são equivalentes.*

(a) *X é um espaço profinito*

(b) *X é compacto, Hausdorff e totalmente desconexo*

(c) *X é compacto, Hausdorff e admite uma base de conjuntos abertos e fechados para a sua topologia*

3.2 Pro-$\mathcal{C}$ grupos

Definição 3.2.1. *Seja $\mathcal{C}$ uma classe não-vazia de grupos finitos (isso vai sempre significar que $\mathcal{C}$ contém todas as imagens isomorfas dos grupos em $\mathcal{C}$). Definimos um pro-$\mathcal{C}$ grupo G como um limite inverso*

$$G = \varprojlim_{i \in I} G_i$$

de um sistema inverso sobrejetivo $\{G_i, \varphi_{ji}, I\}$ de grupos G_i em $\mathcal{C}$, onde cada grupo G_i possui a topologia discreta. Pensamos em um tal pro-$\mathcal{C}$ grupo G como um grupo topológico, cuja topologia é herdada da topologia produto em $\prod_{i \in I} G_i$.

Dizemos que uma classe $\mathcal{C}$ é *fechada por subgrupo* se sempre que $G \in \mathcal{C}$ e $H \leq G$, então $H \in \mathcal{C}$. Observamos que se a classe $\mathcal{C}$ é fechada por subgrupo, então qualquer limite inverso de um (não-necessariamente sobrejetivo) sistema inverso de grupos em $\mathcal{C}$ é um pro-$\mathcal{C}$ grupo.

Um grupo G é um *produto subdireto* de uma coleção de grupos $\{G_j \mid j \in J\}$ se existe uma coleção de subgrupos normais $\{N_j \mid j \in J\}$ de G tal que

$$\bigcap_{j \in J} N_j = 1 \quad \text{e} \quad G/N_j \cong G_j \quad \text{para cada } j \in J.$$

Observemos que se G é um produto subdireto dos grupos $\{G_j \mid j \in J\}$, então G é isomorfo a um subgrupo do produto direto $\prod_{j \in J} G_j$.

As propriedades dos pro-$\mathcal{C}$ grupos são obviamente dependentes do tipo de classe $\mathcal{C}$ que se considera. Vamos enunciar uma série de propriedades que uma classe $\mathcal{C}$ pode satisfazer. De acordo com nossas necessidades, assumiremos que uma classe de grupos finitos $\mathcal{C}$ satisfaz uma ou mais das seguintes propriedades:

($\mathcal{C}1$) $\mathcal{C}$ é fechada por subgrupo.

($\mathcal{C}2$) $\mathcal{C}$ é fechada pela tomada de quocientes, isto é, se $G \in \mathcal{C}$ e $K \trianglelefteq G$, então $G/K \in \mathcal{C}$.

($\mathcal{C}3$) $\mathcal{C}$ é fechada pela formação de produtos diretos finitos, isto é, se $G_i \in \mathcal{C}$ $(i = 1, \ldots, n)$, então

$$\prod_{i=1}^{n} G_i \in \mathcal{C}.$$

($\mathcal{C}4$) Se G é um grupo finito com subgrupos normais N_1 e N_2 tais que $G/N_1, G/N_2 \in \mathcal{C}$, então $G/(N_1 \cap N_2) \in \mathcal{C}$. Equivalentemente, $\mathcal{C}$ é fechado pela formação de produtos subdiretos finitos, isto é, se $G_i \in \mathcal{C}$ $(i = 1, \ldots, n)$ e G é um produto subdireto de $G_1, \ldots, G_n$, então $G \in \mathcal{C}$.

($\mathcal{C}5$) $\mathcal{C}$ é *fechado pela formação de extensões*, isto é, se

$$1 \longrightarrow K \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$$

é uma *sequência exata curta de grupos* (isto é, φ é um monomorfismo, ψ é um epimorfismo e $\mathrm{Im}(\varphi) = \ker(\psi)$) e $K, H \in \mathcal{C}$, então $G \in \mathcal{C}$.

Notemos que ($\mathcal{C}1$) mais ($\mathcal{C}3$) implica em ($\mathcal{C}4$); ($\mathcal{C}4$) implica em ($\mathcal{C}3$); e ($\mathcal{C}5$) implica em ($\mathcal{C}3$).

Por exemplo, $\mathcal{C}$ pode ser a classe de todos os

(a) grupos finitos; então $\mathcal{C}$ satisfaz as condições ($\mathcal{C}1$)–($\mathcal{C}5$). Neste caso um pro-$\mathcal{C}$ grupo é chamado *profinito*. Observemos que todo pro-$\mathcal{C}$ grupo é também profinito.

(b) grupos cíclicos finitos; então $\mathcal{C}$ satisfaz as condições ($\mathcal{C}1$) e ($\mathcal{C}2$), mas não ($\mathcal{C}3$), ($\mathcal{C}4$), ($\mathcal{C}5$). Neste caso um pro-$\mathcal{C}$ grupo é chamado *procíclico*.

(c) grupos solúveis finitos; então $\mathcal{C}$ satisfaz as condições ($\mathcal{C}1$)–($\mathcal{C}5$). Neste caso um pro-$\mathcal{C}$ grupo é chamado *prosolúvel*.

(d) grupos abelianos finitos; então $\mathcal{C}$ satisfaz as condições ($\mathcal{C}1$)–($\mathcal{C}4$), mas não ($\mathcal{C}5$). Neste caso um pro-$\mathcal{C}$ grupo é chamado *proabeliano*.

(e) grupos nilpotentes finitos; então $\mathcal{C}$ satisfaz as condições ($\mathcal{C}1$)–($\mathcal{C}4$), mas não ($\mathcal{C}5$). Neste caso um pro-$\mathcal{C}$ grupo é chamado *pronilpotente*.

(f) p-grupos finitos, para um primo fixado p; então $\mathcal{C}$ satisfaz as condições ($\mathcal{C}1$)–($\mathcal{C}5$). Neste caso um pro-$\mathcal{C}$ grupo é chamado *pro-p*.

Existem alguns nomes especiais para classes $\mathcal{C}$ de grupos finitos que satisfazem algumas das condições acima. Apresentaremos dois deles.

- Uma *formação* de grupos finitos é uma classe não-vazia de grupos finitos $\mathcal{C}$ que satisfaz ($\mathcal{C}2$) e ($\mathcal{C}4$).
- Uma *variedade* de grupos finitos é uma classe não-vazia de grupos finitos $\mathcal{C}$ que satisfaz as condições ($\mathcal{C}1$)–($\mathcal{C}3$)

Notemos que uma variedade é automaticamente uma formação, e que uma formação fechada por subgrupo é uma variedade.

Lema 3.2.2. *Seja*

$$G = \varprojlim_{i \in I} G_i$$

onde $\{G_i, \varphi_{ij}, I\}$ *é um sistema inverso de grupos finitos* G_i*, e sejam*

$$\varphi_i : G \longrightarrow G_i \quad (i \in I)$$

os homomorfismos de projeção. Então

$$\{S_i \mid S_i = \mathrm{Ker}(\varphi_i)\}$$

é um sistema fundamental de vizinhanças abertas do elemento identidade 1 *em* G.

O seguinte análogo do Teorema 3.1.6 fornece caracterizações úteis de pro-$\mathcal{C}$ grupos.

Teorema 3.2.3. *Seja $\mathcal{C}$ uma formação de grupos finitos. Então as seguintes condições em um grupo topológico G são equivalentes.*

(a) *G é um pro-$\mathcal{C}$ grupo;*

(b) *G é compacto, Hausdorff, totalmente desconexo e, para cada subgrupo normal aberto U de G, $G/U \in \mathcal{C}$;*

(c) *G é compacto e o elemento identidade 1 de G admite um sistema fundamental $\mathcal{U}$ de vizinhanças abertas U tais que $\bigcap_{U\in\mathcal{U}} U = 1$ e cada U é um subgrupo normal aberto de G com $G/U \in \mathcal{C}$;*

(d) *O elemento identidade 1 de G admite um sistema fundamental $\mathcal{U}$ de vizinhanças abertas U tal que cada U é um subgrupo normal de G com $G/U \in \mathcal{C}$, e*

$$G = \varprojlim_{U\in\mathcal{U}} G/U.$$

Demonstração: (a) $\Rightarrow$ (b): Suponhamos que

$$G = \varprojlim_{i\in I} G_i,$$

onde $\{G_i, \varphi_{ij}, I\}$ é um sistema inverso sobrejetivo de grupos em $\mathcal{C}$. Denotemos por $\varphi_i : G \longrightarrow G_i$ $(i \in I)$ os homomorfismos de projeção. De acordo com o Teorema 3.1.6, G é compacto, Hausdorff e totalmente desconexo. Seja U um subgrupo normal aberto de G. Pelo Lema 3.2.2, existe um $S_i = \mathrm{Ker}(\varphi_i)$ com $S_i \leq U$. Logo G/U é um grupo quociente de G/S_i. Como $G/S_i \in \mathcal{C}$ e $\mathcal{C}$ é fechado pela tomada de quocientes, tem-se $G/U \in \mathcal{C}$.

(b) $\Rightarrow$ (c): Pelo Teorema 3.1.6, o conjunto $\mathcal{V}$ de vizinhanças abertas e fechadas de 1 em G é um sistema fundamental de vizinhanças abertas de 1 e

$$\bigcap_{V\in\mathcal{V}} V = \{1\}.$$

Portanto, é suficiente mostrar que se V é uma vizinhança aberta e fechada de 1, então ela contém um subgrupo normal e aberto de G.

Se X é um subconjunto de G e n é um número natural, apenas para fins desta prova, denotamos por X^n o conjunto de todos os produtos $x_1 \cdots x_n$, onde $x_1, \ldots, x_n \in X$; além disso, denotamos por X^{-1} o conjunto de todos os elementos x^{-1}, onde $x \in X$.

Definamos $F = (G - V) \cap V$. Como V é compacto, V^2 também o é; logo, F é fechado e, portanto, compacto. Seja $x \in V$; então $x \notin G - F$. Pela continuidade da multiplicação, existem vizinhanças abertas V_x e S_x de x e 1 respectivamente tais que $V_x, S_x \subseteq V$ and $V_x S_x \subseteq G - F$. Pela compacidade de V, existem finitos $x_1, \ldots, x_n$ tais $V_{x_1}, \ldots, V_{x_n}$ constituem uma cobertura para V. Pomos $S = \bigcap_{i=1}^{n} S_{x_i}$, e seja $W = S \cap S^{-1}$. Então W é uma vizinhança simétrica de 1 (isto é, $w \in W$ se, e somente se, $w^{-1} \in W$), $W \subseteq V$, e $VW = G - F$. Portanto $VW \cap F = \emptyset$. Como também temos que $VW \subseteq V^2$, inferimos que $VW \cap (G - V) = \emptyset$; logo $VW \subseteq V$. Consequentemente,

$$VW^n \subseteq V,$$

para cada $n \in \mathbb{N}$. Como W é simétrico, segue que

$$R = \bigcup_{n\in\mathbb{N}} W^n$$

é um subgrupo aberto de G contido em V. Logo a interseção de todos os conjugados de R

$$R_G = \bigcap_{x\in G} (x^{-1}Rx)$$

é um subgrupo normal aberto de G. Finalmente, observemos que $R_G \subseteq V$ pois

$$R_G \leq R \subseteq VR \subseteq \bigcup_{n\in\mathbb{N}} VW^n \subseteq V.$$

Logo R_G é o subgrupo normal aberto desejado contido em V.

