**Universidade Federal de Campina Grande**
**Centro de Ciências e Tecnologia**
**Unidade Acadêmica de Matemática**

# Topologia $\mathfrak{m}$-ádica

por

**Laise Dias Alves Araújo**

sob orientação do

**Prof. Antônio Pereira Brandão Júnior**

Campina Grande - PB
Abril de 2015

**Universidade Federal de Campina Grande**
**Centro de Ciências e Tecnologia**
**Unidade Acadêmica de Matemática**

**Laise Dias Alves Araújo**

# Topologia $\mathfrak{m}$-ádica

Trabalho apresentado ao Curso de Graduação em Matemática da Universidade Federal de Campina Grande como requisito parcial para a obtenção do título de Bacharel em Matemática.

**Prof. Antônio Pereira Brandão Júnior**

Orientador

Campina Grande, 09 de Abril de 2015
Curso de Matemática, Modalidade Bacharelado

# Topologia $\mathfrak{m}$-ádica

por

**Laise Dias Alves Araújo**

Trabalho de Conclusão de Curso defendido e aprovado em 09 de Abril de 2015 pela comissão examinadora constituída pelos professores:

**Prof. Dr. Antônio Pereira Brandão Júnior**
**Orientador**
**UAMat/CCT/UFCG**

**Prof. Dr. Bráulio Maia Júnior**
**Examinador**
**UAMat/CCT/UFCG**

Com nota igual a:

# Resumo

Neste trabalho, apresentaremos um estudo introdutório sobre a Topologia $\mathfrak{m}$-ádica, no qual discutiremos algumas propriedades importantes e a ideia de completamento. Como caso particular do completamento da topologia $\mathfrak{m}$-ádica estudaremos o anel dos inteiros $p$-ádicos onde $p$ é um número natural primo. Além disso, mostraremos que o anel dos endomorfismos do $p$-grupo de Prüfer é isomorfo ao anel dos inteiros $p$-ádicos.

# Abstract

In this work, we will present an introsutory study in $\mathfrak{m}$-adic topology, in which we will cliscuss some important properties on the idea of completeness. As a partular case of the completeness of the $\mathfrak{m}$-adic topology, we will study the $p$-adic integer ring where $p$ is a prime natural number. Also, we will show that Prüfer's $p$-group endomorphism ring is isomorfic to the $p$-adic integer ring.

# Dedicatória

A minha avó, Maria de Lurdes, por todo seu esforço e dedicação.

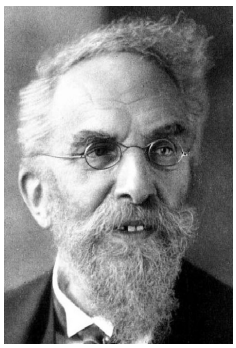
# Sumário

# Introdução

A teoria dos números $p$-ádicos teve inicío em 1897 com o matemático Kurt Hensel. A ideia partiu da expansão em série de Laurent de uma função racional (quociente de dois polinômios) sobre o corpo $\mathbb{C}$ dos complexos. Na época já se sabia que dados uma função racional $f(X)$ sobre $\mathbb{C}$ e $\alpha \in \mathbb{C}$ é possível expandir $f(X)$ numa série de Laurent em torno de $\alpha$:

$$f(X) = \sum_{k=k_0}^{\infty} a_k (X - \alpha)^k$$

onde $k_0 \in \mathbb{Z}$, sendo a convergência garantida em alguma região do plano complexo.



Kurt Hensel.

Observa-se que o corpo $\mathbb{C}(X)$ das funções racionais sobre $\mathbb{C}$ é o corpo de frações do anel de polinômios $\mathbb{C}[X]$ e um polinômio da forma $X - \alpha$ é um elemento irredutível (análogo aos números primos nos inteiros) em $\mathbb{C}[X]$. Observa-se também que o corpo $\mathbb{Q}$ dos racionais é o corpo de frações do anel dos inteiros. Pensando então em uma analogia entre $\mathbb{C}(X)$ e $\mathbb{Q}$ no sentido de expansão em série, Hensel percebeu que, fixado um número natural primo $p$, cada número racional, possui, num certo sentido, uma expansão em série de

potências da forma

$$\sum_{k=k_0}^{\infty} a_k p^k$$

onde $k_0$, $a_k \in \mathbb{Z}$ e $0 \leq a_k < p$. O conjunto de todas as séries deste tipo (que são séries formais) é munido de uma adição e uma multiplicação constituindo um corpo, que é chamado de *corpo dos números p-ádicos* e que contém *propriamente* um subcorpo isomorfo ao corpo dos racionais. As séries formais onde $k_0 = 0$ são chamadas de *inteiros p-ádicos* e constituem um subanel do corpo dos números $p$-ádicos. Este subanel é o que chamamos de *anel dos inteiros p-ádicos*.

Dado um inteiro $p$-ádico $\gamma = \sum_{k=0}^{\infty} a_k p^k$, associamos a ele a sequência de números inteiros

$$(a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, a_0 + a_1 p + a_2 p^2 + a_3 p^3, \ldots).$$

Tomando $x_n = \sum_{k=0}^{n} a_k p^k$, observa-se que $x_{n+1} \equiv x_n \pmod{p^{n+1}}$ para todo $n$ inteiro não negativo. Uma sequência deste tipo é chamada de *sequência coerente* e é uma forma de representação dos inteiros $p$-ádicos. No Capítulo 3 deste trabalho os inteiros $p$-ádicos serão definidos formalmente através de sequências coerentes.

Hoje, o anel dos inteiros $p$-ádicos faz parte de um contexto mais geral, que é a ideia de *topologia* $\mathfrak{m}$*-ádica*. Sejam $A$ um anel comutativo com unidade e $\mathfrak{m}$ um ideal de $A$ tal que a interseção de todas as suas potências é $\{0\}$. Partindo de um ideal nestas condições, podemos definir a *métrica* $\mathfrak{m}$*-ádica*, a qual faz de $A$ um anel topológico. A topologia em questão é a chamada topologia $\mathfrak{m}$-ádica. Considerando $A$ como espaço métrico (munido da métrica $\mathfrak{m}$-ádica), podemos considerar o seu completamento, o qual é também um anel topológico e um espaço métrico completo. Neste contexto, o anel dos inteiros $p$-ádicos aparece como um caso particular. Considerando $p$ um número natural primo e $\mathfrak{m} = p\mathbb{Z}$, ideal dos múltiplos de $p$ do anel $\mathbb{Z}$ dos inteiros, chamamos a métrica $\mathfrak{m}$-ádica neste caso de *métrica p-ádica*. Quando consideramos o anel $\mathbb{Z}$ dos inteiros munido da métrica $p$-ádica, o anel que aparece como completamento é exatamente o anel dos inteiros $p$-ádicos.

Motivado pela importância dos números $p$-ádicos e da topologia $\mathfrak{m}$-ádica, a qual nos mostra a beleza do estudo conjunto da álgebra e da topologia, o presente trabalho tem como objetivo fazer um estudo introdutório dessas ideias, sendo desenvolvido em três capítulos da seguinte maneira: no Capítulo 1 são introduzidos os conceitos e resultados básicos que nos darão suporte ao desenvolvimento do trabalho e assumiremos o conhecimento por parte do leitor de alguns conceitos, tais como grupo, relações de equivalência, etc. Iniciamos com a definição de anel e algumas propriedades, além de

conceitos como subanel, ideal, homomorfismo e anel quociente. Logo após, introduziremos os conceitos de espaços métricos, continuidade, convergência de sequências, sequências de Cauchy, completude e conjuntos abertos e fechados. Neste seguimos essencialmente [7],[6] e [5].

No capítulo 2 apresentamos a definição da métrica $\mathfrak{m}$-ádica e suas propriedades. Em seguida, definiremos sequências coerentes e descreveremos com detalhes o processo de completamento de um anel munido da métrica $\mathfrak{m}$-ádica. Tivemos como referência [3].

O Capítulo 3 será destinado ao anel dos inteiros $p$-ádicos, que é um caso particular do completamento da topologia $\mathfrak{m}$-ádica. Definiremos o $p$-grupo de Prüfer e algumas propriedades importantes, e no final mostraremos que existe um isomorfismo entre o anel dos inteiros $p$-ádicos e o anel dos endomorfismos do $p$-grupo de Prüfer.

# Capítulo 1

# Preliminares

Neste capítulo apresentaremos resultados básicos de anéis e espaços métricos, que serão necessários para o desenvolvimento desse trabalho. Para uma leitura mais detalhada sobres os assuntos aqui tratatos, recomendamos as referências [1], [2], [4],[6] e [5].

Em todo este trabalho iremos considerar as sequintes notações:
$\mathbb{N} = \{1, 2, 3, ...\}$ (conjunto dos números naturais) e $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

## 1.1 Anéis e Subanéis

### 1.1.1 Definição e Exemplos

**Definição 1.1.1.** *Seja $A$ um conjunto não vazio e " $+$ " e " $\cdot$ " duas operações em $A$. Dizemos que a terna $(A, +, \cdot)$ é um anel se valem as seguintes condições:*

*a)* " $+$ " *é associativa, ou seja, $(a + b) + c = a + (b + c)$, para quaisquer $a, b, c \in A$.*

*b)* " $+$ " *é comutativa, ou seja, $a + b = b + a$, para todo $a, b \in A$.*

*c) Existe $0 \in A$ tal que $0 + a = a$, para todo $a \in A$.*

*d) Para cada $a \in A$ existe $-a \in A$ tal que $a + (-a) = 0$.*

*e)* " $\cdot$ " *é associativa, ou seja, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in A$.*

*f) $a \cdot (b+c) = (a \cdot b)+(a \cdot c)$ e $(a+b) \cdot c = (a \cdot c)+(b \cdot c)$, para todo $a, b, c \in A$.*

Por simplicidade de notação, vamos denotar o anel $(A, +, \cdot)$ simplesmente por $A$, ficando as operações " $+$" e " $\cdot$" subentendidas. A operação " $+$" é

normalmente chamada de *soma* ou *adição* e " $\cdot$" de *produto* ou *multiplicação*. Para $a, b \in A$, denotamos $a \cdot b$ por $ab$.

Sendo $A$ um anel, existe um único $0 \in A$ tal que $0 + a = a$, para todo $a \in A$, e este elemento é chamado de zero ou elemento neutro aditivo de $A$. Para cada $a \in A$ existe um único $-a \in A$ tal que $a + (-a) = 0$. O elemento $-a$ é chamado de oposto aditivo de $a$. Observe que $-(-a) = a$.

Sendo A um anel, definimos a *subtração* em $A$ como sendo a operação

$$\begin{array}{rcl} - : A \times A & \longrightarrow & A \\ (a, b) & \longmapsto & a - b = a + (-b) \end{array}$$

**Definição 1.1.2.** *Seja $A$ um anel.*

*a) Dizemos que $A$ é um anel comutativo se $ab = ba$, para quaisquer $a, b \in A$.*

*b) Dizemos que $A$ é um anel com unidade se existe $1 \in A$ tal que $1a = a1$, para todo $a \in A$.*

Sendo $A$ um anel com unidade, observa-se que existe um único $1 \in A$ tal que $1a = a1 = a$, para todo $a \in A$. 1 é chamado de *um* ou *unidade* de $A$.

A partir de agora, a menos de menção em contrário, a palavra anel significará anel *comutativo com unidade*.

**Definição 1.1.3.** *Sejam $A$ um anel com unidade e $a \in A$, dizemos que $a$ é inversível em $A$ se existe $a' \in A$ tal que $a'a = aa' = 1$.*

**Observação 1.1.4.** *Na definição acima o $a'$ é único e geralmente denotado por $a^{-1}$.*

Sendo $A$ um anel com unidade, temos que o conjunto

$$U(A) = \{a \in A \ / \ \text{a é inversível em A}\},$$

é não vazio, pois $1 \in U(A)$.

**Definição 1.1.5.** *Seja $A$ um anel (não trivial, ou seja, $A \neq \{0\}$). Dizemos que $A$ é um corpo se $A$ se $U(A) = A - \{0\}$.*

**Definição 1.1.6.** *Seja $A$ um anel. Definimos um subanel de $A$ como sendo um subconjunto não vazio $B$ de $A$ que satisfaz:*

*a) $x + y$, $-x \in B$, para quaisquer $x, y \in B$.*

*b) $xy \in B$, para quaisquer $x, y \in B$.*

*c) $1 \in B$.*

*Todo subanel $B$ é por si só um anel, basta restrigir as aperações do anel $A$ ao subanel $B$.*

**Exemplo 1.1.7.** *$\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ e $\mathbb{C}$, munidos de suas operações usuais de adição e multiplicação, são anéis comutativos com unidade. Observe que $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ são corpos, e $U(\mathbb{Z}) = \{-1, 1\}$.*

**Exemplo 1.1.8.** *Seja $R$ um anel. Definimos uma série formal na indeterminada $x$ com coeficientes em $R$ como sendo uma expressão da forma*

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \ldots + a_n x^n + \cdots$$

*onde $a_n \in R$ para todo $n \in \mathbb{N}_0$. Normalmente donotamos o conjunto de todas a séries formais por $R[[x]]$.*

*Sejam $f(x) = \sum_{n=0}^{\infty} a_n x^n$, $g(x) = \sum_{n=0}^{\infty} b_n x^n \in R[[x]]$. Considere as seguintes operações de adição e multiplicação em $R[[x]]$:*

$$f(x) + g(x) = \sum_{n=0}^{\infty} c_n x^n \qquad e \qquad f(x)g(x) = \sum_{n=0}^{\infty} d_n x^n,$$

*onde $c_n = a_n + b_n$ e $d_n = \sum_{i=0}^{\infty} a_i b_{n-i}$.*

*Então $R[[x]]$ munido dessas duas operações é um anel, chamando de anel das séries formais na indeterminada $x$ com coeficientes em $R$.*

Considere agora $f(x) = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$ uma série formal na indeterminada $x$. Diremos que $f$ é uma série formal quase nula ou que $f$ é um polinômio na indeterminda $x$, quando existir $n_0 \in \mathbb{N}$ tal que para todo $m \in \mathbb{N}$ com $m > n_0$, tivermos que $a_m = 0$, ou seja, $f$ é da forma

$$f(x) = a_0 + a_1 x + ... + a_{n_0} x^{n_0}.$$

O conjunto de todos os polinômios na indeterminada $x$ munido da soma e do produto usual é um subanel de $R[[x]]$, chamado *anel dos polinômios na indeterminada $x$* e é denotado por $R[x]$.

