UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

DANILO EDUARDO BARROS

NÚMEROS P-ÁDICOS E O TEOREMA DE MONSKY

FORTALEZA

2019

DANILO EDUARDO BARROS

NÚMEROS P-ÁDICOS E O TEOREMA DE MONSKY

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Alberto Duarte Maia

FORTALEZA

2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B276n Barros, Danilo Eduardo.
Números p-ádicos e o teorema de Monsky / Danilo Eduardo Barros. – 2019.
60 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2019.
Orientação: Prof. Dr. José Alberto Duarte Maia.

1. Teorema de Monsky. 2. Lema de Sperner. 3. Números p-ádicos. I. Título.

CDD 510

DANILO EDUARDO BARROS

NÚMEROS P-ÁDICOS E O TEOREMA DE MONSKY

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Aprovada em: 02/08/2019

BANCA EXAMINADORA

Prof. Dr. José Alberto Duarte Maia (Orientador)
Universidade Federal do Ceará (UFC)

Prof. José Afonso de Oliveira
Universidade Federal do Ceará (UFC)

Prof. Dr. Francisco Régis Vieira Alves
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Aos meus pais.

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão às pessoas que tornaram possível a conclusão da minha dissertação. Em primeiro lugar, agradeço aos meus pais, Hélio e Maria, por todo o apoio emocional e financeiro que me proporcionaram durante este período. Sou imensamente grato por vocês me aturarem nos momentos de frustração e desânimo.

Gostaria de agradecer também a minha tia Rita e minha prima Talyta por todo o acolhimento e suporte nesses dois anos e meio de curso. Obrigado por sempre me ouvirem e me encorajarem nos momentos difíceis.

Um agradecimento especial ao meu orientador, o Prof. Dr. José Alberto, por sua disponibilidade, orientação e compreensão. Seus insights e conhecimentos foram cruciais para a conclusão deste trabalho.

Agradeço também a todos os meus colegas de curso pelas conversas e discussões que tanto me motivaram e mantiveram meu interesse pela Matemática. Sem a sua presença e apoio, não teria sido possível chegar até aqui.

Por fim, gostaria de agradecer a todos os professores do programa por todo o conhecimento e orientação transmitidos. E, é claro, a todos que contribuíram de alguma forma para a conclusão deste trabalho.

"O coração da matemática são seus próprios problemas." (HALMOS, 1983, p. 214)

RESUMO

O Teorema de Monsky afirma que um quadrado não pode ser dividido em um número ímpar de triângulos de mesma área. No presente trabalho apresentamos a demonstração desse fato, bem como os conceitos e resultados nescessários para entende-la. A Introdução contem o contexto histórico e algumas tentativas de provar o teorema. Nos capítulos dois e três vemos dois resultados importantes usados na prova: o Lema de Sperner e o Teorema de Chevalley. O capítulo três também contém a construção do corpo dos números p-ádicos e algumas de suas propriedades. No capítulo quatro temos a demonstração do Teorema de Monsky e discutimos possíveis generalizações e problemas em aberto.

Palavras-chave: teorema de Monsky; lema de Sperner; números p-ádicos.

ABSTRACT

Monsky's Theorem states that a square cannot be divided into an odd number of triangles of the same area. In the present work we present the demonstration of this fact, as well as the concepts and results needed to understand it. The Introduction contains the historical context and some attempts to prove the theorem. In chapters two and three we see two important results used in the proof: Sperner's Lemma and Chevalley's Theorem. Chapter three also contains the construction of p-adic numbers field and some of their properties. In chapter four we have the proof of Monsky's Theorem and discuss possible generalizations and open problems.

Keywords: Monsky's theorem; Sperner's lemma; p-adic numbers.