(c) $\Rightarrow$ (d): Seja $\mathcal{U}$ como em (c). Façamos de $\mathcal{U}$ um poset dirigido definindo $U \leq V$ se $U \subseteq V$, para $U, V \in \mathcal{U}$. Consideremos o sistema inverso $\{G/U, \varphi_{UV}\}$ de todos os grupos G/U ($U \in \mathcal{U}$) onde $\varphi_{VU} : G/U \longrightarrow G/V$ é o epimorfismo natural para $U \subseteq V$. Como os epimorfismos canônicos

$$\psi_U : G \longrightarrow G/U$$

são compatíveis, eles induzem um homomorfismo contínuo

$$\psi : G \longrightarrow \varprojlim_{U\in\mathcal{U}} G/U$$

Devemos mostrar que ψ é um isomorfismo de grupos topológicos. De acordo com o Corolário 1.1.6 de [Zal00], ψ é um epimorfismo. Para vermos que ψ é um homeomorfismo, é suficiente provar que ψ é um monomorfismo, visto que G é compacto. Agora, se $x \in G$ e $\psi(x) = 1$, então $x \in U$ para cada $U \in \mathcal{U}$. Como

$$\bigcap_{U\in\mathcal{U}} U = 1,$$

segue que $x = 1$, conforme necessário.

A implicação (d) $\Rightarrow$ (a) é imediata. □

3.3 Grupos Profinitos como Grupos de Galois

Nesta seção, vamos mostrar que, dada uma extensão galoisiana (finita ou infinita) K/F, o grupo de Galois $\mathrm{Gal}(K/F)$ é um grupo profinito. Historicamente, esta é a motivação original para o estudo de grupos profinitos e a teoria de Galois continua sendo a principal área de aplicações de resultados em grupos profinitos.

Teorema 3.3.1. *Seja K/F uma extensão galoisiana. Consideremos a coleção $\mathcal{K} = \{K_i \mid i \in I\}$ de todos os corpos intermediários $F \subseteq K_i \subseteq K$ tais que K_i/F é uma extensão galoisiana finita. Então o grupo de Galois $G = \mathrm{Gal}(K/F)$, munido da Topologia de Krull, é um grupo profinito. Mais ainda,*

$$\mathrm{Gal}(K/F) \cong \varprojlim_{i\in I} \mathrm{Gal}(K_i/F).$$

Demonstração: Para cada $i \in I$, consideremos o grupo de Galois finito $G_i = \mathrm{Gal}(K_i/F)$. Seja $U_i = \mathrm{Gal}(K/K_i)$. Com esta notação, tem-se $G_i \cong G/U_i$. Definimos uma relação de ordem parcial $\preceq$ no conjunto I da seguinte forma. Sejam $i, j \in I$; então

$$i \preceq j \text{ se } K_i \subseteq K_j, \text{ ou equivalentemente se } U_i = \mathrm{Gal}(K/K_i) \geq U_j = \mathrm{Gal}(K/K_j).$$

Claramente $(I, \preceq)$ é um poset. Mais ainda, é um poset dirigido. De fato, se $K_i, K_j \in K$, então existem polinômios $f_i(X), f_j(X) \in F[X]$ stais que K_i e K_j são os corpos de decomposição contidos em K de $f_i(X)$ e $f_j(X)$ sobre F, respectivamente. Seja L o corpo de decomposição sobre F do polinômio $f_i(X)f_j(X)$, com $L \subseteq K$. Então $L \subseteq \mathcal{K}$. Digamos que $L = K_t$ para algum $t \in I$. Então por definição $t \succeq i, j$.

Se $i \preceq j$, definimos

$$\varphi_{ji} : G_j = \mathrm{Gal}(K_j/F) \longrightarrow G_i = \mathrm{Gal}(K_i/F)$$

por restrição, isto é, $\varphi_{ji}(\sigma) = \sigma|_{K_i}$, onde $\sigma \in G_{K_j/F}$. Observemos que φ_{ji} está bem definida, pois $\sigma(K_i) = K_i$, visto que K_i/F é uma extensão normal. Nós obtemos desta maneira um sistema inverso $\{G_i, \varphi_{ji}, I\}$ de grupos de Galois finitos. Consideremos os homomorfismos

$$\Phi : G = \mathrm{Gal}(K/F) \longrightarrow \varprojlim_{i \in I} G_i \leq \prod_{i \in I} G_i$$

definidos por

$$\Phi(\sigma) = (\sigma|_{K_i}).$$

Devemos mostrar que Φ é um isomorfismo de grupos topológicos. Ele é um monomorfismo, visto que $\mathrm{Ker}(\Phi) = \bigcap_{i \in I} G_i = 1$. O homomorfismo Φ é contínuo pois a composição

$$G \longrightarrow \varprojlim_{i \in I} G_i \longrightarrow G_i$$

é contínua para cada $i \in I$. Além disso, Φ é uma aplicação aberta pois

$$\Phi(U_i) = \left(\varprojlim G_i\right) \cap \left[\left(\prod_{K_j \not\subseteq K_i} G_j \right) \times \left(\prod_{K_j \subseteq K_i} \{1\}_j \right) \right].$$

Finalmente, Φ é um epimorfismo. De fato, se $(\sigma_i) \in \varprojlim G_i$, definimos $\sigma : K \longrightarrow K$ por $\sigma(k) = \sigma_i(k)$ para $k \in K_i$; então $\sigma \in G$ and $\Phi(\sigma) = (\sigma_i)$. Com isso nós provamos que $G \cong \varprojlim G_i$. O resultado agora segue da caracterização de grupos profinitos obtida no Teorema 3.2.3. □

Capítulo 4

Números p-ádicos

Neste capítulo, estudaremos a construção e algumas propriedades do corpo $\mathbb{Q}_p$ dos números p-ádicos.

4.1 Métricas nos números racionais

Conhecemos uma métrica em $\mathbb{Q}$, que é induzida pelo valor absoluto. Nesta subseção, veremos outras métricas que podem ser definidas no conjunto dos números racionais.

Definição 4.1.1. *Seja $p \in \{2, 3, 5, 7, 11, 13, ...\}$ um primo qualquer. Para qualquer inteiro não-nulo a, o ordinal p-ádico de a, denotado por $\mathrm{ord}_p a$, é a maior potência de p que divide a, isto é, o maior m tal que $a \equiv 0 \pmod{p^m}$.*

Por exemplo:

$$\mathrm{ord}_5 35 = 1, \qquad \mathrm{ord}_5 250 = 3, \qquad \mathrm{ord}_2 96 = 5, \qquad \mathrm{ord}_2 97 = 0.$$

Se $a = 0$, convencionamos escrever $\mathrm{ord}_p 0 = \infty$. Notemos que ord_p se comporta de forma parecida com o logaritmo: $\mathrm{ord}_p(a_1 a_2) = \mathrm{ord}_p a_1 + \mathrm{ord}_p a_2$.

Para qualquer número racional $x = a/b$, definimos $\mathrm{ord}_p x$ como $\mathrm{ord}_p a - \mathrm{ord}_p b$. Notemos que essa expressão depende apenas de x, e não de a e b, isto é, se escrevermos $x = ac/bc$, obtemos o mesmo valor para $\mathrm{ord}_p x = \mathrm{ord}_p ac - \mathrm{ord}_p bc$.

Definimos então uma aplicação $|\ |_p$ em $\mathbb{Q}$ da seguinte forma:

$$|x|_p = \begin{cases} \dfrac{1}{p^{\mathrm{ord}_p x}}, & \text{se } x \neq 0 \\ 0, & \text{se } x = 0. \end{cases}$$

Proposição 4.1.2. *$|\ |_p$ é uma norma em $\mathbb{Q}$.*

Demonstração: Vamos verificar a desigualdade triangular. Se $x = 0$ ou $y = 0$, ou se $x + y = 0$, a desigualdade triangular é trivial, então vamos supor que x, y e $x + y$ são todos não-nulos. Sejam $x = a/b$ e $y = c/d$ escritos na forma irredutível. Então temos: $x + y = (ad + bc)/bd$, e $\mathrm{ord}_p(x + y) = \mathrm{ord}_p(ad + bc) - \mathrm{ord}_p b - \mathrm{ord}_p d$. Agora, notemos que a maior potência de p que divide a soma de dois números é pelo menos o mínimo entre a maior potência que divide o primeiro e a maior potência que divide o segundo. Desta forma, temos

$$\begin{aligned}\mathrm{ord}_p(x+y) &\geq \min(\mathrm{ord}_p ad, \mathrm{ord}_p bc) - \mathrm{ord}_p b - \mathrm{ord}_p d \\ &= \min(\mathrm{ord}_p a + \mathrm{ord}_p d, \mathrm{ord}_p b + \mathrm{ord}_p c) - \mathrm{ord}_p b - \mathrm{ord}_p d \\ &= \min(\mathrm{ord}_p a - \mathrm{ord}_p b, \mathrm{ord}_p c - \mathrm{ord}_p d) \\ &= \min(\mathrm{ord}_p x, \mathrm{ord}_p y)\end{aligned}$$

Portanto, $|x+y|_p = p^{-\mathrm{ord}_p(x+y)} \leq \max(p^{-\mathrm{ord}_p x}, p^{-\mathrm{ord}_p y}) = \max(|x|_p, |y|_p)$, e isto é $\leq |x|_p + |y|_p$. As outras propriedades de norma são imediatas. Logo, $|\ |_p$ é uma norma em $\mathbb{Q}$, como afirmado. □

Na verdade, nós provamos uma desigualdade mais forte do que a triangular, e é essa desigualdade mais forte que leva à definição básica da análise p-ádica.

Definição 4.1.3. *Uma norma é chamada não-arquimediana se a desigualdade* $|x+y| \leq \max(|x|, |y|)$ *sempre for válida. Uma métrica é chamada não-arquimediana se para todo* z *vale* $d(x,y) \leq \max(d(x,z), d(z,y))$*; em particular, uma norma não-arquimediana induz uma métrica não-arquimediana, visto que nesse caso,* $d(x,y) = |x-y| = |(x-z)+(z-y)| \leq \max(|x-z|, |z-y|) = \max(d(x,z), d(z,y))$.

Portanto, $|\ |_p$ é uma norma não-arquimediana em $\mathbb{Q}$. Uma norma (ou métrica) que não é não-arquimediana é chamada arquimediana. O valor absoluto é uma norma arquimediana em $\mathbb{Q}$.

Em qualquer espaço métrico X, existe a noção de uma sequência de Cauchy (a_n) de elementos de X. Isso significa que para qualquer $\varepsilon > 0$, existe um N tal que $d(a_m, a_n) < \varepsilon$ sempre que $m > N$ e $n > N$.

Dizemos que duas métricas d_1 e d_2 em um conjunto X são equivalentes se uma sequência é de Cauchy em relação a d_1 se, e somente se, for de Cauchy em relação a d_2. Dizemos que duas normas são equivalentes se elas induzem métricas equivalentes.