**Exemplo 1.1.9.** *Sejam $A_1, A_2, \ldots, A_n$, com $n \in \mathbb{N}$, anéis. Definimos o produto direto de $A_1, A_2, \ldots, A_n$, denotado por $A_1 \times A_2 \times \cdots \times A_n$, como sendo o anel munido das operações "$+$" e "$\cdot$" definidas por:*

*i)* $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$.

*ii)* $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$.

*para quaisquer* $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in A_1 \times A_2 \times \cdots \times A_n$. *O elemento neutro deste anel é a n-upla constante com todas as entradas iguais a* 0 *e a identidade é a n-upla constante com todas as entradas iguais a* 1.

Ademais, dada uma família de anéis $(A_n)_{n\in\mathbb{N}}$, definimos o produto direto desta família como sendo o conjunto

$$\prod_{n\in\mathbb{N}} A_n = \{(a_1, a_2, a_3, ...) \ / \ a_n \in A_n\}$$

munido das operações de adição e multiplicação efetuadas termo a termo.

**Exemplo 1.1.10.** *Sejam* $G$ *um grupo abeliano (com notação aditiva) e* $End(G)$ *o conjunto de todos os endomorfismos de* $G$. *Dados* $\phi, \psi \in End(G)$, *consideremos* $\phi + \psi : G \longrightarrow G$ *definida por*

$$(\phi + \psi)(g) = \phi(g) + \psi(g),$$

*para* $g \in G$. *Observe que* $\phi + \psi$, $\phi\psi = \phi \circ \psi \in End(G)$ *e assim podemos definir as operações de soma e multiplicação em* $End(G)$*:*

$$\begin{array}{rcl} + : End(G) \times End(G) & \longrightarrow & End(G) \\ (\phi, \psi) & \longmapsto & \phi + \psi \end{array}$$

$$\begin{array}{rcl} \cdot : End(G) \times End(G) & \longrightarrow & End(G) \\ (\phi, \psi) & \longmapsto & \phi \circ \psi \end{array}$$

*Temos que* $End(G)$, *munidos destas operações, é um anel (em geral, não comutativo), chamado de anel dos endomorfismos do grupo* $G$. *O zero deste anel é o endomorfismo nulo (endomorfismo com imagem* $0_G$*) e a unidade é o endomorfismo identidade.*

**Definição 1.1.11.** *Uma sequência num conjunto* $X$ *é uma aplicação* $x : \mathbb{N} \longrightarrow X$. *Podemos denotar a sequência* $x$ *por* $(x_n)_{n\in\mathbb{N}}$ *(ou simplesmente por* $(x_n)$*), onde* $x_n$ *é o valor que a sequência* $x$ *assume no número* $n \in \mathbb{N}$, *sendo chamado de n-ésimo termo da sequência.*

**Exemplo 1.1.12.** *Seja* $A$ *um anel. Definimos* $S(A)$ *como sendo o conjunto de todas as sequências com entradas em* $A$. *Ou seja,*

$$S(A) = \{(x_n)_{n\in\mathbb{N}} \,/\, x_n \in A\}.$$

*O conjunto $S(A)$ munido das operações*

$$\begin{array}{rcl} + : S(A)\times S(A) & \longrightarrow & S(A) \\ ((x_n),(y_n)) & \longmapsto & (x_n)+(y_n) = (x_1+y_1, x_2+y_2, x_3+y_3, \ldots) \end{array}$$

*e*

$$\begin{array}{rcl} \cdot : S(A)\times S(A) & \longrightarrow & S(A) \\ ((x_n),(y_n)) & \longmapsto & (x_n)(y_n) = (x_1y_1, x_2y_2, x_3y_3, \ldots) \end{array}$$

*é um anel, chamado de anel das sequências.*

### 1.1.2 Ideais

**Definição 1.1.13.** *Sejam $A$ um anel e $I$ um subgrupo aditivo de $A$ ($I \neq \emptyset$ e $x+y, -x \in I$, para quaisquer $x, y \in I$). Dizemos que $I$ é um ideal de $A$ se $ax \in I$ para quaisquer $x \in I$ e $a \in A$.*

**Exemplo 1.1.14.** *Se $A$ é um anel, então $\{0\}$ e $A$ são ideais de $A$. Seja $a \in A$, então definimos ideal principal gerado por $a$ como sendo*

$$\langle a \rangle = \{ax/\ x \in A\}.$$

**Exemplo 1.1.15.** *Sejam $A$ um anel e $(I_j)_{j\in\lambda}$ uma família de ideais de $A$. Temos que*

$$\bigcap_{j\in\lambda} I_j \quad e \quad \sum_{j\in\lambda} I_i = \left\{ x_1 + x_2 + \cdots + x_n \,/\, n \in \mathbb{N}, x_i \in \bigcup_{j\in\lambda} I_j \right\}$$

*são ideais de $A$. Particularmante*

$$I + J = \{x + y \,/\, x \in I, y \in J\}.$$

**Exemplo 1.1.16.** *Sejam $A$ um anel e $I_1, I_2, I_3, \ldots, I_n$ ideais $A$. Definimos o produto $I_1 \cdot I_2 \cdot I_3 \cdot \ldots \cdot I_n$ como sendo*

$$I_1 \cdot I_2 \cdot I_3 \cdot \ldots \cdot I_n = \{x_{11} \cdot \ldots \cdot x_{n1} + x_{12} \cdot \ldots \cdot x_{n2} + \ldots + x_{1m} \cdot \ldots \cdot x_{nm} / m \in \mathbb{N}_0, x_{ij} \in I_i\}.$$

*Particularmente,*

$$I \cdot J = \{x_1y_1 + \ldots + x_my_m \,/\, m \in \mathbb{N}, x_i \in I, y_i \in J\},$$

*e*

$$I^n = \underbrace{I \cdot I \cdot I \cdot \ldots \cdot I}_{n-vezes} = \{x_{11} \cdots x_{n1} + x_{12} \cdots x_{n2} + \cdots + x_{1m} \cdots x_{nm} / m \in \mathbb{N}, x_{ij} \in I\}.$$

*Observe que* $I_1 \cdot I_2 \cdot I_3 \cdot \ldots \cdot I_n$ *é um ideal de* $A$ *e*

$$I_1 \cdot I_2 \cdot I_3 \cdot \ldots \cdot I_n \subseteq \bigcap_{i=1}^{n} I_i.$$

**Observação 1.1.17.** *Seja* $n \in \mathbb{N}$. *Temos que* $I^{n+1} \subseteq I^n$. *Mais em geral temos que* $I^n \subseteq I^m$, *para todo* $m \leq n$.

**Exemplo 1.1.18.** *Fixado* $n \in \mathbb{Z}$, *temos que* $n\mathbb{Z} = \{nx / x \in \mathbb{Z}\}$ *é um ideal de* $\mathbb{Z}$ *(ideal principal gerado por* $n$*). Todo ideal de* $\mathbb{Z}$ *é desta forma.*

**Definição 1.1.19.** *Sejam* $A$ *um anel e* $M$ *um ideal próprio de* $A$. *Dizemos que* $M$ *é um ideal maximal de* $A$ *se não existe nenhum ideal* $I$ *de* $A$ *tal que* $M \subsetneq I \subsetneq A$.

**Observação 1.1.20.** *É fato conhecido que todo anel* $A$ *comutativo com unidade possui pelo menos um ideal máximal. Quando existir um único ideal máximal dizemos que* $A$ *é um anel local (veja [1] cap.*1*).*

**Proposição 1.1.21.** *Sejam* $A$ *um anel e* $J$ *um ideal próprio de* $A$. *Se para todo* $a \in A - J$ *temos que* $a \in U(A)$, *então* $A$ *é um anel local e* $J$ *é seu único ideal maximal.*

*Demonstração.* Veja [1], cap.1. □

**Definição 1.1.22.** *Sejam* $A$ *um anel e* $I$, $J$ *ideais de* $A$. *Dizemos que* $I$ *e* $J$ *são ideais coprimos se* $I + J = A$.

**Proposição 1.1.23.** *Se* $I$ *e* $J$ *são ideais coprimos, então valem:*

*i)* $I \cap J = IJ$

*ii)* $I^n$ *e* $J$ *são coprimos para todo* $n \in \mathbb{N}$.

*Demonstração.* Veja [1], cap.1 □

### 1.1.3 Anéis Quocientes e Homomorfismo

Sejam $A$ um anel e $I$ um ideal de $A$. Considere em $A$ a relação "$\equiv (mod\ I)$" definida por:

$$a \equiv b(mod\ I) \text{ se } a - b \in I$$

chamada de relação de coongruência módulo $I$, é uma relação de equivalência. Dado $a \in A$, temos que a classe de equivalência de $a$ com respeito à relação de congruência módulo $I$ é o conjunto

$$a + I = \{a + x / x \in I\}$$

também chamado de *classe lateral de $I$ determinada por $a$*. Costuma-se também denotar $a + I$ por $\bar{a}$.

**Exemplo 1.1.24.** *Sejam $a, b, m \in \mathbb{Z}$. Dizemos que $a$ é congruente a $b$ modulo $m$, e denotamos por $a \equiv b(mod\ m)$, se $m$ divide $(a-b)$. Observe que a relação de congruência módulo $m$ é exatamente a relação de congruência módulo o ideal $\langle m \rangle$ de $\mathbb{Z}$.*

Observe que a aplicação

$$\begin{array}{rcl} f : I & \longrightarrow & a + I \\ x & \longmapsto & a + x \end{array}$$

é uma bijeção. Temos

$$\bigcup_{a \in A} (a + I) = A.$$

Se $a, b \in A$ e $a + I \neq b + I$, então $(a + I) \cap (b + I) = \emptyset$. Para $a, b \in A$, valem:

$$a + I = b + I \iff a \equiv b(mod\ I) \iff a \in b + I \iff b \in a + I.$$

**Observação 1.1.25.** *Sejam $A$ um anel e $I$ um ideal de $A$. Se $a, b, c, d \in A$ são tais que $a \equiv b(mod\ I)$ e $c \equiv d(mod\ I)$, então $a + c \equiv b + d(mod\ I)$ e $ac \equiv bd(mod\ I)$.*

Tomemos agora

$$\frac{A}{I} = \{a + I / a \in A\}$$

e consideremos as operações

$$\begin{array}{rcl} + : \frac{A}{I} \times \frac{A}{I} & \longrightarrow & \frac{A}{I} \\ (\bar{a}, \bar{b}) & \longmapsto & \bar{a} + \bar{b} = \overline{a + b} \end{array}$$

$$\begin{array}{rcl} \cdot : \frac{A}{I} \times \frac{A}{I} & \longrightarrow & \frac{A}{I} \\ (\bar{a}, \bar{b}) & \longmapsto & \bar{a}\bar{b} = \overline{ab} \end{array}$$

observe que estas operações são bem definidas (veja a observeção anterior). Ademais, $A/I$ munido delas, é um anel, chamando de anel quociente de $A$ por $I$. O zero e a unidade de $A/I$ são $\bar{0} = 0 + I = I$ e $\bar{1} = 1 + I$, respectivamente. Ademais, $A/I = \{\bar{0}\}$ se, e somente se $I = A$.

**Definição 1.1.26.** *Sejam $A$ e $R$ anéis. Dizemos que uma aplicação $\varphi : A \longrightarrow R$ é um homomorfismo de anéis se $\varphi(1_A) = 1_R$ e*

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad e \quad \varphi(ab) = \varphi(a)\varphi(b)$$

*para qualquer $a, b \in A$.*

Sendo $\varphi : A \longrightarrow R$ um homomorfismo de anéis, definimos o *núcleo* e a *imagem* de $\varphi$, denotados por $Ker(\varphi)$ e $Im(\varphi)$, respectivamente, como sendo os conjuntos

$$Ker(\varphi) = \{a \in A / \varphi(a) = 0_R\}$$

e

$$Im(\varphi) = \{\varphi(a) / a \in A\}.$$

**Proriedades básicas de homomorfismos**. Seja $\varphi : A \longrightarrow R$ um homomorfismo de anéis. Então,

i) $\varphi(0_A) = 0_R$.

ii) $\varphi(-a) = -\varphi(a)$, $\forall a \in A$.

iii) $\varphi(na) = n\varphi(a)$, $\forall a \in A$ e $\forall n \in \mathbb{Z}$.

iv) $\varphi(a^n) = \varphi(a)^n$, $\forall a \in A$ e $\forall \in \mathbb{Z}$.

v) $Ker(\varphi)$ é um ideal do anel $A$.

vi) $Im(\varphi)$ é um subanel do anel $R$.

*Demonstração.* Para os ítens $(i)$, $(ii)$, $(iii)$ e $(iv)$ veja na referência [4] cap.1. Os demais se demonstram com cálculos básicos. □

**Definição 1.1.27.** *Definimos isomorfismo como sendo um homomorfismo bijetivo.*

Sejam $A$ e $R$ anéis. Se existe algum isomorfismo $\varphi : A \longrightarrow R$, dizemos que $A$ e $R$ são anéis isomorfos, e denotamos por $A \cong R$. Neste caso, observa-se que $\varphi^{-1} : R \longrightarrow A$ é também um isomorfismo.