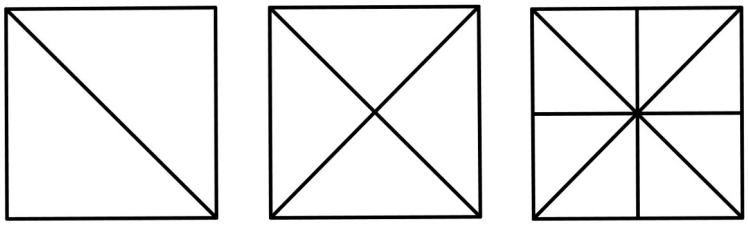
LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Consideremos um quadrado. É fácil dividi-lo em 2, 4 e até mesmo 8 triângulos de mesma área:

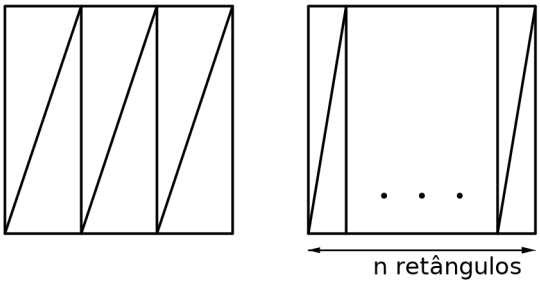
Figura 1 – 2, 4 e 8 triângulos de mesma área



Fonte: elaborada pelo autor.

Pensando mais um pouco, descobrimos que é possível dividi-lo em qualquer número par de triângulos de mesma área. De fato, se quisermos 2n triângulos, com $n > 0$, basta dividir o quadrado em n retângulos de mesma área e traçar uma diagonal de cada retângulo:

Figura 2 – 6 e 2n triângulos de mesma área.



Fonte: elaborada pelo autor.

Isto sugere a seguinte questão:

Será possível dividir um quadrado em um número ímpar de triângulos não sobrepostos e de mesma área?

O matemático americano Fred Richman se deparou com esse problema em 1965 enquanto preparava um exame de mestrado e o publicou no periódico The American Mathematical Monthly (1967, página 329). Desde então foram feitas várias tentativas de resolver o problema, inclusive pelo próprio Richman que conseguiu demonstrar

- a impossibilidade da divisão para 3 e 5 triângulos;

- que se a divisão é possível para n triângulos, então também é possível para n + 2, ou seja, se a construção vale para algum número ímpar, vale para todos os números ímpares maiores do que ele;
- e que quadriláteros com ângulos arbritariamente próximos de 90 º podem ser divididos em um número ímpar de triângulos de mesma área.

Em 1968, John Thomas, da Universidade do Estado do Novo México, provou que a resposta para um caso particular do problema de Richman é negativa: Consideremos o quadrado de vértices $(0,0)$, $(1,0)$, $(1,1)$ e $(0,1)$ no plano cartesiano, é impossível dividi-lo em um número ímpar n de triângulos de mesma área com vértices de coordenadas racionais com denominadores ímpares.

A solução de Thomas envolve a classificação dos vértices dos triângulos em quatro tipos, de acordo com a paridade dos numeradores das coordenadas. Ele prova que se a construção for possível, então existe um triângulo com três tipos específicos de vértices. Calculando a área desse triângulo usando as coordenadas dos vértices e comparando o resultado com o valor esperado, $\frac{1}{n}$, chegamos a uma contradição. Aproximadamente dois anos depois, Paul Monsky, matemático estadunidense da Universidade Brandeis, completou o resultado de John Thomas, mostrando que

É impossível dividir um quadrado em número ímpar de triângulos não sobrepostos, todos de mesma área.

A prova do Teorema de Monsky usa resultados de duas áreas distintas da matemática (o Lema de Sperner, da combinatória, e a Teoria de Valorizações, da Álgebra), criando uma nova forma de abordar problemas parecidos e, de certo modo, é a única demonstração do teorema conhecida ate hoje.

2 LEMA DE SPERNER

Em 1911, o matemático holandês Luitzen Brouwer publicou o seu famoso teorema do ponto fixo:

Toda função contínua $f : B^n \to B^n$ *de uma bola n-dimensional nela mesma possui um ponto fixo, ou seja, um ponto* $x \in B^n$ *tal que* $f(x) = x$.

