UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
BACHARELADO EM MATEMÁTICA

Gustavo Dutra Sousa

O Corpo dos Números p–ádicos: propriedades estruturais e dinâmicas

Juiz de Fora
2023

Gustavo Dutra Sousa

O Corpo dos Números p–ádicos: propriedades estruturais e dinâmicas

Trabalho de conclusão de curso apresentado ao Departamento de Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de bacharel em Matemática.

Orientadora: Profa. Dra. Ana Tércia Monteiro Oliveira

Juiz de Fora

2023

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Dutra, Gustavo.
O Corpo dos Números p–ádicos : propriedades estruturais e dinâmicas / Gustavo Dutra Sousa. – 2023.
69 f. : il.

Orientadora: Ana Tércia Monteiro Oliveira
Trabalho de Conclusão de Curso – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Bacharelado em Matemática, 2023.

1. Valor absoluto p–ádico. 2. Números p–ádicos. 3. Sistemas Dinâmicos. I. Oliveira, Ana Tércia Monteiro, orient. II. Título.

Gustavo Dutra Sousa

O Corpo dos Números p–ádicos: propriedades estruturais e dinâmicas

Trabalho de conclusão de curso apresentado ao Departamento de Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de bacharel em Matemática.

Aprovada em 20 de dezembro de 2023

BANCA EXAMINADORA

Profa. Dra. Ana Tércia Monteiro Oliveira - Orientadora
Universidade Federal de Juiz de Fora

Prof. Dr. Regis Castijos Alves Soares Júnior
Universidade Federal de Juiz de Fora

Profa. Dra. Sara Cristina Campos Borges
Universidade Federal de Juiz de Fora

Dedico este trabalho a todos que me apoiaram.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer ao meu padrasto, Alexsander Pinto da Silva. Foi sorte a minha ter sido criado por uma pessoa que foi capaz de me ensinar tanto, me inspirando e sendo um exemplo diário. Se sou quem sou hoje, devo grande parte a você. Se cheguei aonde estou agora, grande parte é pela forma que fui educado e motivado pela pessoa que você é. A você, só tenho a agradecer.

Tão importante quanto, gostaria de agradecer minha mãe, Raquel Dutra Oliveira Pinto, que sempre me apoiou e confiou em mim, que mesmo longe sempre buscou se fazer próxima, que através das mais singelas atitudes, buscava demonstrar todo seu amor. Obrigado por me mostrar que o amor não se dá apenas pelos grandes feitos, mas, principalmente, pelas pequenos e contínuos gestos.

Reservo lugar também para meu irmão, João Gabriel Dutra Pinto, que, mesmo sem saber, esteve comigo durante toda minha jornada, me motivando a ser a melhor versão de mim mesmo, sempre batalhar e nunca desistir frente desafio algum. Nos momentos mais tristes e paralisantes, foi em você em quem pensei para superar tudo e prosseguir, afinal de contas, eu sou seu irmão mais velho e meu papel é te mostrar que tudo é possível e que sonhos, podem sim, se tornar realidade.

Ademais, gostaria de agradecer minha fiel companheira e melhor amiga, Duda, a melhor cachorrinha que uma pessoa poderia querer. Apesar de que você não vai conseguir ler o que escrevo, espero que de alguma forma você saiba o carinho e amor que sinto por você. Sempre ao meu lado, sempre brincalhona e preguiçosa, sempre amável. Durante as noites do Ensino Remoto, não teria conseguido estudar por tantas horas se não fosse sua aconchegante companhia.

Dedico um agradecimento especial para Maria Eduarda Toledo dos Reis, que em diversos momentos foi o apoio que precisava, o incentivo que me faltava, a motivação que eu necessitava, o carinho que pedia silenciosamente, o conforto que minha cabeça e mente careciam. Quando me sentia sozinho e com saudades de casa, recorria a sua reconfortante e amorosa convivência. Quando me sentia desnecessário e sem rumo, você me mostrava que eu ainda era importante. Quando os estudos pesavam e o cansaço prevalecia, sempre podia tirar férias através dos mais simples momentos que partilhávamos, me mostrando que a felicidade está, de fato, nas coisas simples.

Agradeço a todos meus familiares. Em particular, a minha avó, Edith de Souza Pacheco, que ao longo da faculdade não me forneceu apenas uma casa, mas um lar, me fazendo companhia, se preocupando comigo e buscando me auxiliar e me agradar de todos os modos possíveis. Também agradeço ao meu avô, Manoel Fernando Gonçalves de Oliveira, que sempre acreditou em mim e investiu no meu futuro, me auxiliando com as dificuldades e contribuindo para meus estudos.

Agradeço a minha orientadora, Ana Tércia Monteiro Oliveira, que me acompanhou desde o primeiro período de faculdade, me orientando e me guiando para que pudesse alcançar meu potencial máximo. Sou grato pelas muitas horas dedicadas à minha formação e a todos os conselhos que me levaram a se tornar o matemático que sou hoje.

Agradeço a todos os meus amigos que me acompanharam e aliviaram minha jornada acadêmica. Agradeço em especial aos amigos que fiz ao longo do curso, que, por estarem em uma situação similar, compreendiam as dificuldades encontradas e sempre me motivavam a continuar os estudos, me apoiando e compartilhando horas de estudo.

Agradeço a todos os professores que participaram da minha formação e contribuíram para o meu conhecimento. Em particular, agradeço ao professor Regis e a professora Sara, por terem aceitado participar da banca.

Agradeço a Universidade Federal de Juiz de Fora pelo ensino público, gratuito e de qualidade e por todos os profissionais que aqui atuam pelo excelente serviço prestado.

Por fim, agradeço por ter tanto a agradecer.

“Vejo que esperas de mim algo de grande, talvez de belo. É lamentável, porque só dou o que posso.” Dostoiévski

RESUMO

Partindo do valor absoluto p–ádico, construiremos o corpo dos números p–ádicos, $\mathbb{Q}_p$, como um completamento de $\mathbb{Q}$. A fim de dar destaque a importância desse estudo, também apresentaremos o Teorema de Ostrowski. Estudaremos as propriedades de $\mathbb{Q}_p$ e, em particular, do anel dos inteiros p–ádicos, $\mathbb{Z}_p$. Ao final do trabalho, com os artifícios construídos ao longo do texto, analisaremos a existência de pontos fixos da dinâmica quadrática sobre $\mathbb{Z}_p$.

Palavras-chave: valor absoluto p–ádicos; números p–ádicos; sistemas dinâmicos.

ABSTRACT

Starting from the p–adic absolute value , we will construct the field of p–adic numbers, $\mathbb{Q}_p$, as a completion of $\mathbb{Q}$. In order to highlight the importance of this study, we will also present Ostrowski's Theorem. We will study the properties of $\mathbb{Q}_p$ and, in particular, the ring of p–adic integers, $\mathbb{Z}_p$. At the end of the work, with the devices constructed throughout the text, we will analyze the existence of fixed points of quadratic dynamics over $\mathbb{Z}_p$.

Keywords: p–adic absolute value; p–adic numbers; dynamic systems.

SUMÁRIO

1 INTRODUÇÃO

Os números p–ádicos, onde p é um número primo, foram introduzidos em 1904 pelo matemático alemão Kurt Hensel e tinham como motivação central certos problemas de Teoria dos Números. Por exemplo, a resolução de congruências módulo p^n, tais como $x^2 + 1 \equiv 0 \ (mod\ 5^n)$. Notemos que, para $n = 1$, $x \in \mathbb{Z}$ é uma solução se, e somente se, $x \equiv 2 \ (mod\ 5)$ ou $x \equiv 3 \ (mod\ 5)$. Se $n = 2$, $x \in \mathbb{Z}$ é uma solução se, e somente se, $x \equiv 7 \ (mod\ 5^2)$ ou $x \equiv 18 \ (mod\ 5^2)$, onde $7 = 2 + 1 \cdot 5$ e $18 = 3 + 3 \cdot 5$. Prosseguindo com os valores de n, percebeu-se que existem duas sequências $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$ de inteiros compreendidos entre 0 e 4 de modo que $x \in \mathbb{Z}$ é uma solução de $x^2 + 1 \equiv 0 \ (mod\ 5^n)$ se, e somente se, $x \equiv \sum_{i=0}^{n-1} a_i \cdot 5^i \ (mod\ 5^n)$ ou $x \equiv \sum_{i=0}^{n-1} b_i \cdot 5^i \ (mod\ 5^n)$, onde $a_0 = 2, a_1 = 1, b_0 = 3$ e $b_1 = 3$. Por esse motivo, o estudo das séries do formato $\sum_{i=0}^{\infty} c_i \cdot 5^i$, onde $c_i \in \{0, 1, 2, 3, 4\}$, para todo $i \in \mathbb{N}$, se tornaram relevantes. Contudo, trabalhando em $\mathbb{R}$ essas séries não convergem. Assim, buscou-se um ambiente onde tais séries fossem convergentes. Nesse caso, o ambiente em questão seria o corpo dos números 5–ádicos.

De modo geral, com o desenvolvimento do estudos dos números p–ádicos, percebeu-se a existência de um rico ambiente, onde a topologia adotada propiciava que certos problemas se tornassem mais simples, por exemplo, a convergência de séries.

Por volta de 1980, os números p–ádicos e suas propriedades se tornaram relevantes em outro âmbito, que os relacionavam com sistemas dinâmicos. Buscando a descrição de fenômenos físicos, percebeu-se que as características únicas advindas da métrica p–ádica impactavam diretamente o compreeendimento da Teoria das Cordas, uma das áreas da Física. Desse modo, a investigação das propriedades de sistemas dinâmicos definidos sobre números p–ádicos ganhou destaque.

O corpo central do trabalho é formado por diversos capítulos, que estão organizados do seguinte modo:

1. No Capítulo 2 fornecemos alguns conteúdos e resultados básicos que deverão ser relembrados para um melhor compreendimento dos capítulos seguintes. Neste capítulo, as principais referências utilizadas foram (2), (4), (5), (8) e (9);

2. No Capítulo 3 introduzimos o leitor ao valor absoluto p–ádico em $\mathbb{Q}$, peça fundamental para o desenvolvimento do trabalho. Além disso, exibimos algumas de suas propriedades fundamentais. Neste capítulo, as principais referências utilizadas foram (1), (6), (7) e (10);

3. No Capítulo 4 apresentamos a distância p–ádica, proveniente do valor absoluto p–ádico, e, com esses objetos em mãos, construímos o corpo dos números p–ádicos,

$\mathbb{Q}_p$, através de um anel quociente. Neste capítulo, as principais referências utilizadas foram (1), (6), (7) e (10);

4. No Capítulo 5 listamos algumas das propriedades de $\mathbb{Q}_p$ e estendemos a noção de valor absoluto $p-$ádico para o mesmo, verificando que muitas das propriedades válidas em $\mathbb{Q}$ se mantém no novo ambiente, implicando em características particulares de $\mathbb{Q}_p$. Neste capítulo, as principais referências utilizadas foram (1), (6), (7) e (10);

5. No Capítulo 6 redirecionamos o nosso foco para o anel dos inteiros $p-$ádicos, $\mathbb{Z}_p$. Aqui veremos que, apesar de ser apenas um subconjunto de $\mathbb{Q}_p$, o anel dos inteiros $p-$ádicos apresenta características tão interessantes quando o próprio corpo dos números $p-$ádicos. Em particular, apresentaremos dois resultados centrais, ambos atribuídos a Hensel. Neste capítulo, as principais referências utilizadas foram (1), (6), (7) e (10)

6. No Capítulo 7, buscamos analisar a dinâmica de equações quadráticas, dando enfoque no estudo de pontos fixos, com o auxílio das ferramentas e propriedades estudadas anteriormente. Neste capítulo, as principais referências utilizadas foram (3) e (11);

7. Por fim, no Apêndice é apresentado o Teorema de Ostrowski e os conteúdos necessários para sua compreensão. Tal teorema se torna relevante pois ressalta a importância dos números $p-$ádicos através de uma perspectiva analítica. Neste capítulo, a principal referência utilizada foi (7).

2 PRELIMINARES

Neste capítulo veremos algumas definições e resultados que serão importantes para uma melhor compreensão do conteúdo principal do trabalho.

2.1 CONCEITOS ALGÉBRICOS

Comecemos por alguns conceitos e resultados algébricos.

2.1.1 Anéis e Ideais

Definição 2.1. *Seja A um conjunto não vazio munido das operações*

$$+: \begin{array}{ccc} A\times A & \to & A \\ (a,b) & \mapsto & a+b \end{array} \quad e \quad \cdot: \begin{array}{ccc} A\times A & \to & A \\ (a,b) & \mapsto & a\cdot b \end{array}$$

denominadas adição e multiplicação respectivamente.

*Diremos que $(A,+,\cdot)$ é um **anel** se, dados $a,b,c \in A$, as seguintes 6 propriedades são satisfeitas:*

1 - Associatividade da Adição: (a+b)+c=a+(b+c);

2 - Comutatividade da Adição: a+b=b+a;

3 - Existência do Elemento Neutro da Adição: Existe $0 \in A$ tal que $a+0=0+a=a$, para todo $a \in A$;

4 - Existência do Elemento Simétrico: Para todo $a \in A$ existe $x \in A$, denotado por $-a$,modo que $a+x=x+a=0$;

5 - Associatividade da Multiplicação: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$;

6 - Distributividade à esquerda e à direita: $a\cdot(b+c)=a\cdot b+a\cdot c$ e $(a+b)\cdot c = a\cdot c+b\cdot c$.

Ademais, dado um anel $(A,+,\cdot)$, se

*7 - Existe $1 \in A, 1 \neq 0$, tal que $1\cdot a = a\cdot 1 = a$, para todo $a \in A$, dizemos que $(A,+,\cdot)$ é um **anel com unidade 1**;*

*8 - Para todo $a,b \in A$, $a\cdot b = b\cdot a$, dizemos que $(A,+,\cdot)$ é um **anel comutativo**;*

*9 - Para todo $a,b \in A$, $a\cdot b = 0$, implica em $a=0$ ou $b=0$, dizemos que $(A,+,\cdot)$ é um **anel sem divisores de zero**.*

Se $(A, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um ***domínio de integridade****.*

Por fim, se um domínio de integridade $(A, +, \cdot)$ satisfaz a propriedade abaixo, dizemos que $(A, +, \cdot)$ é um ***corpo****.*

10 - Para todo $a \in A, a \neq 0$, existe $y \in A$, denotado por a^{-1}, tal que $a \cdot y = y \cdot a = 1$.

Definição 2.2. *Sejam $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A, fechado para as operações $+$ e $\cdot$. Se $(B, +, \cdot)$ for um anel com as operações de A, dizemos que B é um* ***subanel*** *de A.*

Proposição 2.1. *Sejam $(A, +, \cdot)$ um anel e B um subconjunto de A. Então, B é um subanel de A se, e somente se, as seguintes condições são satisfeitas:*

1. *$0 \in B$;*
2. *Se $x, y \in B$, então $x - y \in B$;*
3. *Se $x, y \in B$, então $x \cdot y \in B$.*

Demonstração: Ver (5). ■

Definição 2.3. *Seja A um anel e seja I um subanel de A. Dizemos que I é um*

1. ***Ideal a esquerda*** *de A se, $a \cdot x \in I$, para todo $a \in A$ e para todo $x \in I$;*
2. ***Ideal a direita*** *de A se, $x \cdot a \in I$, para todo $a \in A$ e para todo $x \in I$;*
3. ***Ideal*** *de A se for simultaneamente um ideal a esquerda e um ideal a direita.*

Definição 2.4. *Um ideal I de A é dito um* ***ideal maximal*** *se $I \neq A$ e para todo ideal J de A tal que $I \subset J \subset A$, temos ou $J = I$ ou $J = A$.*

Seja A um anel qualquer e seja I um ideal de A. A partir dessas estruturas construiremos o que será denominado por conjunto quociente. Para tanto, precisamos dos conceitos a seguir.

Definição 2.5. *Dado um conjunto A, chama-se* ***relação de equivalência*** *em A, toda relação $\mathcal{R} \subset A \times A$ reflexiva, simétrica e transitiva, ou seja, que satisfaz:*

1. *$(x, x) \in \mathcal{R}$, para todo $x \in A$;*
2. *Se $(x, y) \in \mathcal{R}$, então $(y, x) \in \mathcal{R}$, para todo $x, y \in A$;*

3. *Se* $(x,y),(y,z) \in \mathcal{R}$, *então* $(x,z) \in \mathcal{R}$, *para todo* $x,y,z \in A$.

Observação 2.1. *Seja* A *um conjunto e* $\mathcal{R}$ *uma relação em* A. *Dados* $x,y \in A$, *usaremos a notação* $x\mathcal{R}y$ *para representar* $(x,y) \in \mathcal{R}$.

Seja A um anel qualquer e seja I um ideal de A. Dados $x,y \in A$ consideremos a relação $\equiv (mod\ I)$ em A, onde

$$x \equiv y\ (mod\ I) \Leftrightarrow x - y \in I.$$

Proposição 2.2. *A relação definida acima é uma relação de equivalência em* A.

Demonstração: De fato, sejam $x,y,z \in A$. Temos,

1. Como $x - x = 0 \in I$, temos $x \equiv x\ (mod\ I)$;
2. Se $x \equiv y\ (mod\ I)$, então $x - y \in I$, e consequentemente, $-(x-y) = y - x \in I$, ou seja, $y \equiv x\ (mod\ I)$;
3. Sejam $x \equiv y\ (mod\ I)$ e $y \equiv z\ (mod\ I)$, então $x-y, y-z \in I$, assim, $(x-y)+(y-z) = x - z \in I$, isto é, $x \equiv z\ (mod\ I)$.

■

Definição 2.6. *Dado* $x \in A$, *definimos a* ***classe de equivalência*** *de* x *mediante a relação* $\equiv\ (mod\ I)$ *como* $\overline{x} = \{y \in A; x \equiv y\ (mod\ I)\}$.

Observação 2.2. *Note que, se* $y \in \overline{x}$, *então* $x - y \in I$. *Por isso, também podemos representar a classe de* x *por* $\overline{x} = x + I = \{x + z; z \in I\}$.

Definição 2.7. *Sejam* A *um anel e* I *um ideal de* A. *Chamaremos de* ***conjunto quociente de*** A ***pelo ideal*** I *o conjunto* $A/I = \{\overline{x} = x + I; x \in A\}$.

Teorema 2.1. *Seja* A *um anel comutativo com unidade* 1 *e seja* I *um ideal de* A. *Então* I *é um ideal maximal de* A *se, e somente se,* A/I *é um corpo.*

Demonstração: Ver (5). ■

Por fim, também definiremos um homomorfismo de anéis, que será importante no Capítulo 5.

Definição 2.8. *Sejam* A, A' *anéis. Uma função* $f : A \to A'$ *diz-se um* ***homomorfismo*** *se, para todo* $x,y \in A$, *as condições abaixo são satisfeitas:*

1. $f(x+y) = f(x) + f(y)$;
2. $f(x \cdot y) = f(x) \cdot f(y)$.

2.1.2 Divisibilidade e MDC

Definição 2.9. *Dados dois inteiros a e b, dizemos que b **divide** a, e denotamos $b \mid a$, se, e somente se, existe um inteiro q tal que $a = bq$.*

Teorema 2.2 (Algoritmo da Divisão de Euclides). *Sejam a e b inteiros com $b \neq 0$. Então existem únicos inteiros q e r tais que $a = b \cdot q + r$, onde $0 \leq r \leq b - 1$.*

Demonstração: Ver (2). ■

Definição 2.10. *Sejam a e b dois inteiros não simultaneamente nulos. Chama-se **máximo divisor comum** de a e b, e denota-se por $\mathrm{mdc}(a, b)$, o inteiro positivo d que satisfaz as condições:*

1. *$d \mid a$ e $d \mid b$;*
2. *Se c é um inteiro tal que $c \mid a$ e $c \mid b$, então $c \leq d$.*

Teorema 2.3 (Teorema de Bézout). *Sejam a e b inteiros não simultaneamente nulos e $d = \mathrm{mdc}(a, b)$. Então existem inteiros x e y tais que $d = a \cdot x + b \cdot y$.*

Demonstração: Ver (2). ■

Proposição 2.3. *Sejam $a, b, c \in \mathbb{Z}$. Temos $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, c) = 1$ se, e somente se, $\mathrm{mdc}(a, bc) = 1$.*

Demonstração: Ver (2). ■

2.1.3 O Teorema Fundamental da Aritmética

Teorema 2.4 (Teorema Fundamental da Aritmética). *Todo número inteiro não nulo n pode ser escrito na forma,*

$$n = u \cdot p_1 \cdot \ldots \cdot p_k,$$

onde $u \in \{-1, 1\}$ e $p_1 \leq p_2 \leq \ldots \leq p_k$ são números primos positivos. Mais ainda, essa expressão é única a não ser pela ordem dos fatores.

Demonstração: Ver (5). ■

Corolário 2.1. *Fixado p primo e dado $m \in \mathbb{Z}$ não nulo, existe um único natural l e $a \in \mathbb{Z}$ tais que $m = p^l \cdot a$, com $\mathrm{mdc}(p, a) = 1$.*

Demonstração: Ver (2). ■

2.2 VALORES ABSOLUTOS E MÉTRICAS

Para o desenvolvimento do tema aqui estudado, um dos principais conceitos é o de valor absoluto p–ádico. Desse modo, para auxiliar na construção futura, relembraremos nessa seção algumas propriedades gerais referentes aos valores absolutos e métricas.

Definição 2.11. *Seja $\mathbb{K}$ um corpo arbitrário. Uma aplicação $|\cdot| : \mathbb{K} \to \mathbb{R}$ é dita um* ***valor absoluto em*** *$\mathbb{K}$, se as seguintes condições são satisfeitas:*

1- $|x| \geq 0$, *para todo* $x \in \mathbb{K}$;

2- $|x| = 0$ *se, e somente se,* $x = 0$;

3- $|x \cdot y| = |x| \cdot |y|$, *para todo* $x, y \in \mathbb{K}$;

4- $|x + y| \leq |x| + |y|$, *para todo* $x, y \in \mathbb{K}$.

Em particular, se a aplicação $|\cdot| : \mathbb{K} \to \mathbb{R}$ satisfaz as condições $1, 2$ e 3 e a condição abaixo:

5- $|x + y| \leq \max\{|x|, |y|\}$, *para todo* $x, y \in \mathbb{K}$,

dizemos que $|\cdot|$ é um valor absoluto ***ultramétrico*** *ou* ***não-arquimediano****.*

Exemplo 2.1 (Valor Absoluto Trivial). *Considere a função $|\cdot| : \mathbb{K} \to \mathbb{R}$ definida por:*

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

A aplicação acima é um valor absoluto em $\mathbb{K}$ e é chamada de valor absoluto trivial.

De fato,

1. *Se $x \in \mathbb{K}$, então $|x| = 1$ ou $|x| = 0$, e portanto, $|x| \geq 0$;*
2. *É imediato pela definição;*
3. *Analisaremos os seguintes casos para $x, y \in \mathbb{K}$:*

   a) $x, y \neq 0$
   $\Rightarrow x \cdot y \neq 0 \Rightarrow |x \cdot y| = 1 = 1 \cdot 1 = |x| \cdot |y|$;

b) $x = 0$ *ou* $y = 0$
$\Rightarrow x \cdot y = 0 \Rightarrow |x \cdot y| = 0 = |x| \cdot |y|$.

4. Analisaremos os seguintes casos para $x, y \in \mathbb{K}$*:*

a) $x + y \neq 0$
Neste caso, $1 \leq |x| + |y|$*. Assim,* $|x + y| = 1 \leq |x| + |y|$;

b) $x + y = 0$
$\Rightarrow |x + y| = 0 \leq |x| + |y|$.