**Teorema 1.1.28.** *(**Teorema Fundamental do homomorfismo**) Sejam $A$ e $R$ anéis e $\varphi : A \longrightarrow R$ um homomorfismo de anéis. Sendo $I = Ker(\varphi)$, temos $A/I \cong Im(\varphi)$ .*

# 1.2 Espaços métricos

## 1.2.1 Métrica

A partir de agora denotamos $\mathbb{R}_+ = \{x \in \mathbb{R} / \ x \geq 0\}$.

**Definição 1.2.1.** *Seja $M$ um conjunto não vazio. O par $(M, d)$ é chamado de espaço métrico quando a aplicação $d : M \times M \longrightarrow \mathbb{R}_+$ satisfaz as seguintes condições:*
1) *$d_m(x, y) \geq 0$ e $d_m(x, y) = d_m(y, x)$, para quaisquer $x, y \in M$;*
2) *$d_m(x, y) = 0 \Longleftrightarrow x = y$;*
3) *$d_m(x, y) \leq d_m(x, z) + d_m(z, y)$, para quaisquer $x, y, z \in M$.*

Uma aplicação $d$ nas condições acima é chamada de *métrica*. É interessante observar que métrica é a formulação matemática do conceito de distância.

**Exemplo 1.2.2.** *Seja $X$ um conjunto não vazio. Definimos a métrica discreta sobre $X$ como sendo a seguinte aplicação*

$$\begin{array}{rcl} d : X \times X & \longrightarrow & \mathbb{R} \\ (x, y) & \longmapsto & d(x, y) = \left\{ \begin{array}{ll} 1 & se \quad x \neq y \\ 0 & se \quad x = y \end{array} \right. . \end{array}$$

**Exemplo 1.2.3.** *Sejam $(M_1, d_1)$ e $(M_2, d_2)$ espaços métricos, e $M = M_1 \times M_2$. A seguinte aplicação*

$$\begin{array}{rcl} d' : M \times M & \longrightarrow & \mathbb{R} \\ ((x_1, x_2), (y_1, y_2)) & \longmapsto & d'((x_1, x_2), (y_1, y_2)) = \max\{d_1(x_1, y_1), d_2(x_2, y_2)\} \end{array}$$

*é uma métrica(ver [6] cap.1), chamada de* métrica do máximo.

### 1.2.2 Conjuntos abertos e fechados

**Definição 1.2.4.** *Sejam $(M, d)$ um espaço métrico, $x \in M$ e $\epsilon > 0$. Chamamos de bola aberta de centro $x$ e raio $\epsilon$ o conjunto*

$$B(x, \epsilon) = \{y \in M / d(x, y) < \epsilon\}$$

*e chamamos de bola fechada de centro $x$ e raio $\epsilon$ o conjunto*

$$B[x, \epsilon] = \{y \in M / d(x, y) \leq \epsilon\}.$$

Claramente, $B(x, \epsilon) \subseteq B[x, \epsilon]$.

Sejam $X$ um conjunto e $a \in X$. Diz-se que o ponto $a$ é interior ao conjunto $X$ quando, para algum $r > 0$, tem-se $B(a; r) \subset X$. Isto significa que todos os pontos suficientemente próximos de $a$ também pertencem a $X$. O conjunto $int(X)$ dos pontos interiores a $X$ chama-se o interior do conjunto X. Evidentemente, $int(X) \subset X$.

**Definição 1.2.5.** *Um subconjunto $A$ de um espaço métrico $M$ chama-se aberto quando todos os seus pontos são interiores isto é, quando $A = int(A)$.*

**Exemplo 1.2.6.** *Toda bola aberta num espaço métrico é um exemplo de conjunto aberto.*

**Definição 1.2.7.** *Uma **topologia** num conjunto $X$ é uma coleção $\tau$ de partes de $X$, chamados os abertos da topologia, com as seguintes propriedades:*

*i) $\emptyset$ e $X$ pertencem a $\tau$;*

*ii) Se $A_1, A_2, \ldots, A_n \in \tau$, então $A_1 \cap A_2 \cap \ldots \cap A_n \in \tau$;*

*iii) Dada uma família arbitrária $(A_\lambda)_{\lambda \in L}$, com $A_\lambda \in \tau$, para cada $\lambda \in L$, tem-se $\bigcup_{\lambda \in L} A_\lambda \in \tau$.*

Um espaço topológico é um par $(X, \tau)$ onde $X$ é um conjunto e $\tau$ é uma topologia em $X$.

**Exemplo 1.2.8.** *Seja $M = (M, d)$ um espaço métrico. Existe uma topologia natural sobre $M$, construída a partir da métrica $d$ da seguinte forma:*

$$\tau = \{X \subseteq M / \ X = int(X)\}.$$

*Temos que $\tau$ é uma topologia sobre $M$, dita a topologia induzida pela metrica $d$. Assim, todo espaço métrico $M = (M, d)$ pode ser considerado como um espaço topológico $M = (M, \tau)$, onde a topologia $\tau$ é a topologia induzida pela métrica $d$, da forma acima descrita.*

**Exemplo 1.2.9.** *Dado um conjunto não vazio $X$, definimos a topologia discreta em $X$ como sendo a coleção $\tau$ de todos os subconjuntos de $X$. Dizemos que $(X, \tau)$ é um espaço topológico discreto. Observe que esta topologia é induzida pela métrica do Exemplo 1.2.2.*

**Definição 1.2.10.** *Sejam $(M, d)$ um espaço métrico e $Y \subseteq M$. Dizemos que $Y$ é limitado se existem $x \in M$ e $\epsilon > 0$ tais que $Y \subseteq B(x, \epsilon)$.*

### 1.2.3 Função contínua

**Definição 1.2.11.** *Sejam $(M_1, d_1)$, $(M_2, d_2)$ espaços métricos. Dizemos que uma função $f : M_1 \longrightarrow M_2$ é contínua no ponto $x \in M_1$ se para todo $\epsilon > 0$, existe $\delta > 0$ tal que para todo $y \in M_1$ tal que $d_1(x, y) < \delta$, temos que $d_2(f(x), f(y)) < \epsilon$. Se $f$ é contínua em todo ponto $x \in M$, dizemos simplesmente que $f$ é uma função contínua.*

**Proposição 1.2.12.** *Seja $f : M_1 \longrightarrow M_2$. As sequintes afirmações são equivalentes*

*i) $f$ é uma função contínua.*

*ii) A imagem inversa de um fechado por $f$ é um fechado.*

*iii) A imagem inversa de um aberto por $f$ é um aberto.*

*Demonstração.* Ver em [6], cap.1. □

**Definição 1.2.13.** *Sejam $(M_1, d_1)$, $(M_2, d_2)$ espaços métricos. Dizemos que uma função $f : M_1 \longrightarrow M_2$ é um homeomorfismo se é uma bijeção contínua cuja inversa é também contínua.*

Havendo um homeomorfismo $f : M_1 \longrightarrow M_2$, dizemos que os espaços $M_1$ e $M_2$ são homeomorfos.

**Definição 1.2.14.** *Uma aplicação $f : M \to N$, nos quais $M$, $N$ são espaços métricos, é chamada de imersão isométrica quando $d(f(x), f(y)) = d(x, y)$, para quisquer $x, y \in M$.*

Uma imersão isométrica é sempre injetora pois, para $x, y \in M$,

$$f(x) = f(y) \Longrightarrow d(x, y) = d(f(x), f(y)) = 0 \Longrightarrow x = y.$$

Definimos isometria como sendo uma imersão isométrica sobrejetiva. Toda imersão isométrica $f : M \longrightarrow N$ define uma isometria de $M$ sobre o subespaço métrico $f(M) \subset N$. Não é difícil ver que toda isometria é um homeomorfismo.

### 1.2.4 Convergência de sequências

**Definição 1.2.15.** *Seja $M$ um espaço métrico. Dizemos que o ponto $a$ é o limite da sequência $(x_n)$ em $M$ quando, para todo $\epsilon > 0$ dado arbitrariamente, é possível obter $n_0 \in \mathbb{N}$ tal que $n \geq n_0 \Longrightarrow |x_n - a| < \epsilon$. Noutras palavras:* $\lim x_n = a$ *em $X$ se, e somente se $d(x_n, a) \to 0$ para todo $n \geq n_0$ na reta.*

Mostra-se que quando uma sequência $x_n$ possui limite, este é único. Escreve-se então $\lim x_n = a$.

**Definição 1.2.16.** *Quando existe $a = \lim x_n \in X$, diz-se que a sequência de pontos $x_n \in M$ é convergente em $M$, e converge para $a$. Se não existe* $\lim x_n$ *em $M$, dizemos que a sequência é divergente em $M$.*

Diz-se que o ponto $a$ é aderente ao conjunto $X$ quando existe uma sequência $(x_n) \subset X$ tal que $\lim x_n = a$. Chama-se fecho do conjunto $X$ ao conjunto $\overline{X}$ formado por todos os pontos aderentes a $X$. Portanto, $a \in \overline{X} \Longleftrightarrow a = \lim x_k$, $x_k \in X$.

**Definição 1.2.17.** *Um conjunto $F$ chama-se fechado quando $\overline{F} = F$, isto é, quando o limite de toda sequência convergente de pontos de $F$ é ainda um ponto de $F$.*

**Definição 1.2.18.** *Um subconjunto $X \subset M$ diz-se denso em $M$ quando $\overline{X} = M$, ou equivalentemente, quando toda bola aberta em $M$ contém algum ponto de $X$, ou ainda, para todo aberto não vazio $A$ em $M$, tem-se $A \cap X \neq \emptyset$.*

**Definição 1.2.19.** *Uma sequência é dita de Cauchy se, dado $\epsilon > 0$, existe $n_0 \in N$ tal que*

$$m, n \geq n_0 \Longrightarrow d(a_n, a_m) < \epsilon.$$

**Teorema 1.2.20.** *Toda sequência convergente é de Cauchy.*

*Demonstração.* veja em [5], cap.4. □

A recíproca do teorema acima não é verdadeira. Para ver isto, tomemos uma sequência de números racionais $(x_n)$ convergindo para um número irracional $a$. Sendo $(x_n)$ convergente em $\mathbb{R}$, segue-se do teorema anterior que $(x_n)$ é uma sequência de Cauchy no espaço métrico $\mathbb{Q}$ dos números racionais. Mas, evidentimente $(x_n)$ não é convergente em $\mathbb{Q}$.

**Definição 1.2.21.** *Quando toda sequência de Cauchy num espaço métrico $M$ é convergente, dizemos que o espaço $M$ é completo.*

# Capítulo 2

# Topologia $\mathfrak{m}$-Ádica

Neste capítulo iremos introduzir a topologia $\mathfrak{m}$-ádica. Nosso estudo, que foi baseado na referência [8], será voltado para o caso particular quando a topologia $\mathfrak{m}$-ádica é métrizável. Para um estudo do caso geral, recomendamos os livros [1] e [9].

## 2.1 Métrica $\mathfrak{m}$-ádica

Sejam $A$ um anel e $\mathfrak{m}$ um ideal de $A$ tal que $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$. Para cada $x \in A - \{0\}$, tomemos

$$v_{\mathfrak{m}}(x) = max\{n \in \mathbb{N}_0; x \in \mathfrak{m}^n\}.$$

Definimos também $v_{\mathfrak{m}}(0) = +\infty$. Para quaisquer $x, y \in A - \{0\}$ temos então:

a) $v_{\mathfrak{m}}(x) = v_{\mathfrak{m}}(-x)$.

b) $v_{\mathfrak{m}}(x+y) \geq min\{v_{\mathfrak{m}}(x), v_{\mathfrak{m}}(y)\}$.

c) $v_{\mathfrak{m}}(xy) \geq v_{\mathfrak{m}}(x) + v_{\mathfrak{m}}(y) \geq v_{\mathfrak{m}}(y)$.

d) Se $x \in U(A)$, então $v_{\mathfrak{m}}(xy) = v_{\mathfrak{m}}(y)$.

*Demonstração.* a) Se $x \in A$, então $-x \in \mathfrak{m}^n$ se, e somente se, $x \in \mathfrak{m}^n$, pois $\mathfrak{m}^n$ é um ideal.

b) Sejam $n_1, n_2 \in \mathbb{N}_0$ tais que $n_1 = v_{\mathfrak{m}}(x)$ e $n_2 = v_{\mathfrak{m}}(y)$, e suponha sem perda de generalidade que $n_1 \geq n_2$. Assim $x \in \mathfrak{m}^{n_1}$ e $y \in \mathfrak{m}^{n_2}$, com $\mathfrak{m}^{n_1} \subseteq \mathfrak{m}^{n_2}$. Daí $x + y \in \mathfrak{m}^{n_2}$ e portanto $v_{\mathfrak{m}}(x+y) \geq n_2 = \min\{v_{\mathfrak{m}}(x), v_{\mathfrak{m}}(y)\}$.

c) Consideremos $xy \neq 0$, pois no caso $xy = 0$ a desigualdade fica clara. Então, sejam $n_1, n_2 \in \mathbb{N}_0$ tais que $v_{\mathfrak{m}}(x) = n_1$ e $v_{\mathfrak{m}}(y) = n_2$. Logo $x \in \mathfrak{m}^{n_1}$ e $y \in \mathfrak{m}^{n_2}$ e assim $xy \in \mathfrak{m}^{n_1+n_2}$. Por definição de $v_{\mathfrak{m}}$, tem-se que $v_{\mathfrak{m}}(xy) \geq n_1 + n_2 \geq n_2$, ou seja, $v_{\mathfrak{m}}(xy) \geq v_{\mathfrak{m}}(x) + v_{\mathfrak{m}}(y) \geq v_{\mathfrak{m}}$.

d) Já sabemos que $v_{\mathfrak{m}}(xy) \geq v_{\mathfrak{m}}(y)$. Sendo $u = xy$ onde $x \in U(A)$,então $y = x^{-1}u$ e assim $v_{\mathfrak{m}}(y) = v_{\mathfrak{m}}(x^{-1}u) \geq v_{\mathfrak{m}}(u) = v_{\mathfrak{m}}(xy)$.