O teorema acima, cujos termos usados no enunciado serão definidos posteriormente, tem várias interpretações interessantes. Uma delas é a seguinte: Um recipiente com água inicialmente em repouso é movimentado de modo que toda a água permaneça em seu interior. Então, a todo instante existe uma molécula de água que ocupa a mesma posição que ocupava quando o recipiente estava em repouso. Aqui o recipiente com água é a “bola"e o ato de movimenta-lo a função contínua.

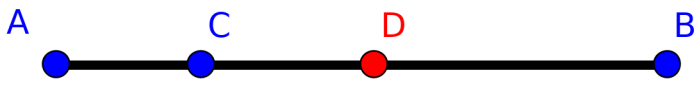
A demonstração do teorema do ponto fixo de Brouwer para o caso n-dimensional não é simples, ou pelo menos não era até 1928, quando o matemático alemão Emanuel Sperner, com apenas 23 anos, provou um belo resultado combinatório do qual o Teorema do ponto fixo de Brouwer pode ser deduzido mais facilmente e que terá papel importante na demonstração do Teorema de Monsky.

O objetivo desse capítulo é enunciar e provar o Lema de Sperner para os casos uni, bi e n-dimensional. Encerraremos com a demonstração do Teorema do ponto fixo de Brower.

2.1 Lema de Sperner para Segmentos

Seja S um segmento de reta cujas extremidades mais um número finito de pontos interiores foram coloridos usando as cores 1 e 2. Dizemos que um subsegmento S’⊂ S é primitivo e que suas extremidades são adjacentes, se S’ não possuir pontos coloridos além das próprias extremidades. Dizemos que S é do tipo 12 se suas extremidades tiverem cores diferentes.

Figura 3 – As cores 1 e 2 são azul e vermelho, nessa ordem. Os subsegmentos AC, CD e BD são primitivos, enquanto AB e BC não são. Os segmentos CD e BD são do tipo 12, enquanto AC não é

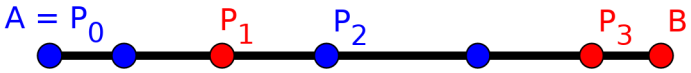


Fonte: elaborada pelo autor.

Lema 2.1. Se S é um segmento de reta do tipo 12, então ele contem um número ímpar de subsegmentos primitivos do tipo 12. Caso contrário, ou seja, caso S tenha as extremidades de mesma cor, o número de tais subsegmentos é par.

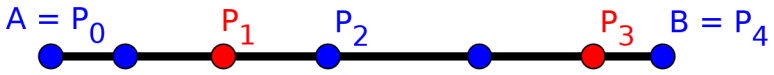
Demonstração. Suponhamos que S tem extremidades A, B e que seja orientado de A para B. Sejam $P_0 = A$ e P_{k+1} o ponto mais próximo de P_k, à direita, com cor diferente de P_k (se tal ponto existir). Conseguimos assim uma sequência de pontos $P_0, P_1, P_2, \ldots P_n$ com cores que se alternam e onde P_n tem a mesma cor que B. É fácil ver que cada um dos n segmentos P_kP_{k+1} contem um único subsegmento primitivo do tipo 12, em que P_{k+1} é uma das extremidades. Logo n é o número de subsegmentos primitivos do tipo 12 contidos em S. Daí, se S for do tipo 12, ou seja, se A e B tiverem cores diferentes, então n é ímpar. Caso contrário, ou seja, caso A e B tenham a mesma cor, n é par. □

Figura 4 – Segmento do tipo 12, três subsegmentos primitivos do tipo 12



Fonte: elaborada pelo autor.