Na definição de $|\ |_p$, ao invés de $(1/p)^{\mathrm{ord}_p x}$, poderíamos ter escrito $\rho^{\mathrm{ord}_p x}$ para qualquer $\rho \in (0,1)$. Nós teríamos obtido uma norma não-arquimediana equivalente. Tem-se também uma família de normas arquimedianas que são equivalentes ao valor absoluto usual $|\ |$, a saber, as normas $|\ |^\alpha$ quando $0 < \alpha \leq 1$.

Às vezes escrevemos $|\ |_\infty$ para denotar o valor absoluto usual. Esta é apenas uma convenção de notação e não pretende implicar qualquer relação direta entre $|\ |_\infty$ e $|\ |_p$.

O termo norma "trivial" se refere à norma $|\ |$ tal que $|0| = 0$ e $|x| = 1$ para $x \neq 0$.

Teorema 4.1.4. (Ostrowski). *Toda norma não-trivial* $\|\ \|$ *em* $\mathbb{Q}$ *é equivalente a* $|\ |_p$ *para algum primo* p *ou para* $p = \infty$.

Demonstração: Caso (i). Suponhamos que existe um inteiro positivo n tal que $\|n\| > 1$. Seja n_0 o menor n com essa propriedade. Como $\|n_0\| > 1$, existe um número real positivo α tal que $\|n_0\| = n_0^\alpha$. Agora escrevamos qualquer inteiro positivo n na base n_0, isto é, na forma

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s, \quad \text{onde } 0 \leq a_i < n_0 \text{ e } a_s \neq 0.$$

Então

$$\begin{aligned}\|n\| &\leq \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \cdots + \|a_s n_0^s\| \\ &= \|a_0\| + \|a_1\| \cdot n_0^\alpha + \|a_2\| \cdot n_0^{2\alpha} + \cdots + \|a_s\| \cdot n_0^{s\alpha}.\end{aligned}$$

Como todos os a_i são $< n_0$, pela nossa escolha de n_0 temos $\|a_i\| \leq 1$, e então

$$\begin{aligned}\|n\| &\leq 1 + n_0^{\alpha} + n_0^{2\alpha} + \cdots + n_0^{s\alpha} \\ &= n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-s\alpha}) \\ &\leq n^{\alpha}\left[\sum_{i=0}^{\infty}(1/n_0^{\alpha})^i\right],\end{aligned}$$

pois $n \geq n_0^s$. A expressão dentro dos colchetes é uma constante finita, que chamaremos de C. Logo,

$$\|n\| \leq Cn^{\alpha} \quad \text{para todo } n = 1, 2, 3, \ldots.$$

Agora tomamos qualquer n and qualquer N grande, e pomos n^N no lugar de n na desigualdade acima; então tiramos a raíz N-ésima. Obtemos

$$\|n\| \leq \sqrt[N]{C}n^{\alpha}.$$

Fazendo N tender para infinito para n fixado, obtém-se $\|n\| \leq n^{\alpha}$.

Podemos obter a outra desigualdade da seguinte forma. Se n for escrito na base n_0 como antes, temos $n_0^{s+1} > n \geq n_0^s$. Como $\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leq \|n\| + \|n_0^{s+1} - n\|$, temos

$$\begin{aligned}\|n\| &\geq \|n_0^{s+1}\| - \|n_0^{s+1} - n\| \\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^{\alpha},\end{aligned}$$

visto que $\|n_0^{s+1}\| = \|n_0\|^{s+1}$, e podemos usar a primeira desigualdade (isto é, $\|n\| \leq n^{\alpha}$) no termo que está sendo subtraído. Logo,

$$\begin{aligned}\|n\| &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^{\alpha} \quad \text{(visto que } n \geq n_0^s\text{)} \\ &= n_0^{(s+1)\alpha}\left[1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right] \\ &\geq C'n^{\alpha}\end{aligned}$$

para alguma constante C' que pode depender de n_0 e α mas não de n. Como antes, agora usamos essa desigualdade para n^N, tiramos a raiz N-ésima, e fazemos N tender para infinito, finalmente obtendo: $\|n\| \geq n^{\alpha}$.

Portando, $\|n\| = n^{\alpha}$. Pelas propriedades de norma, segue que $\|x\| = |x|^{\alpha}$ para todo $x \in \mathbb{Q}$, e uma norma como esta é equivalente à norma do valor absoluto $|\ |$. Isso conclui a prova do teorema no Caso (i).

Caso (ii). Suponhamos que $\|n\| \leq 1$ para todos os inteiros positivos n. Seja n_0 o menor n tal que $\|n\| < 1$; n_0 existe pois assumimos que $\|\ \|$ é não-trivial.

O número n_0 deve ser primo, pois se $n_0 = n_1 \cdot n_2$ com n_1 e n_2 ambos $< n_0$, então $\|n_1\| = \|n_2\| = 1$, e portanto $\|n_0\| = \|n_1\| \cdot \|n_2\| = 1$. Logo seja p o primo n_0.

Afirmamos que $\|q\| = 1$ se q é um primo diferente de p. Suponhamos que não; então $\|q\| < 1$, e para algum N grande temos $\|q^N\| = \|q\|^N < \frac{1}{2}$. Além disso, para algum M grande, temos $\|p^M\| < \frac{1}{2}$. Como p^M e q^N são co-primos, podemos encontrar inteiros m e n tais que: $mp^M + nq^N = 1$. Mas então

$$1 = \|1\| = \|mp^M + nq^N\| \leq \|mp^M\| + \|nq^N\| = \|m\|\|p^M\| + \|n\|\|q^N\|,$$

como consequência das propriedades de uma norma. Mas $\|m\|, \|n\| \leq 1$, logo

$$1 \leq \|p^M\| + \|q^N\| < \frac{1}{2} + \frac{1}{2} = 1,$$

uma contradição. Portanto, $\|q\| = 1$.

O trabalho está praticamente finalizado, visto que qualquer inteiro positivo a pode ser fatorado em divisores primos: $a = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$. Então

$$\|a\| = \|p_1\|^{b_1} \|p_2\|^{b_2} \cdots \|p_r\|^{b_r}.$$

Mas o único $\|p_i\|$ que não é igual a 1 será $\|p\|$ se um dos p_i's for p. O seu b_i correspondente será $\mathrm{ord}_p a$. Logo, se denotarmos $\rho = \|p\| < 1$, temos

$$\|a\| = \rho^{\mathrm{ord}_p a}.$$

Pelas propriedades de norma, podemos concluir que essa igualdade é válida para qualquer número racional não-nulo x no lugar de a. E uma norma que satisfaz essa propriedade é equivalente a $|\ |_p$, o que conclui a prova do teorema de Ostrowski. □

Nossa intuição sobre distância está baseada, é claro, na métrica arquimediana $|\ |_\infty$. Algumas propriedades das métricas não arquimedianas $|\ |_p$ parecem muito estranhas no início e demora um pouco até nos acostumarmos. Aqui estão dois exemplos.

Para qualquer métrica, a propriedade $d(x, y) \leq d(x, z) + d(z, y)$ é conhecida como desigualdade triangular pois no caso do corpo $\mathbb{C}$ dos números complexos (com a métrica $d(a + bi, c + di) = \sqrt{(a - c)^2 + (b - d)^2}$) ela diz que no plano complexo a soma de dois lados de um triângulo é maior do que o terceiro lado.

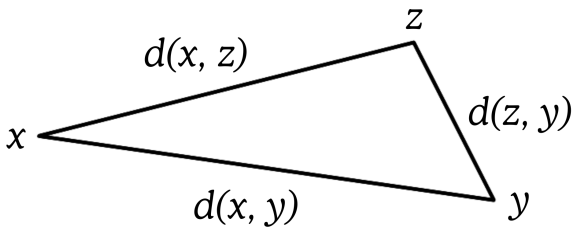


Figura 4.1: Desigualdade Triangular

Vejamos o que ocorre com uma norma não-arquimediana em um corpo F. Por simplicidade, vamos supor $z = 0$. Então, pela desigualdade triangular não-arquimediana, temos: $|x - y| \leq \max(|x|, |y|)$. Suponhamos que os "lados" x e y possuem "comprimentos" diferentes, digamos $|x| < |y|$. O terceiro lado $|x - y|$ tem comprimento

$$|x - y| \leq |y|.$$

Mas

$$|y| = |x - (x - y)| \leq \max(|x|, |x - y|)$$

Como $|y|$ não é $\leq |x|$, devemos ter $|y| \leq |x-y|$, e logo $|y| = |x-y|$.

Portanto, se dois lados x e y não são iguais em comprimento, o maior deles deve ter o mesmo comprimento do terceiro lado. Ou seja, todo triângulo é isósceles.

Isso realmente não deveria ser muito surpreendente se pensarmos no que isso diz no caso de $|\ |_p$ em $\mathbb{Q}$. Isso diz que, se dois números racionais são divisíveis por potências diferentes de p, então a sua diferença é divisível precisamente pela menor potência de p (que é o que significa ter o mesmo "tamanho" que o maior dos dois).

Essa propriedade básica de um corpo não-arquimediano – que $|x \pm y| \leq \max(|x|, |y|)$, com a igualdade ocorrendo se $|x| \neq |y|$ – será chamada de "princípio do triângulo isósceles" daqui em diante.

Como um segundo exemplo, definimos o disco aberto de raio r (r é um número real positivo) com centro a (a é um elemento do corpo F) como

$$D(a;r) = \{x \in F; |x-a| < r\}.$$

Suponhamos que $|\ |$ é uma norma não-arquimediana. Seja b um elemento qualquer em $D(a;r)$. Então

$$D(a;r) = D(b;r),$$

isto é, todo ponto no disco é um centro. Porque isso ocorre? Bem,

$$\begin{aligned} x \in D(a;r) &\Rightarrow |x-a| < r \\ &\Rightarrow |x-b| = |(x-a)+(a-b)| \\ &\qquad \leq \max(|x-a|, |a-b|) \\ &\qquad < r \\ &\Rightarrow x \in D(b;r) \end{aligned}$$

e a implicação reversa é demonstrada exatamente da mesma maneira.

Se definirmos o disco fechado de raio r e centro a como

$$D[a;r] = \{x \in F; |x-a| \leq r\},$$

para $|\ |$ não-arquimediana, nós analogamente encontramos que cada ponto em $D[a;r]$ é um centro.

4.2 O corpo dos números p-ádicos

Ao longo desta subseção, vamos fixar um número primo $p \neq \infty$.

Seja S o conjunto de sequências $\{a_i\}$ de números racionais tais que, dado $\varepsilon > 0$, existe N tal que $|a_i - a_j|_p < \varepsilon$ se ambos $i, j > N$. Dizemos que duas dessas sequências de Cauchy $\{a_i\}$ e $\{b_i\}$ são equivalentes se $|a_i - b_i|_p \to 0$ quando $i \to \infty$. Definimos o conjunto $\mathbb{Q}_p$ como o conjunto das classes de equivalência de sequências de Cauchy.