□

**Observação 2.1.1.** *Se $x = 0$ ou $y = 0$, as arfimações são imediatas, convencionando-se que $+\infty > n$, para todo $n \in \mathbb{N}_0$.*

Definimos agora a seguinte aplicação:

$$\begin{aligned} d_{\mathfrak{m}} : A \times A &\longrightarrow \mathbb{R}_+ \\ (x, y) &\longrightarrow d_{\mathfrak{m}}(x, y) = e^{-v_{\mathfrak{m}}(x-y)} \end{aligned}$$

convencionando-se que $e^{-\infty} = 0$.

**Proposição 2.1.2.** *Para quaisquer $x, y, z \in A$ temos:*

*i)* $d_{\mathfrak{m}}(x, y) \geq 0$ *e* $d_{\mathfrak{m}}(x, y) = d_{\mathfrak{m}}(y, x)$.

*ii)* $d_{\mathfrak{m}}(x, y) = 0 \Longleftrightarrow x = y$.

*iii)* $d_{\mathfrak{m}}(x, y) \leq \max\{d_{\mathfrak{m}}(x, z), d_{\mathfrak{m}}(z, y)\}$.

*iv)* $d_{\mathfrak{m}}(x + z, y + z) = d_{\mathfrak{m}}(x, y)$.

*Demonstração.* i) Sabemos que $d_{\mathfrak{m}}(x, y) = e^{-v_{\mathfrak{m}}(x-y)} \geq 0$ e que $v_{\mathfrak{m}}(x-y) = v_{\mathfrak{m}}(-(x-y)) = v_{\mathfrak{m}}(y-x)$. Assim,

$$d_{\mathfrak{m}}(x, y) = e^{-v_{\mathfrak{m}}(x-y)} = e^{-v_{\mathfrak{m}}(y-x)} = d_{\mathfrak{m}}(y, x).$$

ii) Se $x \neq y$, então $x - y \neq 0$. Logo $e^{-v_{\mathfrak{m}}(x-y)} > 0$. Por outro lado se $x = y$, então $d_{\mathfrak{m}}(x, y) = e^{-v_{\mathfrak{m}}(x-y)} = e^{-v_{\mathfrak{m}}(0)} = e^{-\infty} = 0$

iii) Consideremos $x, y, z \in A$. Temos que $d_{\mathfrak{m}}(x, y) = e^{-v_{\mathfrak{m}}(x-z-y+z)} = e^{-v_{\mathfrak{m}}((x-z)+(z-y))} \leq \max\{d_{\mathfrak{m}}(x, z), d_{\mathfrak{m}}(z, y)\}$, pois

$$v_{\mathfrak{m}}((x-z)+(z-y)) \geq \min\{v_{\mathfrak{m}}(x-z), v_{\mathfrak{m}}(z-y)\}$$

e daí

$$-v_{\mathfrak{m}}((x-z)+(z-y)) \leq \max\{-v_{\mathfrak{m}}(x-z), -v_{\mathfrak{m}}(z-y)\}$$

iv) $d_{\mathfrak{m}}(x+z, y+z) = e^{-v_{\mathfrak{m}}(x+z-y-z)} = e^{-v_{\mathfrak{m}}(x-y)} = d_{\mathfrak{m}}(x,y)$.

□

Temos então que $d_{\mathfrak{m}}$ é mais que uma métrica,ou seja, é uma *ultra-métrica*, uma métrica que satisfaz a condição (iii) acima, que é mais forte que a desigualdade triangular, chamada de métrica $\mathfrak{m}$-ádica. Assim $d_{\mathfrak{m}}$ induz em $A$ uma topologia, chamada *topologia* $\mathfrak{m}$*-ádica*.

**Proposição 2.1.3.** *Munido da topologia* $\mathfrak{m}$*-ádica,* $A$ *é um anel topológico, ou seja, as operações de adição e multiplicação são contínuas.*

*Demonstração.* Considere em $A \times A$ a métrica do máximo (veja o exemplo 1.2.3), definida por:

$$d'((x_1,y_1),(x_2,y_2)) = \max\{d_{\mathfrak{m}}(x_1,x_2), d_{\mathfrak{m}}(y_1,y_2)\}.$$

Seja a aplicação $f$ definida abaixo:

$$\begin{array}{rcl} f : A \times A & \longrightarrow & A \\ (x,y) & \longrightarrow & f(x,y) = x+y. \end{array}$$

Dados $x_1, x_2, y_1, y_2 \in A$, temos

$$\begin{array}{rcl} v_{\mathfrak{m}}(f(x_1,y_1) - f(x_2,y_2)) & = & v_{\mathfrak{m}}((x_1+y_1)-(x_2+y_2)) \\ & = & v_{\mathfrak{m}}((x_1-x_2)+(y_1-y_2)) \geq \\ & \geq & \min\{v_{\mathfrak{m}}(x_1-x_2), v_{\mathfrak{m}}(y_1-y_2)\}. \end{array}$$

Mas,

$$-\min\{v_{\mathfrak{m}}(x_1-x_2), v_{\mathfrak{m}}(y_1-y_2)\} \leq \max\{-v_{\mathfrak{m}}(x_1-x_2), -v_{\mathfrak{m}}(y_1-y_2)\},$$

e daí $d_{\mathfrak{m}}(f(x_1,y_1), f(x_2,y_2)) \leq d'((x_1,y_1),(x_2,y_2))$.

Observe agora que

$$x_1y_1 - x_2y_2 = x_1(y_1-y_2) + y_2(x_1-x_2).$$

Daí

$$\begin{array}{rcl} v_{\mathfrak{m}}(x_1y_1 - x_2y_2) & \geq & \min\{v_{\mathfrak{m}}(x_1(y_1-y_2)), v_{\mathfrak{m}}(y_2(x_1-x_2))\} \\ & \geq & \min\{v_{\mathfrak{m}}(y_1-y_2), v_{\mathfrak{m}}(x_1-x_2)\} \end{array}$$

e assim

$$-v_{\mathfrak{m}}(x_1y_1 - x_2y_2) \leq \max\{-v_{\mathfrak{m}}(y_1-y_2), -v_{\mathfrak{m}}(x_1-x_2)\}.$$

Considerando então

$$\begin{aligned} g : A \times A &\longrightarrow A \\ (x, y) &\longrightarrow g(x, y) = xy \end{aligned}$$

temos que

$$d_{\mathfrak{m}}(g(x_1, y_1), g(x_2, y_2)) \leq \max\{d_{\mathfrak{m}}(x_1, x_2), d_{\mathfrak{m}}(y_1, y_2)\} = d'((x_1, y_1), (x_2, y_2)).$$

Portanto, concluímos que as operações de soma e produto em A são funções contínuas. □

Vamos agora falar de convergência de sequências com respeito à métrica $\mathfrak{m}$-ádica.

**Proposição 2.1.4.** *Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência em A, munido da métrica $\mathfrak{m}$-ádica e $a \in A$. As seguintes afirmações são equivalentes:*

*a) A sequência $(a_n)$ converge para a;*

*b) Dado $k \in \mathbb{N}$, existe $n_0 \in \mathbb{N}$ tal que $a_n - a \in \mathfrak{m}^k$ para todo $n \geq n_0$;*

*c) $v_{\mathfrak{m}}(a_n - a) \longrightarrow +\infty$;*

*Demonstração.* a) Dado $k \in \mathbb{N}$, tomemos $n_0 \in \mathbb{N}$ tal que $d_{\mathfrak{m}}(a_n, a) \leq e^{-k}$ para todo $n \geq n_0$. Dessa forma, para todo $n \geq n_0$, temos que

$$d_{\mathfrak{m}}(a_n, a) = e^{-v_{\mathfrak{m}}(a_n - a)} \leq e^{-k},$$

donde $v_{\mathfrak{m}}(a_n - a) \geq k$ e portanto $a_n - a \in \mathfrak{m}^k$.

b) Dado $k \in \mathbb{N}$, existe $n_0 \in \mathbb{N}$ tal que $a_n - a \in \mathfrak{m}^k$ para todo $n \geq n_0$. Logo, $v_{\mathfrak{m}}(a_n - a) \geq k$ para todo $n \geq n_0$.

c) Sabendo que $\lim v_{\mathfrak{m}}(a_n - a) = +\infty$, então temos que

$$\lim d_{\mathfrak{m}}(a_n, a) = \lim e^{-v_{\mathfrak{m}}(a_n - a)} = 0$$

quando $n \longrightarrow +\infty$. Logo $a_n \longrightarrow a$, quando $n \longrightarrow +\infty$.

□

**Corolário 2.1.5.** *Temos que $a_n \longrightarrow 0$ na topologia $\mathfrak{m}$-ádica se, e somente se, $v_m(a_n) \longrightarrow +\infty$.*

**Proposição 2.1.6.** *Considere em A a métrica m-ádica. Sendo $(a_n), (b_n)$ e $(x_n)$ sequências em A tais que $a_n \longrightarrow a$ e $b_n \longrightarrow b$, com $a, b \in A$, valem:*

*a)* $a_n \pm b_n \longrightarrow a \pm b$ *e* $a_n b_n \longrightarrow ab$.

*b) Se* $a = 0$, *então* $a_n x_n \longrightarrow 0$.

*c)* $(x_n)$ *é sequência de Cauchy se, e somente se,* $x_{n+1} - x_n \longrightarrow 0$ *(ou equivalentemente,* $d_m(x_{n+1}, x_n) \longrightarrow 0$*).*

*d) Se* $A$ *é completo, então a série* $\sum x_n$ *converge, se e somente se,* $x_n \longrightarrow 0$.

*Demonstração.* a) Dado $k \in \mathbb{N}$ temos que existem $n_1, n_2 \in \mathbb{N}$ tais que

$$n \geq n_1 \Longrightarrow a_n - a \in \mathfrak{m}^k \qquad \text{e} \qquad n \geq n_2 \Longrightarrow b_n - b \in \mathfrak{m}^k.$$

Tomando $n_0 = max\{n_1, n_2\}$ tem-se que para todo $n \geq n_0$ vale $a_n - a, b_n - b \in \mathfrak{m}^k$. Como $\mathfrak{m}^k$ é um ideal,

$$(a_n + b_n) - (a + b) = a_n - a + b_n - b \in \mathfrak{m}^k.$$

Logo $(a_n + b_n) \longrightarrow a + b$. De forma análoga, $a_n - b_n \longrightarrow a - b$.

Agora observe que $(a_n b_n - ab) = a_n(b_n - b) + b(a_n - a)$, Sendo $a_n, b \in A$ e $b_n - b, a_n - a \in \mathfrak{m}^k$, então vale que $(a_n b_n - ab) \in \mathfrak{m}^k$, pois $\mathfrak{m}^k$ é um ideal de $A$. Assim, se $n \geq n_0$, tem-se $a_n b_n - ab \in \mathfrak{m}^k$ e daí $a_n b_n \longrightarrow ab$.

b) Sendo $a_n \longrightarrow 0$, então para cada $k \in \mathbb{N}$ existe $n_0 \in \mathbb{N}$ tal que $a_n \in \mathfrak{m}^k$ para $n \geq n_0$. Como $\mathfrak{m}^k$ é um ideal e $x_n \in A$, temos que, para todo $n \geq n_0$, $a_n x_n \in \mathfrak{m}^k$. Logo $a_n x_n \longrightarrow 0$.

c) Sendo $(x_n)$ uma sequência de Cauchy, temos que para todo $\epsilon > 0$ dado, existe $n_0 \in \mathbb{N}$ tal que $n, k > n_0$ implica $d_{\mathfrak{m}}(x_k, x_n) < \epsilon$. Particulamente, para $k = n + 1$. Logo, $d_{\mathfrak{m}}(x_{n+1}, x_n) < \epsilon$ para todo $n \geq n_0$.

Reciprocamente, supondo que $x_{n+1} - x_n \longrightarrow 0$, dado $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $d_{\mathfrak{m}}(x_{n+1}, x_n) < \epsilon$ para todo $n \geq n_0$. Logo, dados $m > n > n_0$, temos

$$dm(x_m, x_n) \leq \max\{d_m(x_m, x_{m-1}), d_m(x_{m-1}, x_{m-2}), ..., d_{\mathfrak{m}}(x_{n+1}, x_n)\} < \epsilon.$$

d) Considere $s_n = \sum_{i=1}^{n} x_i$. Sendo $\sum x_n$ convergente, existe $S = \lim s_n$ e é claro que $S = \lim s_{n-1}$, assim

$$0 = S - S = \lim(s_n - s_{n-1}) = \lim x_n$$

Reciprocamente, suponha $\lim_{k\to\infty} x_k = 0$ e observe que $s_{n+1} - s_n = x_{n+1}$. Como por hipótese temos que $x_k \to 0$ então $s_{n+1} - s_n = x_{n+1} \to 0$

quando $n \to \infty$.Pelo lema acima, $(s_n)_{n\in\mathbb{N}}$ é de Cauchy e sendo $A$ completo, concluimos que $\sum x_n$ é convergente.