Figura 5 – Extemidades de mesma cor, 4 subsegmentos primitivos do tipo 12



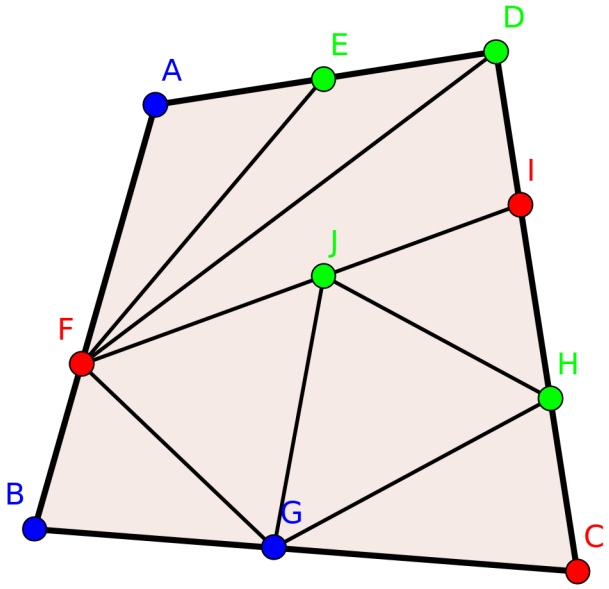
Fonte: elaborada pelo autor.

2.2 Lema de Sperner para Polígonos

Seja R um polígono. Consideremos uma dissecção de R, ou seja, a divisão de R em um número finito de triângulos T_i não sobrepostos. Chamaremos de vértices e lados, respectivamente, os vértices e lados de R ou de algum T_i. Consideremos também uma coloração dos vértices usando três cores 1, 2 e 3, de modo que nenhum lado contenha vértices das três cores. Um triângulo T_i será dito completo se possuir vértices das três cores.

Lema 2.2. Se R tem um número ímpar de lados do tipo 12, então existe um triânguloT_i completo.

Figura 6 – Os triângulos AFE, FGJ e CGH são completos

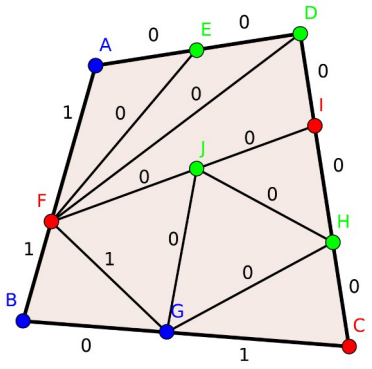


Fonte: elaborada pelo autor.

Observação: o lema acima também pode ser enunciado e provado olhando para todos os lados com extremidades de cores diferentes, não apenas para os lados do tipo 12.

Demonstração. Vamos atribuir pesos a cada subsegmento primitivo de modo que eles recebam peso 1 se forem do tipo 12 e peso 0, caso contrário. Definimos o peso de um triângulo como a soma dos pesos dos subsegmentos primitivos que compõem os seus lados.

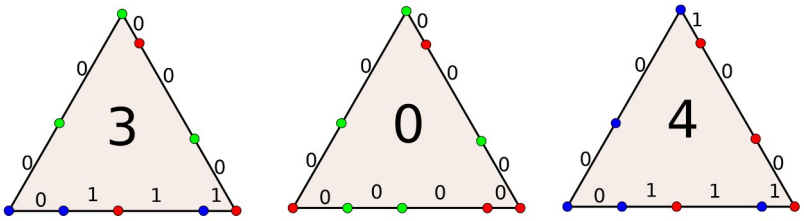
Figura 7 – As cores 1, 2 e 3 são azul, vermelho e verde, respectivamente. O triângulo ADF tem peso 1, o triângulo BFG tem peso 2 e o triângulos DFI tem peso 0



Fonte: elaborada pelo autor.

Note que se um triângulo é completo, então ele tem peso ímpar, pois possui um único lado do tipo 12 que, pelo lema 2.1, contem um número ímpar de subsegmentos primitivos do tipo 12. Caso contrário, ou seja, se um triângulo não é completo, então ele tem 0 ou 2 lados do tipo 12 e consequentemente tem peso par.

Figura 8 – O número grande no interior do triângulo representa seu peso



Fonte: elaborada pelo autor.