Portanto, $|\cdot|$ *é um valor absoluto.*

Exemplo 2.2 (Valor Absoluto Real). *A função* $|\cdot|_\infty : \mathbb{Q} \to \mathbb{R}$ *definida como*

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

é um valor absoluto em $\mathbb{Q}$ *e é chamado de valor absoluto real.*

De fato, sejam $x, y \in \mathbb{Q}$*. Então,*

1. Pela definição da aplicação, $|x|_\infty \geq 0$*;*

2. Se $|x|_\infty = 0$*, então* $x = 0$*, pois, caso contrário,* $|x|_\infty = x \neq 0$ *ou* $|x|_\infty = -x \neq 0$*. Ademais, se* $x = 0$*, temos* $|x|_\infty = 0$*;*

3. Analisaremos os seguintes casos:

a) $x, y \geq 0$
$\Rightarrow |x \cdot y|_\infty = x \cdot y = |x|_\infty \cdot |y|_\infty$*;*

b) $x, y < 0$
$\Rightarrow |x \cdot y|_\infty = x \cdot y = (-x) \cdot (-y) = |x|_\infty \cdot |y|_\infty$*;*

c) $x < 0 \leq y$
$\Rightarrow |x \cdot y|_\infty = -(x \cdot y) = (-x) \cdot y = |x|_\infty \cdot |y|_\infty$*;*

d) $y < 0 \leq x$
A prova é análoga ao caso anterior.

4. Primeiramente, notemos que $|x|_\infty = \max\{x, -x\}$*. Assim,*

$$|x + y|_\infty = \max\{x + y, -(x + y)\} \leq \max\{x, -x\} + \max\{y, -y\} = |x|_\infty + |y|_\infty$$
$$\therefore \quad |x + y|_\infty \leq |x|_\infty + |y|_\infty.$$

Portanto, conclui-se que $|\cdot|_\infty$ *é um valor absoluto.*

A proposição a seguir nos mostra que todo valor absoluto ultramétrico é um valor absoluto.

Proposição 2.4. *Seja* $|\cdot| : \mathbb{K} \to \mathbb{R}$ *um valor absoluto ultramétrico. Temos* $|x+y| \leq |x| + |y|$, *para todo* $x, y \in \mathbb{K}$.

Demonstração: De fato, como $|\cdot|$ é um valor absoluto ultramétrico,

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

Ademais, como $|x| \geq 0, \forall x \in \mathbb{K}$, segue que

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

Portanto, $|x + y| \leq |x| + |y|$. ■

A proposição seguinte reúne algumas propriedades básicas de um valor absoluto qualquer.

Proposição 2.5. *Seja* $|\cdot| : \mathbb{K} \to \mathbb{R}$ *um valor absoluto. Então,*

1. $|1| = 1$;
2. $|-x| = |x|$, *para todo* $x \in \mathbb{K}$;
3. $|x^{-1}| = |x|^{-1}$, *para todo* $x \in \mathbb{K}, x \neq 0$.

Demonstração:

1. Naturalmente, $1 = 1 \cdot 1$, logo, pela definição de valor absoluto, segue que:

$$|1| = |1 \cdot 1| = |1| \cdot |1| \Rightarrow |1| \cdot |1|^{-1} = |1| \cdot |1| \cdot |1|^{-1} \Rightarrow |1| = 1.$$

2. Partindo do item anterior e da definição de valor absoluto, temos

$$1 = |1| = |(-1) \cdot (-1)| = |-1| \cdot |-1| \Rightarrow 1 = |-1|^2$$

$$\Rightarrow |-1| = 1.$$

Daí,

$$|-x| = |(-1) \cdot x| = |-1| \cdot |x| = 1 \cdot |x| = |x|$$

$$\Rightarrow |-x| = |x|.$$

3. Novamente, pelos resultados obtidos nos itens anteriores e da própria definição de valor absoluto, temos, para $x \neq 0$,

$$1 = |1| = |x \cdot x^{-1}| = |x| \cdot |x^{-1}| \Rightarrow 1 = |x| \cdot |x^{-1}| \Rightarrow |x^{-1}| = |x|^{-1}.$$

Concluindo a prova da proposição. ■

Observação 2.3. *Note que, a partir da proposição acima, podemos concluir que, dado um valor absoluto ultramétrico $|\cdot| : \mathbb{K} \to \mathbb{R}$, temos $|x - y| \leq \max\{|x|, |y|\}$. De fato,*

$$|x - y| = |x + (-y)| \leq \max\{|x|, |-y|\} = \max\{|x|, |y|\}.$$

Proposição 2.6. *Seja $|\cdot| : \mathbb{K} \to \mathbb{R}$ um valor absoluto ultramétrico. Então,*

$$|x_1 + x_2 + \ldots + x_n| \leq \max\{|x_1|, |x_2|, \ldots, |x_n|\}.$$

Demonstração: Para $n = 1$, temos, naturalmente, $|x_1| = \max\{|x_1|\}$.

Suponhamos que a afirmativa seja válida para $n = k$. Assim,

$$\begin{aligned} |x_1 + x_2 + \ldots + x_k + x_{k+1}| &\leq \max\{|x_1 + x_2 + \ldots + x_k|, |x_{k+1}|\} \\ &\leq \max\{\max\{|x_1|, |x_2|, \ldots, |x_k|\}, |x_{k+1}|\} \\ &= \max\{|x_1|, |x_2|, \ldots, |x_k|, |x_{k+1}|\}. \end{aligned}$$

Portanto, pelo Princípio de Indução Matemática, segue o resultado.

■

A partir do conceito de valor absoluto, podemos definir uma métrica. Antes deste caso particular, vejamos a definição geral.

Definição 2.12. *Seja M um conjunto não vazio. A função $d : M \times M \to \mathbb{R}$ é chamada de **métrica** em M se as seguintes condições são satisfeitas para todo $x, y, z \in M$:*

1. $d(x, y) \geq 0$;
2. $d(x, y) = 0 \Leftrightarrow x = y$;
3. $d(x, y) = d(y, x)$;
4. $d(x, z) \leq d(x, y) + d(y, z)$.

*Neste caso, (M, d) é dito um **espaço métrico**.*

Definição 2.13. *Seja (M, d) um espaço métrico. Se $d(x, z) \leq \max\{d(x, y), d(y, z)\}$, para todo $x, y, z \in M$, então d é dita uma **ultramétrica** ou uma **métrica não-arquimediana**.*

Proposição 2.7. *Sejam $\mathbb{K}$ um corpo e $|\cdot|$ um valor absoluto em $\mathbb{K}$. Então a função $d : \mathbb{K} \times \mathbb{K} \to \mathbb{R}$ definida por $d(x, y) = |x - y|$ é uma métrica em $\mathbb{K}$. Neste caso, d é uma métrica induzida pelo valor absoluto $|\cdot|$.*

Demonstração: Sejam $x, y, z \in \mathbb{K}$. Então,

1. Pela Definição 2.11, $d(x, y) = |x - y| \geq 0$;

2. Segue que $d(x, y) = 0 \Leftrightarrow |x - y| = 0$, e, pela Definição 2.11,

$$|x - y| = 0 \Leftrightarrow x - y = 0 \Leftrightarrow x = y.$$

3. Pela Proposição 2.5, $|x| = |-x|$. Logo,

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

$$\therefore \quad d(x, y) = d(y, x).$$

4. Usando a Definição 2.11, temos

$$d(x, z) = |x - z| = |(x - y) + (y - z)| \leq |x - y| + |y - z| = d(x, y) + d(y, z)$$

$$\therefore d(x, z) \leq d(x, y) + d(y, z).$$

Deste modo, demonstramos que d, é, de fato, uma métrica em $\mathbb{K}$. ■

Corolário 2.2. *Sejam $\mathbb{K}$ um corpo e $|\cdot|$ um valor absoluto ultramétrico em $\mathbb{K}$. Então, a função $d : \mathbb{K} \times \mathbb{K} \to \mathbb{R}$ definida por $d(x, y) = |x - y|$ é uma ultramétrica em $\mathbb{K}$.*

Demonstração: Como $|\cdot|$ é um valor absoluto, pela Proposição 2.7 , d é uma métrica. Basta mostrar que $d(x, z) \leq \max\{d(x, y), d(y, z)\}$. Assim, como $|x - z| \leq \max\{|x - y|, |y - z|\}$ segue que

$$d(x, z) = |x - z| \leq \max\{|x - y|, |y - z|\} = \max\{d(x, y), d(y, z)\}.$$

Logo, d é uma ultramétrica em $\mathbb{K}$. ■

2.3 SEQUÊNCIAS

A seguir lembraremos os conceitos de sequência limitada, sequência convergente e sequência de Cauchy, assim como a relação entre eles. Para tal, consideremos o espaço métrico M munido da métrica proveniente do valor absoluto $|\cdot|$ ultramétrico e uma sequência $(q_n)_{n\in\mathbb{N}}$ em M.

Definição 2.14. *A sequência* $(q_n)_{n\in\mathbb{N}}$ *é* ***limitada*** *em* M *se, e somente se, existe um número real* $L > 0$ *tal que* $|q_n| \leq L, \forall n \in \mathbb{N}$.

Definição 2.15. *Dizemos que a sequência* $(q_n)_{n\in\mathbb{N}}$ *converge para* $q \in M$ *quando para todo* $\varepsilon > 0$, *existe* $n_0 = n_0(\varepsilon) \in \mathbb{N}$ *tal que* $d(q_n, q) = |q_n - q| \leq \varepsilon, \forall n \geq n_0$. *Neste caso, dizemos que* $(q_n)_{n\in\mathbb{N}}$ *é* ***convergente*** *em* M.

Definição 2.16. *Dizemos que* $(q_n)_{n\in\mathbb{N}}$ *é uma* ***sequência de Cauchy*** *em* M *se, para todo* $\varepsilon > 0$, *existe* $n_0 = n_0(\varepsilon) \in \mathbb{N}$ *tal que* $d(q_m, q_n) = |q_m - q_n| \leq \varepsilon$, *para quaisquer* $m, n \geq n_0$.

Proposição 2.8. *Toda sequência convergente em* M *é de Cauchy.*

Demonstração: Considere $(q_n)_{n\in\mathbb{N}}$ uma sequência convergente para $q \in M$. Assim, para todo $\varepsilon > 0$, existe n_0 natural tal que $|q_n - q| \leq \varepsilon$, para todo $n \geq n_0$. Daí, para $m, n \geq n_0$, temos

$$|q_m - q_n| = |(q_m - q) + (q - q_n)| \leq \max\{|q_m - q|, |q - q_n|\} = \max\{|q_m - q|, |q_n - q|\} \leq \varepsilon$$

Logo, $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.

■

Proposição 2.9. *Toda sequência de Cauchy em* M *é limitada.*

Demonstração: Seja $(q_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy em M. Então, existe n_0 natural tal que para quaisquer $m, n \geq n_0$, temos

$$|q_m - q_n| \leq 1.$$

Assim, para $n \geq n_0$,

$$|q_n| \leq \max\{|q_n - q_{n_0}|, |q_{n_0}|\} \leq \max\{1, |q_{n_0}|\}.$$

Tomemos $C = \max\{|q_n|; 1 \leq n \leq n_0\}$. Então, para todo $n \in \mathbb{N}$,

$$|q_n| \leq \max\{C, 1\}$$

Portanto, $(q_n)_{n\in\mathbb{N}}$ é limitada. ■

Definição 2.17. *Dizemos que um espaço métrico* (M, d) *é* ***completo*** *quando toda sequência de Cauchy em* M *é convergente.*

Exemplo 2.3. *Seja $(\mathbb{Q}, d)$, onde d é a métrica proveniente do valor absoluto trivial. Então, $(\mathbb{Q}, d)$ é completo.*

De fato, seja $(x_n)_{n\in\mathbb{N}}$ um sequência de Cauchy em $\mathbb{Q}$. Então, existe $n_0 \in \mathbb{N}$ de modo que $|x_n - x_m| \leq \frac{1}{2}$, para todo $m, n \geq n_0$. Desse modo, $x_n - x_m = 0$, ou seja, $x_n = x_m$, para todo $m, n \geq n_0$. Logo, a partir de um determinado índice, a sequência $(x_n)_{n\in\mathbb{N}}$ é constante, e portanto, converge para algum elemento de $\mathbb{Q}$.

2.4 CONTINUIDADE

Uma parte que será fundamental para o estudo da dinâmica p–ádica relaciona-se com funções contínuas. Assim, é importante lembrarmos das definições e resultados a seguir.

Definição 2.18. *Sejam $(M, d_1), (N, d_2)$ espaços métricos. Dizemos que a aplicação $f : M \to N$ é **contínua no ponto** $a \in M$ quando, para todo $\varepsilon > 0$, existe $\delta > 0$ tal que $d_1(x, a) < \delta$ implica $d_2(f(x), f(a)) \leq \varepsilon$.*

Definição 2.19. *Sejam M, N espaços métricos. Dizemos que a aplicação $f : M \to N$ é **contínua** quando f for contínua em todos os pontos $a \in M$.*

Definição 2.20. *Sejam M, N espaços métricos. Um **homeomorfismo** de M sobre N é uma bijeção contínua $f : M \to N$ cuja inversa $f^{-1} : N \to M$ também é contínua.*

3 O VALOR ABSOLUTO P–ÁDICO

Para dar início ao objeto de estudo desse trabalho, apresentaremos o valor absoluto p–ádico.

Definição 3.1. *Fixemos um número primo p. Se $x \in \mathbb{Q}, x \neq 0$, existe um único $n \in \mathbb{Z}$ tal que $x = p^n \cdot \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$, onde* $\text{mdc}(a,p) = \text{mdc}(b,p) = 1$. *Definamos a* ***função*** $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ *por*

$$|x|_p = \begin{cases} p^{-n}, & \text{se } x \neq 0, \\ 0, & \text{se } x = 0. \end{cases}$$

Provaremos que a função $|\cdot|_p$ definida acima é um valor absoluto ultramétrico em $\mathbb{Q}$.

Proposição 3.1. *Para quaisquer $x, y \in \mathbb{Q}$, tem-se*

1. $|x|_p \geq 0$;
2. $|x|_p = 0$ *se, e somente se,* $x = 0$;
3. $|x \cdot y|_p = |x|_p \cdot |y|_p$;
4. $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

Demonstração: Para $x, y \neq 0$, consideremos $x = p^n \cdot \frac{a}{b}$ e $y = p^m \cdot \frac{a'}{b'}$, onde $a, b, a', b', n, m \in \mathbb{Z}$, $b, b' \neq 0$ e $\text{mdc}(a,p) = \text{mdc}(b,p) = \text{mdc}(a',p) = \text{mdc}(b',p) = 1$. Então,

1. Se $x = 0$, por definição, $|x|_p = 0$. Ademais, se $x \neq 0$, temos $|x|_p = p^{-n} = \frac{1}{p^n} \geq 0$. Logo, $|x|_p \geq 0$, para todo $x \in \mathbb{Q}$;

2. $\Rightarrow$) Suponhamos $x \neq 0$, então $|x|_p = p^{-n} \neq 0$;

   $\Leftarrow$) Por definição, se $x = 0$, temos $|x|_p = 0$;

3. No caso em que $x = 0$ ou $y = 0$, segue de imediato.

   Suponhamos $x, y \neq 0$. Assim, $|x|_p = p^{-n}$ e $|y|_p = p^{-m}$, e portanto, $|x|_p \cdot |y|_p = p^{-(n+m)}$. Por outro lado,

   $$x \cdot y = p^n \cdot \frac{a}{b} \cdot p^m \cdot \frac{a'}{b'} = p^{n+m} \cdot \frac{a \cdot a'}{b \cdot b'},$$

   e, pela Proposição 2.3, $\text{mdc}(a \cdot a', p) = \text{mdc}(b \cdot b', p) = 1$. Deste modo, $|x \cdot y|_p = p^{-(n+m)} = |x|_p \cdot |y|_p$.

4. Sejam $x, y \in \mathbb{Q}$. Temos os seguintes casos:

   a) $x = 0$ e $y \neq 0$
   Neste caso, $|x|_p = 0$ e $|y|_p = p^{-m}$. Daí,

   $$|x + y|_p = |y|_p = p^{-m} = \max\{0, p^{-m}\} = \max\{|x|_p, |y|_p\};$$

   b) $x \neq 0$ e $y = 0$
   A prova é análoga ao caso acima;

   c) $x = y = 0$
   De fato,

   $$|x + y|_p = |0|_p = 0 = \max\{0, 0\} = \max\{|x|_p, |y|_p\};$$

   d) $x, y \neq 0$
   Neste caso, $|x|_p = p^{-n}$ e $|y|_p = p^{-m}$. Sem perda de generalidade, consideremos $n \geq m$. Deste modo, $\max\{|x|_p, |y|_p\} = |y|_p = p^{-m}$.
   Em contrapartida,

   $$x + y = p^n \cdot \frac{a}{b} + p^m \cdot \frac{a'}{b'} = p^m \cdot \frac{\left(p^{n-m} \cdot a \cdot b' + a' \cdot b\right)}{b \cdot b'} = p^m \cdot \frac{\alpha}{b \cdot b'},$$

   onde $\alpha = \left(p^{n-m} \cdot a \cdot b' + a' \cdot b\right) \in \mathbb{Z}$ e $\text{mdc}(b \cdot b', p) = 1$. Pelo Teorema Fundamental da Aritmética, existem c, β inteiros tais que $\alpha = p^\beta \cdot c$, onde $\text{mdc}(c, p) = 1$ e $\beta \geq 0$. Assim,

   $$x + y = p^m \cdot \frac{\alpha}{b \cdot b'} = p^m \cdot \frac{p^\beta \cdot c}{b \cdot b'} = p^{(m+\beta)} \cdot \frac{c}{b \cdot b'},$$

   onde $\text{mdc}(c, p) = \text{mdc}(b \cdot b', p) = 1$. Portanto,

   $$|x + y|_p = p^{-(m+\beta)} = p^{-m} \cdot p^{-\beta} \leq p^{-m} = \max\{|x|_p, |y|_p\}.$$

■

Portanto, a função $|\cdot|_p$ é um valor absoluto ultramétrico em $\mathbb{Q}$ conhecido por **valor absoluto p-ádico dos números racionais**.

Note que, pela definição de $|\cdot|_p$, quanto maior a potência de p presente na decomposição em fatores primos de um número racional, menor será seu valor absoluto p-ádico. Além disso, dado um número racional não nulo x, pelo Teorema Fundamental da Aritmética, existem únicos primos distintos $p_1, \cdots, p_n$ e correspondentes inteiros não nulos $a_1, \cdots, a_n$, de modo que $x = \mu \cdot p_1^{a_1} \cdot \cdots \cdot p_n^{a_n}$, onde $\mu \in \{-1, 1\}$. Daí, $|x|_{p_i} = p_i^{-a_i}$, para cada $i = 1, \cdots, n$. Por outro lado, $|x|_p = 1$, para todo $p \notin \{p_1, \cdots, p_n\}$.

Exemplo 3.1. *Consideremos* $\frac{650}{189} = 2^1 \cdot 3^{-3} \cdot 5^2 \cdot 7^{-1} \cdot 13$. *Então,*

$$\left|\frac{650}{189}\right|_p = \begin{cases} \frac{1}{2} & , \quad se\ p = 2, \\ 27 & , \quad se\ p = 3, \\ \frac{1}{25} & , \quad se\ p = 5, \\ 7 & , \quad se\ p = 7, \\ \frac{1}{13} & , \quad se\ p = 13, \\ 1 & , \quad se\ p = 11\ \ ou\ p \geq 17. \end{cases}$$

Antes de prosseguirmos na construção de $\mathbb{Q}_p$, vejamos algumas propriedades do valor absoluto p-ádico, que nos darão uma melhor compreensão do mesmo.

Um primeiro fato curioso é que, no estudo do valor absoluto real, nota-se uma ligação direta entre este e a ordenação dos números racionais na reta. Entretanto, com o valor absoluto p-ádico, os números racionais se reorganizam no plano, diferente do usual.

Para exemplificar, consideremos o valor absoluto 2-ádico. Temos que $7 = 2^0 \cdot 7$ e $8 = 2^3$, logo, $|7|_2 = 2^{-0} = 1$ e $|8|_2 = 2^{-3} = \frac{1}{8}$, ou seja, a distância do 7 até a origem é maior do que a distância do 8 até a origem.

Na figura a seguir, levando em consideração a distância 2-ádica de alguns números racionais até a origem, apresentamos como os mesmos se distribuem no plano.

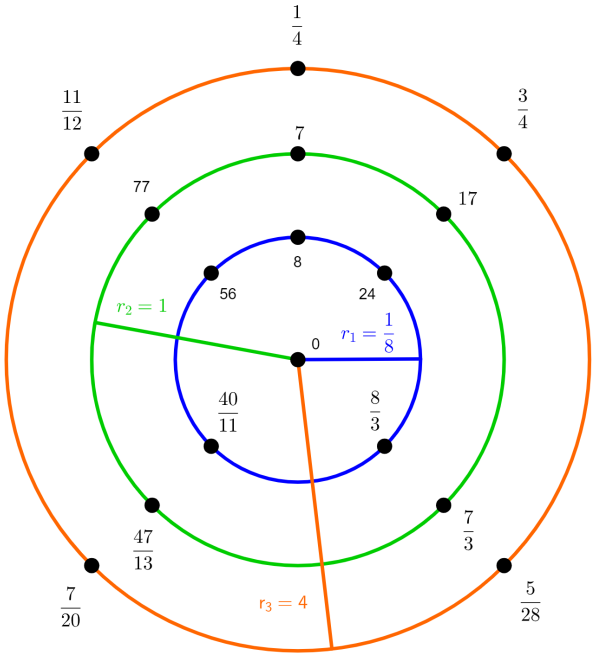

Figura 1 – Distribuição de alguns números racionais no plano segundo a métrica 2-ádica.

Proposição 3.2. *Se* $x, y \in \mathbb{Q}$ *e* $|x|_p < |y|_p$, *então* $|x + y|_p = \max\{|x|_p, |y|_p\}$.

Demonstração: De fato, pela propriedade do valor absoluto ultramétrico e pela hipótese, segue que

$$|x+y|_p \leq \max\{|x|_p, |y|_p\} = |y|_p. \tag{3.1}$$

Por outro lado, $|y|_p = |(y+x)+(-x)|_p \leq \max\{|y+x|_p, |-x|_p\} = \max\{|x+y|_p, |x|_p\}$. Como $|x|_p < |y|_p$ então, $\max\{|x+y|_p, |x|_p\} = |x+y|_p$. Assim,

$$|y|_p \leq |x+y|_p. \tag{3.2}$$

Deste modo, pelas equações (3.1) e (3.2), concluímos que $|y|_p = |x+y|_p$. ■

A proposição acima, chamada em algumas referências de Princípio do Triângulo Isósceles, nos diz que, segundo a norma p–ádica todo triângulo é isósceles.