□

**Exemplo 2.1.7.** *Seja $A$ é um anel e $\mathfrak{m} = \{0\}$. Observe que $\mathfrak{m}^n = \{0\}$, para todo $n \in \mathbb{N}$. Logo, para todo $x, y \in A$ com $x \neq y$, temos que $v_{\mathfrak{m}}(x-y) = 0$ e daí $d_{\mathfrak{m}}(x,y) = e^{-v_{\mathfrak{m}}(x-y)} = 1$. Agora se $x = y$ temos que $v_{\mathfrak{m}}(x-y) = +\infty$, logo $d_{\mathfrak{m}}(x,y) = e^{-v_{\mathfrak{m}}(x-y)} = 0$. Portanto,a topologia $\mathfrak{m}$-ádica é discreta.Mais geralmente, se $\mathfrak{m}$ é um ideal de $A$ tal que $\mathfrak{m}^n = 0$ para algum $n \in \mathbb{N}$, então a topologia $\mathfrak{m}$-ádica é discreta, visto que, tomando $k_0 = min\{k \in \mathbb{N}_0 \,/\, \mathfrak{m}^k = \{0\}\}$ tem-se que*

$$x \neq y \Longrightarrow v_{\mathfrak{m}}(x-y) < k_0 \Longrightarrow d_{\mathfrak{m}}(x,y) = e^{-v_{\mathfrak{m}}(x-y)} > e^{-k_0}$$

*e, para $x = y$, temos $v_{\mathfrak{m}}(x-y) = v_{\mathfrak{m}}(0) \Longrightarrow d(x,y) = 0$.*

**Exemplo 2.1.8.** *Sejam $A[[x]]$ o anel das séries formais na indeterminada $x$ com coeficientes em $A$ e $\mathfrak{m} = \langle x \rangle$. Temos que $A[[x]]$, munido da métrica $\mathfrak{m}$-ádica, é completo. Observe inicialmente que se $\mathfrak{m} = \langle x \rangle$ então $\mathfrak{m}^n = \langle x^n \rangle$, então $\sum_{j=0}^{\infty} a_j x^j \in \mathfrak{m}^n$ se, e somente se, $a_0 = a_1 = a_2 = \cdots = a_{n-1} = 0$.*

*Considere agora uma sequência de Cauchy $(f_n)_{n\in\mathbb{N}}$ em $A[[x]]$ , digamos $f_n = \sum_{j=0}^{\infty} a_{n_j} x^j$ para todo $n \in \mathbb{N}$. Temos que $f_{n+1} - f_n \longrightarrow 0$ e assim $v_{\mathfrak{m}}(f_{n+1} - f_n) \longrightarrow +\infty$ quando $n \longrightarrow +\infty$. Veja que para cada $k$ natural existe $n_0 \in \mathbb{N}$ $f_{n+1} - f_n \in \mathfrak{m}^k$, e daí $a_{n+1,j} = a_{nj}$, para quaisquer $n \geq n_0$ e $j = 1, 2, \ldots, k$.*

*Assim, para casa $j \in \{1, ..., k\}$, tomemos $a_j = a_{n_0+1,j} = a_{n_0+2,j} = ....$ Como $k$ é arbitrário, fica definido $a_j \in A$ nestas condições para todo $j \in \mathbb{N}$ e assim podemoms tomar $f = \sum_{j=0}^{\infty} a_j x^j$. Obeserve que para cada $k \in \mathbb{N}$ temos*

$$n \geq n_0 \Longrightarrow f_n - f = \sum_{j=0}^{\infty} (a_{nj} - a_j) x^j \in \mathfrak{m}^k$$

*Logo,* $\lim f_n = f$.

**Proposição 2.1.9.** *Sejam $A$ um anel e $\mathfrak{m}$ um ideal de $A$ tal que $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \{0\}$.Considerando a métrica $\mathfrak{m}$-ádica, valem:*

*a) Se $a \in A$ e $n \in \mathbb{N}_0$, então $a + \mathfrak{m}^n$ é uma bola aberta e fechada em $A$. Reciprocamente, toda bola em $A$ é desta forma.*

*b) Se $J$ é um subgrupo aditivo aberto de $A$, então $J$ também é fechado.*

*c) Se $J$ é ideal de $A$, então o fecho de $J$ é o conjunto $\bigcap_{n=1}^{\infty}(J+\mathfrak{m}^n)$ .*

*d) Se $J$ é ideal de $A$, então $J$ é denso em $A$ se, e somente se, $J$ e $\mathfrak{m}$ são coprimos.*

*Demonstração.* a) Tomemos $\epsilon \in \mathbb{R}$ tal que $e^{-n} < \epsilon < e^{1-n}$. Dado $x \in A$, temos que se $x \in a + m^n$, então $x = a + y$, com $y \in \mathfrak{m}^n$, e assim $x - a \in m^n$. Logo $v_m(x-a) \geq n$ o que implica $d_m(x,a) \leq e^{-n} < \epsilon$. Portanto, $a + m^n \subseteq B(a;\epsilon) \subseteq B[a;\epsilon]$.

Veja que se $x \in B[a;\epsilon]$, então $d_{\mathfrak{m}}(a,x) \leq \epsilon < e^{1-n}$ e daí $v_{\mathfrak{m}}(x-a) > n-1$, pois $e^{-v_{\mathfrak{m}}(a-x)} < e^{1-n}$ implica em $-v_{\mathfrak{m}}(a-x) < 1-n$. Logo, $x - a \in \mathfrak{m}^k$ e assim $a + \mathfrak{m}^n = B(a;\epsilon) = B[a;\epsilon]$.

Seja $\delta \in \mathbb{R}$, $\delta > 0$, e tomemos $n_0 = min\{n \in \mathbb{N}_0 \ / \ e^{-n} < \delta\}$ e $n_1 = min\{n \in \mathbb{N}_0 \ / \ e^{-n} \leq \delta\}$. Fixemos $a \in A$. Dado $x \in A - \{a\}$, temos

$$x \in a + \mathfrak{m}^{n_1} \Longleftrightarrow x - a \in \mathfrak{m}^{n_1} \Longleftrightarrow v_{\mathfrak{m}}(x-a) \geq n_1 \Longleftrightarrow d_{\mathfrak{m}}(x,a) \leq e^{-n_1}.$$

Ademais, como $v_{\mathfrak{m}}(x-a) \in \mathbb{N}_0$, temos que se $d_{\mathfrak{m}}(x,a) \leq \delta$, então $v_{\mathfrak{m}}(x-a) \geq n_1$. Logo, $a + \mathfrak{m}^{n_1} = B[a;\delta]$.

Temos também que

$$x \in a + \mathfrak{m}^{n_0} \Longleftrightarrow x - a \in \mathfrak{m}^{n_0} \Longleftrightarrow v_{\mathfrak{m}}(x-a) \geq n_0 \Longleftrightarrow d_{\mathfrak{m}}(x,a) \leq e^{-n_0}.$$

Ademais, como $v_{\mathfrak{m}}(x-a) \in \mathbb{N}_0$, temos que se $d_{\mathfrak{m}}(x,a) < \delta$, então $v_{\mathfrak{m}}(x-a) \geq n_0$. Logo, $a + \mathfrak{m}^{n_0} = B(a;\delta)$.

b) Temos que $A - J = \bigcup_{a \in A-J}(a+J)$ e que, para cada $a \in A$,

$$\begin{array}{rcl} f_a : A & \longrightarrow & A \\ x & \longrightarrow & f_a(x) = a + x \end{array}$$

é um homeomorfismo (na verdade é uma isometria), e para ver isso observe que $d_{\mathfrak{m}}(f_a(x), f_a(y)) = d_{\mathfrak{m}}(a+x, a+y) = d_{\mathfrak{m}}(x,y)$.Então $f_a(J) = a + J$ é aberto e a união de abertos é aberto, implicando assim que $A - J$ é aberto e portanto, $J$ é fechado.

c) Fixemos $k_0 \in \mathbb{N}$, arbitrário. Suponhamos $(a_n)$ e $(b_n)$ sequências contidas em $J$ e em $\mathfrak{m}^{k_0}$, respectivamente, tais que $(a_n + b_n) \longrightarrow a \in A$. Tomando $n_0 \in \mathbb{N}$ tal que $a_n + b_n - a \in \mathfrak{m}^{k_0}$ para todo $n \geq n_0$, temos que $a_{n_0} - a \in \mathfrak{m}^{k_0}$ e assim $a \in a_{n_0} + \mathfrak{m}^{k_0} \subseteq J + \mathfrak{m}^{k_0}$.Logo $J + \mathfrak{m}^{k_0}$ é fechado.

Portanto, $\overline{J} \subseteq \bigcap_{n=1}^{\infty}(J+\mathfrak{m}^n)$. Por outro lado, se $a \in \bigcap_{n=1}^{\infty}(J+\mathfrak{m}^n)$, para cada $n \in \mathbb{N}$ existem $a_n \in J$ e $b_n \in \mathfrak{m}^n$ tais que $a_n + b_n = a$. Como $b_n \longrightarrow 0$ (pelo corolário 2.1.4) temos que $a_n \longrightarrow a$ e assim $a \in \overline{J}$.

d) Supondo $J$ denso em $A$, então $\overline{J} = A$ e pelo ítem $(c)$, temos que $\overline{J} = \bigcap_{n=1}^{\infty}(J+m^n)$, e assim $J + m = A$. Portanto, $m$ e $J$ são coprimos.

Por outro lado, se $m$ e $J$ são coprimos tem-se que $m^n$ e $J$ são coprimos para todo $n \in \mathbb{N}$. Logo, $\overline{J} = \bigcap_{n=1}^{\infty}(J+m^n) = A$. Portanto, $J$ é denso em $A$.

□

**Exemplo 2.1.10.** *Consideremos a sequência $a_n = \sum_{j=0}^{2n-1} 2^j$ em $\mathbb{Z}$, munido da métrica 2-ádica. Observe que $a_n \in J = 3\mathbb{Z}$ para todo $n \in \mathbb{N}$, visto que $a_n = 2^{2n} - 1$. Logo $a_n \longrightarrow -1$. Logo, $J$ não é fechado.Observe que $3\mathbb{Z} + 2\mathbb{Z} = \mathbb{Z}$, ou seja, $J$ e $2\mathbb{Z}$ são coprimos.*

**Teorema 2.1.11.** *Sejam $A$ e $A_1$ anéis e $m$ um ideal de $A$ tal que $\bigcap_{n=1}^{\infty}\mathfrak{m}^n = 0$. Se $\varphi : A \longrightarrow A_1$ é um homomorfismo sobrejetivo e $J = ker\varphi$ é fechado em relação à topologia $\mathfrak{m}$-ádica, então $\bigcap_{n=1}^{\infty}\varphi(\mathfrak{m})^n = 0$ e $\varphi : (A, d_{\mathfrak{m}}) \longrightarrow (A_1, d_{\varphi(\mathfrak{m})})$ é contínua.*

*Demonstração.* Se $y \in \bigcap_{n=1}^{\infty}\varphi(\mathfrak{m})^n$, então existe $x_n \in \mathfrak{m}^n$ tal que $y = \varphi(x_n)$ para cada $n \in \mathbb{N}$. Veja que dado $n \in \mathbb{N}$, como $y = \varphi(x_n) = \varphi(x_1)$, temos $x_1 - x_n \in J$, donde $x_1 \in x_n + J \subseteq \mathfrak{m}^n + J$. Então, $x_1 \in \bigcap_{n=1}^{\infty}(J+\mathfrak{m}^n) = J$, pois $J$ é fechado. Logo $y = 0$.

Tome $x, y \in A$, com $x \neq y$. Temos que $x - y \in \mathfrak{m}^{v_{\mathfrak{m}}(x-y)}$ como $\varphi$ é um homomorfismo, $\varphi(x-y) \in \varphi(\mathfrak{m}^{v_{\mathfrak{m}}(x-y)})$, ou seja, $\varphi(x) - \varphi(y) \in \varphi(\mathfrak{m})^{v_{\mathfrak{m}}(x-y)}$, donde segue que $v_{\mathfrak{m}}(\varphi(x) - \varphi(y)) \geq v_{\mathfrak{m}}(x-y)$. Logo,$d_{\varphi(\mathfrak{m})}(\varphi(x), \varphi(y)) \leq d_{\mathfrak{m}}(x, y)$ e assim $\varphi$ é contínua. □

**Observação 2.1.12.** *A recíproca do teorema anterior é verdadeira e segue do fato de que imagem inversa de fechado por uma função contínua é fechado, obeservando-se que $\{0\}$ é fechado em $A_1$.*

### 2.1.1 Completamento

Sejam $A$ um anel e $\mathfrak{m}$ um ideal de $A$ tal que $\bigcap_{n=1}^{\infty}\mathfrak{m}^n = 0$. Vamos agora mostrar que o anel topológico $(A, d_{\mathfrak{m}})$ possui um completamento, ou seja, vamos mostrar que existem um anel $\hat{A}$ e uma métrica $\hat{d}_{\mathfrak{m}}$, com $(\hat{A}, \hat{d}_{\mathfrak{m}})$ completo e um monomorfismo isométrico $\varphi : A \longrightarrow \hat{A}$ tais que $\varphi(A)$ é denso em

$\hat{A}$. Ademais, este completamento é único, a menos de isomorfismo isométrico.

**Definição 2.1.13.** *Considerando o produto direto*

$$\prod_{n=1}^{\infty} \frac{A}{\mathfrak{m}^n} = \{(a_1 + \mathfrak{m}, a_2 + \mathfrak{m}^2, a_3 + \mathfrak{m}^3, \ldots)/a_i \in A\}.$$

*dizemos que a sequência* $(a_1 + \mathfrak{m}, a_2 + \mathfrak{m}^2, a_3 + \mathfrak{m}^3, \ldots)$ *neste produto direto é coerente se* $a_{n+1} \equiv a_n (mod\ \mathfrak{m}^n)$ *para todo* $n \in \mathbb{N}$.