Para qualquer $x \in \mathbb{Q}$, seja $\{x\}$ a sequência de Cauchy "constante" em que todos os termos são iguais a x. É óbvio que $\{x\} \sim \{x'\}$ se, e somente se, $x = x'$. A classe de equivalência de $\{0\}$ é denotada simplesmente por 0.

Definimos a norma $|\ |_p$ de uma classe de equivalência a como $\lim_{i\to\infty} |a_i|_p$, onde $\{a_i\}$ é um representante qualquer de a. O limite existe pois

1. Se $a = 0$, então por definição $\lim_{i\to\infty} |a_i|_p = 0$.

2. Se $a \neq 0$, então para algum ε e para todo N existe um $i_N > N$ com $|a_{i_N}|_p > \varepsilon$.

Escolhendo N suficientemente grande para que $|a_i - a_j|_p < \varepsilon$ quando $i, j > N$, temos:

$$|a_i - a_{i_N}|_p < \varepsilon \text{ para todo } i > N.$$

Como $|a_{i_N}|_p > \varepsilon$, segue-se pelo "princípio do triângulo isósceles" que $|a_i|_p = |a_{i_N}|_p$. Logo, para todo $i > N$, $|a_i|_p$ tem o valor constante $|a_{i_N}|_p$. Esse valor constante é então $\lim_{i\to\infty} |a_i|_p$

Uma diferença importante do processo de completar $\mathbb{Q}$ para obter $\mathbb{R}$ deve ser notada. Indo de $\mathbb{Q}$ para $\mathbb{R}$ os valores possíveis de $|\ | = |\ |_\infty$ foram extendidos para incluir todos os números reais não-negativos. Mas indo de $\mathbb{Q}$ para $\mathbb{Q}_p$ os valores possíveis de $|\ |_p$ permanecem os mesmos, a saber, $\{p^n\}_{n\in\mathbb{Z}} \cup \{0\}$.

Dadas duas classes de equivalência a e b de sequências de Cauchy, escolhemos quaisquer representantes $\{a_i\} \in a$ e $\{b_i\} \in b$, e definimos $a \cdot b$ como a classe de equivalência representada pela sequência de Cauchy $\{a_i b_i\}$. Se tivéssemos escolhido outras sequências $\{a'_i\} \in a$ e $\{b'_i\} \in b$, teríamos obtido

$$\begin{aligned} |a'_i b'_i - a_i b_i|_p &= |a'_i(b'_i - b_i) + b_i(a'_i - a_i)|_p \\ &\leq \max(|a'_i(b'_i - b_i)|_p, |b_i(a'_i - a_i)|_p); \end{aligned}$$

à medida que $i \to \infty$, a primeira expressão se aproxima de $|a|_p \cdot \lim |b'_i - b_i|_p = 0$, e a segunda expressão se aproxima de $|b|_p \cdot \lim |a'_i - a_i|_p = 0$. Logo, $\{a'_i b'_i\} \sim \{a_i b_i\}$.

Definimos similarmente a soma de duas classes de equivalência de sequências de Cauchy escolhendo uma sequência em cada classe, definindo a adição termo a termo, e mostrando que a classe de equivalência da soma depende apenas das classes de equivalência das duas parcelas. Inversos aditivos também são definidos da maneira óbvia.

Para inversos multiplicativos, temos que ser um pouco cuidadosos por causa da possibilidade de existirem termos nulos em uma sequência de Cauchy. No entanto, é fácil ver que toda sequência de Cauchy é equivalente a uma sem termos nulos (por exemplo, se $a_i = 0$, substitua a_i por $a'_i = p^i$). Então tome a sequência $\{1/a_i\}$. Essa sequência será Cauchy a menos que $|a_i|_p \to 0$, isto é, a menos que $\{a_i\} \sim \{0\}$. Mais ainda, se $\{a_i\} \sim \{a'_i\}$ e nenhum a_i ou a'_i é zero, então $\{1/a_i\} \sim \{1/a'_i\}$ é facilmente provado.

Agora podemos verificar que o conjunto $\mathbb{Q}_p$ das classes de equivalência de sequências de Cauchy é um corpo com adição, multiplicação e inversos definidos como acima. Por exemplo, distributividade: sejam $\{a_i\}$, $\{b_i\}$, $\{c_i\}$ representantes de a, b, $c \in \mathbb{Q}_p$; então $a(b + c)$ é a classe de equivalência de

$$\{a_i(b_i + c_i)\} + \{a_i b_i + a_i c_i\},$$

e $ab + ac$ é também a classe de equivalência dessa sequência.

$\mathbb{Q}$ pode ser identificado com o subcorpo de $\mathbb{Q}_p$ formado pelas classes de equivalência que contêm uma sequência de Cauchy constante. Sob essa identificação, notemos que $|\ |_p$ em $\mathbb{Q}_p$ se restringe a $|\ |_p$ usual em $\mathbb{Q}$.

Finalmente, vamos mostrar que $\mathbb{Q}_p$ é completo: se $\{a_j\}_{j=1,2,\ldots}$ é uma sequência de classes de equivalência que é Cauchy em $\mathbb{Q}_p$, e se tomarmos sequências de Cauchy

representantes de número racionais $\{a_{ji}\}_{i=1,2,...}$ para cada a_j, onde para cada j tem-se $|a_{ji} - a_{ji'}|_p < p^{-j}$ sempre que $i, i' \geq N_j$, então a classe de equivalência de $\{a_{jN_j}\}_{j=1,2,...}$ é o limite dos a_j.

Provavelmente é adequado passar por uma construção como essa, para não esquecer totalmente os fundamentos axiomáticos sobre os quais tudo se apoia. Neste caso em particular, a abordagem abstrata também nos dá a chance de comparar a construção p-ádica com a construção dos reais, e ver que o procedimento é logicamente o mesmo. No entanto, após o Teorema 4.2.2, seria sensato esquecer o mais rápido possível sobre "classes de equivalência de sequências de Cauchy" e começar a pensar em termos mais concretos. Para demonstrar este Teorema, vamos precisar do seguinte Lema.

Lema 4.2.1. *Se $x \in \mathbb{Q}$ e $|x|_p \leq 1$, então para qualquer i existe um inteiro $\alpha \in \mathbb{Z}$ tal que $|\alpha - x|_p \leq p^{-i}$. O inteiro α pode ser escolhido no conjunto $\{0, 1, 2, 3, ..., p^i - 1\}$.*

Demonstração: Seja $x = a/b$ escrito na forma irredutível. Como $|x|_p \leq 1$, segue que p não divide b, e portanto b e p^i são co-primos. Logo podemos encontrar inteiros m e n tais que: $mb + np^i = 1$. Seja $\alpha = am$. A ideia é que mb difere de 1 por uma quantidade p-adicamente pequena, de modo que m é uma boa aproximação para $1/b$, e então am é uma boa aproximação para $x = a/b$. Mais precisamente, temos:

$$\begin{aligned} |\alpha - x|_p &= |am - (a/b)|_p = |a/b|_p |mb - 1|_p \\ &\leq |mb - 1|_p = |np^i|_p = |n|_p / p^i \leq 1/p^i. \end{aligned}$$

Finalmente, podemos adicionar um múltiplo de p^i ao inteiro α para obter um inteiro de 0 a $p^i - 1$ tal que $|\alpha - x|_p \leq p^{-i}$ continua valendo. Assim o lema está provado. □

Teorema 4.2.2. *Toda classe de equivalência a em $\mathbb{Q}_p$ tal que $|a|_p \leq 1$ possui exatamente uma sequência de Cauchy representante da forma $\{a_i\}$ tal que:*

(a) $0 \leq a_i < a_{i+1}$ *para* $i = 1, 2, 3, ...$

(b) $a_i \equiv a_{i+1} \pmod{p^i}$ *para* $i = 1, 2, 3, ...$

Demonstração: Primeiramente, provamos a unicidade. Se $\{a'_i\}$ é uma sequência diferente satisfazendo (a) e (b), e se $a_{i_0} \neq a'_{i_0}$, então $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}}$, pois ambos estão entre 0 e p^{i_0}. Mas então, para todo $i \geq i_0$, tem-se $a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \pmod{p^{i_0}}$, isto é, $a_i \not\equiv a'_i \pmod{p^{i_0}}$. Logo

$$|a_i - a'_i|_p > 1/p^{i_0}$$

para todo $i \geq i_0$, e $\{a_i\} \not\sim \{a'_i\}$.

Agora suponhamos que temos uma sequência de Cauchy $\{b_i\}$. Para cada $j = 1, 2, 3, ...$, seja $N(j)$ um número natural tal que $|b_i - b_{i'}|_p \leq p^{-j}$ sempre que $i, i' \geq N(j)$. (Podemos tomar a sequência $N(j)$ de forma que ela seja estritamente crescente com j; em particular, $N(j) \geq j$.) Notemos que $|b_i|_p \leq 1$ se $i \geq N(1)$, pois para todo $i' \geq N(1)$

$$\begin{aligned} |b_i|_p &\leq \max(|b_{i'}|_p, |b_i - b_{i'}|_p) \\ &\leq \max(|b_{i'}|_p, 1/p), \end{aligned}$$

e $|b_{i'}|_p \to |a|_p \leq 1$ quando $i' \to \infty$.

Agora vamos usar o Lema 4.2.1 para encontrar uma sequência de inteiros a_j, onde $0 \leq a_j < p_j$, tal que

$$|a_j - b_{N(j)}|_p \leq 1/p^j.$$

Afirmamos que $\{a_j\}$ é a sequência desejada. Resta mostrar que $a_{j+1} \equiv a_j \pmod{p^j}$ e que $\{b_i\} \sim \{a_j\}$. A primeira afirmação segue pois

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \\ &\leq \max(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p) \\ &\leq \max(1/p^{j+1}, 1/p^j, 1/p^j) \\ &= 1/p^j. \end{aligned}$$

A segunda afirmação segue pois, dado qualquer j, para $i \geq N(j)$, tem-se

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p) \\ &\leq \max(1/p^j, 1/p^j, 1/p^j) \\ &= 1/p^j. \end{aligned}$$

Logo $|a_i - b_i|_p \to 0$ quando $i \to \infty$. O teorema está provado. □

E se o nosso número p-ádico a não satisfaz a condição $|a|_p \leq 1$? Então podemos multiplicar a por uma potência p^m de p (no caso, pela potência de p que é igual a $|a|_p$), para obter um número p-ádico $a' = ap^m$ que satisfaz $|a'|_p \leq 1$. Então a' é representado por uma sequência $\{a'_i\}$ como no teorema, e $a = a'p^{-m}$ é representado por uma sequência $\{a_i\}$ em que $a_i = a'_i p^{-m}$.

Agora é conveniente escrever todos os a'_i na sequência para a' na base p, isto é,

$$a'_i = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1} p^{i-1},$$

onde os b's são inteiros em $\{0, 1, ..., p-1\}$. A condição $a'_i \equiv a'_{i+1} \pmod{p^i}$ significa precisamente que

$$a'_{i+1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1} p^{i-1} + b_i p^i,$$

onde os dígitos b_0 a b_{i-1} são todos iguais aos de a'_i. Assim, a' pode ser pensado intuitivamente como um número, escrito na base p, que se estende infinitamente para a direita, isto é, nós adicionamos um novo dígito cada vez que passamos de a'_i para a'_{i+1}.