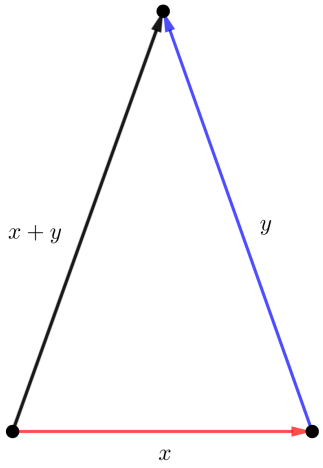

Figura 2 – Interpretação da Proposição 3.2

Proposição 3.3. *Para quaisquer $x, y \in \mathbb{Q}$, temos $||x|_p - |y|_p|_\infty \leq |x-y|_p$, onde $|\cdot|_\infty$ representa o valor absoluto real.*

Demonstração: Com efeito,

$$|x|_p = |(x-y)+y|_p \leq \max\{|x-y|_p, |y|_p\} \leq |x-y|_p + |y|_p$$

$$\Rightarrow |x|_p - |y|_p \leq |x-y|_p. \tag{3.3}$$

De modo análogo,

$$|y|_p - |x|_p \leq |y-x|_p = |x-y|_p$$

$$\Rightarrow |y|_p - |x|_p \leq |x-y|_p$$

$$\Rightarrow -(|x|_p - |y|_p) \leq |x-y|_p. \tag{3.4}$$

Visto que $|z|_\infty = \max\{-z, z\}$, para todo $z \in \mathbb{Q}$,

$$||x|_p - |y|_p|_\infty = \max\{-(|x|_p - |y|_p), |x|_p - |y|_p\}.$$

Logo, pelas expressões (3.3) e (3.4), concluímos que

$$||x|_p - |y|_p|_\infty = \max\{-(|x|_p - |y|_p), |x|_p - |y|_p\} \leq |x-y|_p.$$

■

A proposição anterior nos diz que a diferença radial de dois elementos sempre será menor ou igual a distância, proveniente do valor absoluto p-ádico, entre eles. Repare que, na figura a seguir, a marcação em vermelho, referente ao $|x-y|_p = |-y|_p = |y|_p$, é maior que $||x|_p - |y|_p|_\infty$, marcado em laranja.

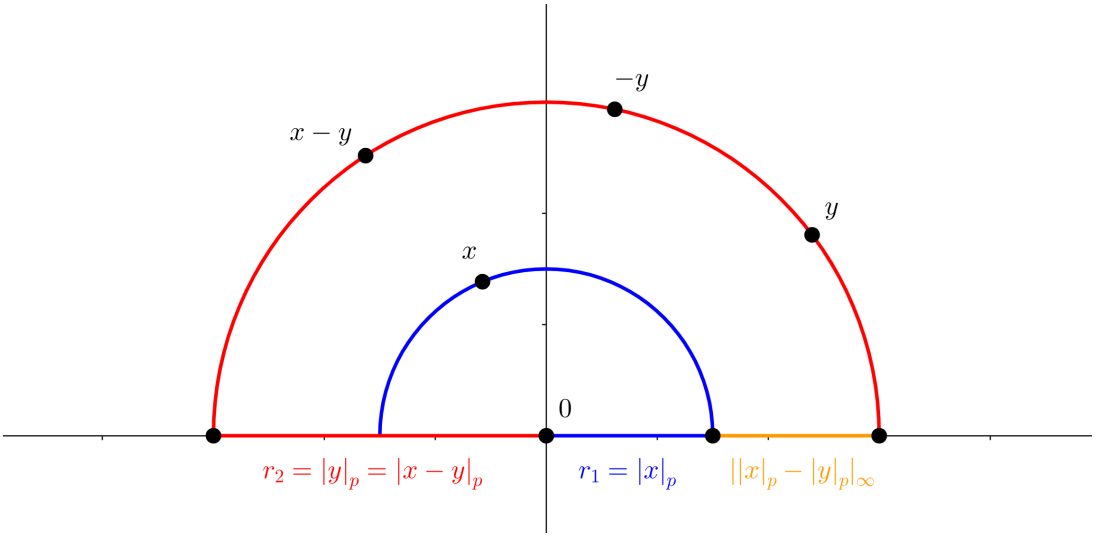

Figura 3 – Interpretação da Proposição 3.3

Proposição 3.4. *Seja* $(q_n)_{n\in\mathbb{N}} \in \mathbb{Q}$. *Então,* $\lim_{n\to\infty} |q_n|_p = 0$ *se, e somente se,* $(q_n)_{n\in\mathbb{N}} \overbrace{\longrightarrow}^{|\cdot|_p} 0$, *quando* $n \to \infty$.

Demonstração:

$\Rightarrow$) Seja $\varepsilon > 0$. Por hipótese, existe $n_0 \in \mathbb{N}$ tal que $||q_n|_p - 0|_\infty \leq \varepsilon$, sempre que $n \geq n_0$. Daí, $|q_n|_p \leq \varepsilon$, sempre que $n \geq n_0$. Logo, $\lim_{n\to\infty} q_n = 0$, na norma $|\cdot|_p$.

$\Leftarrow$) Seja $\varepsilon > 0$. Então, existe $n_0 \in \mathbb{N}$ tal que $|q_n - 0|_p \leq \varepsilon$, sempre que $n \geq n_0$. Daí, $||q_n|_p - 0|_\infty = |q_n - 0|_p \leq \varepsilon$, sempre que $n \geq n_0$. Logo, $\lim_{n\to\infty} |q_n|_p = 0$. ■

4 A CONSTRUÇÃO DE $\mathbb{Q}_p$

No que segue, fixado $p \in \mathbb{N}$ primo, direcionaremos nosso estudo para a completude de $\mathbb{Q}$ munido da distância proveniente do valor absoluto p-ádico, definida conforme consta na proposição abaixo.

Proposição 4.1. *A função $d : \mathbb{Q}\times\mathbb{Q} \to \mathbb{R}$, definida por $d(x, y) = |x-y|_p$ é uma ultramétrica em $\mathbb{Q}$.*

Demonstração: Segue diretamente do Corolário 2.2 ■

Seja A o conjunto de todas as sequências de Cauchy em $(\mathbb{Q}, |\cdot|_p)$. Dadas as sequências $(q_n)_{n\in\mathbb{N}}, (q'_n)_{n\in\mathbb{N}} \in A$, consideremos as seguintes operações em A:

1. $(q_n)_{n\in\mathbb{N}} + (q'_n)_{n\in\mathbb{N}} = (q_n + q'_n)_{n\in\mathbb{N}}$;
2. $(q_n)_{n\in\mathbb{N}} \cdot (q'_n)_{n\in\mathbb{N}} = (q_n \cdot q'_n)_{n\in\mathbb{N}}$.

Proposição 4.2. *O conjunto A munido das operações definidas acima é um anel comutativo com unidade.*

Demonstração: Sejam $(q_n)_{n\in\mathbb{N}}, (q'_n)_{n\in\mathbb{N}}, (t_n)_{n\in\mathbb{N}} \in A$.

1. As operações definidas em A são fechadas.
   De fato, seja $\varepsilon > 0$.

   a) Por hipótese, existem $n_1, n_2 \in \mathbb{N}$ tais que

   $$|q_m - q_n|_p \leq \varepsilon, \text{ para quaisquer } m, n \geq n_1$$

   e

   $$|q'_m - q'_n|_p \leq \varepsilon \text{ para quaisquer } m, n \geq n_2.$$

   Tomemos $n_0 = \max\{n_1, n_2\}$. Então,

   $$|(q_m + q'_m) - (q_n + q'_n)|_p = |(q_m - q_n) + (q'_m - q'_n)|_p \leq \max\{|q_m - q_n|_p, |q'_m - q'_n|_p\} \leq \varepsilon,$$

   para quaisquer $m, n \geq n_0$. Logo, $(q_n + q'_n)_{n\in\mathbb{N}} \in A$.

   b) Pela Proposição 2.9, $(q_n)_{n\in\mathbb{N}}$ e $(q'_n)_{n\in\mathbb{N}}$ são limitadas. Assim, existe $M > 0$ tal que $|q_n|_p \leq M$ e $|q'_n|_p \leq M$, para todo $n \in \mathbb{N}$. Como estas sequências são de Cauchy, existem $n_1, n_2 \in \mathbb{N}$ tais que

   $$|q_m - q_n|_p \leq \frac{\varepsilon}{M}, \text{ para quaisquer } m, n \geq n_1$$

e

$$|q'_m - q'_n|_p \leq \frac{\varepsilon}{M}, \text{ para quaisquer } m, n \geq n_2.$$

Tomemos $n_0 = \max\{n_1, n_2\}$.

Então, para todo $m, n \geq n_0$,

$$|q_m \cdot q'_m - q_n \cdot q'_n|_p = |q_m \cdot q'_m - q_n \cdot q'_m + q_n \cdot q'_m - q_n \cdot q'_n|_p$$

$$= |q'_m \cdot (q_m - q_n) + q_n \cdot (q'_m - q'_n)|_p \leq \max\{|q'_m \cdot (q_m - q_n)|_p, |q_n \cdot (q'_m - q'_n)|_p\}$$

$$= \max\{|q'_m|_p \cdot |q_m - q_n|_p, |q_n|_p \cdot |q'_m - q'_n|_p\} \leq M \cdot \frac{\varepsilon}{M} = \varepsilon.$$

Logo, $(q_n \cdot q'_n)_{n\in\mathbb{N}} \in A$.

2. Associatividade da adição
   Segue que

$$((q_n)_{n\in\mathbb{N}} + (q'_n)_{n\in\mathbb{N}}) + (t_n)_{n\in\mathbb{N}} = (q_n + q'_n)_{n\in\mathbb{N}} + (t_n)_{n\in\mathbb{N}} = ((q_n + q'_n) + (t_n))_{n\in\mathbb{N}}$$

$$= ((q_n) + (q'_n + t_n))_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}} + (q'_n + t_n)_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}} + ((q'_n)_{n\in\mathbb{N}} + (t_n)_{n\in\mathbb{N}}).$$

3. Comutatividade da adição
   Temos

$$(q_n)_{n\in\mathbb{N}} + (q'_n)_{n\in\mathbb{N}} = (q_n + q'_n)_{n\in\mathbb{N}} = (q'_n + q_n)_{n\in\mathbb{N}} = (q'_n)_{n\in\mathbb{N}} + (q_n)_{n\in\mathbb{N}}.$$

4. Existência de elemento neutro da adição
   Tomemos $e_n = 0$, para todo $n \in \mathbb{N}$. Então,

$$(q_n)_{n\in\mathbb{N}} + (e_n)_{n\in\mathbb{N}} = (q_n + e_n)_{n\in\mathbb{N}} = (q_n + 0)_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}}.$$

5. Existência do elemento simétrico
   Para cada $(q_n)_{n\in\mathbb{N}} \in A$, tomemos $x_n = -q_n$, para todo $n \in \mathbb{N}$. Então,

$$(q_n)_{n\in\mathbb{N}} + (x_n)_{n\in\mathbb{N}} = (q_n + x_n)_{n\in\mathbb{N}} = (q_n + (-q_n))_{n\in\mathbb{N}} = (0)_{n\in\mathbb{N}} = (e_n)_{n\in\mathbb{N}}.$$

6. Associatividade da multiplicação
   Segue que

$$((q_n)_{n\in\mathbb{N}} \cdot (q'_n)_{n\in\mathbb{N}}) \cdot (t_n)_{n\in\mathbb{N}} = (q_n \cdot q'_n)_{n\in\mathbb{N}} \cdot (t_n)_{n\in\mathbb{N}} = ((q_n \cdot q'_n) \cdot (t_n))_{n\in\mathbb{N}}$$

$$= ((q_n) \cdot (q'_n \cdot t_n))_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}} \cdot (q'_n \cdot t_n)_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}} \cdot ((q'_n)_{n\in\mathbb{N}} \cdot (t_n)_{n\in\mathbb{N}}).$$

7. Comutatividade da multiplicação
   Temos

$$(q_n)_{n\in\mathbb{N}} \cdot (q'_n)_{n\in\mathbb{N}} = (q_n \cdot q'_n)_{n\in\mathbb{N}} = (q'_n \cdot q_n)_{n\in\mathbb{N}} = (q'_n)_{n\in\mathbb{N}} \cdot (q_n)_{n\in\mathbb{N}}.$$

8. Existência do elemento neutro multiplicativo (unidade do anel)
   Tomemos $u_n = 1$, para todo $n \in \mathbb{N}$. Então,

$$(q_n)_{n\in\mathbb{N}} \cdot (u_n)_{n\in\mathbb{N}} = (q_n \cdot u_n)_{n\in\mathbb{N}} = (q_n \cdot 1)_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}}.$$

9. Distributividade à esquerda e à direita
   De fato,

$$(q_n)_{n\in\mathbb{N}} \cdot ((q'_n)_{n\in\mathbb{N}} + (t_n)_{n\in\mathbb{N}}) = (q_n)_{n\in\mathbb{N}} \cdot (q'_n + t_n)_{n\in\mathbb{N}} = ((q_n) \cdot (q'_n + t_n))_{n\in\mathbb{N}}$$

$$= (q_n \cdot q'_n + q_n \cdot t_n)_{n\in\mathbb{N}} = (q_n \cdot q'_n)_{n\in\mathbb{N}} + (q_n \cdot t_n)_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}} \cdot (q'_n)_{n\in\mathbb{N}} + (q_n)_{n\in\mathbb{N}} \cdot (t_n)_{n\in\mathbb{N}}.$$

   Além disso,

$$((q_n)_{n\in\mathbb{N}} + (q'_n)_{n\in\mathbb{N}}) \cdot (t_n)_{n\in\mathbb{N}} = (t_n)_{n\in\mathbb{N}} \cdot ((q_n)_{n\in\mathbb{N}} + (q'_n)_{n\in\mathbb{N}})$$

$$= (t_n)_{n\in\mathbb{N}} \cdot (q_n)_{n\in\mathbb{N}} + (t_n)_{n\in\mathbb{N}} \cdot (q'_n)_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}} \cdot (t_n)_{n\in\mathbb{N}} + (q'_n)_{n\in\mathbb{N}} \cdot (t_n)_{n\in\mathbb{N}}.$$

Pelos itens 1,2,3,4,5,6 e 9 concluímos que A é um anel. Ademais, os itens 7 e 8, nos garantem a comutatividade e a unidade de A, respectivamente.

■

Chamaremos de diferença em A e denotaremos por $-$, a seguinte operação:

$$\begin{array}{rccc} - : & A \times A & \longrightarrow & A \\ & ((q_n)_{n\in\mathbb{N}}, (q'_n)_{n\in\mathbb{N}}) & \mapsto & (q_n)_{n\in\mathbb{N}} - (q'_n)_{n\in\mathbb{N}} = (q_n)_{n\in\mathbb{N}} + (-q'_n)_{n\in\mathbb{N}} \end{array}$$

Proposição 4.3. *Se $(q_n)_{n\in\mathbb{N}} \in A$, então $(|q_n|_p)_{n\in\mathbb{N}}$ é uma sequência de Cauchy em $\mathbb{R}$. Em particular, $(|q_n|_p)_{n\in\mathbb{N}}$ é convergente em $\mathbb{R}$.*

Demonstração: Sejam $(q_n)_{n\in\mathbb{N}} \in A$ e $\varepsilon > 0$. Então, existe $n_0 \in \mathbb{N}$ tal que, para quaisquer $m, n \in \mathbb{N}$ com $m, n \geq n_0$, temos $|q_m - q_n|_p \leq \varepsilon$. Pela Proposição 3.3,

$$||q_m|_p - |q_n|_p|_\infty \leq |q_m - q_n|_p \leq \varepsilon$$

$$\Rightarrow ||q_m|_p - |q_n|_p|_\infty \leq \varepsilon,$$

para todo $m, n \geq n_0$. Portanto, $(|q_n|_p)_{n\in\mathbb{N}}$ é uma sequência de Cauchy em $\mathbb{R}$. ■

A seguir, consideremos I o conjunto das sequências de A que convergem para 0, isto é,

$$I = \left\{(q_n)_{n\in\mathbb{N}} \in A; \lim_{n\to\infty} q_n = 0 \text{ na norma } |\cdot|_p\right\}.$$

Proposição 4.4. *I é um ideal maximal de A.*

Demonstração: A prova segue nas seguintes etapas:

1. I é um subanel de A.

   a) $0 \in I$: De fato, a sequência constante $e_n = 0, \forall n \in \mathbb{N}$, naturalmente, converge para 0, logo, pertence a I;

   b) I é fechado para a diferença: Sejam $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in I$ e $\varepsilon > 0$. Então, existem $n_1, n_2 \in \mathbb{N}$ tais que

   $$|a_n|_p \leq \varepsilon, \text{ para todo } n \geq n_1$$

   e

   $$|b_n|_p \leq \varepsilon, \text{ para todo } n \geq n_2.$$

   Tomemos $n_0 = \max\{n_1, n_2\}$. Assim,

   $$|a_n - b_n|_p = |a_n + (-b_n)|_p \leq \max\{|a_n|_p, |-(b_n)|_p\} = \max\{|a_n|_p, |b_n|_p\} \leq \varepsilon$$

   $$\Rightarrow |a_n - b_n|_p \leq \varepsilon, \forall n \geq n_0.$$

   Logo, $(a_n)_{n\in\mathbb{N}} - (b_n)_{n\in\mathbb{N}} = (a_n - b_n)_{n\in\mathbb{N}} \in I$;

   c) I é fechado para o produto: Sejam $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in I$ e $\varepsilon > 0$. Então, como $(a_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy, pela Proposição 2.9, existe $M > 0$ tal que

   $$|a_n|_p \leq M, \text{ para todo } n \in \mathbb{N}.$$

   Por outro lado, existe $n_0 \in \mathbb{N}$ tal que

   $$|b_n|_p \leq \frac{\varepsilon}{M}, \text{ para todo } n \geq n_0.$$

   Assim,

   $$|a_n \cdot b_n|_p = |a_n|_p \cdot |b_n|_p \leq M \cdot \frac{\varepsilon}{M} = \varepsilon, \text{ para todo } n \geq n_0.$$

   Portanto, $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (a_n \cdot b_n)_{n\in\mathbb{N}} \in I$.

2. $A \cdot I \subset I$ e $I \cdot A \subset I$.

   Vimos que A é comutativo, logo, basta provar apenas uma das inclusões. Provaremos a primeira delas.

   Sejam $(a_n)_{n\in\mathbb{N}} \in A, (q_n)_{n\in\mathbb{N}} \in I$ e $\varepsilon > 0$. Pela Proposição 2.9, existe $M > 0$ tal que $|a_n|_p \leq M, \forall n \in \mathbb{N}$. Ademais, existe $n_0 \in \mathbb{N}$ tal que $|q_n|_p \leq \frac{\varepsilon}{M}, \forall n \geq n_0$. Deste modo,

   $$|a_n \cdot q_n|_p = |a_n|_p \cdot |q_n|_p \leq M \cdot \frac{\varepsilon}{M} = \varepsilon, \forall n \geq n_0.$$

   Assim, concluímos que $(a_n)_{n\in\mathbb{N}} \cdot (q_n)_{n\in\mathbb{N}} \in I$, e, consequentemente, I é um ideal de A.

3. I é um ideal maximal de A.

   Seja B um ideal de A, $I \subset B \subset A$, $B \neq I$.

   Afirmação: $(1, 1, \ldots, 1, \ldots) \in B$.

   De fato, como $I \subset B$ e $B \neq I$, existe $(q_n)_{n\in\mathbb{N}} \in B - I$. Pela Proposição 4.3, existe $r \in \mathbb{R}$, $r \geq 0$, tal que $\lim_{n\to\infty} |q_n|_p = r$. Como $(q_n)_{n\in\mathbb{N}} \notin I$, obrigatoriamente, $r > 0$. Daí, existe $n_0 \in \mathbb{N}$ tal que $|q_n|_p \geq \frac{r}{2}, \forall n \geq n_0$. Assim, para todo $n \geq n_0$, $|q_n|_p \neq 0$, isto é, $q_n \neq 0$. Consideremos a sequência $(0, \ldots, 0, q_{n_0}^{-1}, q_{n_0+1}^{-1}, q_{n_0+2}^{-1}, \ldots)$, com as $n_0 - 1$ primeiras coordenadas nulas. Notemos que esta sequência é um elemento de A, pois, para quaisquer $m, n \geq n_0$,

   $$|q_m^{-1} - q_n^{-1}|_p = \frac{|q_n - q_m|_p}{|q_m|_p \cdot |q_n|_p} \leq \frac{4 \cdot |q_n - q_m|_p}{r^2}.$$

   Assim, dado $\varepsilon > 0$ arbitrário, como $(q_n)_{n\in\mathbb{N}}$ é de Cauchy em $(\mathbb{Q}, |\cdot|_p)$, existe $n_1 \in \mathbb{N}$ tal que, para quaisquer $m, n \geq n_1$, temos $|q_n - q_m|_p \leq \frac{r^2 \cdot \varepsilon}{4}$. Tomemos $n_2 = \max\{n_0, n_1\}$. Então,

   $$|q_m^{-1} - q_n^{-1}|_p \leq \frac{4 \cdot |q_n - q_m|_p}{r^2} \leq \frac{4}{r^2} \cdot \frac{r^2 \cdot \varepsilon}{4} = \varepsilon, \forall m, n \geq n_2.$$

   Finalmente, visto que $(0, \ldots, 0, q_{n_0}^{-1}, q_{n_0+1}^{-1}, q_{n_0+2}^{-1}, \ldots) \in A$ e usando o fato de que B é um ideal de A, segue que

   $$(q_0, \ldots, q_{n_0-1}, q_{n_0}, q_{n_0+1}, \ldots) \cdot (0, \ldots, 0, q_{n_0}^{-1}, q_{n_0+1}^{-1}, \ldots) = (0, \ldots, 0, 1, 1, \ldots) \in B.$$

   Por outro lado, a sequência com os $n_0 - 1$ primeiros termos iguais a 1 e os demais iguais a 0, $(1, 1, \ldots, 1, 0, 0, \ldots)$, pertence a $I \subset B$. Consequentemente,

   $$(1, \ldots, 1, 1, 1, 1 \ldots) = (1, \ldots, 1, 0, 0, 0, \ldots) + (0, \ldots, 0, 1, 1, 1, \ldots) \in B.$$

   Por fim, como B é um ideal,

   $$(a_0, a_1, a_2, \ldots) = (a_0, a_1, a_2, \ldots) \cdot (1, 1, 1, \ldots) \in B,$$

   para todo $(a_n)_{n\in\mathbb{N}} \in A$. Logo, $A \subset B$, e, portanto, $B = A$.

■

No que segue formalizaremos a construção de $\mathbb{Q}_p$ através da relação de equivalência $\mathcal{R}_\mathcal{I}$ em A, definida em função de I.

Consideremos $\mathcal{R}_\mathcal{I}$ a seguinte relação em A,

$$(q_n)_{n\in\mathbb{N}} \mathcal{R}_\mathcal{I} (q'_n)_{n\in\mathbb{N}} \Leftrightarrow (q_n - q'_n)_{n\in\mathbb{N}} \in I,$$

para todo $(q_n)_{n\in\mathbb{N}}, (q'_n)_{n\in\mathbb{N}} \in A$.

Proposição 4.5. *$\mathcal{R}_{\mathcal{I}}$ é uma relação de equivalência.*

Demonstração: Sejam $(q_n)_{n\in\mathbb{N}}, (q'_n)_{n\in\mathbb{N}}, (t_n)_{n\in\mathbb{N}} \in A$.

1. Reflexividade
   Como $\lim_{n\to\infty}(q_n - q_n)_{n\in\mathbb{N}} = 0$ em $|\cdot|_p$, então, $(q_n - q_n)_{n\in\mathbb{N}} \in I$, logo, $(q_n)_{n\in\mathbb{N}}\mathcal{R}_{\mathcal{I}}(q_n)_{n\in\mathbb{N}}$.

2. Simetria
   Suponhamos que $(q_n)_{n\in\mathbb{N}}\mathcal{R}_{\mathcal{I}}(q'_n)_{n\in\mathbb{N}}$ e seja $\varepsilon > 0$. Então, existe $n_0 \in \mathbb{N}$ tal que

   $$|q_n - q'_n|_p \leq \varepsilon, \text{ para todo } n \geq n_0.$$

   Assim,

   $$|q'_n - q_n|_p = |q_n - q'_n|_p \leq \varepsilon, \text{ para todo } n \geq n_0.$$

   Logo, $(q'_n)_{n\in\mathbb{N}}\mathcal{R}_{\mathcal{I}}(q_n)_{n\in\mathbb{N}}$.