**Observação 2.1.14.** *Observe que se*

$$(a_1 + \mathfrak{m}, a_2 + \mathfrak{m}^2, a_3 + \mathfrak{m}^3, \ldots) = (b_1 + \mathfrak{m}, b_2 + \mathfrak{m}^2, b_3 + \mathfrak{m}^3, \ldots),$$

*com* $a_i, b_i \in A$, *e* $a_{n+1} \equiv a_n (mod\ \mathfrak{m}^n)$, *então* $b_{n+1} \equiv b_n (mod\ \mathfrak{m}^n)$, *pois* $a_n \equiv b_n (mod\ \mathfrak{m}^n)$ *para todo* $n \in \mathbb{N}$, *e daí* $b_{n+1} = b_n \equiv a_n \equiv a_{n+1} (mod\ \mathfrak{m}^n)$, *daí concluímos que a definição dada acima é boa. Além do mais, para* $m, n \in \mathbb{N}$, *com* $m > n$,

$$\begin{aligned}
a_{n+1} \equiv a_n (mod\ \mathfrak{m}^n) &\implies a_{n+1} - a_n \in \mathfrak{m}^n \\
a_{n+2} \equiv a_{n+1} (mod\ \mathfrak{m}^{n+1}) &\implies a_{n+2} - a_{n+1} \in \mathfrak{m}^{n+1} \\
a_{n+3} \equiv a_{n+2} (mod\ \mathfrak{m}^{n+2}) &\implies a_{n+3} - a_{n+2} \in \mathfrak{m}^{n+2} \\
&\vdots \\
a_m \equiv a_{m-1} (mod\ \mathfrak{m}^{m-1}) &\implies a_m - a_{m-1} \in \mathfrak{m}^{m-1}
\end{aligned}$$

*Desde que* $\mathfrak{m}^{m-1} \subseteq \mathfrak{m}^{m-2} \subseteq \cdots \subseteq \mathfrak{m}^{n+1} \subseteq \mathfrak{m}^n$, *temos que vale a seguinte implicação*

$$m \geq n \Longrightarrow a_m \equiv a_n (mod\ \mathfrak{m}^n).$$

Veja que sendo $\alpha = (a_1 + \mathfrak{m}, a_2 + \mathfrak{m}^2, a_3 + \mathfrak{m}^3, \ldots)$ e $\beta = (b_1 + \mathfrak{m}, b_2 + \mathfrak{m}^2, b_3 + \mathfrak{m}^3, \ldots)$ sequências coerentes,então $a_{n+1} \equiv a_n (mod\ \mathfrak{m}^n)$ e $b_{n+1} \equiv b_n (mod\ \mathfrak{m}^n)$. Logo, $a_{n+1} + b_{n+1} \equiv a_n + b_n (mod\ \mathfrak{m}^n)$ e $a_{n+1} b_{n+1} \equiv a_n b_n (mod\ \mathfrak{m}^n)$ e daí, a soma e o produto de sequêcias coerentes ainda são coerentes. Ademais, toda sequência da forma $(a + \mathfrak{m}, a + \mathfrak{m}^2, a + \mathfrak{m}^3, \ldots)$, com $a \in A$, é coerente, particularmente a unidade de $\prod_{n=1}^{\infty} \frac{A}{\mathfrak{m}^n}$ ( caso $a = 1$) é uma sequência coerente. Assim, $\hat{A} = \left\{\alpha \in \prod_{n=1}^{\infty} \frac{A}{\mathfrak{m}^n} / \alpha \text{ é coerente}\right\}$ é um subanel de $\prod_{n=1}^{\infty} \frac{A}{\mathfrak{m}^n}$.

**Definição 2.1.15.** *Para cada* $k \in \mathbb{N}$, *defina*

$$J_k = \{(a_1 + \mathfrak{m}, a_2 + \mathfrak{m}^2, a_3 + \mathfrak{m}^3, \ldots) \in \hat{A} / a_k \in \mathfrak{m}^k\} \text{ e } J_0 = \hat{A}.$$

Temos que $J_k$ é um ideal de $\hat{A}$. Observe que $a_k \in \mathfrak{m}^k$ equivale a $\overline{a_k} = a_k + \mathfrak{m}^k = \overline{0}$ em $A/\mathfrak{m}^k$, e daí

$$\bigcap_{k=1}^{\infty} J_k = \{0\}.$$

**Observação 2.1.16.** *Seja $\alpha = (a_1 + \mathfrak{m}, a_2 + \mathfrak{m}^2, a_3 + \mathfrak{m}^3, \ldots) \in \hat{A}$. Então :*

*i) Se $\alpha \in J_k$ e $n \leq k$, temos que $\mathfrak{m}^k \subseteq \mathfrak{m}^n$ e $a_n \equiv a_k (mod\ \mathfrak{m}^n)$, e daí $a_n \in \mathfrak{m}^n$. Logo,*

$$J_0 \supseteq J_1 \supseteq J_2 \supseteq \cdots \supseteq J_k \supseteq J_{k+1} \supseteq \cdots$$

*ii) Se $a_k \notin \mathfrak{m}^k$ (ou seja, $\alpha \notin J_k$) e $n \geq k$, então $a_n \notin \mathfrak{m}^n$.*

Feita essa observação, podemos então definir

$$\hat{v}_{\mathfrak{m}}(\alpha) = \max(\{n \in \mathbb{N} / a_n \in \mathfrak{m}^n\} \cup \{0\}) = \max\{k \in \mathbb{N}_0 \ / \ \alpha \in J_k\}.$$

Veja que $\hat{v}_{\mathfrak{m}}((\bar{0}, \bar{0}, \bar{0}, \ldots)) = +\infty$ e que $J_k = \{\alpha \in \hat{A} / \hat{v}_{\mathfrak{m}}(\alpha) \geq k\}$. Ademais, se $\alpha = (a_1 + \mathfrak{m}, a_2 + \mathfrak{m}^2, a_3 + \mathfrak{m}^3, \ldots) \in J_{k_1}$ e $\beta = (b_1 + \mathfrak{m}, b_2 + \mathfrak{m}^2, b_3 + \mathfrak{m}^3, \ldots) \in J_{k_2}$, então $a_{k_1} \in \mathfrak{m}^{k_1}$ e $b_{k_2} \in \mathfrak{m}^{k_2}$. Sabendo que $a_{k_1+k_2} \equiv a_{k_1} (mod\ \mathfrak{m}^{k_1})$ e que $b_{k_1+k_2} \equiv b_{k_2} (mod\ \mathfrak{m}^{k_2})$ seque que $a_{k_1+k_2} \in \mathfrak{m}^{k_1}$ e $b_{k_1+k_2} \in \mathfrak{m}^{k_2}$, donde $a_{k_1+k_2} b_{k_1+k_2} \in \mathfrak{m}^{k_1+k_2}$, e consequentemente $J_{k_1} \cdot J_{k_2} \subseteq J_{k_1+k_2}$. Logo,para $\alpha, \beta \in \hat{A}$, valem:

$$\hat{v}_{\mathfrak{m}}(\alpha) = \hat{v}_{\mathfrak{m}}(-\alpha) \ , \ \hat{v}_{\mathfrak{m}}(\alpha + \beta) \geq \min\{\hat{v}_{\mathfrak{m}}(\alpha), \hat{v}_{\mathfrak{m}}(\beta)\}$$

e

$$\hat{v}_{\mathfrak{m}}(\alpha\beta) \geq \hat{v}_{\mathfrak{m}}(\alpha) + \hat{v}_{\mathfrak{m}}(\beta).$$

Definimos agora

$$\begin{array}{rcl} \hat{d}_{\mathfrak{m}} : \hat{A} \times \hat{A} & \longrightarrow & R_+ \\ (\alpha, \beta) & \longrightarrow & \hat{d}_{\mathfrak{m}}(\alpha, \beta) = e^{-\hat{v}_{\mathfrak{m}}(\alpha - \beta)} \end{array}$$

convencionando-se que $e^{-\infty} = 0$. Temos que $\hat{d}_{\mathfrak{m}}$ é uma ultramétrica em $\hat{A}$. De fato, sabemos que

$$\hat{d}_{\mathfrak{m}}(\alpha, \beta) = e^{-\hat{v}_{\mathfrak{m}}(\alpha - \beta)} \geq 0$$

e que

$$\hat{v}_{\mathfrak{m}}(\alpha - \beta) = \hat{v}_{\mathfrak{m}}(-(\alpha - \beta)) = \hat{v}_{\mathfrak{m}}(\beta - \alpha).$$

Assim,

$$\hat{d}_{\mathfrak{m}}(\alpha,\beta) = e^{-\hat{v}_{\mathfrak{m}}(\alpha-\beta)} = e^{-\hat{v}_{\mathfrak{m}}(\beta-\alpha)} = \hat{d}_{\mathfrak{m}}(\beta,\alpha).$$

Veja que se $\hat{d}_{\mathfrak{m}}(\alpha,\beta) = e^{-\hat{v}_{\mathfrak{m}}(\alpha-\beta)} = 0$, então $\hat{v}_{\mathfrak{m}}(\alpha-\beta) = +\infty$. Logo $\alpha-\beta = 0$, implicando $\alpha = \beta$. Reciprocamente,se $\alpha = \beta$, então $\hat{d}_{\mathfrak{m}}(\alpha,\beta) = e^{-\hat{v}_{\mathfrak{m}}(\alpha-\beta)} = e^{-\infty} = 0$.

Agora consideremos $\alpha,\beta,\gamma \in \hat{A}$. Temos que

$$\hat{d}_{\mathfrak{m}}(\alpha,\beta) = e^{-\hat{v}_{\mathfrak{m}}(\alpha+\gamma-\gamma-\beta)} = e^{-\hat{v}_{\mathfrak{m}}((\alpha-\gamma)+(\gamma-\beta))} \leq \max\{\hat{d}_{\mathfrak{m}}(\alpha,\gamma), \hat{d}_{\mathfrak{m}}(\gamma,\beta)\},$$

pois

$$\hat{v}_{\mathfrak{m}}((\alpha-\gamma)+(\gamma-\beta)) \geq \min\{\hat{v}_{\mathfrak{m}}(\alpha-\gamma), \hat{v}_{\mathfrak{m}}(\gamma-\beta)\}$$

donde

$$-\hat{v}_{\mathfrak{m}}((\alpha-\gamma)+(\gamma-\beta)) \leq \max\{-\hat{v}_{\mathfrak{m}}(\alpha-\gamma), -\hat{v}_{\mathfrak{m}}(\gamma-\beta)\}.$$

Ademais, vale $\hat{d}_m(\alpha+\gamma,\beta+\gamma) = e^{-\hat{v}_{\mathfrak{m}}(\alpha+\gamma-\gamma-\beta)} = e^{-\hat{v}_{\mathfrak{m}}(\alpha-\beta)} = \hat{d}_{\mathfrak{m}}(\alpha,\beta)$.

**Teorema 2.1.17.** *$(\hat{A},\hat{d}_{\mathfrak{m}})$ é um completamento de $(A,d_{\mathfrak{m}})$.*

*Demonstração.* Considerando a aplicação

$$\begin{array}{rcl} \varphi : A & \longrightarrow & \hat{A} \\ x & \longrightarrow & \varphi(x) = (x+\mathfrak{m}, x+\mathfrak{m}^2, x+\mathfrak{m}^3, \ldots). \end{array}$$

Temos que $\varphi$ é um homomorfismo e é uma imersão isométrica, sendo portanto injetivo. De fato, dados $x,y \in A$, temos

$$\begin{array}{rcl} \hat{v}_{\mathfrak{m}}(\varphi(x)-\varphi(y)) & = & \max(\{n \in \mathbb{N} \,/\, x-y \in \mathfrak{m}^n\} \cup \{0\}) \\ & = & \max(\{n \in \mathbb{N}_0 \,/\, x-y \in \mathfrak{m}^n\} = v_{\mathfrak{m}}(x-y) \end{array}$$

ou seja, $d_{\mathfrak{m}}(x,y) = \hat{d}_{\mathfrak{m}}(\varphi(x),\varphi(y))$. Para mostrar que $\varphi(A)$ é denso em $\hat{A}$, tomemos $\alpha = (a_1+\mathfrak{m}, a_2+\mathfrak{m}^2, a_3+\mathfrak{m}^3, \ldots) \in \hat{A}$ e definamos a sequência $(\alpha_n)_{n\in\mathbb{N}}$ em $\varphi(A)$ dada por

$$\alpha_n = (a_n+\mathfrak{m}, a_n+\mathfrak{m}^2, a_n+\mathfrak{m}^3, \ldots).$$

Assim,

$$\alpha_n - \alpha = (\bar{0},\bar{0},\bar{0},\ldots,\bar{0},(a_n-a_{n+1})+m^{n+1},(a_n-a_{n+2})+m^{n+2},\ldots)$$

uma vez que para $m \in \mathbb{N}$, com $m \leq n$, temos $a_m \equiv a_n (mod\ \mathfrak{m}^m)$ e assim $a_n+\mathfrak{m}^m = a_m+\mathfrak{m}^m$. Segue então que $\hat{v}_{\mathfrak{m}}(\alpha_n-\alpha) \geq n$, para todo $n \in \mathbb{N}$ e assim $\alpha_n \longrightarrow \alpha$ em $\hat{A}$.

Considere agora uma sequência de Cauchy $(\alpha_n)$ em $\hat{A}$, digamos $\alpha_n = (a_{n1} + \mathfrak{m}, a_{n2} + \mathfrak{m}^2, a_{n3} + \mathfrak{m}^3, \ldots)$. Temos que,

$$\alpha_{n+1} - \alpha_n \longrightarrow 0$$

e assim $\hat{v}_{\mathfrak{m}}(\alpha_{n+1} - \alpha_n) \longrightarrow +\infty$. Como

$$\alpha_{n+1} - \alpha_n = ((a_{n+1,1} - a_{n1}) + \mathfrak{m}, (a_{n+1,2} - a_{n2}) + \mathfrak{m}^2, (a_{n+1,3} - a_{n3}) + \mathfrak{m}^3, \ldots),$$

para cada $k \in \mathbb{N}$ existe $n_0 \in \mathbb{N}$ tal que $\hat{v}_{\mathfrak{m}}(\alpha_{n-1} - \alpha_n) \geq k$, ou seja, $\alpha_{n-1} - \alpha_n \in J_k$ para todo $n \geq n_0$. Logo $a_{n+1,j} + \mathfrak{m}^j = a_{n_j} + \mathfrak{m}^j$, para todo $n \geq n_0$ e todo $j = 1, 2, 3, \ldots, k$. Concluímos então que, para cada $j \in \mathbb{N}$, a sequência $(a_{nj} + \mathfrak{m}^j)_{n \in \mathbb{N}}$ em $\frac{A}{\mathfrak{m}^j}$ é constante a partir de um certo ponto, e denotemos por $a_j + m^j$ esta constante. Assim, existe $k_j \in \mathbb{N}$ tal que $a_{nj} + \mathfrak{m}^j = a_j + \mathfrak{m}$ para todo $n \geq k_j$.