Nosso a original pode então ser pensado como um número decimal de base p que tem apenas um número finito de dígitos "à direita do ponto decimal" (isto é, correspondendo a potências negativas de p, mas na verdade escrito a partir da esquerda) mas que possui infinitos dígitos para potências positivas de p:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \cdots$$

Aqui, por enquanto, a expressão à direita é apenas uma abreviação para a sequência $\{a_i\}$, onde $a_i = b_0 p^{-m} + \cdots + b_{i-1} p^{i-1-m}$, isto é, uma forma conveniente de pensar a sequência $\{a_i\}$ toda de uma vez. Logo veremos que essa igualdade é em um sentido preciso uma igualdade "real". Essa igualdade é chamada de "expansão p-ádica" de a.

Agora, seja $\mathbb{Z}_p = \{a \in \mathbb{Q}_p; |a|_p \leq 1\}$. Este é o conjunto de todos os números em $\mathbb{Q}_p$ cuja expansão p-ádica não envolve potências negativas de p. Um elemento de $\mathbb{Z}_p$ é chamado um "inteiro p-ádico". (A partir de agora, para evitar confusão, quando nos referirmos a um inteiro antigo em $\mathbb{Z}$, diremos "inteiro racional".) A soma, a diferença e o produto de dois elementos de $\mathbb{Z}_p$ está em $\mathbb{Z}_p$, logo $\mathbb{Z}_p$ é um subanel do corpo $\mathbb{Q}_p$.

Se $a, b \in \mathbb{Q}_p$, escrevemos $a \equiv b \pmod{p^n}$ se $|a - b|_p \leq p^{-n}$, ou equivalentemente, $(a - b)/p^n \in \mathbb{Z}_p$, isto é, se o primeiro dígito não-nulo na expansão p-ádica de $a - b$ ocorre não antes do p^n-ésimo lugar. Se a e b não estão apenas em $\mathbb{Q}_p$ mas estão na verdade em $\mathbb{Z}$ (isto é, são inteiros racionais), então esta definição está de acordo com a definição anterior de $a \equiv b \pmod{p^n}$.

Definimos $\mathbb{Z}_p^*$ como $\{x \in \mathbb{Z}_p; 1/x \in \mathbb{Z}_p\}$, ou equivalentemente como $\{x \in \mathbb{Z}_p; x \not\equiv 0 (\text{mod } p)\}$, ou equivalentemente como $\{x \in \mathbb{Z}_p; |x|_p = 1\}$. Um inteiro p-ádico em $\mathbb{Z}_p^*$ é também chamado uma "unidade p-ádica".

Agora, seja $\{b_i\}_{i=-m}^{\infty}$ uma sequência qualquer de inteiros p-ádicos. Consideremos a soma

$$S_N = \frac{b_{-m}}{p^m} + \frac{b_{-m+1}}{p^{m-1}} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_N p^N.$$

Essa sequência de somas parciais é claramente Cauchy: se $M > N$, então $|S_N - S_M|_p < 1/p^N$. Logo ela converge para um elemento de $\mathbb{Q}_p$. Como no caso de séries de números reais, definimos $\sum_{i=-m}^{\infty} b_i p^i$ como esse limite em $\mathbb{Q}_p$.

Mais geralmente, se $\{c_i\}$ é uma sequência qualquer de números p-ádicos tal que $|c_i|_p \to 0$ quando $i \to \infty$, a sequência de somas parciais $S_N = c_1 + c_2 + \cdots + c_N$ converge para um limite, o qual denotamos por $\sum_{i=1}^{\infty} c_i$. Isso ocorre pois: $|S_M - S_N|_p = |c_{N+1} + c_{N+2} + \cdots + c_M|_p \leq \max(|c_{N+1}|_p, |c_{N+2}|_p, \cdots, |c_M|_p)$ que $\to 0$ quando $N \to \infty$. Assim, séries p-ádicas são mais fáceis de verificar quanto à convergência do que séries de números reais. Uma série converge em $\mathbb{Q}_p$ se, e somente se, seus termos se aproximam de zero. Não existe algo como a série harmônica $1 + \frac{1}{2} + \frac{1}{3} + \cdots$ de números reais, que diverge mesmo que seus termos se aproximem de 0. Lembremos que a razão para isso é que $|\ |_p$ de uma soma é limitada pelo máximo (ao invés de apenas a soma) das $|\ |_p$ das parcelas quando $p \neq \infty$, isto é, quando $|\ |_p$ é não-arquimediana.

Retornando agora a expansões p-ádicas, vemos que a série infinita à direita na definição de expansão p-ádica

$$\frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m-1} p + b_{m-2} p^2 + \cdots$$

(aqui $b_i \in \{0, 1, 2, ..., p-1\}$) converge para a, e portanto a igualdade pode ser vista no sentido da soma de uma série infinita.

Notemos que a afirmação da unicidade no Teorema 4.2.2 é algo que não temos no caso arquimediano. Ou seja, decimais terminais também podem ser representados por dízimas que possuem algum período: $1 = 0.999\ldots = 0.\overline{9}$. Porém, se duas expansões p-ádicas convergem para o mesmo número em $\mathbb{Q}_p$, então elas são as mesmas, isto é, todos os seus dígitos são os mesmos.

4.3 Aritmética em $\mathbb{Q}_p$

A mecânica de adição, subtração, multiplicação e divisão de números p-ádicos é muito parecida com as operações correspondentes em decimais. A única diferença é que os algoritmos são feitos da esquerda para a direita ao invés da direita para a esquerda. Aqui estão dois exemplos em $\mathbb{Q}_7$:

$$\begin{array}{rccccccc} & 3 & + & 6\cdot 7 & + & 2\cdot 7^2 & +\cdots \\ \times & 4 & + & 5\cdot 7 & + & 1\cdot 7^2 & +\cdots \\ \hline & 5 & + & 4\cdot 7 & + & 4\cdot 7^2 & +\cdots \\ & & & 1\cdot 7 & + & 4\cdot 7^2 & +\cdots \\ & & & & & 3\cdot 7^2 & +\cdots \\ \hline & 5 & + & 5\cdot 7 & + & 4\cdot 7^2 & +\cdots \end{array}$$

$$\begin{array}{rccccccc} & 2\cdot 7^{-1} & + & 0\cdot 7^0 & + & 3\cdot 7^1 & +\cdots \\ - & 4\cdot 7^{-1} & + & 6\cdot 7^0 & + & 5\cdot 7^1 & +\cdots \\ \hline & 5\cdot 7^{-1} & + & 0\cdot 7^0 & + & 4\cdot 7^1 & +\cdots \end{array}$$

Como outro exemplo, vamos tentar extrair o análogo para $\sqrt{6}$ em $\mathbb{Q}_5$, isto é, queremos encontrar $a_0, a_1, a_2, \ldots$, $0 \le a_i \le 4$, tais que

$$(a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots)^2 = 1 + 1 \cdot 5.$$

Comparando os coeficientes de $1 = 5^0$ em ambos os lados, tem-se $a_0^2 \equiv 1 \pmod 5$, e portanto $a_0 = 1$ ou 4. Tomemos $a_0 = 1$. Então comparando os coeficientes de 5 em ambos os lados, encontramos $2a_1 \cdot 5 \equiv 1 \cdot 5 \pmod{5^2}$, logo $2a_1 \equiv 1 \pmod 5$, e então $a_1 = 3$. No próximo passo temos:

$$1 + 1 \cdot 5 \equiv (1 + 3 \cdot 5 + a_2 \cdot 5^2)^2 \equiv 1 + 1 \cdot 5 + 2a_2 \cdot 5^2 \pmod{5^3}.$$

Portanto $2a_2 \equiv 0 \pmod 5$, e $a_2 = 0$. Procedendo desta maneira, vamos encontrar uma série

$$a = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + a_4 \cdot 5^4 + a_5 \cdot 5^5 + \cdots$$

onde cada a_i depois a_0 está unicamente determinado.

Mas lembremos que nós temos duas escolhas para a_0: 1 e 4. E se tivéssemos escolhido 4 ao invés de 1? Nós teríamos obtido:

$$\begin{aligned} -a = {} & 4 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 \\ & + (4 - a_4) \cdot 5^4 + (4 - a_5) \cdot 5^5 + \cdots . \end{aligned}$$

O fato de nós termos duas escolhas para a_0, e então, uma vez que escolhemos a_0, uma única possibilidade para $a_1, a_2, a_3, \ldots$, apenas reflete o fato de que um elemento não-nulo em um corpo como $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Q}_p$ sempre possui duas raízes quadradas no corpo se tiver alguma.

Nem todos os números em $\mathbb{Q}_5$ possuem raízes quadradas. Nós vimos que o 6 possui, mas e o 7, por exemplo? Se tivermos

$$(a_0 + a_1 \times 5 + \cdots)^2 = 2 + 1 \times 5,$$

então teríamos $a_0^2 \equiv 2 \pmod 5$. Mas isso é impossível, como vemos ao verificar os valores possíveis para a_0 $(0, 1, 2, 3, 4)$.

Este método de resolução da equação $x^2 - 6 = 0$ in $\mathbb{Q}_5$ – inicialmente resolvendo a congruência $a_0^2 - 6 \equiv 0 \pmod 5$ e, em seguida, encontrando os a_i restantes de uma forma "passo a passo" – é na verdade bastante geral, como demonstrado no seguinte resultado, conhecido como "Lema de Hensel".

Teorema 4.3.1. (Lema de Hensel). *Seja $F(x) = c_0 + c_1x + \cdots + c_nx^n$ um polinômio cujos coeficientes são inteiros p-ádicos. Seja $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1}$ a derivada de $F(x)$. Seja a_0 um inteiro p-ádico tal que $F(a_0) \equiv 0 \pmod p$ e $F'(a_0) \not\equiv 0 \pmod p$. Então existe um único inteiro p-ádico a tal que*

$$F(a) = 0 \quad e \quad a \equiv a_0 \pmod p.$$

Pode-se encontrar uma demonstração desse resutltado em [Kob12, Teorema 3]. No caso particular visto acima, tem-se $F(x) = x^2 - 6$, $F'(x) = 2x$, $a_0 = 1$.

Vejamos agora algunas aplicações do Lema de Hensel.