3. Transitividade
   Suponhamos que $(q_n)_{n\in\mathbb{N}}\mathcal{R}_{\mathcal{I}}(q'_n)_{n\in\mathbb{N}}$, $(q'_n)_{n\in\mathbb{N}}\mathcal{R}_{\mathcal{I}}(t_n)_{n\in\mathbb{N}}$ e seja $\varepsilon > 0$. Então, existem $n_1, n_2 \in \mathbb{N}$ tais que

   $$|q_n - q'_n|_p \leq \varepsilon, \text{ para todo } n \geq n_1$$

   e

   $$|q'_n - t_n|_p \leq \varepsilon, \text{ para todo } n \geq n_2.$$

   Tomemos $n_0 = \max\{n_1, n_2\}$. Assim, para todo $n \geq n_0$,

   $$|q_n - t_n|_p = |(q_n - q'_n) + (q'_n - t_n)|_p \leq \max\{|q_n - q'_n|_p, |q'_n - t_n|_p\} \leq \varepsilon.$$

   Logo, $(q_n - t_n)_{n\in\mathbb{N}} \in I$, isto é, $(q_n)_{n\in\mathbb{N}}\mathcal{R}_{\mathcal{I}}(t_n)_{n\in\mathbb{N}}$.

■

Para cada $(q_n)_{n\in\mathbb{N}} \in A$, chamaremos de **classe de equivalência** de $(q_n)_{n\in\mathbb{N}}$ o conjunto

$$\overline{(q_n)}_{n\in\mathbb{N}} = \{(q'_n)_{n\in\mathbb{N}} \in A; (q'_n)_{n\in\mathbb{N}}\mathcal{R}_{\mathcal{I}}(q_n)_{n\in\mathbb{N}}\}.$$

Teorema 4.1. *Sejam $a = (q_n)_{n\in\mathbb{N}}, b = (q'_n)_{n\in\mathbb{N}} \in A$. Então:*

1. *$a \in \overline{a}$;*
2. *$\overline{a} = \overline{b} \Leftrightarrow a\mathcal{R}_{\mathcal{I}}b$;*
3. *$\overline{a} \neq \overline{b} \Leftrightarrow \overline{a} \cap \overline{b} = \varnothing$.*

Demonstração:

1. Como $\mathcal{R}_{\mathcal{I}}$ é uma relação reflexiva então $a\mathcal{R}_{\mathcal{I}}a$. Assim, $a \in \overline{a}$.

2. ($\Rightarrow$) Suponhamos que $\overline{a} = \overline{b}$. Pelo item anterior, $a \in \overline{a} = \overline{b}$, e portanto, $a \in \overline{b}$. Logo, $a\mathcal{R}_{\mathcal{I}}b$.

   ($\Leftarrow$) Suponhamos que $a\mathcal{R}_{\mathcal{I}}b$. Mostraremos que $\overline{a} = \overline{b}$, ou seja, $\overline{a} \subset \overline{b}$ e $\overline{b} \subset \overline{a}$.

   Seja $x \in \overline{a}$. Então, $x\mathcal{R}_{\mathcal{I}}a$. Como $a\mathcal{R}_{\mathcal{I}}b$, pela propriedade transitiva, $x\mathcal{R}_{\mathcal{I}}b$. Logo, $x \in \overline{b}$, e portanto, $\overline{a} \subset \overline{b}$.

   Seja $x \in \overline{b}$. Então, $x\mathcal{R}_{\mathcal{I}}b$, e, pela propriedade simétrica, $b\mathcal{R}_{\mathcal{I}}x$. Como $a\mathcal{R}_{\mathcal{I}}b$, pela transitividade, $a\mathcal{R}_{\mathcal{I}}x$. Assim, $x\mathcal{R}_{\mathcal{I}}a$, e portanto, $x \in \overline{a}$. Logo, $\overline{b} \subset \overline{a}$.

3. ($\Rightarrow$) Suponhamos que $\overline{a} \cap \overline{b} \neq \varnothing$. Então, existe $z \in \overline{a} \cap \overline{b}$. Daí, $z\mathcal{R}_{\mathcal{I}}a$ e $z\mathcal{R}_{\mathcal{I}}b$. Pelo item anterior, $\overline{z} = \overline{a}$ e $\overline{z} = \overline{b}$, donde $\overline{a} = \overline{b}$. Contradição.

   ($\Leftarrow$) Suponhamos que $\overline{a} = \overline{b}$. Então, $a \in \overline{a} = \overline{b}$. Logo, $\overline{a} \cap \overline{b} \neq \varnothing$.

■

Definição 4.1. *Chama-se **partição** de um conjunto não vazio A, todo subconjunto P do conjunto das partes de A que satisfaz as seguintes condições:*

1. *Se $X \in P$, então $X \neq \varnothing$;*
2. *Se $X_i, X_j \in P$, $X_i \neq X_j$, então $X_i \cap X_j = \varnothing$;*
3. $\bigcup_{X \in P} X = A$.

O teorema abaixo é essencial para correlatar o conceito de relação de equivalência com o conceito de partição de um conjunto.

Teorema 4.2. *O conjunto quociente $\frac{A}{\mathcal{R}_{\mathcal{I}}}$, formado pelas classes de equivalência segundo $\mathcal{R}_{\mathcal{I}}$, é uma partição de A.*

Demonstração: É imediato do Teorema 4.1. ■

O conjunto quociente $\frac{A}{\mathcal{R}_{\mathcal{I}}}$ é chamado de **conjunto dos números p-ádicos** e denotado por $\mathbb{Q}_p$. No que segue, consideremos as seguintes operações em $\mathbb{Q}_p$.

$$\begin{array}{rccc} + : & \mathbb{Q}_p \times \mathbb{Q}_p & \longrightarrow & \mathbb{Q}_p \\ & (\overline{(q_n)}_{n\in\mathbb{N}}, \overline{(q'_n)}_{n\in\mathbb{N}}) & \mapsto & \overline{(q_n)}_{n\in\mathbb{N}} + \overline{(q'_n)}_{n\in\mathbb{N}} = \overline{(q_n + q'_n)}_{n\in\mathbb{N}} \end{array}$$

$$\begin{array}{rccc} \cdot : & \mathbb{Q}_p \times \mathbb{Q}_p & \longrightarrow & \mathbb{Q}_p \\ & (\overline{(q_n)}_{n\in\mathbb{N}}, \overline{(q'_n)}_{n\in\mathbb{N}}) & \mapsto & \overline{(q_n)}_{n\in\mathbb{N}} \cdot \overline{(q'_n)}_{n\in\mathbb{N}} = \overline{(q_n \cdot q'_n)}_{n\in\mathbb{N}} \end{array}$$

Proposição 4.6. *As operações acima estão bem definidas.*

Demonstração: Consideremos $\overline{(q_n)}_{n\in\mathbb{N}} = \overline{(t_n)}_{n\in\mathbb{N}}$, $\overline{(q'_n)}_{n\in\mathbb{N}} = \overline{(t'_n)}_{n\in\mathbb{N}} \in \mathbb{Q}_p$. Então,

$$\lim_{n\to\infty} q_n - t_n = 0 \quad \text{e} \quad \lim_{n\to\infty} q'_n - t'_n = 0.$$

Para provar que a operação + está bem definida, devemos aferir que $\overline{(q_n)}_{n\in\mathbb{N}} + \overline{(q'_n)}_{n\in\mathbb{N}} = \overline{(t_n)}_{n\in\mathbb{N}} + \overline{(t'_n)}_{n\in\mathbb{N}}$, isto é, $\overline{(q_n + q'_n)}_{n\in\mathbb{N}} = \overline{(t_n + t'_n)}_{n\in\mathbb{N}}$. De fato,

$$(q_n + q'_n)_{n\in\mathbb{N}} - (t_n + t'_n)_{n\in\mathbb{N}} = (q_n - t_n)_{n\in\mathbb{N}} + (q'_n - t'_n)_{n\in\mathbb{N}}.$$

Assim, $\lim_{n\to\infty}((q_n + q'_n) - (t_n + t'_n)) = 0$, e, portanto, $(q_n + q'_n)_{n\in\mathbb{N}} - (t_n + t'_n)_{n\in\mathbb{N}} \in I$. Logo, $(q_n + q'_n)_{n\in\mathbb{N}} \mathcal{R}_{\mathcal{I}} (t_n + t'_n)_{n\in\mathbb{N}}$ e, pelo Teorema 4.1, $\overline{(q_n + q'_n)}_{n\in\mathbb{N}} = \overline{(t_n + t'_n)}_{n\in\mathbb{N}}$.

Analogamente, para provar que a operação $\cdot$ está bem definida, mostraremos que $(q_n \cdot q'_n)_{n\in\mathbb{N}} \mathcal{R}_{\mathcal{I}} (t_n \cdot t'_n)_{n\in\mathbb{N}}$. Com efeito,

$$\begin{aligned}(q_n \cdot q'_n)_{n\in\mathbb{N}} - (t_n \cdot t'_n)_{n\in\mathbb{N}} &= (q_n \cdot q'_n)_{n\in\mathbb{N}} + (q_n \cdot t'_n)_{n\in\mathbb{N}} - (q_n \cdot t'_n)_{n\in\mathbb{N}} - (t_n \cdot t'_n)_{n\in\mathbb{N}} \\ &= (q_n \cdot (q'_n - t'_n))_{n\in\mathbb{N}} + (t'_n \cdot (q_n - t_n))_{n\in\mathbb{N}}.\end{aligned}$$

Desse modo, $\lim_{n\to\infty}(q_n \cdot q'_n) - (t_n \cdot t'_n) = \lim_{n\to\infty}(q_n \cdot (q'_n - t'_n)) + (t'_n \cdot (q_n - t_n)) = 0$, visto que, pela Proposição 2.9, $(q_n)_{n\in\mathbb{N}}$ e $(t'_n)_{n\in\mathbb{N}}$ são limitadas e $\lim_{n\to\infty} q_n - t_n = \lim_{n\to\infty} q'_n - t'_n = 0$. Portanto, $(q_n \cdot q'_n)_{n\in\mathbb{N}} - (t_n \cdot t'_n)_{n\in\mathbb{N}} \in I$. ∎

Como I é um ideal maximal, pelo Teorema 2.1, $\mathbb{Q}_p$, munido das operações acima, é um corpo. Assim, denotaremos $\mathbb{Q}_p$ como o **corpo dos números p-ádicos**. Além disso, conforme veremos a seguir, $\mathbb{Q}_p$ contém uma cópia de $\mathbb{Q}$.

5 PROPRIEDADES DE $\mathbb{Q}_p$

Com o corpo dos números p–ádicos construído e suas operações bem definidas, este capítulo tem como intuito investigar algumas de suas propriedades. Para reforçar a importância de um bom compreendimento dos elementos e das propriedades de $\mathbb{Q}_p$, recomendamos a leitura do Apêndice , onde é apresentado o Teorema de Ostrowski.

Proposição 5.1. *Seja $\varphi : \mathbb{Q} \to \mathbb{Q}_p$, dada por $\varphi(q) = \overline{q}$, onde $\overline{q}$ denota a classe de equivalência da sequência constante $(q, q, \ldots, q, \ldots)$. Então, φ é um homomorfismo de anéis injetor.*

Demonstração: Sejam $p, q \in \mathbb{Q}$. Assim,

$$\varphi(p+q) = \overline{p+q} = \overline{(p+q)}_{n\in\mathbb{N}} = \overline{(p)}_{n\in\mathbb{N}} + \overline{(q)}_{n\in\mathbb{N}} = \overline{p} + \overline{q} = \varphi(p) + \varphi(q).$$

e

$$\varphi(p\cdot q) = \overline{p\cdot q} = \overline{(p\cdot q)}_{n\in\mathbb{N}} = \overline{(p)}_{n\in\mathbb{N}} \cdot \overline{(q)}_{n\in\mathbb{N}} = \overline{p}\cdot\overline{q} = \varphi(p)\cdot\varphi(q).$$

Ademais,

$$\varphi(p) = \varphi(q) \Rightarrow \overline{p} = \overline{q} \Rightarrow \overline{(p)}_{n\in\mathbb{N}} = \overline{(q)}_{n\in\mathbb{N}} \Rightarrow (p-q)_{n\in\mathbb{N}} \in I \Rightarrow \lim_{n\to\infty} p - q = 0 \Rightarrow p = q.$$

Portanto, φ é um homomorfismo de anéis injetor. ∎

A partir deste momento, denotaremos $\varphi(\mathbb{Q})$ por $\mathbb{Q}$, visto que as operações de $\mathbb{Q}$ são preservadas pelo homomorfismo. Além disso, cada número racional q será representado em $\mathbb{Q}_p$ pela classe $\overline{(q)}_{n\in\mathbb{N}}$.

No que segue, mostraremos que dado um elemento de $\mathbb{Q}_p$, independente do representante da classe que o determina, as sequências que o representa convergirão para o mesmo disco p-ádico.

Proposição 5.2. *Se $(q_n)_{n\in\mathbb{N}}, (q'_n)_{n\in\mathbb{N}} \in A$ e $\overline{(q_n)}_{n\in\mathbb{N}} = \overline{(q'_n)}_{n\in\mathbb{N}}$, então $\lim_{n\to\infty} |q_n|_p = \lim_{n\to\infty} |q'_n|_p$.*

Demonstração: Pela Proposição 4.3, sabemos que $(|q_n|_p)_{n\in\mathbb{N}}$ e $(|q'_n|_p)_{n\in\mathbb{N}}$ convergem em $\mathbb{R}$. Ademais, como $\overline{(q_n)}_{n\in\mathbb{N}} = \overline{(q'_n)}_{n\in\mathbb{N}}$, segue que $\lim_{n\to\infty} |q_n - q'_n|_p = 0$. Logo, para todo $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que

$$|q_n - q'_n|_p \leq \varepsilon, \text{ para todo } n \geq n_0.$$

Pela Proposição 3.3,

$$||q_n|_p - |q'_n|_p|_\infty \leq |q_n - q'_n|_p \leq \varepsilon, \text{ para todo } n \geq n_0.$$

Daí, $\lim_{n\to\infty} (|q_n|_p - |q'_n|_p) = 0$, ou seja, $\lim_{n\to\infty} |q_n|_p = \lim_{n\to\infty} |q'_n|_p$. ∎

Nosso próximo passo é estender o valor absoluto p-ádico definido em $\mathbb{Q}$ ao corpo dos números p-ádicos, $\mathbb{Q}_p$. Assim, para cada $x \in \mathbb{Q}_p$, definimos

$$|x|_p = \lim_{n\to\infty} |q_n|_p,$$

onde $(q_n)_{n\in\mathbb{N}} \in A$ e $\overline{(q_n)}_{n\in\mathbb{N}} = x$.

Proposição 5.3. *A aplicação*

$$x \in \mathbb{Q}_p \mapsto |x|_p \in \mathbb{R}$$

está bem definida.

Demonstração: De fato, sejam $\overline{(q_n)}_{n\in\mathbb{N}}, \overline{(q'_n)}_{n\in\mathbb{N}} \in \mathbb{Q}_p$, tais que $\overline{(q_n)}_{n\in\mathbb{N}} = \overline{(q'_n)}_{n\in\mathbb{N}}$. Pela Proposição 5.2,

$$\lim_{n\to\infty} |q_n|_p = \lim_{n\to\infty} |q'_p|,$$

logo, o valor absoluto p-ádico está bem definido em $\mathbb{Q}_p$. ■

Proposição 5.4. *A aplicação $\varphi : \mathbb{Q} \to \mathbb{Q}_p$, dada por $\varphi(q) = \overline{q}$, satisfaz $|\varphi(q)|_p = |q|_p$, para todo $q \in \mathbb{Q}$.*

Demonstração: De fato,

$$|\varphi(q)|_p = |\overline{q}|_p = \lim_{n\to\infty} |q_n|_p = |q|_p,$$

onde $q_n = q$, para todo $n \in \mathbb{N}$. ■

Proposição 5.5. *Para quaisquer $x, y \in \mathbb{Q}_p$, a aplicação*

$$x \in \mathbb{Q}_p \mapsto |x|_p \in \mathbb{R}$$

satisfaz as condições a seguir:

1. $|x|_p \geq 0$;
2. $|x|_p = 0$ *se, e somente se,* $x = 0$;
3. $|x \cdot y|_p = |x|_p \cdot |y|_p$;
4. $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

Demonstração: Sejam $x, y \in \mathbb{Q}_p, x = \overline{(q_n)}_{n\in\mathbb{N}}, y = \overline{(q'_n)}_{n\in\mathbb{N}}$, onde $(q_n)_{n\in\mathbb{N}}, (q'_n)_{n\in\mathbb{N}} \in A$.

1. Como $|x|_p = \lim_{n\to\infty} |q_n|_p$ e $|q_n|_p \geq 0$, para todo $n \in \mathbb{N}$, segue que $|x|_p \geq 0$.

2. Note que,

$$|x|_p = 0 \Leftrightarrow \lim_{n\to\infty} |q_n|_p = 0 \Leftrightarrow \lim_{n\to\infty} q_n = 0 \text{ na métrica } |\cdot|_p \Leftrightarrow \overline{(q_n)}_{n\in\mathbb{N}} = \overline{0} \Leftrightarrow x = \overline{0}.$$

3. Sob as hipóteses dadas, $x \cdot y = \overline{(q_n \cdot q'_n)}_{n\in\mathbb{N}}$. Assim,

$$|x \cdot y|_p = \lim_{n\to\infty} |q_n \cdot q'_n|_p = \lim_{n\to\infty} |q_n|_p \cdot |q'_n|_p = \left(\lim_{n\to\infty} |q_n|_p\right) \cdot \left(\lim_{n\to\infty} |q'_n|_p\right) = |x|_p \cdot |y|_p.$$

4. Como $x + y = \overline{(q_n + q'_n)}_{n\in\mathbb{N}}$, temos

$$\begin{aligned} |x + y|_p = \lim_{n\to\infty} |q_n + q'_n|_p &\leq \left(\lim_{n\to\infty} \max\{|q_n|_p, |q'_n|_p\}\right) \\ &= \max\left\{\lim_{n\to\infty} |q_n|_p, \lim_{n\to\infty} |q'_n|_p\right\} \\ &= \max\{|x|_p, |y|_p\}. \end{aligned}$$

■

Deste modo, a partir da proposição acima, dizemos que a aplicação

$$x \in \mathbb{Q}_p \mapsto |x|_p \in \mathbb{R}^+$$

é o **valor absoluto p-ádico em $\mathbb{Q}_p$.**

Uma importante propriedade que se mantém, é o Princípio do Triângulo Isósceles.

Proposição 5.6. *Se $x, y \in \mathbb{Q}_p$ e $|x|_p < |y|_p$, então $|x + y|_p = \max\{|x|_p, |y|_p\}$.*

Demonstração: De fato, segue que

$$|x + y|_p \leq \max\{|x|_p, |y|_p\} = |y|_p. \tag{5.1}$$

Por outro lado, $|y|_p = |(y + x) + (-x)|_p \leq \max\{|y + x|_p, |-x|_p\} = \max\{|x + y|_p, |x|_p\}$. Por hipótese, $|x|_p < |y|_p$, e consequentemente, $\max\{|x + y|_p, |x|_p\} = |x + y|_p$. Assim,

$$|y|_p \leq |x + y|_p. \tag{5.2}$$

Deste modo, pelas equações (5.1) e (5.2), concluímos que $|y|_p = |x + y|_p$, como queríamos demonstrar. ■

Mostraremos no teorema a seguir que $(\mathbb{Q}_p, |\cdot|_p)$ é completo e $\mathbb{Q}$ é denso em $(\mathbb{Q}_p, |\cdot|_p)$.

Teorema 5.1. *As seguintes afirmações são válidas.*

1. *$\mathbb{Q}$ é denso em $(\mathbb{Q}_p, |\cdot|_p)$;*
2. *$(\mathbb{Q}_p, |\cdot|_p)$ é completo.*

Demonstração:

1. Sejam $x = \overline{(q_n)}_{n\in\mathbb{N}} \in \mathbb{Q}_p$ e $\varepsilon > 0$. Como $(q_n)_{n\in\mathbb{N}} \in A$, existe $n_0 \in \mathbb{N}$ tal que $|q_m - q_n|_p \leq \varepsilon$, para quaisquer $m, n \geq n_0$. Assim,

$$\lim_{n\to\infty} |q_n - q_{n_0}|_p \leq \varepsilon \Rightarrow |x - q_{n_0}|_p \leq \varepsilon.$$

   Portanto, $q_{n_0} = \overline{(q_{n_0})} \in \mathbb{Q} \cap B_\varepsilon(x)$.

2. Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy em $(\mathbb{Q}_p, |\cdot|_p)$. Pelo item anterior, garantimos que, para cada $n \in \mathbb{N}$, existe $q_n \in \mathbb{Q}$ tal que $|x_n - q_n|_p \leq \dfrac{1}{n+1}$. Separaremos a prova deste item em duas etapas.

   a) $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.
   De fato, seja $\varepsilon > 0$. Então, para quaisquer $m, n \in \mathbb{N}$, temos

$$\begin{aligned} |q_m - q_n|_p &= |q_m - x_m + x_m - x_n + x_n - q_n|_p \\ &\leq \max\{|q_m - x_m|_p, |x_m - x_n|_p, |x_n - q_n|_p\} \\ &\leq \max\left\{\frac{1}{m+1}, |x_m - x_n|_p, \frac{1}{n+1}\right\}. \end{aligned}$$

   Por outro lado, existe $n_1 \in \mathbb{N}$ tal que, se $n \geq n_1$, então $\dfrac{1}{n+1} \leq \varepsilon$. Além disso, existe n_2 natural de modo que $|x_m - x_n|_p \leq \varepsilon$ sempre que $m, n \geq n_2$. Assim, para $m, n \geq \max\{n_1, n_2\}$, temos $|q_m - q_n|_p \leq \varepsilon$. Portanto, $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.

   b) $(x_n)_{n\in\mathbb{N}}$ converge para $x = \overline{(q_n)}_{n\in\mathbb{N}} \in \mathbb{Q}_p$.
   Seja $\varepsilon > 0$. Por um lado, existe n_1 natural tal que, se $n \geq n_1$, então $\dfrac{1}{n+1} \leq \varepsilon$. Por outro lado, para cada $n \in \mathbb{N}$, temos

$$|q_n - x|_p = \lim_{m\to\infty} |q_n - q_m|_p,$$

   pois $q_n - x = \overline{(q_n - q_m)}_{m\in\mathbb{N}}$. Assim, como $\lim\limits_{m,n\to\infty} |q_n - q_m|_p = 0$, existe n_2 natural tal que, se $n \geq n_2$, então $|q_n - x|_p \leq \varepsilon$.
   Entretanto,

$$|x_n - x|_p = |x_n - q_n + q_n - x|_p \leq \max\{|x_n - q_n|_p, |q_n - x|_p\} \leq \max\left\{\frac{1}{n+1}, |q_n - x|_p\right\} \leq \varepsilon$$

   para todo $n \geq \max\{n_1, n_2\}$. Logo, a sequência de Cauchy $(x_n)_{n\in\mathbb{N}}$ converge para x em $(\mathbb{Q}_p, |\cdot|_p)$.

■

A partir do teorema anterior constataremos alguns resultados interessantes a respeito de $\mathbb{Q}_p$.