Considere agora

$$\alpha = (a_1 + \mathfrak{m}, a_2 + \mathfrak{m}^2, a_3 + \mathfrak{m}^3, ...)$$

Dado $j \in \mathbb{N}$, temos

$$\alpha_n - \alpha = (\bar{0}, \bar{0}, \bar{0}, \ldots, \bar{0}, (a_{n,j+1} - a_{j+1}) + \mathfrak{m}^{j+1}, (a_{n,j+2} - a_{j+2}) + \mathfrak{m}^{j+2}, \ldots),$$

e assim $\hat{v}_{\mathfrak{m}}(\alpha_n - \alpha) \geq j$, para todo $n \geq k_j$, logo $\alpha_n \longrightarrow \alpha$, e assim $(\hat{A}, \hat{d}_{\mathfrak{m}})$ é completo. □

**Teorema 2.1.18.** *Sejam $(A, d)$ e $(A_1, d_1)$ anéis topológicos completos, onde $d$ e $d_1$ são métricas. Se $R$ e $R_1$ são subanéis densos de $A$ e $A_1$, respectivamente, tais que existe um isomorfismo isométrico $\varphi : R \to R_1$, então existe um único isomorfismo isométrico $\hat{\varphi} : A \longrightarrow A_1$ estendendo $\varphi$.*

*Demonstração.* Sejam $a \in A$ e $(a_n)$ e $(b_n)$ sequências em $R$ que convergem para $a$. Então $(a_n)$ e $(b_n)$ são sequências de Cauchy em $R$ e $(a_n - b_n) \longrightarrow 0$ em $A$, donde $(\varphi(a_n)$ e $(\varphi(b_n)$ são sequências de Cauchy em $R_1$ e $(\varphi(a_n) - \varphi(b_n) \longrightarrow 0$, pois $\varphi$ é um isomorfismo de anéis. Como $A_1$ é completo, $(\varphi(a_n)$ e $(\varphi(b_n)$ são convergentes em $A_1$ e, além disso, têm o mesmo limite, o qual vamos denotar por $\overline{\varphi}(a)$. Temos então uma aplicação

$$\begin{array}{rcl} \overline{\varphi} : A & \longrightarrow & A_1 \\ a & \longrightarrow & \overline{\varphi}(a) \end{array}$$

com $\overline{\varphi}(x) = \varphi(x)$ para $x \in R$. Sendo $x, y \in A$, consideremos $(x_n)$ e $(y_n)$ em $R$ tais que $x_n \longrightarrow x$ e $y_n \longrightarrow y$. Temos então $d(x_n, y_n) \longrightarrow d(x, y)$ e, consequentemente, $d_1(\varphi(x_n), \varphi(y_n)) \longrightarrow d(x, y)$. Como $d_1(\varphi(x_n), \varphi(y_n)) \longrightarrow$

$d(\overline{\varphi}(x), \overline{\varphi}(y))$, temos pela unicidade de limite que $d(\overline{\varphi}(x), \overline{\varphi}(y)) = d(x, y)$, donde $\overline{\varphi}$ é uma imersão isométrica e portanto é injetora.

Temos também que $x_n + y_n \longrightarrow x + y$ em $A$ e daí

$$\overline{\varphi}(x_n + y_n) \longrightarrow \overline{\varphi}(x + y)$$

em $A_1$, pois $\overline{\varphi}$ é imersão isométrica. Como $x_n, y_n \in R$, temos que $x_n + y_n \in R$ e assim

$$\overline{\varphi}(x_n + y_n) = \varphi(x_n + y_n) = \varphi(x_n) + \varphi(y_n).$$

Logo, como $\varphi(x_n) \to \overline{\varphi}(x)$ e $\varphi(y_n) \to \overline{\varphi}(y)$,

$$\overline{\varphi}(x_n + y_n) \longrightarrow \overline{\varphi}(x) + \overline{\varphi}(y) \text{ em } A_1.$$

Segue então que $\overline{\varphi}(x + y) = \overline{\varphi}(x) + \overline{\varphi}(y)$. Analogamente se mostra que $\overline{\varphi}(x \cdot y) = \overline{\varphi}(x) \cdot \overline{\varphi}(y)$.

Dado $y \in A_1$, tomemos $(y_n)$ uma sequêcia em $R_1$ que converge para $y$. Consideremos agora $x_n = \varphi^{-1}(y_n)$ para todo $n \in \mathbb{N}$. Como $\varphi$ é uma isometria temos que $(x_n)$ é uma sequêcia de Cauchy em $A$ e assim existe $x \in A$ tal que $x_n \longrightarrow x$ em $A$. Sendo $x_n = \varphi^{-1}(y_n)$, então $\varphi(x_n) = y_n$ e assim $\overline{\varphi}(x) = y$, por definição de $\overline{\varphi}$. Portanto, $\overline{\varphi}$ é sobrejetora. □

**Teorema 2.1.19.** *Sejam $A$ um anel e $m$ um ideal maximal de $A$ tal que $\bigcap_{n=1}^{\infty} m^n = \{0\}$. Então, $\hat{A}$ é um anel local.*

*Demonstração.* Sendo

$$J = \{(a_1 + m, a_2 + m^2, a_3 + m^3, \ldots) \in \hat{A} / \ a_1 \in m\},$$

temos que $J$ é um ideal próprio de $\hat{A}$. Com base na Proposição 1.1.21, basta mostrar que $\hat{A} - J \subseteq U(\hat{A})$. De fato, se $\varphi = (a_1 + m, a_2 + m^2, a_3 + m^3, \ldots) \in \hat{A} - J$, então $a_1 \notin m$ e portanto $(a_1) + m = A$, uma vez que $m$ é ideal maximal de $A$. Como $a_n \equiv a_1 (mod\ m)$, temos que $a_n \notin m$ e assim existe $b_n \in A$ tal que $a_n \cdot b_n \equiv 1 (mod\ m^n)$. Temos então a sequêcia $\beta = (b_1 + m, b_2 + m^2, b_3 + m^3, \ldots)$ em $\prod_{n=1}^{\infty} \frac{A}{m^n}$ e observamos que $\alpha\beta = (1 + m, 1 + m^2, 1 + m^3, \ldots)$. Resta agora mostrar que $\beta \in \hat{A}$. Mas observe que para todo $n \in \mathbb{N}$, temos que $a_{n+1} \cdot b_{n+1} \equiv 1 (mod\ m^{n+1})$ e $a_n \cdot b_n \equiv 1 (mod\ m^n)$, donde $a_{n+1} \cdot b_{n+1} \equiv a_n b_n (mod\ m^n)$. Como $a_{n+1} b_{n+1} \equiv a_n b_{n+1} (mod\ m^n)$, concluímos que $a_n b_{n+1} \equiv a_n b_n (mod\ m^n)$. Multiplicando esta última congruência por $b_n$, chegamos a $b_{n+1} \equiv b_n (mod\ m^n)$. □

# Capítulo 3

# Os inteiros $p$-ádicos

## 3.1 Definição e exemplos

Considere o anel $S(\mathbb{Z})$ de todas as sequências em $\mathbb{Z}$(veja o Exemplo 1.1.12). Fixado $p \in \mathbb{N}$ um primo qualquer, uma sequência em $S(\mathbb{Z})$ é dita coerente quando

$$x_n \equiv x_{n+1}(mod\ p^n) \text{ para todo } n \in \mathbb{N}. \tag{3.1}$$

Definamos o conjunto $\Omega_p$ como sendo o conjunto das sequências de inteiros coerentes, ou seja,

$$\Omega_p = \{(x_n) \in S(\mathbb{Z})/\ (a_n)\ \text{ é coerente }\}.$$

O conjunto $\Omega_p$ munido dessa propriedade (3.1) é um subanel do anel $S(\mathbb{Z})$. De fato, dadas $(x_n), (y_n) \in \Omega_p$ temos por (3.1) que

$$x_n \equiv x_{n+1}(mod\ p^n)$$

e

$$y_n \equiv y_{n+1}(mod\ p^n)$$

Usando propriedades de congruência veja que vale

$$x_n + y_n \equiv x_{n+1} + y_{n+1}(mod\ p^n)$$

e

$$x_n y_n \equiv x_{n+1} y_{n+1}(mod\ p^n),$$

isto é,

$$(x_n) + (y_n), (x_n)(y_n) \in \Omega_p.$$

Ademais, $u = (1, 1, 1, 1, \ldots)$, a unidade de $S(\mathbb{Z})$, pertence a $\Omega_p$. Portanto, $\Omega_p$ é um anel comutativo com unidade.

Observe que o conjunto

$$I = \{(x_n) \in \Omega_p / \ p^n | x_n, \forall\ n \in \mathbb{N}\} \text{ onde } p|x_n \text{ significa } p \text{ divide } x_n$$

é um ideal do anel $\Omega_p$. De fato, veja inicialmente que $I$ é um subgrupo aditivo de $\Omega_p$, uma vez que, dados $(x_n), (y_n) \in I$, temos que $(x_n + y_n) \in I$, pois $p^n|x_n$ e $p^n|y_n$, logo $p^n|(x_n + y_n)$ e $p| - x_n$.

Além do mais, dados $(x_n) \in \Omega_p$ e $(y_n) \in I$, temos que $(x_n y_n) \in I$ pois, $p^n|x_n y_n$ para todo $n \in \mathbb{N}$.

Agora vamos olhar para o anel quociente

$$\frac{\Omega_p}{I} = \{\overline{(x_n)} / \ (x_n) \in \Omega_p\}$$

donde $\overline{(x_n)} = (x_n) + I$. Esse anel quociente será chamado de *anel dos inteiros p-ádicos*, e será denotado por $\mathbb{Z}(p)$.

**Definição 3.1.1.** *Se $(x_n) \in S(\mathbb{Z})$ satisfaz:*

*a) $x_{n+1} \equiv x_n (mod\ p^n)$ (ou seja, $(x_n)$ é coerente);*

*b) $0 \leq x_n < p^n$,*

então $(x_n)$ é chamada de *sequência canônica*.

**Lema 3.1.2.** *Existe uma correspondência biunivoca entre $\mathbb{Z}(p)$ e o conjunto das sequências canônicas.*

*Demonstração.* Sejam $(x_n)$ e $(y_n)$ sequências em $\Omega_p$. Observe que

$$\overline{(x_n)} = \overline{(y_n)} \Longleftrightarrow x_n \equiv y_n (mod\ p^n)\ \forall\ n \in \mathbb{N}.$$

Supondo que $(x_n)$ e $(y_n)$ são sequências canônicas tais que $\overline{(x_n)} = \overline{(y_n)}$ temos

$$0 \leq x_n < p^n \qquad , \qquad 0 \leq y_n < p^n$$

e daí

$$-p^n < x_n - y_n < p^n.$$

Como $p^n$ divide $(x_n - y_n)$ devemos ter $x_n - y_n = 0$, e daí $x_n = y_n$.

Ademais, para $(a_n) \in \Omega_p$ e para todo $n \in \mathbb{N}$, existem únicos $q_n$ e $r_n \in \mathbb{Z}$ tais que

$$a_n = p^n q_n + r_n$$

com $0 \leq r_n < p^n$. Observe que $(r_n) \in \Omega_p$. De fato, $r_{n+1} - r_n = a_{n+1} - p^{n+1}q_{n+1} - a_n + p^n q_n$ e sendo $(a_n)$ uma sequência coerente temos $(a_{n+1} - a_n) = p^n k$ com $k \in \mathbb{Z}$ e daí $a_{n+1} - p^{n+1}q_{n+1} - a_n + p^n q_n = (p^n q_n - p^{n+1}q_{n+1}) = p^n k + (p^n q_n - p^{n+1}q_{n+1}) = p^n(k + q_n - pq_{n+1}) = p^n K$ com $K = (k + q_n - pq_{n+1}) \in \mathbb{Z}$. Além do mais,

$$\overline{(r_n)} = \overline{a_n - p^n q_n} = \overline{a_n}$$

.

□

Podemos ver também $\mathbb{Z}(p)$ como sendo o completamento de $\mathbb{Z}$ com respeito à topologia $p$-ádica. Para tanto, seja $m = p\mathbb{Z}$ o ideal principal gerado por $p$ do anel $\mathbb{Z}$. É bom oberservar que $m^n = p^n\mathbb{Z}$ e também que $\bigcap_{n=1}^{\infty} m^n = 0$, uma vez que se $x \in \bigcap_{n=1}^{\infty} m^n$ então $p^n$ divide $x$ para todo $n \in \mathbb{N}$, e assim $x = 0$.

Considere o produto direto

$$\prod_{n=1}^{\infty} \frac{\mathbb{Z}}{m^n} = \{(a_1 + m, a_2 + m^2, a_3 + m^3, \ldots)/a_i \in \mathbb{Z}\}.$$

Já vimos anteriormente que $\hat{A} = \{\alpha \in \prod_{n=1}^{\infty} \frac{\mathbb{Z}}{m^n} / \ \alpha \text{ é coerente}\}$ é um subanel de $\prod_{n=1}^{\infty} \frac{\mathbb{Z}}{m^n}$ e é exatamente o complemento de $\mathbb{Z}$, munido da métrica $p$-ádica.