Exemplo 4.3.2. *Para cada inteiro k entre 0 e $p-1$, $k^p \equiv k \pmod p$. Seja $f(x) = x^p - x$. Temos então $f(k) \equiv 0 \pmod p$ e $f'(k) = pk^{p-1} - 1 \equiv -1 \not\equiv 0 \pmod p$. Pelo Lema de Hensel, existe um único $\omega_k \in \mathbb{Z}_p$ tal que $\omega_k^p = \omega_k$ e $\omega_k \equiv k \pmod p$. Por exemplo, $\omega_0 = 0$ e $\omega_1 = 1$. Quando $p > 2$, $\omega_{p-1} = -1$. Outros ω_k para $p > 2$ são mais interessantes. Para $p = 5$, ω_k é uma raiz de $x^5 - x = x(x^4 - 1) = x(x-1)(x+1)(x^2+1)$. Logo ω_2 e ω_3 são raízes quadradas de -1 em $\mathbb{Z}_5$:*

$$\begin{aligned} \omega_2 &= 2 + 5 + 2 \cdot 5^2 + 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + 2 \cdot 5^6 + 3 \cdot 5^7 + \cdots, \\ \omega_3 &= 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + 2 \cdot 5^6 + 5^7 + \cdots. \end{aligned}$$

Oa números ω_k para $0 \le k \le p-1$ são distintos porque já são distintos quando reduzidos mod p*, logo $x^p - x = x(x^{p-1} - 1)$ se decompõe completamente em $\mathbb{Z}_p[x]$. Suas raízes em $\mathbb{Z}_p$ são 0 e as raízes $(p-1)$-ésimas da unidade. O número ω_k é chamado o Representante de Teichmüller para k.*

O Lema de Hensel é frequentemente considerado um método para encontrar raízes de polinômios, mas isso é apenas um aspecto: a existência de uma raiz. Há também uma parte de unicidade no Lema de Hensel: ele nos diz que existe uma única raiz dentro de uma certa distância de uma raiz aproximada. Usaremos essa unicidade para encontrar todas as raízes da unidade em $\mathbb{Q}_p$.

Teorema 4.3.3. *As raízes da unidade em $\mathbb{Q}_p$ são as $(p-1)$-ésimas raízes da unidade para p ímpar e ± 1 para $p = 2$.*

Demonstração: Se $x^n = 1$ em $\mathbb{Q}_p$, então $|x|_p^n = 1$, logo $|x|_p = 1$. Isso significa que toda raiz da unidade em $\mathbb{Q}_p$ está em $\mathbb{Z}_p^*$. Portanto, trabalhamos em $\mathbb{Z}_p^*$ desde o início.

Primeiramente, vamos considerar raízes da unidade de ordem co-primo com p. Suponhamos que ζ_1 e ζ_2 são raízes da unidade em $\mathbb{Z}_p^*$ cujas ordens são números co-primos com p. Seja m o produto das ordens dessas raízes da unidade. Então ambas são raízes de $f(x) = x^m - 1$ e m é co-primo com p. Como

$$|f'(\zeta_i)|_p = |m\zeta_i^{m-1}|_p = 1,$$

o aspecto de unicidade do Lema de Hensel implica que a única raiz α de $x^m - 1$ satisfazendo $|\alpha - \zeta_1|_p < 1$ é ζ_1. Logo, se $\zeta_2 \equiv \zeta_1 \bmod p\mathbb{Z}_p$, então $\zeta_2 = \zeta_1$: raízes

distintas de unidade em $\mathbb{Z}_p^*$ cujas ordens são co-primos com p devem ser incongruentes mod$p$. No Exemplo 4.3.2, nós encontramos em cada classe lateral não-nula mod$p\mathbb{Z}_p$ uma raiz de $x^{p-1}-1$, e $p-1$ é co-primo com p. Portanto, cada classe de congruência mod$p\mathbb{Z}_p$ contém uma raiz $(p-1)$-ésima da unidade, logo as únicas raízes da unidade de ordem co-primo com p em $\mathbb{Q}_p$ são as raízes de $x^{p-1}-1$.

Agora consideramos raízes da unidade de ordem potência de p. Mostraremos que a única raiz p-ésima da unidade em $\mathbb{Z}_p^*$ é 1 para p ímpar, e que as únicas raízes quartas da unidade em $\mathbb{Z}_2^*$ são ± 1. Isso implica que as únicas raízes p^n-ésimas ($n \in \mathbb{N}$) da unidade em $\mathbb{Z}_p^*$ são 1 para p ímpar e ± 1 para $p = 2$. (Por exemplo, se houvesse uma raiz p^n-ésima da unidade não-trivial em $\mathbb{Q}_p$ para $p \neq 2$, então haveria uma raiz da unidade em $\mathbb{Q}_p$ de ordem p, mas vamos mostrar que não existe nenhuma). Esta parte da demonstração não usará o Lema de Hensel.

Primeiramente consideramos p ímpar e supomos que $\zeta^p = 1$ em $\mathbb{Z}_p^*$ com $\zeta \neq 1$. Como $\zeta^p \equiv \zeta \pmod{p\mathbb{Z}_p}$, temos $\zeta \equiv 1 \pmod{p\mathbb{Z}_p}$. Portanto, $\zeta = 1 + py$ com $y \in \mathbb{Z}_p$. Como $\zeta \neq 1$, ζ é uma raiz de $(x^p-1)/(x-1) = 1 + x + x^2 + \cdots + x^{p-1}$. Para todos os inteiros $k \geq 0$, $(1+py)^k \equiv 1 + kpy \pmod{p^2\mathbb{Z}_p}$, pelo teorema do binômio. Assim,

$$\begin{aligned} 0 &= 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} \\ &= \sum_{k=0}^{p-1} \zeta^k \\ &\equiv \sum_{k=0}^{p-1} (1 + kpy) \pmod{p^2\mathbb{Z}_p} \\ &\equiv p + \frac{p(p-1)}{2} py \pmod{p^2\mathbb{Z}_p}. \end{aligned} \tag{1}$$

Como p é ímpar, $(p-1)/2 \in \mathbb{Z}$, então (1) implica $0 \equiv p \pmod{p^2}$, o que é uma contradição. Portanto, não há raiz p-ésima da unidade em $\mathbb{Q}_p$ além de 1.

Agora consideramos o caso $p = 2$. Queremos mostrar que as únicas raízes quartas da unidade em $\mathbb{Z}_2^*$ são ± 1. Se $\zeta \in \mathbb{Z}_2^*$ é uma raiz quarta da unidade e $\zeta \neq \pm 1$, então $\zeta^2 = -1$, portanto $\zeta^2 \equiv -1 \pmod{4\mathbb{Z}_2}$. No entanto,

$$\zeta \in \mathbb{Z}_2^* \Longrightarrow \zeta \equiv 1 \text{ ou } 3 \pmod{4\mathbb{Z}_2} \Longrightarrow \zeta^2 \equiv 1 \pmod{4\mathbb{Z}_2}$$

e $1 \not\equiv -1 \pmod{4\mathbb{Z}_2}$. Assim, não há raiz quarta da unidade em $\mathbb{Q}_2$ além de ± 1.

Para um primo p, uma raiz da unidade é um (único) produto de uma raiz da unidade de ordem potência de p e uma raiz da unidade de ordem co-primo com p, então as únicas raízes da unidade em $\mathbb{Q}_p$ são as raízes de $x^{p-1}-1$ para $p \neq 2$ e ± 1 para $p = 2$. □

Capítulo 5

Extensões Ciclotômicas

Começaremos este Capítulo abordando extensões ciclotômicas de um corpo arbitrário F. Em seguida, veremos o caso particular de extensões ciclotômicas de $\mathbb{Q}$. Por fim, apresentaremos um resultado a respeito de uma extensão galoisiana infinita $F/\mathbb{Q}$.

5.1 Extensões Ciclotômicas

Definição 5.1.1. *Seja F um corpo arbitrário. Se $\omega \in \overline{F}$ (fecho algébrico de F) e $\omega^n = 1$, então ω é uma raiz n-ésima da unidade. Se a ordem de ω é n no grupo multiplicativo $\overline{F}^*$, então ω é uma raiz n-ésima primitiva da unidade. Se ω é uma raiz da unidade qualquer, então a extensão de corpos $F(\omega)/F$ é chamada uma extensão ciclotômica.*

Destacamos dois fatos sobre raízes da unidade. Primeiro, se $\omega \in F$ é uma raiz n-ésima primitiva da unidade, então vemos que $\text{char}(F)$ não divide n pois, se $n = pm$, onde $\text{char}(F) = p$, então $0 = \omega^n - 1 = (\omega^m - 1)^p$. Portanto, $\omega^m = 1$ e, logo, a ordem de ω não seria n. Segundo, se ω é uma raiz n-ésima da unidade, então a ordem de ω no grupo F^* divide n, logo a ordem de ω é igual a algum divisor m de n. O elemento ω é portanto uma raiz m-ésima primitiva da unidade.

As n-ésimas raízes da unidade em um corpo K são exatamente o conjunto das raízes de $x^n - 1$. Suponhamos que $x^n - 1$ se decompõe sobre K, e seja G o conjunto das raízes n-ésimas da unidade em K. Então G é um subgrupo finito de K^*, logo G é cíclico. Qualquer gerador de G é portanto uma raiz n-ésima primitiva da unidade.

Para descrever extensões ciclotômicas, precisamos usar a *função phi de Euler*. Se n é um inteiro positivo, seja $\phi(n)$ o número de inteiros positivos menores do que ou iguais a n que são co-primos com n. Precisamos também saber algumas propriedades do grupo dos elementos invertíveis do anel $\mathbb{Z}/n\mathbb{Z}$. Se R é um anel comutativo com unidade 1, então o conjunto

$$R^* = \{a \in R;\ \text{existe } b \in R \text{ tal que } ab = 1\}$$

é um grupo pela multiplicação. Ele é chamado o grupo dos invertíveis de R. Se $R = \mathbb{Z}/n\mathbb{Z}$, então

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a + n\mathbb{Z};\ \text{mdc}(a, n) = 1\}.$$

Portanto, $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$.

Vamos precisar também do teste da derivada, um critério para saber se um polinômio é separável. Este critério está no Lema abaixo e será usado no Teorema 5.1.3.

Lema 5.1.2. (Teste de derivada) *Seja F um corpo e $f(x) \in F[x]$. Se $f(x)$ e $f'(x)$ são co-primos em $F[x]$, então $f(x)$ é separável.*

Demonstração: Vamos provar a contrapositiva: Se $f(x)$ não é separável, então $f(x)$ e $f'(x)$ não são co-primos. Seja K um corpo de decomposição de $f(x)$ e suponhamos que $f(x)$ não é separável. Então $f(x)$ deve possuir uma raiz repetida u em K. Logo, $f(x) = (x-u)^2 g(x)$ para algum $g(x) \in K[x]$ e

$$f'(x) = (x-u)^2 g'(x) + 2(x-u)g(x).$$

Portanto, $f'(u) = 0 \cdot g'(u) + 0 \cdot g(u) = 0$ e u é também uma raiz de $f'(x)$. Se $p(x) \in F[x]$ é o polinômio minimal de u, então $p(x)$ é não-constante e divide $f(x)$ e $f'(x)$. Portanto, $f(x)$ e $f'(x)$ não são co-primos. □

Agora vamos descrever extensões ciclotômicas de um corpo base arbitrário.

Teorema 5.1.3. *Suponhamos que* $\mathrm{char}(F)$ *não divide n e seja K um corpo de decomposição de $x^n - 1$ sobre F. Então K/F é galoisiana, $K = F(\omega)$ é gerado por qualquer raiz n-ésima primitiva da unidade ω e* $\mathrm{Gal}(K/F)$ *é isomorfo a um subgrupo de $(\mathbb{Z}/n\mathbb{Z})^*$. Portanto,* $\mathrm{Gal}(K/F)$ *é abeliano e $[K:F]$ divide $\phi(n)$.*

Demonstração: Como $\mathrm{char}(F)$ não divide n, o teste da derivada mostra que $x^n - 1$ é separável sobre F. Portanto, K é normal e separável sobre F; logo, K é galoisiana sobre F. Seja ω uma raiz n-ésima primitiva da unidade. Então todas as raízes n-ésimas da unidade são potências de ω, logo $x^n - 1$ se decompõe sobre $F(\omega)$. Com isso, concluímos que $K = F(\omega)$.