Sejam F e I a soma dos pesos dos subsegmentos primitivos na fronteira e no interior de R, respectivamente, e T a soma dos pesos de todos os triângulos T_i. Observe que, no cálculo de T, cada subsegmento primitivo no interior de R contribui duas vezes com seu peso, pois está contido na fronteira de dois triângulos ao mesmo tempo, enquanto cada subsegmento primitivo na fronteira de R contribui uma vez. Daí,

$$T = F + 2I. \tag{2.1}$$

Porém F é ímpar, pois R possui um número ímpar de lados do tipo 12 e, pelo lema 2.1, cada um desses lados possui um número ímpar de subsegmentos primitivos do tipo 12 (e a soma de uma quantidade ímpar de números ímpares é sempre ímpar). Portanto T é ímpar e, consequentemente, deve existir algum triângulo T_i de peso ímpar, ou seja, um triângulo completo. □

2.3 Espaço e Dimensão

Segundo (COXETER, 1973), existem três maneiras de desenvolver a geometria de quatro ou mais dimensões: a axiomática, a algébrica (ou analítica) e a intuitiva. Poucas pessoas tem a capacidade de visualizar com naturalidade objetos com mais de três dimensões. Por isso, a abordagem intuitiva, onde a geometria n-dimensional é desenvolvida por meio de analogias com dimensões menores, mostra-se bem proveitosa. Porém essa abordagem apresenta algumas falhas. Por exemplo, o comprimento de um cículo é $2\pi R$, a área da superfície de uma esfera é $4\pi R^2$, mas a superfície de uma esfera 4-dimensional é $2\pi^2 R^3$ (resultado não muito intuitivo). Falhas como essa podem ser corrigidas apelando-se para ferramentas algébricas ou analíticas. É o que faremos nesse trabalho.

Grosso modo, a dimensão de um espaço (ou de um objeto) é o menor número de parâmetros nescessários para descrever um ponto dentro dele: uma reta tem dimensão 1, pois

cada ponto dela fica determinado por um único número real; um plano e a superfície de uma esfera tem dimensão 2, pois cada ponto dele(a) fica determinado por um par de números reais - lembre da latitude e da longitude que usamos para localizar pontos na superfície de nosso planeta (que é quase esférico); já o interior de um cubo ou de uma esfera tem dimensão 3, pois são nescessários três números reais para localizar um ponto dentro deles. Seguindo com esse raciocínio, um espaço ou objeto *n*-dimensional é aquele em que cada ponto pode ser descrito usando uma lista de *n* números reais. Isso motiva a seguinte

Definição 2.1. Seja n um número natural. O espaço euclidiano n-dimensional, denotado por $\mathbb{R}^n$, é o conjunto formado por todas as listas ordenadas de n números reais, ou seja,

$$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) | x_1, \ldots, x_n \in \mathbb{R}\}.$$

Dados $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$ em $\mathbb{R}^n$ tem-se $x = y$ se, e somente se $x_1 = y_1, ..., x_n = y_n$.

Particularmente, $\mathbb{R}^1 = \mathbb{R}$ é a reta numérica, ou seja, o conjunto dos números reais, $\mathbb{R}^2$ é o plano cartesiano, e $\mathbb{R}^3$ o espaço euclidiano tridimensional.

Dados $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$ em $\mathbb{R}^n$ e um número real α, podemos introduzir uma estrutura em $\mathbb{R}^n$ definindo a soma $x + y$ e o produto $\alpha \cdot x$ do seguinte modo

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n),$$
$$\alpha \cdot x = (\alpha x_1, \ldots, \alpha x_n).$$

Também podemos definir uma distância entre elementos do $\mathbb{R}^n$ generalizando as fórmulas para o cálculo de distância no plano e no espaço tridimensional. A distância entre x e y é

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + \ldots + (x_n - y_n)^2}.$$

Veremos agora a definição de simplexo que é uma generalização de triângulo ou de tetraedro para dimensões arbitrárias.