Consideremos agora a seguinte aplicação

$$\begin{array}{rcl} \Psi : \Omega_p & \longrightarrow & \hat{A} \\ \alpha & \longmapsto & \Psi(\alpha) = (a_1 + m, a_2 + m^2, a_3 + m^3, \ldots). \end{array}$$

Temos que $\Psi$ é um homomorfismo sobrejetivo. De fato, dados $\alpha, \beta \in \Omega_p$ temos que

$$\begin{array}{rcl} \Psi(\alpha + \beta) & = & ((a_1 + b_1) + m, (a_2 + b_2) + m^2, (a_3 + b_3) + m^3, \ldots) \\ & = & (a_1 + m, a_2 + m^2, a_3 + m^3, \ldots) + (b_1 + m, b_2 + m^2, b_3 + m^3, \ldots) \\ & = & \Psi(\alpha) + \Psi(\beta) \end{array}$$

e

$$\begin{array}{rcl} \Psi(\alpha\beta) & = & ((a_1 b_1) + m, (a_2 b_2) + m^2, (a_3 b_3) + m^3, \ldots) \\ & = & (a_1 + m, a_2 + m^2, a_3 + m^3, \ldots)(b_1 + m, b_2 + m^2, b_3 + m^3, \ldots) \\ & = & \Psi(\alpha)\Psi(\beta) \end{array}$$

Ademais, todo elemento de $\hat{A}$ é da forma $(a_1 + m, a_2 + m^2, a_3 + m^3, \ldots)$, com $a_{n+1} \equiv a_n (mod\ p^n)$ para todo $n \in \mathbb{N}$, ou seja, $(a_n)$ coerente.
Pelo Teorema Fundamental dos Homomorfismos temos que

$$\Omega_p / Ker\Psi \cong \hat{A}.$$

Mas observe que,

$$Ker\Psi = \{\alpha \in \Omega_p / \ \Psi(\alpha) = 0\},$$

ou seja,

$$Ker\Psi = \{(x_n) \in \Omega_p / \ a_n \in m^n\} = \{(a_n) \in \Omega_p / \ p^n | a_n, \forall n \in \mathbb{N}\} = I.$$

Portanto, $\mathbb{Z}(p) = \Omega_p / I \cong \hat{A}$.

**Observação 3.1.3.** *Veja que $\mathbb{Z}(p)$ é um anel local, pois considerando o ideal $m = p\mathbb{Z}$ do anel $\mathbb{Z}$, temos que $m$ é um ideal maximal de $\mathbb{Z}$. Além do mais $\bigcap_{n=1}^{\infty} m^n = 0$. Logo, pelo Teorema 2.1.17, $\hat{A}$ é um anel local. Mas como acabamos de ver, $\mathbb{Z}(p) \cong \hat{A}$.*

## 3.2 O $p$-grupo de Prüfer

Iremos dar ínicio a esta seção com a definição de ordem de um elemento no grupo. Assumiremos que o leitor tenha conchecimento sobre grupos, subgrupos, grupos quocientes e homomorfismos de grupos.

**Definição 3.2.1.** *Sejam $(G, +)$ um grupo aditivo e $g \in G$. Para $m \in \mathbb{Z}$ definimos*

$$mg = \begin{cases} g + g + \ldots + g & se \quad m > 0 \\ 0_G & se \quad m = 0 \\ -(|m|)g & se \quad m < 0 \end{cases}.$$

**Definição 3.2.2.** *Sejam $(G, +)$ um grupo aditivo e $a \in G$. Define-se a ordem de $a$ como sendo o menor inteiro positivo $n$ tal que $na = e_G$ e denota-se por $o(a) = n$ . No caso que não existir tal $n \in \mathbb{N}$, dizemos que $o(a)$ é infinita.*

Sejam $G$ um grupo e $a \in G$. O conjunto $H = \langle a \rangle = \{na \ / \ n \in \mathbb{Z}\}$ é um subgrupo $G$, chamado de subgrupo gerado por $a$. É fato conhecido que $|\langle a \rangle| = o(a)$.

**Observação 3.2.3.** *Sejam $G$ um grupo e $a \in G$. Para quaisquer $m, n \in \mathbb{N}$ e supondo $o(a)$ finita, valem:*

*a) $ma = na$ se, e somente se $m \equiv n (mod\ o(a))$;*

*b) $ma = 0$ se, e somente se $o(a) | m$.*

O $p$-grupo de Prüfer é um grupo que tem propriedades muito interessantes e que desempenha um papel muito importante no estudo dos grupos abelianos. Faremos agora um breve estudo deste grupo e do seu anel de endomorfismos, o qual é isomorfo ao anel dos ineiros $p$-ádicos. Um estudo mais aprofundado do $p$-grupo de Prüfer pode encontrado em [7], capítulo 4.

Seja $p \in \mathbb{Z}$ primo e considere o subgrupo aditivo dos racionais

$$A = \left\{ \frac{a}{p^n} / a \in \mathbb{Z}, n \geq 0 \right\}$$

Temos que o grupo quociente $A/\mathbb{Z} = \{\overline{r} = r + \mathbb{Z} \ / r \in A\}$ é chamado de $p$-grupo de Prüfer (uma homenagem ao teorista de grupos, analísta e geometra Heinz Prüfer). Esse grupo é normalmente denotado por $C_{p^\infty}$. Definindo, para todo $n \in \mathbb{Z}$, com $n \geq 0$,

$$\alpha_n = \overline{1/p^n} \quad \text{e} \quad H_n = \langle \alpha_n \rangle,$$

tem-se

$$C_{p^\infty} = \bigcup_{n=0}^{\infty} H_n \quad \text{e} \quad o(\alpha_n) = p^n.$$

De fato, observe que a inclusão $\bigcup_{n=0}^{\infty} H_n \subseteq C_{p^\infty}$ é de fácil percepção. Por outro lado, se $g \in C_{p^\infty}$, então $g = \overline{a/p^n}$, para algum $a \in \mathbb{Z}$ e $n \in \mathbb{Z}_+$. Assim

$$g = \overline{a/p^n} = a \cdot \overline{1/p^n} = a \cdot \alpha_n \in \langle \alpha_n \rangle \subseteq H_n$$

Logo, $g \in \bigcup_{n=0}^{\infty} H_n$ mostrando a igualdade.

Observe que

$$\alpha_n = \overline{1/p^n} = \overline{p^{m-n}/p^n} = p^{m-n} \cdot \overline{1/p^m} = p^{m-n}\alpha_m$$

para $m \geq n$, donde

$$\alpha_n \in \langle \alpha_m \rangle = H_m$$

e assim

$$H_n \subseteq H_m, \forall m \geq n.$$

**Observação 3.2.4.** *Sendo $\gamma \in C_{p^\infty}$ tal que $p^n\gamma = \overline{0}$ (ou seja, $o(\gamma)|p^n$), então $\gamma \in \langle \alpha_n \rangle = H_n$, uma vez que, $p^n\gamma = \overline{0}$ implica em $\overline{p^n r} = \overline{0}$ (onde $\overline{r} = \gamma$), daí $p^n r = k$ com $k \in \mathbb{Z}$ e assim $\gamma = k\overline{1/p^n} = k\alpha_n \in H_n$.*

Veja que tomando $H$ um subgrupo próprio de $C_{p^\infty}$, deve existir $n \in \mathbb{N}_0$ tal que $\alpha_n \notin H$ e daí $\alpha_m \notin H$ para $m \geq n$. Logo deve existir

$$n_0 = \max\{n \in \mathbb{N}_0 \ / \ \alpha_n \in H\}.$$

Assim, $\alpha_{n_0} \in H$ e isso implica que $H_{n_0} \subseteq H$.

Por outro lado, se $g \in H$, então $g = a\alpha_m$, para algum $a \in \mathbb{Z}$ e $m \in \mathbb{N}_0$. Como podemos supor o $mdc(a, p^m) = 1$, tomemos $t, s \in \mathbb{Z}$ tais que $t.a + s.p^m = 1$ e daí,

$$ta\alpha_m + sp^n\alpha_m = \alpha_m$$

donde $tg = \alpha_m$ e daí $\alpha_m \in H$. Logo, $m \leq n_0$, e assim $\alpha_m \in H_{n_0}$ e vamos ter $g \in H_{n_0}$ e portanto $H = H_{n_0}$.

Vamos agora descrever o anel $End(C_{p^\infty})$ dos endormorfismos de $C_{p^\infty}$ ( veja exemplo 1.1.10).

**Observação 3.2.5.** *Se $h, f \in End(C_{p^\infty})$ e $f(\alpha_n) = h(\alpha_n)$, para todo $n \in \mathbb{N}_0$, então $f \equiv h$. Basta ver que se $\gamma \in C_{p^\infty}$, então $\gamma = a\alpha_n$ com $a \in \mathbb{N}$, assim $f(\gamma) = f(a\alpha_n) = af(\alpha_n) = ah(\alpha_n) = h(a\alpha_n) = h(\gamma)$.*

Fixado $u = (x_n) \in \Omega_p$ considere a aplicação abaixo

$$\begin{array}{rcl} f_u : C_{p^\infty} & \longrightarrow & C_{p^\infty} \\ a\alpha_n & \longrightarrow & f_u(a\alpha_n) = ax_n\alpha_n. \end{array}$$

Observe que $f_u$ é uma aplicação bem definida. De fato, se $a\alpha_n = b\alpha_m$, então, desde que $\alpha_n = p^{m-n}\alpha_m$, temos que

$$a \cdot p^{m-n} \equiv b(mod\ p^m).$$

Assim,

$$bx_m\alpha_m = (ap^{m-n} + qp^m)x_m\alpha_m = ax_mp^{m-n}\alpha_m = ax_m\alpha_n = ax_n\alpha_n.$$

**Observação 3.2.6.** *Se $\gamma_1, \gamma_2 \in C_{p^\infty} = \bigcup_{n=0}^{\infty} H_n$, então $\gamma_1 \in H_n$ e $\gamma_2 \in H_m$. Supondo sem perda de generalidade $n \geq m$, temos que $H_n \supseteq H_m$ e assim $\gamma_2 \in H_n$.*

Observe que $f_u$ é um endomorfismo. De fato, dadas $\gamma_1, \gamma_2 \in C_{p^\infty}$,

$$f_u(\gamma_1 + \gamma_2) = f((a+b)\alpha_n) = (a+b)x_n\alpha_n = ax_n\alpha_n + bx_n\alpha_n = f_u(\gamma_1) + f_u(\gamma_2).$$

Consideremos agora a sequinte aplicação

$$\begin{array}{rcl} \varphi : \Omega_p & \longrightarrow & End(C_{p^\infty}) \\ u & \longrightarrow & f_u \end{array}$$

é bem definida, uma vez que todo $f_u$, com $u$ fixo é um elemento do $End(C_{p^\infty})$. Ademais, $\varphi$ é um homomorfismo sobrejetivo de aneis. De fato, considere $u = (x_n), v = (y_n) \in \Omega_p$. Como

$$(f_u + f_v)(\alpha_n) = f_u(\alpha_n) + f_v(\alpha_n) = x_n\alpha_n + y_n\alpha_n = f(u+v)(\alpha_n)$$

e

$$f_u \circ f_v(\alpha_n) = f_u(f_v(\alpha_n)) = f_u(y_n\alpha_n) = x_n(y_n\alpha_n) = (x_n y_n)\alpha_n = f_{uv}(\alpha_n)$$

temos

$$\varphi(u+v) = f(u+v) = f_u + f_v = \varphi(u) + \varphi(v)$$

e

$$\varphi(uv) = f_{uv} = f_u f_v = \varphi(u)\varphi(v).$$

Como todo $f_u \in End(C_{p^\infty})$, vamos mostrar que todo $End(C_{p^\infty})$ é dessa forma. Seja $f \in End(C_{p^\infty})$. Para cada $n \in \mathbb{N}$, temos que $p^n\alpha_n = \overline{0}$ e assim vale

$$\overline{0} = f(\overline{0}) = f(p^n\alpha_n) = p^n f(\alpha_n)$$

ou seja, $f(\alpha_n) \in H_n$. Logo, $f(\alpha_n) = x_n\alpha_n$, com $x_n \in \mathbb{Z}$. Assim geramos uma sequência de inteiros $u = (x_1, x_2, ..., x_n, ...)$. Basta agora vermos se $u \in \Omega_p$. De fato, como $f(\alpha_n) = f(p\alpha_{n+1}) = pf(\alpha_{n+1})$, então $x_n\alpha_n = px_{n+1}\alpha_{n+1}$, ou seja, $x_n\alpha_n = x_{n+1}\alpha_n$. Da observação 3.2.1 temos que $x_n \equiv x_{n+1}(mod\ p^n)$ para todo $n \in \mathbb{N}$.

Usando o teorema fundamental dos homomorfismos temos que

$$\frac{\Omega_p}{Ker\varphi} \cong End(C_{p^\infty})$$

Agora observe que,

$$Ker\varphi = \{u = (x_n) \in \Omega_p \ / \ f_u = 0\} = \{(x_n) \in \Omega_p \ / \ p^n | x_n \ \forall \ n \in \mathbb{N}\} = I.$$

Portanto,

$$\mathbb{Z}(p) = \frac{\Omega_p}{I} \cong End(C_{p^\infty}),$$

Como esse resultado acabamos de mostrar o sequinte teorema.

**Teorema 3.2.7.** *O anel $End(C_{p^\infty})$ é isomorfo ao anel dos inteiros p-ádicos.*

# Referências Bibliográficas


[1] ATIYAH, M. F. MACDONALD, I. G. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Westview Press, 1969.

[2] FRALEIGH, J. B. *A First Course in Abstract Algebra*. 5ª Edição. Addison-Wesley world student series. Pearson Education, 1993.

[3] GODINHO, H. SHOKRANIAN, S., SOARES, M. *Teoria dos Números*. Editora Universidade de Brasília. Brasília, Brasil: IMPA, 1999.

[4] GONÇALVES, A. *Introdução à Álgebra*. Projeto Euclides. Rio de Janeiro, Brasil: IMPA, 1979.

[5] LIMA, E. L. *Curso de Análise*. Volume 1. 13ª Edição. Rio de Janeiro, Brasil: IMPA, 2011.

[6] LIMA, E. L. *Espaços Métricos*. 4ª Edição. Rio de Janeiro, Brasil: IMPA, 2009.

[7] ROBINSON, D.J.S. *A Course in Theory of Groups*. New York, Springer Verlag, 1995.

[8] SAMUEL, P. *Anneaux Factoriels*. Sociedade de Matemática de São Paulo, 1963.

[9] SAMUEL, P.,ZARISKI, O. *Commutative Algebra*, vol.II New York, Springer Verlag, 1960.