Qualquer automorfismo de K que fixa F é determinado pelo que ele faz em ω. No entanto, qualquer automorfismo restringe-se a um automorfismo de grupo do conjunto de raízes da unidade, logo ele envia o conjunto das raízes n-ésimas primitivas da unidade em si mesmo. Qualquer raiz n-ésima primitiva da unidade em K é da forma ω^t para algum t co-primo com n. Portanto, a aplicação

$$\begin{array}{rccc} \theta: & \mathrm{Gal}(K/F) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ & \sigma & \longmapsto & t + n\mathbb{Z} \ , \end{array}$$

onde $\sigma(\omega) = \omega^t$, está bem definida. Se $\sigma, \tau \in \mathrm{Gal}(K/F)$, com $\sigma(\omega) = \omega^t$ e $\tau(\omega) = \omega^s$, então $(\sigma\tau)(\omega) = \sigma(\omega^s) = \omega^{st}$, logo θ é um homomorfismo de grupos. O Kernel de θ é o conjunto de todos os σ com $\sigma(\omega) = \omega$; isto é, $\ker(\theta) = \langle \mathrm{id} \rangle$. Portanto, θ é injetiva, logo $\mathrm{Gal}(K/F)$ é isomorfo a um subgrupo do grupo abeliano $(\mathbb{Z}/n\mathbb{Z})^*$, um grupo de ordem $\phi(n)$. Isso completa a demonstração. □

Exemplo 5.1.4. *A estrutura de F determina o grau de $[F(\omega)/F]$ ou, equivalentemente, a ordem de* $\mathrm{Gal}(F(\omega)/F)$. *Por exemplo, seja $\omega = e^{2\pi i/8}$ uma raiz oitava primitiva da unidade em $\mathbb{C}$. Então $\omega^2 = i$ é uma raiz quarta primitiva da unidade. O grau de $\mathbb{Q}(\omega)$ sobre $\mathbb{Q}$ é 4, como veremos abaixo. Se $F = \mathbb{Q}(i)$, então o grau de $F(\omega)$ sobre F é 2, visto que ω satisfaz o polinômio $x^2 - i$ sobre F e $\omega \notin F$. Se $F = \mathbb{R}$, então $\mathbb{R}(\omega) = \mathbb{C}$, logo $[\mathbb{R}(\omega) : \mathbb{R}] = 2$. Na verdade, se $n \geq 3$ e se τ é qualquer raiz n-ésima primitiva da unidade em $\mathbb{C}$, então $\mathbb{R}(\omega) = \mathbb{C}$, logo $[\mathbb{R}(\tau) : \mathbb{R}] = 2$.*

No exemplo abaixo, denotamos o corpo $\mathbb{Z}/p\mathbb{Z}$ dos inteiros mod p por $\mathbb{F}_p$ e o polinômio minimal de ω sobre F por $\min(F, \omega)$.

Exemplo 5.1.5. *Seja $F = \mathbb{F}_2$. Se ω é uma raiz cúbica primitiva da unidade sobre F, então ω é uma raiz de $x^3 - 1 = (x-1)(x^2+x+1)$. Como $\omega \neq 1$ e x^2+x+1 é irredutível sobre F, temos $[F(\omega) : F] = 2$ e $\min(F, \omega) = x^2 + x + 1$.*

Se ρ é uma raiz sétima primitiva da unidade, então fatorando $x^7 - 1$, obtemos

$$x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1).$$

O polinômio minimal de ρ é portanto uma dessas equações cúbicas, logo $[F(\rho) : F] = 3$. Das seis raízes sétimas primitivas da unidade, três possuem x^3+x+1 como seu polinômio minimal, enquanto as outras possuem x^3+x^2+1 como seu. Esse comportamento é diferente das extensões ciclotômicas de $\mathbb{Q}$, como veremos abaixo, visto que todas as raízes n-ésimas primitivas da unidade sobre $\mathbb{Q}$ possuem o mesmo polinômio minimal.

5.2 Extensões Ciclotômicas de $\mathbb{Q}$

Agora vamos focar a atenção nas extensões ciclotômicas de $\mathbb{Q}$. Sejam $\omega_1, ..., \omega_r$ as raízes n-esimas primitivas da unidade em $\mathbb{C}$. Então

$$\{\omega_1, ..., \omega_r\} = \{e^{2\pi it/n}; \text{mdc}(t, n) = 1\},$$

logo existem $\phi(n)$ raízes n-ésimas primitivas da unidade em $\mathbb{C}$.

Definição 5.2.1. *O n-ésimo polinômio ciclotômico $\Psi_n(x) = \prod_{mdc(i,n)=1} (x - \omega_i)$ é o polinômio mônico em $\mathbb{C}[x]$ cujas raízes são exatamente as raízes n-ésimas primitivas da unidade em $\mathbb{C}$.*

Por exemplo,

$$\begin{aligned}\Psi_1(x) &= x - 1\\ \Psi_2(x) &= x + 1\\ \Psi_4(x) &= (x-i)(x+i) = x^2 + 1\end{aligned}$$

Mais ainda, se p é primo, então todas as raízes p-ésimas da unidade são primitivas exceto pela raiz 1. Portanto,

$$\Psi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Por essa definição de $\Psi_n(x)$, não está claro que $\Psi_n(x) \in \mathbb{Q}[x]$, nem que $\Psi_n(x)$ é irredutível sobre $\mathbb{Q}$. No entanto, vamos verificar o primeiro desses fatos no seguinte Lema e o segundo no Teorema 5.2.3

Lema 5.2.2. *Seja n um inteiro positivo. Então $x^n - 1 = \prod_{d|n} \Psi_d(x)$. Mais ainda, $\Psi_n(x) \in \mathbb{Z}[x]$.*

Demonstração: Sabemos que $x^n - 1 = \prod(x - \omega)$, onde ω varia sobre o conjunto das raízes n-ésimas da unidade. Se d é a ordem de ω em $\mathbb{C}^*$, então d divide n, e ω é uma raiz d-ésima da unidade. Reunindo todos os termos de raiz d-ésima da unidade nesta fatoração, obtemos a primeira afirmação.

Para a segunda, utilizamos indução em n; o caso $n = 1$ é claro, visto que $\Psi_1(x) = x - 1$. Suponhamos que $\Psi_d(x) \in \mathbb{Z}[x]$ para todo $d < n$. Então pela primeira parte, temos

$$x^n - 1 = \left(\prod_{d|n, d<n} \Psi_d(x) \right) \cdot \Psi_n(x).$$

Como $x^n - 1$ e $\prod_{d|n} \Psi_d(x)$ são polinômios mônicos em $\mathbb{Z}[x]$, o algoritmo da divisão para polinômios mostra que $\Psi_n(x) \in \mathbb{Z}[x]$. □

Podemos utilizar este lema para calcular os polinômios ciclotômicos $\Psi_n(x)$ por recursão. Por exemplo, para calcular $\Psi_8(x)$, temos

$$x^8 - 1 = \Psi_8(x)\Psi_4(x)\Psi_2(x)\Psi_1(x)$$

logo

$$\Psi_8(x) = \frac{x^8 - 1}{(x-1)(x+1)(x^2+1)} = x^4 + 1$$

O próximo teorema é o fato principal sobre polinômios ciclotômicos e nos permite determinar o grau de uma extensão ciclotômica sobre $\mathbb{Q}$.

Teorema 5.2.3. *Seja n um inteiro positivo. Então $\Psi_n(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração: Para provar que $\Psi_n(x)$ é irredutível sobre $\mathbb{Q}$, suponhamos que não. Como $\Psi_n(x) \in \mathbb{Z}[x]$ e é mônico, $\Psi_n(x)$ é redutível sobre $\mathbb{Z}$ pelo Lema de Gauss.

Digamos que $\Psi_n = f(x)h(x)$ com $f(x), h(x) \in \mathbb{Z}[x]$ ambos mônicos e f irredutível sobre $\mathbb{Z}$. Seja ω uma raiz de f. Afirmamos que ω^p é uma raiz de f para todos os primos p que não dividem n. Se isso for falso para um primo p, então como ω^p é uma raiz n-ésima primitiva da unidade, ω^p é uma raiz de h. Como $f(x)$ é mônico, o algoritmo da divisão mostra que $f(x)$ divide $h(x^p)$ em $\mathbb{Z}[x]$. A aplicação $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ definida pela redução dos coeficientes mod p é um homomorfismo de anéis (aqui $\mathbb{F}_p$ representa o anel $\mathbb{Z}/p\mathbb{Z}$ dos inteiros mod p). Para $g \in \mathbb{Z}[x]$, seja $\bar{g}$ a imagem de $g(x)$ in $\mathbb{F}_p[x]$. A redução mod p fornece $\overline{\Psi_n(x)} = \bar{f} \cdot \bar{h}$.

Como $\Psi_n(x)$ divide $x^n - 1$, o teste da derivada mostra que $\Psi_n(x)$ não possui raízes repetidas em qualquer extensão de $\mathbb{F}_p$, visto que p não divide n. Agora, como $a^p = a$ para todo $a \in \mathbb{F}_p$, vemos que $\overline{h(x^p)} = \overline{h(x)^p}$. Portanto, $\overline{f}$ divide $\overline{h^p}$, logo qualquer fator irredutível $\overline{q} \in \mathbb{F}_p[x]$ de $\bar{f}$ também divide $\bar{h}$. Logo, $\overline{q^2}$ divide $\overline{fh} = \overline{\Psi_n(x)}$, o que contradiz o fato de $\overline{\Psi_n}$ não possuir raízes repetidas.

Isso prova que se ω é uma raiz de f, então ω^p é também uma raiz de f, onde p é um primo que não divide n. Mas isso significa que todas as raízes n-ésimas primitivas da unidade são raízes de f, pois se α é uma raíz n-ésima primitivas da unidade, então $\alpha = \omega^t$, onde t é co-primo com n. Então $\alpha = \omega^{p_1 \cdots p_r}$, onde cada p_i é co-primo com

n. Vemos que ω^{p_1} é uma raiz de f, logo $(\omega^{p_1})^{p_2} = \omega^{p_1 p_2}$ é também uma raiz de f. Continuando com este processo, vemos que α é uma raiz f. Portanto, toda raiz n-esima primitiva da unidade é uma raiz de f, logo $\Psi_n(x) = f$. Isso prova que $\Psi_n(x)$ é irredutível sobre $\mathbb{Z}$, e portanto $\Psi_n(x)$ é também irredutível sobre $\mathbb{Q}$. □

Se ω é uma raiz n-ésima primitiva da unidade em $\mathbb{C}$, então o Teorema acima mostra que $\Psi_n(x)$ é o polinômio minimal de ω sobre $\mathbb{Q}$. O seguinte Corolário descreve extensões ciclotômicas de $\mathbb{Q}$.