Corolário 5.1. *As imagens de $\mathbb{Q}$ e $\mathbb{Q}_p$ pelo valor absoluto p-ádico $|\cdot|_p$ coincidem, ou seja,*

$$\{|q|_p; q \in \mathbb{Q}\} = \{|x|_p; x \in \mathbb{Q}_p\}.$$

Demonstração: Seja $x \in \mathbb{Q}_p, x \neq 0$. Vamos mostrar que existe $q \in \mathbb{Q}$ de modo que $|x|_p = |q|_p$. Realmente, pelo primeiro item do Teorema 5.1, existe $q \in \mathbb{Q}$ tal que $|q - x|_p = |x - q|_p < |x|_p$. Por fim, pela Proposição 5.6,

$$|(q - x) + x|_p = |x|_p \Rightarrow |q|_p = |x|_p,$$

como queríamos demonstrar. ∎

No próximo resultado veremos que a convergência do termo geral da série para zero é uma condição suficiente para a convergência da mesma.

Corolário 5.2. *Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência em $\mathbb{Q}_p$. Então a série $\sum_{i=0}^{\infty} x_n$ converge em $(\mathbb{Q}_p, |\cdot|_p)$ se, e somente se, $\lim_{n\to\infty} x_n = 0$ em $(\mathbb{Q}_p, |\cdot|_p)$.*

Demonstração:
$\Rightarrow$) Seja $\varepsilon > 0$ e $S = \sum_{i=0}^{\infty} x_n$. Consideremos $S_{n+1} = \sum_{i=0}^{n+1} x_i$ e $S_n = \sum_{i=0}^{n} x_i$. Por hipótese, existem $n_1, n_2 \in \mathbb{N}$ tais que $|S_{n+1} - S|_p \leq \varepsilon$ sempre que $n \geq n_1$ e $|S_n - S|_p \leq \varepsilon$ sempre que $n \geq n_2$. Tomemos $n_0 = \max\{n_1, n_2\}$. Então,

$$|x_{n+1}|_p = |S_{n+1} - S_n|_p = |(S_{n+1} - S) - (S_n - S)|_p \leq \max\{|(S_{n+1} - S)|_p, |(S_n - S)|_p\} \leq \varepsilon.$$

Logo, $\lim_{n\to\infty} x_n = 0$ em $(\mathbb{Q}_p, |\cdot|_p)$.
$\Leftarrow$) Suponhamos que $\lim_{n\to\infty} x_n = 0$ em $(\mathbb{Q}_p, |\cdot|_p)$. Logo, para todo $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $|x_n|_p \leq \varepsilon$, para todo $n \geq n_0$. Consideremos as somas parciais $S_n = \sum_{i=0}^{n} x_i, n \in \mathbb{N}$. Segue que,

$$\begin{aligned} |S_{n+k} - S_n|_p &= |x_{n+k} + x_{n+k-1} + \ldots + x_{n+2} + x_{n+1}|_p \\ &\leq \max\{|x_{n+k}|_p, |x_{n+k-1}|_p, \ldots, |x_{n+2}|_p, |x_{n+1}|_p\} \\ &\leq \varepsilon, \text{ para todo } n \geq n_0. \end{aligned}$$

Pela desigualdade acima, concluímos que $(S_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy em $(\mathbb{Q}_p, |\cdot|_p)$, consequentemente, pelo Teorema 5.1, $\sum_{n=0}^{\infty} x_n$ converge em $(\mathbb{Q}_p, |\cdot|_p)$. ∎

6 O ANEL DOS INTEIROS P–ÁDICOS

Prosseguindo no nosso estudo sobre o corpo dos números p-ádicos, vamos direcionar nossa atenção para o seguinte subconjunto de $\mathbb{Q}_p$:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p; |x|_p \leq 1\}.$$

Proposição 6.1. *$\mathbb{Z}_p$ é um subanel de $\mathbb{Q}_p$.*

Demonstração: Naturalmente, $\mathbb{Z}_p \subset \mathbb{Q}_p$. Assim, para provar a proposição, basta verificar a veracidade dos itens abaixo.

1. $0 \in \mathbb{Z}_p$.
   De fato, $|0|_p = \lim_{n\to\infty} |q_n|_p$, onde $q_n = 0$, para todo $n \in \mathbb{N}$, isto é,
   $$|0|_p = \lim_{n\to\infty} |0|_p = 0 \leq 1.$$
   Logo, $0 \in \mathbb{Z}_p$.

2. Se $x, y \in \mathbb{Z}_p$, então $x - y \in \mathbb{Z}_p$.
   Realmente, como $x, y \in \mathbb{Z}_p$, segue que $|x|_p, |y|_p \leq 1$. Consequentemente,
   $$|x - y|_p \leq \max\{|x|_p, |y|_p\} \leq 1.$$
   Deste modo, $x - y \in \mathbb{Z}_p$.

3. Se $x, y \in \mathbb{Z}_p$, então $x \cdot y \in \mathbb{Z}_p$.
   Com efeito, para $x, y \in \mathbb{Z}_p$, temos $|x|_p, |y|_p \leq 1$. Daí,
   $$|x \cdot y|_p = |x|_p \cdot |y|_p \leq 1 \cdot 1 = 1$$
   Portanto, $x \cdot y \in \mathbb{Z}_p$.

■

A partir desse momento, nos referiremos a $\mathbb{Z}_p$ como o **anel dos inteiros p-ádicos**.

Proposição 6.2. *$\mathbb{Z}_p$ é fechado.*

Demonstração: Basta mostrarmos que $\mathbb{Q}_p - \mathbb{Z}_p = \{x \in \mathbb{Q}_p; |x|_p > 1\}$ é aberto.

Seja $x \in \mathbb{Q}_p - \mathbb{Z}_p$. Tome $r = |x|_p - 1 > 0$.

Afirmação: $B_r(x) \subset \mathbb{Q}_p - \mathbb{Z}_p$.

De fato, se $y \in B_r(x)$, então $|y - x|_p < r = |x|_p - 1 < |x|_p$. Assim, pela Proposição 5.6,

$$|y|_p = |(y - x) + x|_p = |x|_p > 1.$$

Portanto, $y \in \mathbb{Q}_p - \mathbb{Z}_p$. Logo, $\mathbb{Q}_p - \mathbb{Z}_p$ é aberto. ■

Proposição 6.3. *Seja* $(a_n)_{n\in\mathbb{N}}$ *uma sequência de números inteiros tal que* $0 \leq a_n \leq p-1$, *para todo* $n \in \mathbb{N}$. *Então,* $\sum_{n=0}^{\infty} a_n \cdot p^n \in \mathbb{Z}_p$.

Demonstração: Como $0 \leq a_n \leq p-1$, segue que p não divide a_n, logo, $|a_n|_p = 1$, para todo $n \in \mathbb{N}$. Daí,

$$|a_n \cdot p^n|_p = |a_n|_p \cdot |p^n|_p = 1 \cdot \frac{1}{p^n} = \frac{1}{p^n} \leq 1, \text{ para todo } n \in \mathbb{N}.$$

Assim, $a_n \cdot p^n \in \mathbb{Z}_p$. Além disso, existe $n_0 \in \mathbb{N}$ tal que $\frac{1}{p^{n_0}} \leq \varepsilon$ e, portanto, $|a_n \cdot p^n|_p = \frac{1}{p^n} \leq \varepsilon$, para todo $n \geq n_0$. Logo, $\lim_{n\to\infty} a_n \cdot p^n = 0$ em $(\mathbb{Q}_p, |\cdot|_p)$. Consequentemente, $\sum_{n=0}^{\infty} a_n \cdot p^n$ converge em $(\mathbb{Q}_p, |\cdot|_p)$. Ademais, como $\mathbb{Z}_p$ é um anel e um conjunto fechado, $\sum_{i=0}^{n} a_i \cdot p^i \in \mathbb{Z}_p$ e

$$\lim_{n\to\infty} \left(\sum_{i=0}^{n} a_i \cdot p^i \right) = \sum_{n=0}^{\infty} a_n \cdot p^n \in \mathbb{Z}_p.$$

■

Proposição 6.4. $\mathbb{Z}$ *é um subconjunto de* $\mathbb{Z}_p$.

Demonstração: Seja $z \in \mathbb{Z} \subset \mathbb{Q}_p$. Então, $z = \overline{(x)}_{n\in\mathbb{N}}$, para algum inteiro x. Pelo Teorema Fundamental da Aritmética, $x = a \cdot p^k$, com $a \in \mathbb{Z}, k \in \mathbb{N}$ e $\text{mdc}(a, p) = 1$. Assim,

$$|z|_p = \lim_{n\to+\infty} |x|_p = |x|_p = |a \cdot p^k|_p = \frac{1}{p^k} \leq 1.$$

Logo, $z \in \mathbb{Z}_p$. ■

Proposição 6.5. $\mathbb{Z}$ *é denso em* $\mathbb{Z}_p$.

Demonstração: Consideremos $\mathcal{A} = \{q \in \mathbb{Q}; |q|_p \leq 1\}$.

1. $\mathcal{A}$ é denso em $\mathbb{Z}_p$.
   Com efeito, sejam $x \in \mathbb{Z}_p$ e $\varepsilon > 0$. Consideremos $\varepsilon' \in \mathbb{R}^+$ tal que $\varepsilon' < \min\{1, \varepsilon\}$. Como $\mathbb{Q}$ é denso em $\mathbb{Q}_p$, existe $q \in \mathbb{Q}$ tal que $|q - x|_p \leq \varepsilon'$. Note que,

   $$|q|_p = |q - x + x|_p \leq \max\{|q - x|_p, |x|_p\} \leq \max\{\varepsilon', 1\} = 1,$$

   ou seja, $|q|_p \leq 1$. Logo, $q \in \mathcal{A}$ e $|q - x|_p \leq \varepsilon' < \varepsilon$.

2. Para cada $x \in \mathcal{A}$, existe uma sequência $(x_n)_{n\in\mathbb{N}}$ em $\mathbb{Z}$ tal que $|x - x_n|_p \leq \frac{1}{p^{n+1}}$, para todo $n \in \mathbb{N}$.

Consideremos $x = \frac{a}{b}$, onde $a, b \in \mathbb{Z}, b \neq 0$ e $\text{mdc}(a,b) = 1$. Como $x \in \mathcal{A}$, $|x|_p = \left|\frac{a}{b}\right|_p = p^{-n}$, para algum $n \in \mathbb{N}$ e, consequentemente, $\text{mdc}(b,p) = 1$. Pelo Teorema 2.3, existem $m, n \in \mathbb{Z}$ tais que

$$1 = m \cdot b + n \cdot p. \tag{6.1}$$

Multiplicando a Equação (6.1) por a, obtemos $a = u_0 \cdot b + v_0 \cdot p$, onde $u_0 = a \cdot m$ e $v_0 = a \cdot n$. Por outro lado, pelo algoritmo da divisão de Euclides, existem $q_0, k_0 \in \mathbb{Z}$ únicos tais que $u_0 = q_0 \cdot p + k_0$ e $0 \leq k_0 \leq p-1$. Portanto,

$$a = (q_0 \cdot p + k_0) \cdot b + v_0 \cdot p = (q_0 \cdot b + v_0) \cdot p + k_0 \cdot b$$

$$\Rightarrow a = a_0 \cdot p + k_0 \cdot b,$$

onde $a_0 = q_0 \cdot b + v_0$. Além disso, como

$$x = \frac{a}{b} = \frac{(a_0 \cdot p + k_0 \cdot b)}{b} = \frac{a_0}{b} \cdot p + k_0,$$

segue que

$$|x - k_0|_p = \left|\frac{a_0}{b} \cdot p\right|_p = \left|\frac{a_0}{b}\right|_p \cdot |p|_p \leq |p|_p = \frac{1}{p},$$

visto que $\left|\frac{a_0}{b}\right|_p = |a_0|_p \cdot \left|\frac{1}{b}\right|_p \leq 1$.

Agora, multiplicando a equação (6.1) por a_0, obtemos $a_0 = u_1 \cdot b + v_1 \cdot p$, onde $u_1 = a_0 \cdot m$ e $v_1 = a_0 \cdot n$. Novamente, pelo algoritmo da divisão de Euclides, existem $q_1, k_1 \in \mathbb{Z}$ únicos tais que $u_1 = q_1 \cdot p + k_1$ e $0 \leq k_1 \leq p-1$. Portanto,

$$a_0 = (q_1 \cdot p + k_1) \cdot b + v_1 \cdot p = (q_1 \cdot b + v_1) \cdot p + k_1 \cdot b$$

$$\Rightarrow a_0 = a_1 \cdot p + k_1 \cdot b,$$

onde $a_1 = q_1 \cdot b + v_1$. Além disso, como

$$x = \frac{a}{b} = \frac{(a_0 \cdot p + k_0 \cdot b)}{b} = \frac{a_0}{b} \cdot p + k_0 = \frac{(a_1 \cdot p + k_1 \cdot b)}{b} \cdot p + k_0 = \frac{a_1}{b} \cdot p^2 + k_0 + k_1 \cdot p,$$

segue que

$$|x - (k_0 + k_1 \cdot p)|_p = \left|\frac{a_1}{b} \cdot p^2\right|_p = \left|\frac{a_1}{b}\right|_p \cdot |p^2|_p \leq |p^2|_p = \frac{1}{p^2},$$

visto que $\left|\frac{a_1}{b}\right|_p = |a_1|_p \cdot \left|\frac{1}{b}\right|_p \leq 1$.

Suponhamos que para l inteiro, $l \geq 0$, existam $k_0, k_1, \ldots, k_l, a_0, a_1, \ldots, a_l \in \mathbb{Z}$ tais que

$$a = a_0 \cdot p + k_0 \cdot b \quad , \quad a_i = a_{i+1} \cdot p + k_{i+1} \cdot b \quad , \quad 0 \leq k_i \leq p-1, \forall i = 0, \ldots, l$$

$$\text{e} \quad |x - (k_0 + k_1 \cdot p + \ldots + k_l \cdot p^l)|_p \leq \frac{1}{p^{l+1}}.$$

Então, pela equação (6.1), $a_l = u_{l+1} \cdot b + v_{l+1} \cdot p$, onde $u_{l+1} = a_l \cdot m$ e $v_{l+1} = a_l \cdot n$. Pelo algoritmo da divisão de Euclides, existem $q_{l+1}, k_{l+1} \in \mathbb{Z}$ únicos tais que $u_{l+1} = q_{l+1} \cdot p + k_{l+1}$ e $0 \leq k_{l+1} \leq p-1$. Portanto,

$$a_l = (q_{l+1} \cdot p + k_{l+1}) \cdot b + v_{l+1} \cdot p = (q_{l+1} \cdot b + v_{l+1}) \cdot p + k_{l+1} \cdot b$$

$$\Rightarrow a_l = a_{l+1} \cdot p + k_{l+1} \cdot b,$$

onde $a_{l+1} = q_{l+1} \cdot b + v_{l+1}$. Note que,

$$a = a_{l+1} \cdot p^{l+2} + k_{l+1} \cdot b \cdot p^{l+1} + \ldots + k_1 \cdot b \cdot p + k_0 \cdot b.$$

Assim,

$$x = \frac{a}{b} = \frac{a_{l+1}}{b} \cdot p^{l+2} + k_0 + k_1 \cdot p + \ldots + k_l \cdot p^l + k_{l+1} \cdot p^{l+1}.$$

Portanto,

$$|x - (k_0 + k_1 \cdot p + \ldots + k_l \cdot p^l + k_{l+1} \cdot p^{l+1})|_p = \left|\frac{a_{l+1}}{b} \cdot p^{l+2}\right|_p = \left|\frac{a_{l+1}}{b}\right|_p \cdot |p^{l+2}|_p \leq |p^{l+2}|_p = \frac{1}{p^{l+2}}.$$

Deste modo, pelo Princípio de Indução Finita, existem $(k_l)_{l \in \mathbb{N}}$ e $(a_l)_{l \in \mathbb{N}}$, sequências de números inteiros, tais que

$$a = a_0 \cdot p + k_0 \cdot b \quad , \quad a_l = a_{l+1} \cdot p + k_{l+1} \cdot b \quad , \quad 0 \leq k_l \leq p-1$$

$$\text{e} \quad |x - (k_0 + k_1 \cdot p + \ldots + k_l \cdot p^l)|_p \leq \frac{1}{p^{l+1}}, \text{para todo } l \in \mathbb{N}.$$

Finalmente, tomando $x_n = k_0 + k_1 \cdot p + \ldots + k_n \cdot p^n \in \mathbb{Z}$, temos $|x - x_n|_p \leq \frac{1}{p^{n+1}}$, para todo $n \in \mathbb{N}$.

3. $\mathbb{Z}$ é denso em $\mathcal{A}$.

   Sejam $x \in \mathcal{A}$ e $r > 0$. Pelo item anterior, existe $x_{n_0} \in \mathbb{Z}$ tal que $|x - x_{n_0}|_p < \frac{1}{p^{n_0+1}} < r$ para algum natural n_0.

4. $\mathbb{Z}$ é denso em $\mathbb{Z}_p$.

   Sejam $z \in \mathbb{Z}_p$ e $r > 0$. Pelo item 1, existe $a \in \mathcal{A}$ tal que $|z - a|_p < \frac{r}{2}$. Por outro lado, pelo item 3, existe $x \in \mathbb{Z}$ tal que $|x - a| < \frac{r}{2}$. Portanto,

   $$|z - x|_p \leq \max\{|z - a|_p, |a - x|_p\} < \frac{r}{2} < r.$$

   Logo, $\mathbb{Z}$ é denso em $\mathbb{Z}_p$.

■

Observação 6.1. *Mantendo as notações da demonstração do teorema acima, temos*

$$\begin{aligned} 0 \leq x_n &= k_0 + k_1 \cdot p + \ldots + k_n \cdot p^n \\ &\leq (p-1) + (p-1) \cdot p + \ldots + (p-1) \cdot p^n \\ &= (p-1)(1 + p + \ldots + p^n) \\ &= (p-1) \cdot \frac{1 - p^{n+1}}{1-p} \\ &= p^{n+1} - 1 \\ &< p^{n+1}. \end{aligned}$$

Assim, $0 \leq x_n < p^{n+1}$.

Proposição 6.6. *Sejam* $(x_n)_{n\in\mathbb{N}}$ *e* $(x'_n)_{n\in\mathbb{N}}$ *sequências de números inteiros tais que*

$$0 \leq x_n, x'_n < p^{n+1}, |x - x_n|_p \leq \frac{1}{p^{n+1}} \quad e \quad |x - x'_n|_p \leq \frac{1}{p^{n+1}}.$$

Então, $x_n = x'_n$, *para todo* $n \in \mathbb{N}$.

Demonstração: De fato, pelo Teorema Fundamental da Aritmética, existem $k \in \mathbb{N}$, $q \in \mathbb{Z}$ tais que $\text{mdc}(p, q) = 1$ e $x_n - x'_n = p^k \cdot q$. Daí,

$$\frac{1}{p^k} = |x_n - x'_n|_p \leq \max\{|x - x_n|_p, |x - x'_n|_p\} \leq \frac{1}{p^{n+1}}.$$

Assim, $k \geq n + 1$, isto é, $k = (n + 1) + l$, para algum inteiro $l \geq 0$. Consequentemente,

$$x_n - x'_n = p^{n+1} \cdot p^l \cdot q \Rightarrow x_n \equiv x'_n \ (mod\ p^{n+1}).$$

Ademais, como $0 \leq x_n, x'_n < p^{n+1}$, então $x_n = x'_n$. ■

Observação 6.2. *Sejam* $a, b \in \mathbb{Q}_p$. *Da demonstração da proposição anterior, podemos concluir que, se* $|a - b|_p \leq \frac{1}{p^n}$, *então,* $a \equiv b \ (mod\ p^n)$.

Proposição 6.7. *Sejam* $a, b \in \mathbb{Q}_p$. *Então,* $|a - b|_p \leq \frac{1}{p^n}$ *se, e somente se,* $a \equiv b \ (mod\ p^n)$.

Demonstração: Se $a \equiv b \ (mod\ p^n)$, então $a - b = p^n \cdot q$, para algum $q \in \mathbb{Z}$. Daí,

$$|a - b|_p = |p^n \cdot q|_p = |p^n|_p \cdot |q|_p = \frac{1}{p^n} \cdot |q|_p \leq \frac{1}{p^n}.$$

■

Corolário 6.1. *$\mathbb{Z}_p$ é completo.*

Demonstração: Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy em $\mathbb{Z}_p \subset \mathbb{Q}_p$. Pelo Teorema 5.1, existe $x \in \mathbb{Q}_p$ tal que $\lim_{n\to\infty} x_n = x$. Como $\mathbb{Z}_p$ é fechado, $x \in \mathbb{Z}_p$. Logo, $\mathbb{Z}_p$ é completo. ■

6.1 OS RESULTADOS DE HENSEL

No que segue, veremos dois resultados de extrema importância, ambos atribuídos à Hensel. O primeiro nos dá uma caracterização dos elementos de $\mathbb{Z}_p$, enquanto o segundo nos dá condições suficientes para a existência de pelo menos uma raiz de um polinômio com coeficientes em $\mathbb{Z}_p$.

Teorema 6.1 (Desenvolvimento de Hensel de um inteiro p-ádico). *Se $x \in \mathbb{Z}_p$, existe uma única sequência $(k_n)_{n\in\mathbb{N}}$ de números inteiros compreendidos entre 0 e $p-1$ tal que $x = \sum_{n=0}^{\infty} k_n \cdot p^n$.*

Demonstração: Pela Proposição 6.5, para cada $x \in \mathbb{Z}_p$, existem $(k_n)_{n\in\mathbb{N}}$ e $(x_n)_{n\in\mathbb{N}}$, sequências de números inteiros, tais que

$$0 \le k_n \le p-1, \quad x_n = k_0 + k_1 \cdot p + \ldots + k_n \cdot p^n \quad \text{e} \quad |x - x_n|_p \le \frac{1}{p^{n+1}}, \text{para todo } n \in \mathbb{N}.$$

Assim, $x = \sum_{n=0}^{\infty} k_n \cdot p^n$.

Por outro lado, suponhamos que $x = \sum_{n=0}^{\infty} b_n \cdot p^n$, com $0 \le b_n \le p-1, \forall n \in \mathbb{N}$. Para cada $n \in \mathbb{N}$, consideremos $x'_n = b_0 + b_1 \cdot p + \ldots + b_n \cdot p^n$.

Pela Observação 6.1, $0 \le x_n, x'_n < p^{n+1}$.

Além disso, fixado $n \in \mathbb{N}$ arbitrário, temos

$$\begin{aligned}
|x - x'_n|_p &= \left| \left(\lim_{k\to\infty} b_0 + b_1 \cdot p + \ldots + b_n \cdot p^n + \ldots b_k \cdot p^k \right) - (b_0 + b_1 \cdot p + \ldots + b_n \cdot p^n) \right|_p \\
&= \left| \left(\lim_{k\to\infty} b_0 + b_1 \cdot p + \ldots + b_n \cdot p^n + \ldots b_k \cdot p^k \right) - \left(\lim_{k\to\infty} b_0 + b_1 \cdot p + \ldots + b_n \cdot p^n \right) \right|_p \\
&= \left| \lim_{k\to\infty} b_{n+1} \cdot p^{n+1} + \ldots + b_k \cdot p^k \right|_p \\
&= \left| \lim_{k\to\infty} p^{n+1} \cdot (b_{n+1} + \ldots + b_k \cdot p^{k-(n+1)}) \right|_p \\
&= \left| \lim_{k\to\infty} p^{n+1} \right|_p \cdot \left| \lim_{k\to\infty} b_{n+1} + \ldots + b_k \cdot p^{k-(n+1)} \right|_p \\
&= |p^{n+1}|_p \cdot \left| \lim_{k\to\infty} b_{n+1} + \ldots + b_k \cdot p^{k-(n+1)} \right|_p
\end{aligned}$$

Por outro lado, $b_{n+1} + \ldots + b_k \cdot p^{k-(n+1)} \in \mathbb{Z}_p$ e, consequentemente, $\lim_{k\to\infty} b_{n+1} + \ldots + b_k \cdot p^{k-(n+1)} \in \mathbb{Z}_p$. Assim,

$$\begin{aligned} |x - x'_n|_p &= |p^{n+1}|_p \cdot \left| \lim_{k\to\infty} b_{n+1} + \ldots + b_k \cdot p^{k-(n+1)} \right|_p \\ &\leq |p^{n+1}|_p \\ &= \frac{1}{p^{n+1}}. \end{aligned}$$

Desse modo, pela Proposição 6.6, $x_n = x'_n$, para todo $n \in \mathbb{N}$. Portanto, segue a unicidade.

■

A seguir abordaremos o desenvolvimento de Hensel de alguns números inteiros.

Consideremos $p, q \in \mathbb{Z}_+$, p primo. Pelo Teorema de Representação de um Número na Base p, existem $m \in \mathbb{N}$, $a_i \in \mathbb{N}$, $0 \leq a_i < p$, para todo $i = 0, \ldots, m$, tais que

$$q = a_m \cdot p^m + \cdots + a_1 \cdot p + a_0.$$

Segue de forma natural que

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

onde $a_i = 0$, para todo $i > m$, é o desenvolvimento de Hensel de q. De fato, para todo $\varepsilon > 0$,

$$\left| \sum_{i=0}^{\infty} a_i \cdot p^i - q \right|_p = |0|_p = 0 < \varepsilon, \forall n \geq m.$$

Portanto, $q = \sum_{i=0}^{\infty} a_i \cdot p^i$.

Dando continuidade com o desenvolvimento de Hensel dos números inteiros, trazemos o próximo exemplo.

Exemplo 6.1. *O desenvolvimento de Hensel de -1 é* $\sum_{n=0}^{\infty} (p-1) \cdot p^n$.

De fato, consideremos $S_n = \sum_{i=0}^{n} (p-1) \cdot p^i$, *para cada* $n \in \mathbb{N}$. *Deste modo,*

$$S_n = (p-1) \cdot \left(\sum_{i=0}^{n} p^i \right) = (p-1) \cdot \frac{1 - p^{n+1}}{1-p} = p^{n+1} - 1.$$

Assim, para cada $\varepsilon > 0$, *tome* $n_0 \in \mathbb{N}$ *tal que* $p^{-(n_0+1)} < \varepsilon$. *Então,*

$$|S_n - (-1)|_p = |p^{n+1}|_p = p^{-(n+1)} \leq p^{-(n_0+1)} < \varepsilon, \forall n \geq n_0.$$

Logo,

$$\sum_{n=0}^{\infty} (p-1) \cdot p^n = \lim_{n\to\infty} S_n = -1.$$

Corolário 6.2. *Sejam p e q inteiros positivos, p primo, $q \leq p$. Então, o desenvolvimento de Hensel de $-q$ é $\sum_{i=0}^{\infty} a_i \cdot p^i$, onde $a_0 = p - q$ e $a_i = p - 1$, para todo $i \neq 0$.*

Demonstração: Consideremos $\varepsilon > 0$ e

$$\begin{aligned} S_n &= a_0 + a_1 \cdot p + a_2 \cdot p^2 + \ldots + a_{n-1} \cdot p^{n-1} \\ &= (p-q) + (p-1) \cdot p + (p-1) \cdot p^2 + \ldots + (p-1) \cdot p^{n-1}. \end{aligned}$$

Assim, tomemos $n_0 \in \mathbb{N}$ tal que $p^{-n_0} < \varepsilon$. Daí,

$$\begin{aligned} |S_n - (-q)|_p &= |p + (p-1) \cdot p + (p-1) \cdot p^2 + \ldots + (p-1) \cdot p^{n-1}|_p \\ &= |(p-1) \cdot (1 + p + p^2 + \ldots + p^{n-1}) + 1|_p \\ &= \left| (p-1) \cdot \frac{1-p^n}{1-p} + 1 \right|_p \\ &= |-(1-p^n) + 1|_p \\ &= |p^n|_p = p^{-n} < \varepsilon, \text{para todo } n \geq n_0. \end{aligned}$$

Logo, $-q = \sum_{i=0}^{\infty} a_i \cdot p^i$, onde $a_0 = p - q$ e $a_i = p - 1$, para todo $i \neq 0$.

■

Definição 6.1. *Seja $f(x) \in \mathbb{Z}_p[x]$, isto é, $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0$, com $a_i \in \mathbb{Z}_p$, para todo $i = 0, 1, \ldots, n$ e $a_n \neq 0$. Chamamos de **derivada formal** de $f(x)$ o seguinte elemento de $Z_p[x]$*

$$f'(x) = a_n \cdot n \cdot x^{n-1} + a_{n-1} \cdot (n-1) \cdot x^{n-2} + \ldots + a_1.$$

Proposição 6.8. *Seja $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0 \in \mathbb{Z}_p[x]$. Então, para x e y, variáveis independentes,*

$$f(x+y) = f(x) + f_1(x) \cdot y + f_2(x) \cdot y^2 + \cdots + f_n(x) \cdot y^n,$$

onde $f_i(x) = \dfrac{f^{(i)}(x)}{i!} \in \mathbb{Z}_p[x]$, para cada $i \in \{1, \ldots, n\}$, onde $f^{(i)}(x)$ é a i–ésima derivada formal de $f(x)$.

Demonstração: De fato, para $n = 1$, $f(x) = a_1 \cdot x + a_0$ e

$$f(x+y) = a_1 \cdot (x+y) + a_0 = (a_1 \cdot x + a_0) + a_1 \cdot y = f(x) + f'(x) \cdot y.$$

Suponhamos que o resultado seja válido para $n = k$. Mostraremos que o mesmo também seguirá para $n = k+1$. Desse modo, seja $f(x) = a_{k+1} \cdot x^{k+1} + a_k \cdot x^k + \ldots + a_1 \cdot x + a_0 \in$

$\mathbb{Z}_p[x]$. Consideremos $g(x) = a_k \cdot x^k + \ldots + a_1 \cdot x + a_0$. Daí,

$$\begin{aligned}
f(x+y) &= a_{k+1} \cdot (x+y)^{k+1} + g(x+y) \\
&= a_{k+1} \cdot \sum_{i=0}^{k+1} \binom{k+1}{i} \cdot x^i \cdot y^{(k+1)-i} + g(x) + g'(x) \cdot y + \frac{g''(x)}{2!} \cdot y^2 + \ldots + \frac{g^{(k)}(x)}{k!} \cdot y^k \\
&= a_{k+1} \cdot \left(x^{k+1} + (k+1) \cdot x^k \cdot y + \frac{(k+1) \cdot k}{2!} \cdot x^{k-1} \cdot y^2 + \ldots + \frac{(k+1)!}{k!} \cdot x \cdot y^k + y^{k+1} \right) + g(x) \\
&+ g'(x) \cdot y + \frac{g''(x)}{2!} \cdot y^2 + \ldots + \frac{g^{(k)}(x)}{k!} \cdot y^k \\
&= (a_{k+1} \cdot x^{k+1} + g(x)) + (a_{k+1} \cdot (k+1) \cdot x^k + g'(x)) \cdot y + \left(a_{k+1} \cdot \frac{(k+1) \cdot k}{2!} \cdot x^{k-1} + \frac{g''(x)}{2!} \right) \cdot y^2 \\
&+ \ldots + \left(a_{k+1} \cdot \frac{(k+1)!}{k!} \cdot x + \frac{g^{(k)}(x)}{k!} \right) \cdot y^k + a_{k+1} \cdot y^{k+1} \\
&= f(x) + f'(x) \cdot y + \frac{f''(x)}{2!} \cdot y^2 + \ldots + \frac{f^{(k)}(x)}{k!} \cdot y^k + \frac{f^{(k+1)}(x)}{(k+1)!} \cdot y^{k+1}. \\
&= f(x) + f_1(x) \cdot y + f_2(x) \cdot y^2 + \ldots + f_k(x) \cdot y^k + f_{k+1}(x) \cdot y^{k+1}.
\end{aligned}$$

■

Observação 6.3. *No que segue, dados $a, b \in \mathbb{Z}_p$, $b \neq 0$, assumiremos a notação $\frac{a}{b}$ para representar $a \cdot b^{-1}$.*

Teorema 6.2 (Lema de Hensel). *Seja $f(x) \in \mathbb{Z}_p[x]$ e seja $a_0 \in \mathbb{Z}_p$ tal que $|f(a_0)|_p < |f'(a_0)|_p^2$, onde $f'(x) \in \mathbb{Z}_p[x]$ é a derivada formal de $f(x)$. Então, existe $a \in \mathbb{Z}_p$ tal que $f(a) = 0$.*

Demonstração: Seja $f(x) \in \mathbb{Z}_p[x]$. Consideremos

$$f(x) = \mu_0 + \mu_1 \cdot x + \ldots + \mu_n \cdot x^n,$$

onde $\mu_0, \mu_1, \ldots, \mu_n \in \mathbb{Z}_p$ e $\mu_n \neq 0$. Então, $f'(x) = \mu_1 + 2 \cdot \mu_2 \cdot x + \ldots + n \cdot \mu_n \cdot x^{n-1}$.

Note que se $f(a_0) = 0$, o resultado segue de imediato. Desse modo, vamos assumir que $f(a_0) \neq 0$.

Pela Proposição 6.8,

$$f(x+y) = f(x) + f_1(x) \cdot y + f_2(x) \cdot y^2 + \ldots + f_n(x) \cdot y^n, \tag{6.2}$$

onde $f_i(x) \in \mathbb{Z}_p[x]$, para cada $i \in \{1, \ldots, n\}$. Em particular, $f_1(x) = f'(x)$.

Como $f'(x) \in \mathbb{Z}_p[x]$ e $a_0 \in \mathbb{Z}_p$, então $f'(a_0) \in \mathbb{Z}_p$, isto é, $|f'(a_0)|_p \leq 1$. Consequentemente, $|f'(a_0)|_p^2 \leq |f'(a_0)|_p$. Desse modo, pela hipótese,

$$|f(a_0)|_p < |f'(a_0)|_p^2 \leq |f'(a_0)|_p = |f_1(a_0)|_p,$$

logo, $\left|\dfrac{f(a_0)}{f_1(a_0)}\right|_p < 1$, ou seja, $\dfrac{f(a_0)}{f_1(a_0)} \in \mathbb{Z}_p$. Escrevamos $\dfrac{f(a_0)}{f_1(a_0)} = -b_0$. Então, existe $b_0 \in \mathbb{Z}_p$ tal que $f(a_0) + f_1(a_0) \cdot b_0 = 0$. Assim, por (6.2),

$$\begin{aligned}
|f(a_0+b_0)|_p &= |\underbrace{f(a_0) + f_1(a_0)\cdot b_0}_{=0} + f_2(a_0)\cdot b_0^2 + f_3(a_0)\cdot b_0^3 + \ldots + f_n(a_0)\cdot b_0^n|_p \\
&= |f_2(a_0)\cdot b_0^2 + f_3(a_0)\cdot b_0^3 + \ldots + f_n(a_0)\cdot b_0^n|_p \\
&\leq \max\{|f_2(a_0)\cdot b_0^2|_p, |f_3(a_0)\cdot b_0^3|_p, \ldots, |f_n(a_0)\cdot b_0^n|_p\} \\
&= \max_{i\geq 2}\{|f_i(a_0)|_p \cdot |b_0|_p^i\} \\
&\leq \max_{i\geq 2}\{|b_0|_p^i\} \\
&= |b_0|_p^2,
\end{aligned}$$

visto que $f_i(a_0), b_0 \in \mathbb{Z}_p$. Por conseguinte, utilizando a hipótese,

$$|f(a_0+b_0)|_p \leq |b_0|_p^2 = \left|-\frac{f(a_0)}{f_1(a_0)}\right|_p^2 = \frac{|f(a_0)|_p \cdot |f(a_0)|_p}{|f'(a_0)|_p^2} < \frac{|f(a_0)|_p \cdot |f'(a_0)|_p^2}{|f'(a_0)|_p^2} = |f(a_0)|_p,$$

isto é,

$$|f(a_0+b_0)|_p < |f(a_0)|_p. \tag{6.3}$$

Novamente, pela Proposição 6.8, dados x e y, variáveis independentes, tem-se

$$f_1(x+y) = f_1(x) + g_1(x)\cdot y + \ldots + g_n(x)\cdot y^n,$$

onde $g_i(x) = \dfrac{f_1^{(i)}(x)}{i!}$, para cada $i \in \{1, \ldots, n\}$. Desse modo,

$$\begin{aligned}
|f_1(a_0+b_0) - f_1(a_0)|_p &= |g_1(a_0)\cdot b_0 + \ldots + g_n(a_0)\cdot b_0^n|_p \\
&\leq \max\{|g_1(a_0)\cdot b_0|_p, \ldots, |g_n(a_0)\cdot b_0^n|_p\} \\
&= \max_{i\geq 1}\{|g_i(a_0)|_p \cdot |b_0|_p^i\} \\
&\leq \max_{i\geq 1}\{|b_0|_p^i\} \\
&= |b_0|_p
\end{aligned}$$

pois $|g_i(a_0)|_p, |b_0|_p \leq 1$, para todo $i = 1, \ldots, n$. Assim,

$$|f_1(a_0+b_0) - f_1(a_0)|_p \leq |b_0|_p = \left|-\frac{f(a_0)}{f_1(a_0)}\right|_p = \frac{|f(a_0)|_p}{|f'(a_0)|_p} < \frac{|f'(a_0)|_p^2}{|f'(a_0)|_p} = |f'(a_0)|_p = |f_1(a_0)|_p$$

e, pela Proposição 5.6, $|f_1(a_0+b_0)|_p = |f_1(a_0)|_p$.

Denotaremos $a_1 = a_0 + b_0$. Então,

$$|f(a_1)|_p < |f(a_0)|_p \quad \text{e} \quad |f_1(a_1)|_p = |f_1(a_0)|_p. \tag{6.4}$$

Note que, se $f(a_1) = 0$, a prova do teorema está concluída. Vamos admitir que $f(a_1) \neq 0$. Pela hipótese e por (6.4), segue que

$$|f(a_1)|_p < |f(a_0)|_p < |f_1(a_0)|_p^2 = |f_1(a_1)|_p^2 \leq |f_1(a_1)|_p,$$

$$\Rightarrow \left|\frac{f(a_1)}{f_1(a_1)}\right|_p \leq 1 \Rightarrow b_1 = -\frac{f(a_1)}{f_1(a_1)} \in \mathbb{Z}_p.$$

Daí, $f(a_1) + f_1(a_1) \cdot b_1 = 0$. Além disso,

$$\begin{aligned}
|f(a_1 + b_1)|_p &= |\underbrace{f(a_1) + f_1(a_1) \cdot b_1}_{=0} + f_2(a_1) \cdot b_1^2 + f_3(a_1) \cdot b_1^3 + \ldots + f_n(a_1) \cdot b_1^n|_p \\
&= |f_2(a_1) \cdot b_1^2 + f_3(a_1) \cdot b_1^3 + \ldots + f_n(a_1) \cdot b_1^n|_p \\
&\leq \max\{|f_2(a_1) \cdot b_1^2|_p, |f_3(a_1) \cdot b_1^3|_p, \ldots, |f_n(a_1) \cdot b_1^n|_p\} \\
&= \max_{i \geq 2}\{|f_i(a_1)|_p \cdot |b_1|_p^i\} \\
&\leq \max_{i \geq 2}\{|b_1|_p^i\} \\
&= |b_1|_p^2.
\end{aligned}$$

Ademais, por (6.4),

$$|b_1|_p^2 = \left|-\frac{f(a_1)}{f_1(a_1)}\right|_p^2 = \frac{|f(a_1)|_p \cdot |f(a_1)|_p}{|f'(a_0)|_p^2} < \frac{|f(a_1)|_p \cdot |f(a_0)|_p}{|f'(a_0)|_p^2} < \frac{|f(a_1)|_p \cdot |f'(a_0)|_p^2}{|f'(a_0)|_p^2} = |f(a_1)|_p.$$

Logo,

$$|f(a_1 + b_1)|_p < |f(a_1)|_p. \tag{6.5}$$

No que segue,

$$\begin{aligned}
|f_1(a_1 + b_1) - f_1(a_1)|_p &= |g_1(a_1) \cdot b_1 + \ldots + g_n(a_1) \cdot b_1^n|_p \\
&\leq \max\{|g_1(a_1) \cdot b_1|_p, \ldots, |g_n(a_1) \cdot b_1^n|_p\} \\
&= \max_{i \geq 1}\{|g_i(a_1)|_p \cdot |b_1|_p^i\} \\
&\leq \max_{i \geq 1}\{|b_1|_p^i\} \\
&= |b_1|_p
\end{aligned}$$

Consequentemente,

$$|f_1(a_1+b_1)-f_1(a_1)|_p \leq |b_1|_p = \frac{|f(a_1)|_p}{|f_1(a_1)|_p} = \frac{|f(a_1)|_p}{|f'(a_0)|_p} < \frac{|f(a_0)|_p}{|f'(a_0)|_p} < \frac{|f'(a_0)|_p^2}{|f'(a_0)|_p} = |f'(a_0)|_p = |f_1(a_1)|_p$$

e, pela Proposição 5.6, $|f_1(a_1 + b_1)|_p = |f_1(a_1)|_p$.

Escreveremos $a_2 = a_1 + b_1$. Então,

$$|f(a_2)|_p < |f(a_1)|_p < |f(a_0)|_p \quad \text{e} \quad |f_1(a_2)|_p = |f_1(a_1)|_p = |f(a_0)|_p. \tag{6.6}$$

Caso $f(a_2) = 0$, o teorema está provado. Caso contrário, construímos indutivamente duas sequências $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$ em $\mathbb{Z}_p$ de modo que

$$f(a_n) + f_1(a_n)\cdot b_n = 0,$$

$$a_{n+1} = a_n + b_n,$$

$$|f(a_{n+1})|_p \leq |b_n|_p^2,$$

$$|f(a_{n+1})|_p < |f(a_n)|_p \quad \text{e} \quad |f_1(a_n)|_p = |f_1(a_0)|_p,$$

para todo $n \in \mathbb{N}$. Note que a sequência $|f(a_n)|_p$ é monótona decrescente e limitada inferiormente por 0.

Seja $\alpha = \lim_{n\to\infty} |f(a_n)|_p$. Suponhamos que $\alpha > 0$. Então,

$$|f(a_{n+1})|_p \leq |b_n|_p^2 = \frac{|f(a_n)|_p^2}{|f_1(a_n)|_p^2} = \frac{|f(a_n)|_p^2}{|f'(a_0)|_p^2}.$$

Tomando o limite de n tendendo a infinito, temos

$$\alpha \leq \frac{\alpha^2}{|f'(a_0)|_p^2} \Rightarrow |f'(a_0)|_p^2 \leq \alpha.$$

Já que $(|f(a_n)|_p)_{n\in\mathbb{N}}$ é limitada superiormente por $|f(a_0)|_p$, segue que $|f'(a_0)|_p^2 \leq \alpha \leq |f(a_0)|_p$, absurdo, visto que contradiz a hipótese do teorema. Portanto, $\lim_{n\to\infty} |f(a_n)|_p = 0$, e consequentemente, $\lim_{n\to\infty} f(a_n) = 0$.

Observemos que

$$|a_{n+1} - a_n|_p = |b_n|_p = \frac{|f(a_n)|_p}{|f_1(a_n)|_p} = \frac{|f(a_n)|_p}{|f_1(a_0)|_p},$$

para todo $n \in \mathbb{N}$. Daí, $\lim_{n\to\infty} a_{n+1} - a_n = 0$. Assim, para qualquer $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $|a_{n+1} - a_n|_p \leq \varepsilon$, para todo $n \geq n_0$. Desse modo, para quaiquer $n \geq n_0$ e $k \in \mathbb{N}^*$, temos

$$\begin{aligned} |a_{n+k} - a_n|_p &= |(a_{n+k} - a_{n+k-1}) + (a_{n+k-1} - a_{n+k-2}) + \cdots + (a_{n+2} - a_{n+1}) + (a_{n+1} - a_n)|_p \\ &\leq \max\{|a_{n+k} - a_{n+k-1}|_p, |a_{n+k-1} - a_{n+k-2}|_p, \ldots, |a_{n+2} - a_{n+1}|_p, |a_{n+1} - a_n|_p\} \\ &\leq \varepsilon. \end{aligned}$$

Logo, $(a_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy em $\mathbb{Z}_p$ e, portanto, existe $a \in \mathbb{Z}_p$ tal que $\lim_{n\to\infty} a_n = a$. Por fim,

$$f(a) = f\left(\lim_{n\to\infty} a_n\right) = \lim_{n\to\infty} f(a_n) = 0,$$

isto é, $a \in \mathbb{Z}_p$ é raiz de f.

■

Corolário 6.3. *Suponhamos $p \neq 2$. Seja $b \in \mathbb{Z}_p$, onde $|b|_p = 1$, e admitamos que exista $a_0 \in \mathbb{Z}_p$ tal que $|a_0^2 - b|_p < 1$. Então, existe $a \in \mathbb{Z}_p$ tal que $a^2 = b$, ou seja, b admite uma "raiz quadrada"em $\mathbb{Z}_p$.*

Demonstração: Seja $f(x) = x^2 - b \in \mathbb{Z}_p[x]$. Como $f'(x) = 2x$, segue que

$$|f'(a_0)|_p = |2 \cdot a_0|_p = |2|_p \cdot |a_0|_p = |a_0|_p.$$

Por hipótese, $|a_0^2 - b|_p < 1 = |b|_p$, e, pela Proposição 5.6, $|a_0^2|_p = |b|_p$, logo, $|a_0|_p = 1$. Além disso, $|f'(a_0)|_p = 1$ e,

$$|f(a_0)|_p = |a_0^2 - b|_p < 1 = |f'(a_0)|_p^2.$$

Portanto, pelo Teorema 6.2, existe $a \in \mathbb{Z}_p$ tal que $f(a) = 0$, isto é, $a^2 = b$. ■

Exemplo 6.2. *O número -1 admite raiz quadrada em $\mathbb{Z}_5$, ou seja, $i \in \mathbb{Z}_5$. De fato, tomemos $b = -1$ e $a_0 = 2^{-1}$ no corolário anterior. Daí,*

$$|a_0^2 - b|_5 = |5 \cdot 2^{-2}|_5 = 5^{-1} < 1.$$

Exemplo 6.3. *O número 6 admite raiz quadrada em $\mathbb{Z}_5$, ou seja, $\sqrt{6} \in \mathbb{Z}_5$. De fato, tomemos $b = 6$ e $a_0 = 1$ no corolário anterior. Daí,*

$$|a_0^2 - b|_5 = |-5|_5 = 5^{-1} < 1.$$

7 INTRODUÇÃO À DINÂMICA P–ÁDICA

Visto alguns dos elementos e propriedades fundamentais relacionadas aos números p–ádicos, esse capítulo tem como intuito apresentá-los atrelados a uma abordagem dinamicista. Para tanto, definiremos os elementos básicos da teoria de sistemas dinâmicos e faremos uma breve análise de um determinado tipo de sistema dinâmico p–ádico.

7.1 CONCEITOS INICIAIS

Existem várias definições do que é um sistema dinâmico. Neste trabalho, nos direcionaremos à sistemas dinâmicos discretos, definidos a seguir.