Corolário 5.2.4. *Se K é um corpo de decomposição de $x^n - 1$ sobre $\mathbb{Q}$, então $[K : \mathbb{Q}] = \phi(n)$ e $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Mais ainda, se ω é uma raiz n-ésima primitiva da unidade em K, então $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_i \,;\ \mathrm{mdc}(i,n) = 1\}$, onde σ_i é determinado por $\sigma_i(\omega) = \omega^i$.*

Demonstração: A primeira parte do Corolário segue imediatamente dos Teoremas 5.1.3 e 5.2.3. A descrição de $\mathrm{Gal}(K/\mathbb{Q})$ é uma consequência da demonstração do Teorema 5.1.3.

Exemplo 5.2.5. *Seja ω uma raiz sétima primitiva da unidade em $\mathbb{C}$ e seja $K = \mathbb{Q}(\omega)$. Pelo Corolário* 5.2.4, *$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^*$, o qual é um grupo cíclico de ordem 6. O grupo de Galois de $K/\mathbb{Q}$ é $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$, onde $\sigma_i(\omega) = \omega^i$. Logo, $\sigma_1 = \mathrm{id}$, e é fácil verificar que σ_3 gera esse grupo. Mais ainda, $\sigma_i \circ \sigma_j = \sigma_{ij}$, onde os índices são multiplicados módulo* 7. *Os subgrupos de* $\mathrm{Gal}(K/\mathbb{Q})$ *são portanto*

$$\langle id \rangle,\ \langle \sigma_3^3 \rangle,\ \langle \sigma_3^2 \rangle,\ \langle \sigma_3 \rangle,$$

cujas ordens são $1, 2, 3$ *e* 6, *respectivamente. Vamos encontrar os corpos intermediários correspondentes. Se L é o corpo fixado de $\langle \sigma_3^3 \rangle$, então, como $\sigma_3^3 = \sigma_6$, tem-se $[K : L] = |\langle \sigma_6 \rangle| = 2$ pelo teorema fundamental. Para encontrar L, notemos que ω deve satisfazer uma equação quadrática sobre L e que essa equação é*

$$(x - \omega)(x - \sigma_6(\omega)) = (x - \omega)(x - \omega^6).$$

Expandindo, esse polinômio é

$$x^2 - (\omega + \omega^6)x + \omega\omega^6 = x^2 - (\omega + \omega^6)x + 1.$$

Portanto, $\omega + \omega^6 \in L$. Se denotarmos $\omega = e^{2\pi i/7} = \cos(2\pi/7) + i\mathrm{sen}(2\pi/7)$, então $\omega + \omega^6 = 2\cos(2\pi/7)$. Portanto, ω satisfaz uma equação quadrática sobre $\mathbb{Q}(\cos(2\pi/7))$; logo, L tem grau no máximo 2 sobre este corpo. Isso força $L = \mathbb{Q}(\cos(2\pi/7))$. Com cálculos semelhantes, podemos encontrar o corpo fixado de $\langle \sigma_3^2 \rangle$. Seja M este corpo. A ordem de σ_2 é 3, *logo $[M : \mathbb{Q}] = 2$. Portanto, basta encontrar um elemento de M que não esteja em $\mathbb{Q}$ para gerar M. Seja*

$$\alpha = \omega + \sigma_2(\omega) + \sigma_2^2(\omega) = \omega + \omega^2 + \omega^4.$$

Este elemento está em M pois é fixado por σ. Porém, α não está em $\mathbb{Q}$ visto que não é fixado por σ_6. Para ver isso, notemos que

$$\begin{aligned} \sigma_6(\omega) &= \omega^6 + \omega^{12} + \omega^{24} \\ &= \omega^6 + \omega^5 + \omega^3. \end{aligned}$$

Se $\sigma_6(\alpha) = \alpha$, esta equação nos daria um polinômio de grau 6 para o qual ω é uma raiz, e este polinômio não é divisível por

$$\min(\mathbb{Q}, \omega) = \Psi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

uma contradição. Isso força $\alpha \notin \mathbb{Q}$, logo $M = \mathbb{Q}(\alpha)$. Portanto, os corpos intermediários de $K/\mathbb{Q}$ são

$$K,\ \mathbb{Q}(cos(2\pi/7)),\ \mathbb{Q}(\omega + \omega^2 + \omega^4),\ \mathbb{Q}.$$

Exemplo 5.2.6. *Seja $\omega = e^{2\pi i/8} = (1+i)/\sqrt{2}$ e seja $K = \mathbb{Q}(\omega)$. O grupo de Galois de $K/\mathbb{Q}$ é $\{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$, e note que cada um dos três automorfismos de K diferentes da identidade tem ordem 2. Os subgrupos desse grupo de Galois são portanto*

$$\langle id \rangle,\ \langle \sigma_3 \rangle,\ \langle \sigma_5 \rangle,\ \langle \sigma_7 \rangle,\ \mathrm{Gal}(K/\mathbb{Q}).$$

Cada um dos três corpos intermediários próprios tem grau 2 sobre $\mathbb{Q}$. Um é fácil de encontrar, visto que $\omega^2 = i$ é uma raiz quarta primitiva da unidade. O grupo associado a $\mathbb{Q}(i)$ é $\langle \sigma_5 \rangle$, pois $\sigma_5(\omega^2) = \omega^{10} = \omega^2$. Como $\omega = (1+i)/\sqrt{2}$ e $\omega^{-1} = (1-i)/\sqrt{2}$, vemos que $\sqrt{2} = \omega + \omega^{-1} \in K$. O elemento $\omega + \omega^{-1} = \omega + \omega^7$ é fixado por σ_7; logo, o corpo fixado de $\langle \sigma_7 \rangle$ é $\mathbb{Q}(\sqrt{2})$. Sabemos que $\sqrt{2} \in K$ e $i \in K$, logo $\sqrt{-2} \in K$ Este elemento deve gerar o corpo fixado de $\langle \sigma_3 \rangle$. Os corpos intermediários são portanto

$$K,\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}.$$

A descrição dos corpos intermediários também mostra que $K = \mathbb{Q}(\sqrt{2}, i)$.

5.3 Uma extensão $F/\mathbb{Q}$

Nesta seção, vamos construir uma extensão galoisiana infinita $F/\mathbb{Q}$

Seja p um primo ímpar que deixaremos fixado daqui em diante. Para cada $n \geq 1$, seja ζ_n uma raiz p^n-ésima primitiva da unidade e seja F_n o corpo ciclotômico obtido pela adjunção de ζ_n ao corpo $\mathbb{Q}$ dos números racionais: $F_n = \mathbb{Q}(\zeta_n)$

Observemos que, para todo n, $\zeta_n^{p^{n+1}} = (\zeta_n^{p^n})^p = 1^p = 1$. Ou seja, para todo n, ζ_n é uma raiz p^{n+1}-ésima da unidade. Portanto, tem-se uma sequência crescente de extensões $F_n/\mathbb{Q}$:

$$\mathbb{Q} \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset \cdots$$

Seja $F = \bigcup_{n=1}^{\infty} F_n$. Então $F/\mathbb{Q}$ é uma extensão galoisiana infinita. Nosso intuito é mostrar que o grupo $\mathrm{Gal}(F/\mathbb{Q})$ é isomorfo ao grupo multiplicativo $\mathbb{Z}_p^*$ das unidades p-ádicas. Ora, pelo Corolário 5.2.4, para cada n, tem-se

$$\mathrm{Gal}(F_n/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$$

Agora, para cada $n \in \mathbb{N}$, seja $A_n = (\mathbb{Z}/p^n\mathbb{Z})^*$ e consideremos o sistema inverso de grupos $\{A_n, \varphi_{nm}\}$ onde os homomorfismos φ_{nm} são definidos da seguinte forma:

$$\begin{array}{rccc} \varphi_{ij}: & A_i & \longrightarrow & A_j \\ & a \pmod{p^n} & \longmapsto & a \pmod{p^m} \end{array}$$

Por exemplo, suponhamos que $p = 3$, $n = 5$ e $m = 3$, e seja $a = 220 \in (\mathbb{Z}/3^5\mathbb{Z})^*$. Então, $\varphi_{53}(a) = 4$, visto que $220 \equiv 4 \pmod{3^3}$.

O limite inverso $\varprojlim_{n\in\mathbb{N}} A_n$ é isomorfo ao grupo multiplicativo $\mathbb{Z}_p^*$ (ver [Ser12]). Além disso, pelo Teorema 3.3.1, sabemos que $\mathrm{Gal}(F/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(F_n/\mathbb{Q})$. Assim sendo, temos

$$\mathrm{Gal}(F/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(F_n/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}} A_n \cong \mathbb{Z}_p^*$$

logo $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}_p^*$, como queríamos.

Se $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ e $\{a_n\}_{n=1,2,\ldots}$ é a sua imagem em $\mathbb{Z}_p^*$, podemos, para cada $n \in \mathbb{N}$, tomar a restrição $\sigma|_{F_n}$. Temos $\sigma(\zeta_n) = (\zeta_n)^{a_n}$, onde a_n é o n-ésimo termo de $\{a_n\}$.

Referências Bibliográficas

[Apo13] Tom M. Apostol. *Introduction to Analytic Number Theory*. Springer Science & Business Media, 2013.

[Con15] Keith Conrad. *Hensel's Lemma*. 2015. URL: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`.

[Con20] Keith Conrad. *Infinite Galois Theory (Draf, CTNT 2020)*. Rel. técn. Technical Report, 2020.

[Hun14] Thomas W. Hungerford. *Abstract Algebra: An Introduction*. Cengage Learning, 2014.

[Iwa59a] Kenkichi Iwasawa. "On some properties of Γ-finite modules". Em: *Annals of Mathematics* 70.2 (1959), pp. 291–312.

[Iwa59b] Kenkichi Iwasawa. "On the theory of cyclotomic fields". Em: *Annals of Mathematics* 70.3 (1959), pp. 530–561.

[Kob12] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Vol. 58. Springer Science & Business Media, 2012.

[Mon18] Christe H. Moreira Montijo. "Sobre grupos profinitos de posto finito". Diss. de mestr. Universidade de Brasília, 2018.

[Mor96] Patrick Morandi. *Field and Galois theory*. Vol. 167. Springer Science & Business Media, 1996.

[Mun14] James Munkres. *Topology*. Pearson Education, 2014.

[Oli24] Francisco R. Vieira Alves; Paulo C. Cavalcante de Oliveira. "Sobre os números p-ádicos: aspectos históricos, matemáticos e epistemológicos". Em: *Revista Brasileira de História da Matemática* 24.48 (2024), pp. 1–32.

[Ros12] Edwin Hewitt; Kenneth A. Ross. *Abstract Harmonic Analysis: Volume I: Structure of Topological Groups Integration Theory Group Representations*. Vol. 115. Springer Science & Business Media, 2012.

[Ser12] Jean-Pierre Serre. *A course in arithmetic*. Vol. 7. Springer Science & Business Media, 2012.

[Wil12] Stephen Willard. *General topology*. Courier Corporation, 2012.

[Zal00] Luis Ribes; Pavel Zalesskii. *Profinite groups*. Springer-Verlag, 2000.