Definição 7.1. *Um* ***sistema dinâmico discreto*** *é uma função $f : M \to M$, onde M é um espaço métrico. Nesse caso, a cada estado $x \in M$ do sistema, associamos o estado $f(x) \in M$ em que x se encontrará uma unidade de tempo depois.*

Definição 7.2. *Sejam $f : M \to M$ e $x \in M$. Consideremos*

$$f^0(x) = x, \quad f^1(x) = f(x), \quad f^2(x) = f(f^1(x)), \quad \ldots, \quad f^n(x) = f(f^{n-1}(x)),$$

para todo $n \in \mathbb{N}$. Então, a sequência $(f^n(x))_{n\in\mathbb{N}}$ é chamada ***órbita*** *de x por f.*

Definição 7.3. *Um ponto x_0 é dito* ***ponto fixo*** *de f se satisfaz a igualdade $f(x_0) = x_0$. Em particular, a órbita de x_0 é a sequência constante $(x_0, x_0, \ldots)$.*

Definição 7.4. *Um ponto fixo x_0 de f é dito* ***ponto fixo atrator*** *se existe $r > 0$ tal que $\lim_{n\to\infty} f^n(h) = x_0$, para todo $h \in B_r(x_0)$.*

Definição 7.5. *Um ponto x_0 é dito* ***periódico de período*** *p da função f se $f^p(x_0) = x_0$ e $f^k(x_0) \neq x_0$, para todo $0 < k < p$. Neste caso, a órbita de x_0 é a sequência*

$$(x_0, f(x_0), f^2(x_0), \ldots, f^{p-1}(x_0), x_0, f(x_0), f^2(x_0), \ldots, f^{p-1}(x_0), x_0, \ldots).$$

Uma ferramenta útil para o estudo de certos sistemas dinâmicos é a conjugação, uma mudança de coordenadas que relaciona duas dinâmicas distintas.

Definição 7.6. *Consideremos os sistemas dinâmicos $f : X \to X$ e $g : Y \to Y$. A* ***conjugação*** *é um homeomorfismo $h : X \to Y$ tal que $g \circ h = h \circ f$. Neste caso, dizemos que os sistemas dinâmicos f e g são conjugados pelo homeomorfismo h.*

O conceito de conjugação se mostra relevante visto que duas transformações conjugadas compartilham certas propriedades. Logo, podemos estudar características de um sistema dinâmico f a partir de um outro sistema dinâmico g.

Proposição 7.1. *Sejam $f : X \to X$ e $g : Y \to Y$ sistemas dinâmicos conjugados por um homeomorfismo $h : X \to Y$. Então, x_0 é um ponto periódico de período p para f se, e somente se, $h(x_0)$ é um ponto periódico de período p para g.*

Demonstração: De fato, como $f = h^{-1} \circ g \circ h$, então

$$\begin{aligned} f^n &= \underbrace{f \circ f \circ \ldots \circ f \circ f}_{n \text{ vezes}} \\ &= (h^{-1} \circ g \circ h) \circ (h^{-1} \circ g \circ h) \circ \ldots \circ (h^{-1} \circ g \circ h) \circ (h^{-1} \circ g \circ h) \\ &= h^{-1} \circ g \circ id \circ g \circ id \circ \ldots \circ id \circ g \circ id \circ g \circ h \\ &= h^{-1} \circ g^n \circ h. \end{aligned}$$

Daí,

$$f^n = h^{-1} \circ g^n \circ h \Rightarrow h(f^n(x)) = g^n(h(x)), \forall x \in X.$$

Portanto, $f^p(x_0) = x_0$ se, e somente se, $g^p(h(x_0)) = h(x_0)$.

■

7.2 DINÂMICA P–ÁDICA

A partir desse momento, nosso interesse reside na dinâmica $f : \mathbb{Z}_p \to \mathbb{Z}_p, p \neq 2$, onde $f(x) = x^2 + a_1 \cdot x + a_0 \in \mathbb{Z}_p[x]$. Contudo, analisaremos a existência de pontos fixos desse sistema dinâmico a partir do sistema dinâmico conjugado a f através do homeomorfismo $h : \mathbb{Z}_p \to \mathbb{Z}_p$, $h(x) = x + \dfrac{a_1}{2}$.

Proposição 7.2. *A função h definida acima é um homeomorfismo.*

Demonstração: A prova segue das afirmativas abaixo.

1. h é contínua em $\mathbb{Z}_p$: Sejam $a \in \mathbb{Z}_p$ e $\varepsilon > 0$. Tomemos $\delta = \varepsilon$. Se $|x - a|_p \leq \delta = \varepsilon$, então,
$$|h(x) - h(a)|_p = \left| \left(x + \frac{a_1}{2} \right) - \left(a + \frac{a_1}{2} \right) \right|_p = |x - a|_p \leq \varepsilon.$$

2. h é injetiva: De fato, sejam $x, y \in \mathbb{Z}_p$. Então,
$$h(x) = h(y) \Rightarrow x + \frac{a_1}{2} = y + \frac{a_1}{2} \Rightarrow x = y.$$

3. h é sobrejetiva: Realmente, seja $z \in \mathbb{Z}_p$. Tomemos $x = z - \dfrac{a_1}{2}$. Então,

   - $x \in \mathbb{Z}_p$: Com efeito,
   $$|x|_p = \left| z - \frac{a_1}{2} \right|_p \leq \max \left\{ |z|_p, \left| \frac{a_1}{2} \right|_p \right\} \leq 1,$$
   pois $p \neq 2$.

- $h(x) = z$: Com efeito,
$$h(x) = \left(z - \frac{a_1}{2}\right) + \frac{a_1}{2} = z.$$
Logo, para todo $z \in \mathbb{Z}_p$, existe $x \in \mathbb{Z}_p$ de modo que $h(x) = z$.

4. $h^{-1}(x) = x - \dfrac{a_1}{2}$ é a inversa de h: De certo,
$$h(h^{-1}(x)) = \left(x - \frac{a_1}{2}\right) + \frac{a_1}{2} = x$$
e
$$h^{-1}(h(x)) = \left(x + \frac{a_1}{2}\right) - \frac{a_1}{2} = x.$$

5. h^{-1} é contínua em $\mathbb{Z}_p$: Sejam $a \in \mathbb{Z}_p$ e $\varepsilon > 0$. Tomemos $\delta = \varepsilon$. Se $|x-a|_p \leq \delta = \varepsilon$, então,
$$\left|h^{-1}(x) - h^{-1}(a)\right|_p = \left|\left(x - \frac{a_1}{2}\right) - \left(a - \frac{a_1}{2}\right)\right|_p = |x-a|_p \leq \varepsilon.$$

Portanto, h é um homeomorfismo. ■

Proposição 7.3. *A conjugada de f por h é dada por $g_c : \mathbb{Z}_p \to \mathbb{Z}_p$, tal que $g_c(x) = x^2 + c$ e $c = a_0 + \dfrac{a_1}{2} - \dfrac{a_1^2}{4}$.*

Demonstração: Realmente, basta mostrar que $h \circ f \circ h^{-1} = g_c$. Daí,

$$\begin{aligned} f(h^{-1}(x)) &= \left(x - \frac{a_1}{2}\right)^2 + a_1 \cdot \left(x - \frac{a_1}{2}\right) + a_0 \\ &= \left(x^2 - a_1 \cdot x + \frac{a_1^2}{4}\right) + a_1 \cdot x - \frac{a_1^2}{2} + a_0 \\ &= x^2 - \frac{a_1^2}{4} + a_0. \end{aligned}$$

Consequentemente,

$$\begin{aligned} h \circ f \circ h^{-1} &= \left(x^2 - \frac{a_1^2}{4} + a_0\right) + \frac{a_1}{2} \\ &= x^2 + a_0 + \frac{a_1}{2} - \frac{a_1^2}{4} \\ &= x^2 + c, \text{ onde } c = a_0 + \frac{a_1}{2} - \frac{a_1^2}{4}. \end{aligned}$$

■

Desse modo, analisaremos a dinâmica definida por $g_c : \mathbb{Z}_p \to \mathbb{Z}_p$, onde $g_c(x) = x^2 + c$ e $c \in \mathbb{Z}_p$.

Note que $g_c(x) \in \mathbb{Z}_p[x]$ e que a dinâmica definida por essa está bem definida, pois $\mathbb{Z}_p$ é fechado para as operações de adição e multiplicação.

Nosso interesse inicial está na existência de pontos fixos de g_c, isto é, os valores de $x \in \mathbb{Z}_p$ tais que $g_c(x) = x$.

Consideremos a função $f_c : \mathbb{Z}_p \to \mathbb{Z}_p$, dada por $f_c(x) = x^2 - x + c$. Logo, nosso interesse recai em determinar as raízes de f_c. Para tanto, determinaremos $a_0 \in \mathbb{Z}_p$ tal que

$$|f_c(a_0)|_p < |f_c'(a_0)|_p^2 = |(f_c'(a_0))^2|_p,$$

isto é,

$$|{a_0}^2 - a_0 + c|_p < |4{a_0}^2 - 4a_0 + 1|_p. \tag{7.1}$$

e utilizaremos o Lema de Hensel.

Proposição 7.4. *Seja $a_0 \in \mathbb{Z}_p$, onde $|a_0|_p \notin \{0, 1\}$. Então,*

$$|{a_0}^2 - a_0 + 1|_p = |4{a_0}^2 - 4a_0 + 1|_p = 1.$$

Ademais, se $|{a_0}^2 - a_0 + c|_p < |4{a_0}^2 - 4a_0 + 1|_p$ e $|c|_p \leq 1$ então $|c|_p < 1$.

Demonstração: Realmente, por hipótese, $0 < |a_0|_p < 1$. Logo, $|a_0|_p^2 < |a_0|_p$. Pela Proposição 5.6, $|4 \cdot (a_0^2 - a_0)|_p \leq |a_0^2 - a_0|_p = |a_0|_p < 1 = |1|_p$. Consequentemente, pela mesma proposição,

$$|4 \cdot (a_0^2 - a_0) + 1|_p = |1|_p = 1.$$

e

$$|a_0^2 - a_0 + 1|_p = |1|_p = 1.$$

Agora, se $|c|_p = 1$,

$$|{a_0}^2 - a_0|_p < 1 \Rightarrow |{a_0}^2 - a_0|_p < |c|_p \Rightarrow |{a_0}^2 - a_0 + c|_p = |c|_p = 1.$$

Daí,

$$|{a_0}^2 - a_0 + c|_p < |4{a_0}^2 - 4a_0 + 1|_p \Rightarrow 1 < 1.$$

Absurdo. Logo, $|c|_p < 1$. ∎

Primeiramente, note que se $|c|_p < 1$ então $a_0 = 0$ e $a_0 = 1$ satisfazem a Inequação 7.1. Pela proposição acima, no caso em que $|c|_p = 1$ concluímos que se $a_0 \in \mathbb{Z}_p$ satisfaz a Inequação 7.1 então $|a_0|_p = 0$ ou $|a_0|_p = 1$. A seguir trazemos o caso em que $|a_0|_p = 0$ e alguns casos em que $|a_0|_p = 1$.

1. $|a_0|_p = 0$: Nesse caso, $a_0 = 0$. Porém, se a_0 satisfaz a Inequação (7.1), $|c|_p < |1|_p = 1$. Absurdo. Logo, $a_0 = 0$ não satisfaz a Inequação (7.1).

2. $a_0 = 1$: Analogamente ao caso anterior, a expressão (7.1) se resume a $|c|_p < |1|_p = 1$. Logo, $a_0 = 1$ não satisfaz a Inequação (7.1).

3. $a_0 = -1$: Nesse caso, a Inequação (7.1) resulta na desigualdade $|2 + c|_p < |9|_p$.

   Suponhamos $p \neq 3$. Então,

   $$|2 + c|_p < |9|_p \Leftrightarrow |2 + c|_p < 1.$$

   Em particular, $a_0 = -1$ satisfaz a Inequação (7.1) quando

   $$c = p^k \cdot q - 2 \text{ com } mdc(p, q) = 1,\ k \text{ inteiro},\ k \geq 1.$$

   Supondo $p = 3$ temos

   $$|2 + c|_p < |9|_p \Leftrightarrow |2 + c|_p < \frac{1}{9}.$$

   Em particular, $a_0 = -1$ satisfaz a Inequação (7.1) quando

   $$c = 3^k \cdot q - 2 \text{ com } mdc(3, q) = 1,\ k \text{ inteiro},\ k > 2.$$

   Em suma, podemos resumir os resultados acima no que segue.

Teorema 7.1. *Seja $g_c : \mathbb{Z}_p \to \mathbb{Z}_p$, $g_c(x) = x^2 + c$. Então,*

1. *Se $|c|_p < 1$ então g_c tem pelo menos um ponto fixo em $\mathbb{Z}_p$. Em particular, cada sistema dinâmico da família de funções $g_{p^k \cdot q}(x) = x^2 + p^k \cdot q, k, q \in \mathbb{Z}, k \geq 1, mdc(p, q) = 1$, tem pelo menos um ponto fixo em $\mathbb{Z}_p$.*

2. *Para todo inteiro primo p, $p \neq 3$, cada sistema dinâmico da família de funções $g_{p^k \cdot q - 2}(x) = x^2 + (p^k \cdot q - 2), k, q \in \mathbb{Z}, k \geq 1$, tem pelo menos um ponto fixo em $\mathbb{Z}_p$. Por outro lado, se $p = 3$, $g_{p^k \cdot q - 2}(x) = x^2 + (p^k \cdot q - 2)$, possui pelo menos um ponto fixo, para todo $k \geq 3$.*

Demonstração: Segue do desenvolvimento acima. ∎

Finalizamos com uma condição suficiente, não muito diferente do que acontece na dinâmica real, para que um ponto fixo seja atrator.

Teorema 7.2. *Sejam $g_c : \mathbb{Q}_p \to \mathbb{Q}_p$, $g_c(x) = x^2 + c$, e x_0 um ponto fixo de g_c. Se $|g_c'(x_0)|_p = R < 1$, então x_0 é um ponto fixo atrator de g_c. Mais especificamente, para todo $h \in B_R(x_0)$, $\lim_{n \to \infty} g_c^n(h) = x_0$.*

Demonstração: Seja $A \in \mathbb{R}$ tal que $R < A < 1$. Note que $g_c'(x) = 2 \cdot x$, $g_c''(x) = 2$ e $g_c^{(i)}(x) = 0$, para todo $i \geq 3$. Desse modo, pela Proposição 6.8,

$$g_c(x+y) - g_c(x) = g_c'(x) \cdot y + \frac{g_c''(x)}{2!} \cdot y^2,$$

para quaisquer variáveis independentes $x, y \in \mathbb{Q}_p$.

Consideremos $x = x_0$ e $h = x_0 + y \in B_R(x_0)$. Então,

$$g_c(h) - g_c(x_0) = g_c'(x_0) \cdot (h - x_0) + \frac{g_c''(x_0)}{2} \cdot (h - x_0)^2 \Rightarrow g_c(h) - x_0 = g_c'(x_0) \cdot (h - x_0) + (h - x_0)^2.$$

Daí,

$$\begin{aligned} |g_c(h) - x_0|_p &= |g_c'(x_0) \cdot (h - x_0) + (h - x_0)^2|_p \\ &\leq \max\{|g_c'(x_0) \cdot (h - x_0)|_p, |(h - x_0)^2|_p\} \\ &\leq \max\{|g_c'(x_0)|_p \cdot |(h - x_0)|_p, |(h - x_0)|_p^2\}. \end{aligned}$$

Suponhamos que $\max\{|g_c'(x_0)|_p \cdot |(h - x_0)|_p, |(h - x_0)|_p^2\} = |(h - x_0)|_p^2$. Então,

$$|g_c'(x_0)|_p \cdot |(h - x_0)|_p \leq |(h - x_0)|_p^2 \Rightarrow R = |g_c'(x_0)|_p \leq |h - x_0|_p < R.$$

Absurdo. Logo, $\max\{|g_c'(x_0)|_p \cdot |(h - x_0)|_p, |(h - x_0)|_p^2\} = |g_c'(x_0)|_p \cdot |(h - x_0)|_p$. Consequentemente,

$$\begin{aligned} |g_c(h) - x_0|_p &\leq |g_c'(x_0)|_p \cdot |(h - x_0)|_p \\ \Rightarrow |g_c(h) - x_0|_p &< A \cdot |h - x_0|_p. \end{aligned} \tag{7.2}$$

Daí, $g_c(h) \in B_R(x_0)$ e , por raciocínio análogo,

$$|g_c^2(h) - x_0|_p = |g_c(g_c(h)) - x_0|_p < A \cdot |g_c(h) - x_0|_p.$$

Indutivamente, temos

$$|g_c^n(h) - x_0|_p = |g_c(g_c^{n-1}(h)) - x_0|_p < A \cdot |g_c^{n-1}(h) - x_0|_p.$$

Assim,

$$0 \leq |g_c^n(h) - x_0|_p < \ldots < |g_c^2(h) - x_0|_p < |g_c(h) - x_0|_p < |h - x_0|_p$$

e, para todo $h \in B_R(x_0)$,

$$|g_c^n(h) - x_0|_p < A^n \cdot |h - x_0|_p.$$

Portanto, $\lim_{n \to \infty} g_c^n(h) = x_0$, para todo $h \in B_R(x_0)$. ∎

8 CONCLUSÃO

Através de uma condição mais forte do que a desigualdade triangular, obtemos os valores absolutos ultramétricos. Em particular, o valor absoluto $p-$ádico, peça central para todo o desenvolvimento do presente trabalho. Com esse valor absoluto, muitas são as propriedades que se distinguem do valor absoluto real.

É de conhecimento geral que, com o valor absoluto real, somos capazes de completar o corpo dos números racionais, $\mathbb{Q}$, obtendo o corpo dos números reais, $\mathbb{R}$. Por outro lado, vimos ao longo do texto que, munido do valor absoluto $p-$ádico, também somos capazes de completar $\mathbb{Q}$, contudo, nesse processo construímos o corpo dos números $p-$ádicos, $\mathbb{Q}_p$. No decorrer do trabalho estudamos os elementos deste novo ambiente e também algumas de suas propriedades, que nos fornecem informações suficientes para perceber o quão diferentes esses dois completamentos de $\mathbb{Q}$ são.

Salientadas as diferentes propriedades entre $\mathbb{R}$ e $\mathbb{Q}_p$, ainda temos o Teorema de Ostrowski, apresentado no Apêndice , que ressalta a importância de compreender a estrutura desses dois corpos, visto que, a menos de equivalência, são os únicos completamentos de $\mathbb{Q}$.

Ainda se tratando de números $p-$ádicos, temos o anel dos inteiros $p-$ádicos, $\mathbb{Z}_p$, um subconjunto de $\mathbb{Q}_p$. Ao longo do trabalho verificamos que este subconjunto possui propriedades tão interessantes quanto as do próprio corpo dos números $p-$ádicos. Destacamos o Desenvolvimento de Hensel e o Lema de Hensel, que nos fornecem uma caracterização dos elementos de $\mathbb{Z}_p$ e um método de verificação de existência de raízes polinomiais, respectivamente.

Ao final do trabalho, com os conhecimentos e ferramentas adquiridas ao longo do trabalho, fazemos uma breve análise da dinâmica da família quadrática, onde damos ênfase à análise de pontos fixos. Assim, constatamos que, com a mudança de ambiente, fatos bem estabelecidos na dinâmica real deixam de ser válidos.

REFERÊNCIAS

1 AMICE, Y. **Les nombres p-adiques** . Paris: Presses Universitaires de France, 1975.

2 ARAÚJO, M. J. V. C. **Notas de Aula: Introdução à Teoria dos Números** . Juiz de Fora: UFJF, 2016.

3 BARAVIERA, A. T.; BRANCO F. M. **Sistemas Dinâmicos: uma primeira visão**. Rio Grande do Sul: UFRGS.

4 FILHO, E. A. **Teoria Elementar dos Conjuntos**. São Paulo: Livraria Nobel, 1980.

5 GONÇALVES, A. **Introdução à Álgebra**. Rio de Janeiro: IMPA, 1995.

6 GOUVÊA, F. Q. **Primeiros Passos p–ádicos**. Rio de Janeiro: IMPA, 1989.

7 JÚNIOR, D. P. P. **Uma Introdução aos Corpos Valorizados**. Rio de Janeiro: UFRJ, 2012.

8 LIMA, E. L. **Análise Real: Funções de Uma Variável, vol.1** . Rio de Janeiro: IMPA, 2014.

9 LIMA, E. L. **Espaços Métricos**. Rio de Janeiro: IMPA, 2014.

10 OLIVEIRA. A. T. M. **Uma Introdução aos Números p–ádicos**. Rio de Janeiro: UFF, 2002.

11 THIRAN, E.; VERSTEGEN, D.; WEYERS, J. **p–Adic Dynamics** . Journal of Statistical Physics, Vol. 54, Nos. 3/4, 1989.

APÊNDICE A – O TEOREMA DE OSTROWSKI

Com o objetivo de completar o corpo dos números racionais, $\mathbb{Q}$, e obter um completamento diferente do corpo dos números reais, $\mathbb{R}$, estudamos o valor absoluto p-ádico e obtemos o corpo dos números p-ádicos, $\mathbb{Q}_p$. Uma pergunta natural que nos fazemos é sobre a existência dos completamentos para $\mathbb{Q}$ distintos de $\mathbb{R}$ e $\mathbb{Q}_p$. Em resposta a este questionamento, nos dedicaremos a apresentação do Teorema de Ostrowski.

A seguir trabalharemos algumas definições e proposições que serão necessárias para a demonstração desse teorema, contudo, todas elas serão trabalhadas em $\mathbb{Q}$, apesar de que todas podem ser expandidas para um corpo $\mathbb{K}$ arbitrário.

Teorema .1. *Seja $|\cdot|$ um valor absoluto não trivial em $\mathbb{Q}$. Então $|\cdot|$ é não arquimediano se, e somente se, existe $M > 0$ tal que $|n \cdot 1| \leq M$ para todo $n \in \mathbb{Z}$.*

Demonstração:
$\Rightarrow$) Seja $|\cdot|$ um valor absoluto não arquimediano. Como $|1| = 1$ e $|x + y| \leq \max\{|x|, |y|\}$, para todo $x, y \in \mathbb{Q}$, provaremos que $|n \cdot 1| \leq 1$, para todo $n \in \mathbb{N}$. De fato,

1. Para $n = 1$, $|1 \cdot 1| = |1| = 1$;
2. Suponha que $|(k-1) \cdot 1| = |k-1| \leq 1$, para algum $k \in \mathbb{N}$. Então,

$$|k \cdot 1| = |k| = |1 + (k-1)| \leq \max\{|1|, |k-1|\} \leq 1.$$

Logo, $|n \cdot 1| \leq 1$, para todo $n \in \mathbb{N}$. Ademais, pela Proposição 2.5,

$$|0| = 0 \quad \text{e} \quad |(-n) \cdot 1| = |-(n \cdot 1)| = |n \cdot 1| \leq 1.$$

Portanto, $|n \cdot 1| \leq 1$, para todo $n \in \mathbb{Z}$.
$\Leftarrow$) Sejam $x, y \in \mathbb{Q}$. Como $|\cdot|$ é um valor absoluto, para todo $n \in \mathbb{N}$, temos

$$\begin{aligned}
|x+y|^n &= |(x+y)^n| \\
&= \left| x^n + \binom{n}{1} \cdot x^{n-1} \cdot y + \cdots + \binom{n}{n-1} \cdot x \cdot y^{n-1} + y^n \right| \\
&\leq |x|^n + \left| \binom{n}{1} \right| \cdot |x|^{n-1} \cdot |y| + \cdots + \left| \binom{n}{n-1} \right| \cdot |x| \cdot |y|^{n-1} + |y|^n \\
&\leq M \cdot |x|^n + M \cdot |x|^{n-1} \cdot |y| + \cdots + M \cdot |x| \cdot |y|^{n-1} + M \cdot |y|^n \\
&\leq M \cdot ((\max\{|x|, |y|\})^n + \cdots + (\max\{|x|, |y|\})^n) \\
&\leq M \cdot (n+1) \cdot (\max\{|x|, |y|\})^n.
\end{aligned}$$

Assim,

$$|x+y| \leq \sqrt[n]{M} \cdot \sqrt[n]{n+1} \cdot \max\{|x|, |y|\}.$$

Por fim, tomando o limite quando n tende a infinito, obtemos

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

■

Definição .1. *Sejam $|\cdot|$ e $|\cdot|_1$ valores absolutos em $\mathbb{Q}$. Diz-se que $|\cdot|$ é* ***equivalente*** *a $|\cdot|_1$ se, para $x \in \mathbb{Q}$, $|x| < 1$ implica $|x|_1 < 1$.*

A seguir, sempre consideraremos os valores absolutos definidos em $\mathbb{Q}$.

Exemplo .1. *Sejam $p, q \in \mathbb{N}$, primos distintos. O valor absoluto p-ádico não é equivalente ao valor absoluto q-ádico. De fato, $|q|_q = \frac{1}{q} < 1$. Por outro lado, $|q|_p = 1$.*

Exemplo .2. *Para qualquer natural primo p, o valor absoluto p-ádico não é equivalente ao valor absoluto real, visto que $|p|_p < 1$ e $|p|_\infty = p > 1$.*

Proposição .1. *Se $|\cdot|$ é equivalente a $|\cdot|_1$, então $|\lambda|_1 = 1$ sempre que $|\lambda| = 1$.*

Demonstração: Seja $\lambda \in \mathbb{Q}$ tal que $|\lambda| = 1$. Fixemos $\mu \in \mathbb{Q}$ tal que $0 < |\mu| < 1$. Para qualquer inteiro $n \geq 1$, segue que $|\lambda^n \cdot \mu| = |\lambda|^n \cdot |\mu| < 1$. Visto que $|\cdot|$ é equivalente a $|\cdot|_1$,

$$|\lambda^n \cdot \mu|_1 < 1 \Rightarrow |\lambda|_1^n \cdot |\mu|_1 < 1 \Rightarrow |\lambda|_1^n < \frac{1}{|\mu|_1} \Rightarrow |\lambda|_1 < \frac{1}{\sqrt[n]{|\mu|_1}}.$$

Como $\lim\limits_{n\to\infty} \sqrt[n]{|\mu|_1} = 1$, concluí-se que,

$$|\lambda|_1 \leq 1. \tag{.1}$$

Por outro lado, $|\lambda^{-1}| = |\lambda|^{-1} = 1$. Assim, de forma análoga a etapa anterior, $|\lambda^{-1}|_1 \leq 1$. Daí,

$$\begin{aligned} |\lambda^{-1}|_1 \leq 1 &\Rightarrow |\lambda|_1^{-1} \leq 1 \\ &\Rightarrow |\lambda|_1 \geq 1. \end{aligned} \tag{.2}$$

Portanto, pelas expressões (.1) e (.2), $|\lambda|_1 = 1$. ■

Corolário .1. *Se $|\cdot|$ é equivalente a $|\cdot|_1$, então $|\cdot|_1$ é equivalente a $|\cdot|$.*

Demonstração: Seja $\lambda \in \mathbb{Q}$ tal que $|\lambda|_1 < 1$. Se $|\lambda| = 1$, então, $|\lambda|_1 = 1$, absurdo. Por outro lado,

$$|\lambda| > 1 \Rightarrow |\lambda^{-1}| < 1 \Rightarrow |\lambda^{-1}|_1 < 1 \Rightarrow |\lambda|_1 > 1,$$

novamente, absurdo.

Portanto, $|\lambda| < 1$, ou seja, $|\cdot|_1$ é equivalente a $|\cdot|$. ■

Corolário .2. *Se $|\cdot|$ é equivalente a $|\cdot|_1$, então $|\lambda|_1 > 1$ sempre que $|\lambda| > 1$.*

Demonstração: Segue da demonstração do corolário anterior. ∎

A fim de facilitar a identificação de valores absolutos equivalentes, utiliza-se a seguinte proposição.

Proposição .2. *Sejam $|\cdot|, |\cdot|_1 : \mathbb{Q} \to \mathbb{R}$ valores absolutos equivalentes. Então, existe $\alpha > 0$ tal que $|\cdot|_1 = |\cdot|^\alpha$.*

Demonstração: Seja $\lambda \in \mathbb{Q}, \lambda \neq 0$. Fixemos $\mu \in \mathbb{Q}$ com $|\mu| > 1$, consequentemente, $|\mu|_1 > 1$. Consideremos $f : \mathbb{R} \to \mathbb{R}_+^*$, dada por $f(x) = |\mu|^x$. Como f é bijetiva, existe um único $\beta \in \mathbb{R}$ tal que $f(\beta) = |\lambda|$, ou seja,

$$|\mu|^\beta = |\lambda|. \tag{.3}$$

Consideremos $\dfrac{m}{n} \in \mathbb{Q}$, $\dfrac{m}{n} > \beta$. Como f é crescente, temos

$$|\mu|^{\frac{m}{n}} > |\mu|^\beta \Rightarrow |\mu|^{\frac{m}{n}} > |\lambda| \Rightarrow |\mu|^m > |\lambda|^n \Rightarrow \left|\frac{\mu^m}{\lambda^n}\right| > 1.$$

Portanto, $\left|\dfrac{\mu^m}{\lambda^n}\right|_1 > 1$. Daí,

$$|\mu|_1^m > |\lambda|_1^n \Rightarrow |\mu|_1^{\frac{m}{n}} > |\lambda|_1.$$

Tomando o limite $\dfrac{m}{n} \to \beta$ na desigualdade anterior, segue que

$$(|\mu|_1)^\beta \geq |\lambda|_1. \tag{.4}$$

Agora, consideremos $\dfrac{m}{n} \in \mathbb{Q}$, $\dfrac{m}{n} < \beta$. Então,

$$|\mu|^{\frac{m}{n}} < |\mu|^\beta \Rightarrow |\mu|^{\frac{m}{n}} < |\lambda| \Rightarrow |\mu|^m < |\lambda|^n \Rightarrow \left|\frac{\mu^m}{\lambda^n}\right| < 1.$$

Portanto, $\left|\dfrac{\mu^m}{\lambda^n}\right|_1 < 1$. Daí,

$$|\mu|_1^m < |\lambda|_1^n \Rightarrow |\mu|_1^{\frac{m}{n}} < |\lambda|_1.$$

Tomando o limite $\dfrac{m}{n} \to \beta$ na desigualdade anterior, segue que

$$(|\mu|_1)^\beta \leq |\lambda|_1. \tag{.5}$$

Pelas desigualdades (.4) e (.5), obtemos

$$(|\mu|_1)^\beta = |\lambda|_1. \tag{.6}$$

Tomando o logaritmo natural nas equações (.3) e (.6), obtemos, respectivamente,

$$\beta = \frac{\ln|\lambda|}{\ln|\mu|} \qquad \text{e} \qquad \beta = \frac{\ln|\lambda|_1}{\ln|\mu|_1}.$$

Daí, $\dfrac{\ln|\lambda|_1}{\ln|\lambda|} = \dfrac{\ln|\mu|_1}{\ln|\mu|}$.

Por fim, vamos assumir $\alpha = \dfrac{\ln|\mu|_1}{\ln|\mu|} > 0$, visto que, $|\mu|, |\mu|_1 > 1$. Então,

$$\frac{\ln|\lambda|_1}{\ln|\lambda|} = \alpha \Rightarrow \ln|\lambda|_1 = \ln|\lambda|^\alpha \Rightarrow |\lambda|_1 = |\lambda|^\alpha.$$

■

Observação .1. *Note que, na demonstração da proposição anterior, foi desconsiderado o caso em que* $|\mu| = 1$, *para todo* $\mu \neq 0$. *Neste caso,* $|\mu|_1 = 1$, *para todo* $\mu \neq 0$. *Portanto, qualquer* $\alpha > 0$ *satisfaz a igualdade* $|\cdot|_1 = |\cdot|^\alpha$.

Proposição .3. *Se existe* $\alpha > 0$ *tal que* $|\cdot|_1 = |\cdot|^\alpha$, *então* $|\cdot|_1$ *e* $|\cdot|$ *são equivalentes.*

Demonstração: Seja $\lambda \in \mathbb{Q}$ tal que $|\lambda|_1 < 1$. Então,

$$1 > |\lambda|_1 = |\lambda|^\alpha \Rightarrow 1^{\frac{1}{\alpha}} > |\lambda| \Rightarrow |\lambda| < 1.$$

Portanto, $|\cdot|_1$ e $|\cdot|$ são equivalentes. ■

Teorema .2 (Teorema de Ostrowski). *Se* $|\cdot|$ *é um valor absoluto não trivial em* $\mathbb{Q}$, *então* $|\cdot|$ *é equivalente ao valor absoluto real,* $|\cdot|_\infty$, *ou a algum valor absoluto p-ádico,* $|\cdot|_p$.

Demonstração: A prova do teorema segue das afirmações a seguir.

1. Sejam $m, n \in \mathbb{Z}$, $m, n \geq 2$. Então,

$$|m| \leq (\max\{1, |n|\})^{\frac{\ln m}{\ln n}}.$$

Realmente, pelo Teorema de Representação de um Número na Base n, existem inteiros $a_{i's}$, onde $0 \leq a_i < n$ e $a_r \neq 0$, de modo que $m = a_0 + a_1 \cdot n + \cdots + a_r \cdot n^r$. Além disso, para todo $0 \leq i < r$, tem-se

$$|a_i| = |\underbrace{1 + \cdots + 1}_{a_i \ parcelas}| \leq |1| + \cdots + |1| = a_i < n.$$

Daí,

$$\begin{aligned}|m| &= |a_0 + a_1 \cdot n + \cdots + a_r \cdot n^r| \\ &\leq |a_0| + |a_1| \cdot |n| + \cdots + |a_r| \cdot |n|^r \\ &\leq n + n \cdot |n| + \cdots + n \cdot |n|^r \\ &= n \cdot (1 + |n| + \cdots + |n|^r) \\ &\leq n \cdot (r+1) \cdot (\max\{1, |n|\})^r.\end{aligned}$$

Em contrapartida, como $m = a_0 + a_1 \cdot n + \cdots + a_r \cdot n^r$, então, $n^r \leq m$. Consequentemente, $r \leq \dfrac{\ln m}{\ln n}$. Assim,

$$n \cdot (r+1) \cdot (\max\{1, |n|\})^r \leq n \cdot \left(\frac{\ln m}{\ln n} + 1\right) \cdot (\max\{1, |n|\})^{\frac{\ln m}{\ln n}}.$$

Logo,

$$|m| \leq n \cdot \left(\frac{\ln m}{\ln n} + 1\right) \cdot (\max\{1, |n|\})^{\frac{\ln m}{\ln n}}.$$

Como a desigualdade vale para $m \in \mathbb{Z}$, $m \geq 2$, em particular, podemos aplicá-la para m^s, onde s é um inteiro positivo. Deste modo,

$$\begin{aligned}|m^s| &\leq n \cdot \left(\frac{\ln m^s}{\ln n} + 1\right) \cdot (\max\{1, |n|\})^{\frac{\ln m^s}{\ln n}} \\ \Rightarrow |m|^s &\leq n \cdot \left(s \cdot \frac{\ln m}{\ln n} + 1\right) \cdot (\max\{1, |n|\})^{s \cdot \frac{\ln m}{\ln n}} \\ \Rightarrow |m| &\leq \sqrt[s]{n} \cdot \sqrt[s]{s \cdot \frac{\ln m}{\ln n} + 1} \cdot (\max\{1, |n|\})^{\frac{\ln m}{\ln n}}.\end{aligned}$$

Tomando o limite de s tendendo a infinito na desigualdade acima, obtemos

$$|m| \leq (\max\{1, |n|\})^{\frac{\ln m}{\ln n}}.$$

2. Se $|k| > 1$ para todo inteiro $k \geq 2$, então $|\cdot|$ é equivalente a $|\cdot|_\infty$.

   Sejam $m, n \in \mathbb{Z}, m, n \geq 2$. Então, pela primeira afirmação,

$$|m| \leq (\max\{1, |n|\})^{\frac{\ln m}{\ln n}} \Rightarrow |m| \leq |n|^{\frac{\ln m}{\ln n}}.$$

   Daí,

$$\Rightarrow |m|^{\frac{1}{\ln m}} \leq |n|^{\frac{1}{\ln n}}. \tag{.7}$$

   Por outro lado, trocando os valores de m por n e de n por m, obtemos,

$$|n|^{\frac{1}{\ln n}} \leq |m|^{\frac{1}{\ln m}}. \tag{.8}$$

   Deste modo, por (.7) e (.8), para quaisquer m e n inteiros, $m, n \geq 2$,

$$|n|^{\frac{1}{\ln n}} = |m|^{\frac{1}{\ln m}}. \tag{.9}$$

Como $m \geq 2$, temos $\ln m \geq \ln 2 > 0$, e portanto, $\dfrac{1}{\ln m} > 0$. Pela hipótese, $|m| > 1$. Logo, a função $f : \mathbb{R} \to \mathbb{R}_+^*$, dada por $f(x) = |m|^x$, é crescente. Daí,

$$f\left(\frac{1}{\ln m}\right) > f(0) \Rightarrow |m|^{\frac{1}{\ln m}} > 1.$$

Pelo mesmo argumento, garantimos que $|n|^{\frac{1}{\ln n}} > 1$.

Consideremos a função $g : \mathbb{R} \to \mathbb{R}_+^*$, $g(x) = e^x$. Como g é bijetiva e $|m|^{\frac{1}{\ln m}} > 0$, existe um $\alpha \in \mathbb{R}$ tal que $g(\alpha) = e^\alpha = |m|^{\frac{1}{\ln m}}$, para qualquer inteiro $m \geq 2$. Cabe ressaltar que, por (.9), α é uniforme. Além disso, como g é crescente,

$$g(\alpha) = e^\alpha = |m|^{\frac{1}{\ln m}} > 1 = g(0) \Rightarrow \alpha > 0.$$

Provaremos que $|\lambda| = (|\lambda|_\infty)^\alpha$, para todo $\lambda \in \mathbb{Q}$. Realmente, temos os seguintes casos:

a) $\lambda = 0$: Neste caso, pela definição de valor absoluto, segue que

$$|\lambda| = |0| = 0 = 0^\alpha = (|0|_\infty)^\alpha = (|\lambda|_\infty)^\alpha;$$

b) $\lambda = 1$: Pela Proposição 2.5, temos

$$|\lambda| = |1| = 1 = 1^\alpha = (|1|_\infty)^\alpha = (|\lambda|_\infty)^\alpha;$$

c) $\lambda \in \mathbb{N}, \lambda \geq 2$: Vimos anteriormente que, para qualquer inteiro $m \geq 2$, existe $\alpha \in \mathbb{R}$, tal que $|m|^{\frac{1}{\ln m}} = e^\alpha$. Consideremos $\lambda = m$, então,

$$|\lambda|^{\frac{1}{\ln \lambda}} = e^\alpha \Rightarrow |\lambda| = e^{\alpha \cdot \ln \lambda} = e^{\ln \lambda^\alpha} = \lambda^\alpha = (|\lambda|_\infty)^\alpha$$

$$\Rightarrow |\lambda| = (|\lambda|_\infty)^\alpha.$$

d) $\lambda \in \mathbb{Z}, \lambda < 0$: Pela Proposição 2.5, $|\lambda| = |-\lambda|$, ademais, $|-\lambda| = (|-\lambda|_\infty)^\alpha = (|\lambda|_\infty)^\alpha$. Logo, $|\lambda| = (|\lambda|_\infty)^\alpha$.

e) $\lambda \in \mathbb{Q}$: Seja $\lambda = \dfrac{m}{n}$, onde $m, n \in \mathbb{Z}, n \neq 0$. Pelos itens anteriores, temos

$$|\lambda| = \left|\frac{m}{n}\right| = \frac{|m|}{|n|} = \frac{(|m|_\infty)^\alpha}{(|n|_\infty)^\alpha} = \left(\left|\frac{m}{n}\right|_\infty\right)^\alpha = (|\lambda|_\infty)^\alpha,$$

Portanto, para qualquer $\lambda \in \mathbb{Q}$, $|\lambda| = (|\lambda|_\infty)^\alpha$. Portanto, pela Proposição .3, $|\cdot|$ é equivalente a $|\cdot|_\infty$ em $\mathbb{Q}$.

3. Se $|k| \leq 1$ para algum inteiro $k \geq 2$, então $|\cdot|$ é equivalente a $|\cdot|_p$, para algum p primo.

Considerando a desigualdade provada no primeiro item, tomando $n = k$, concluímos, pela hipótese, que $|m| \leq 1$ para todo m inteiro, $m \geq 2$. Logo, $|m| \leq 1$, para todo $m \in \mathbb{Z}$. Pelo Teorema .1, o valor absoluto $|\cdot|$ é não arquimediano. Ademais, como $|\cdot|$ não é o valor absoluto trivial, existe um inteiro $l \geq 2$ tal que $|l| < 1$.

Consideremos o conjunto

$$I = \{n \in \mathbb{Z}; |n| < 1\}.$$

Note que, $I \subset \mathbb{Z}, I \neq \{0\}$, e, dados $x \in I$ e $y \in \mathbb{Z}$, temos

$$|x \cdot y| = |x| \cdot |y| \leq |x| < 1,$$

logo, $x \cdot y \in I$. Portanto, I é um ideal de $\mathbb{Z}$ pela direita e, pela comutatividade em $\mathbb{Z}$, I é um ideal de $\mathbb{Z}$ pela esquerda. Em suma, I é um ideal de $\mathbb{Z}$, consequentemente, como $\mathbb{Z}$ é domínio principal (ver (5), página 20), segue que

$$I = p \cdot \mathbb{Z} = \{p \cdot k; k \in \mathbb{Z}\},$$

para algum $p \in \mathbb{Z}_+$.

Vimos que $I \neq \{0\}$ e, como $1 \notin I$, $I \neq \mathbb{Z}$. Desse modo, p deve ser um inteiro maior ou igual a 2. Mostraremos que p é primo. Realmente, suponhamos $p = p_1 \cdot p_2$, onde $p_1, p_2 \in \mathbb{Z}$. Como $p \in I$,

$$|p| < 1 \Rightarrow |p_1 \cdot p_2| < 1 \Rightarrow |p_1| \cdot |p_2| < 1 \Rightarrow |p_1| < 1 \text{ ou } |p_2| < 1.$$

Vamos avaliar cada um dos casos que derivam da afirmação acima. Assim,

a) $|p_1| < 1$ e $|p_2| \geq 1$: Então, $p_1 \in I$ e $|p_2| = 1$, consequentemente, $p \mid p_1$ e $p_2 = \pm 1$, implicando em $p_1 = \pm p$;

b) $|p_1| \geq 1$ e $|p_2| < 1$: Segue de forma análoga ao caso acima;

c) $|p_1| < 1$ e $|p_2| < 1$: Neste caso, $p_1, p_2 \in I$, logo, existem $k_1, k_2 \in \mathbb{Z}$ tal que $p_1 = p \cdot k_1$ e $p_2 = p \cdot k_2$, consequentemente,

$$p = p_1 \cdot p_2 = (p \cdot k_1) \cdot (p \cdot k_2) = p^2 \cdot k_1 \cdot k_2 \Rightarrow 1 = p \cdot k_1 \cdot k_2$$

absurdo, visto que, $p \geq 2$.

Desse modo, concluímos que os únicos valores para p_1 e p_2 são $p_1 = \pm p$ e $p_2 = \pm 1$ ou vice-versa, caracterizando p como um número primo.

Consideremos $c = |p|$, desse modo, $0 < c < 1$. Então, tomemos $\alpha = -\dfrac{\ln c}{\ln p}$. Note que $\alpha > 0$. Realmente, como $0 < c < 1$, temos $\ln c < 0$. Por outro lado, como $p \geq 2$, segue que $\ln p > 0$. Assim,

$$\alpha = -\frac{\ln c}{\ln p} > 0.$$

Mostraremos que,

$$|\lambda| = (|\lambda|_p)^\alpha,$$

para todo $\lambda \in \mathbb{Q}$. De fato, temos os seguintes casos:

a) $\lambda = 0$: Neste caso, pela própria definição de valor absoluto, segue que

$$|\lambda| = |0| = 0 = 0^\alpha = (|0|_p)^\alpha = (|\lambda|_p)^\alpha;$$

b) $\lambda = 1$: Pela Proposição 2.5, temos

$$|\lambda| = |1| = 1 = 1^\alpha = (|1|_p)^\alpha = (|\lambda|_p)^\alpha;$$

c) $\lambda \in \mathbb{Z}$: Suponhamos $\lambda \neq 0$ e $\lambda \neq 1$, visto que estes casos já foram provados. Pelo Teorema Fundamental da Aritmética, existe um único $n \in \mathbb{N}$ e um único $s \in \mathbb{Z}$, onde s é um produto de primos e $p \nmid s$, tal que $\lambda = \mu \cdot p^n \cdot s, \mu \in \{-1, 1\}$.

Note que $|s| = 1$, pois se $|s| < 1$, teríamos $s \in I$, consequentemente, $p \mid s$, absurdo. Daí,

$$|\lambda| = |\mu \cdot p^n \cdot s| = |\mu| \cdot |p^n| \cdot |s| = |p|^n = c^n.$$

Em contrapartida,

$$(|\lambda|_p)^\alpha = (p^{-n})^\alpha = p^{n \cdot \frac{\ln c}{\ln p}} = \left(p^{\frac{\ln c}{\ln p}}\right)^n = \left(e^{\ln p \cdot \frac{\ln c}{\ln p}}\right)^n = \left(e^{\ln c}\right)^n = c^n = |\lambda|.$$

Logo, $|\lambda| = (|\lambda|_p)^\alpha, \lambda \in \mathbb{Z}$.

d) $\lambda \in \mathbb{Q}$: Seja $\lambda = \dfrac{m}{n}$, onde $m, n \in \mathbb{Z}, n \neq 0$. Utilizando os itens anteriores, temos

$$|\lambda| = \left|\frac{m}{n}\right| = \frac{|m|}{|n|} = \frac{(|m|_p)^\alpha}{(|n|_p)^\alpha} = \left(\left|\frac{m}{n}\right|_p\right)^\alpha = (|\lambda|_p)^\alpha.$$

Portanto, para qualquer $\lambda \in \mathbb{Q}$, $|\lambda| = (|\lambda|_p)^\alpha$, consequentemente, pela Proposição .3, $|\cdot|$ é equivalente a $|\cdot|_p$ em $\mathbb{Q}$.

■

Diante do Teorema de Ostrowski, concluímos que, a menos de equivalência, os possíveis valores absolutos em $\mathbb{Q}$ são:

1. Valor Absoluto Trivial;
2. Valor Absoluto Real;
3. Valor Absoluto p–ádico, para p primo.

Portanto, como $\mathbb{Q}$ é completo quando munido do valor absoluto trivial, segue que os únicos completamentos de $\mathbb{Q}$, são:

1. O corpo dos números reais, $\mathbb{R}$, proveniente do valor absoluto real;
2. O corpo dos números p-ádicos, $\mathbb{Q}_p$, proveniente do valor absoluto p–ádico.