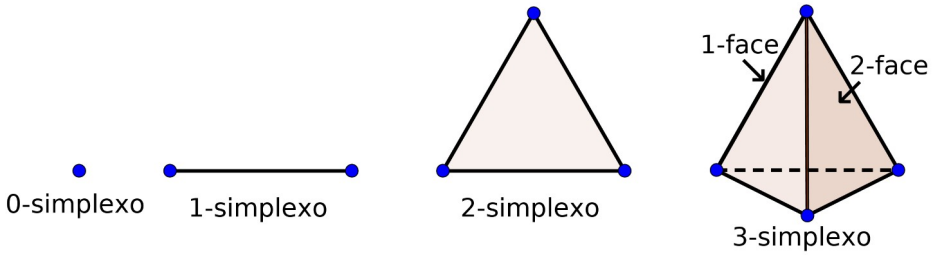
Definição 2.2. Dados $v_1, v_2, \ldots, v_{n+1} \in \mathbb{R}^{n+1}$, com $v_2 - v_1, v_3 - v_1, \ldots, v_{n+1} - v_1$ linearmente independentes, um simplexo n-dimensional, ou n-simplexo, de vértices $v_1, v_2, \ldots, v_{n+1}$ é o conjunto

$$S = \left(\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_{n+1} v_{n+1} \;\middle|\; \alpha_i \geq 0, \sum_{i=1}^{n+1} \alpha_i = 1 \right).$$

Uma face *k*-dimensional, ou *k*-face, de S, onde $0 \leq k \leq n - 1$, é um simplexo *k*-dimensional determinado por $k + 1$ vértices de S.

Por exemplo, um 0-simplexo é um ponto, um 1-simplexo é um segmento de reta, um 2-simplexo é um triângulo e um 3-simplexo é um tetraedro. Em um tetraedro, as faces 2-dimensionais são as faces triângulares do tetraedro e as faces 1-dimensionais são as arestas do tetraedro.

Figura 9 – Simplexos de dimesão 0, 1, 2 e 3



Fonte: elaborada pelo autor.

2.4 Lema de Sperner para Simplexos

Definição 2.3. Uma subdivisão simplicial de um simplexo n-dimensional S é a partição de S em simplexos n-dimensionais menores (que chamaremos de “células") tais que quaisquer duas células são disjuntas ou compartilham uma face inteira de certa dimensão.

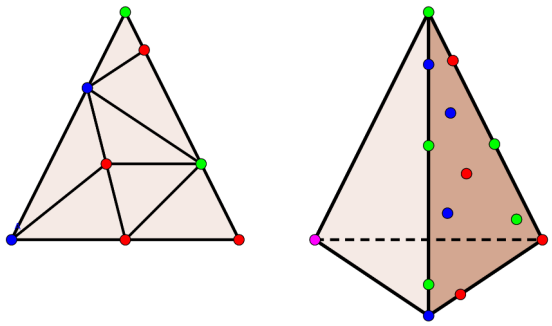
Definição 2.4. Seja S um simplexo n-dimensional. Uma coloração própria de uma subdivisão simplicial de S é a atribuição de cores 1, 2, ..., n, n + 1 aos vértices da subdivisão de modo que

(i) os vértices de S tenham cores diferentes;

(ii) vértices que pertencem a uma face de S (de qualquer dimensão) têm as mesmas cores que os vértices de S que determinam tal face.

Uma célula é dita completa se seus vértices têm cores diferentes.

Figura 10 – Coloração própria de uma subdivisão simplicial de um triângulo e de um tetraedro



Fonte: elaborada pelo autor.

Por exemplo, para n = 2, temos a subdivisão de um triângulo T em células triângulares que são disjuntas ou têm um vértice ou um lado inteiro em comum (essa condição é mais forte do que a imposta no lema 2.2, pois lá um vértice de uma célula triangular poderia pertencer ao interior do lado de outra célula triângular).

Uma coloração própria dessa subdivisão atribui cores diferentes aos vértices de T e vértices interiores a um lado de T recebem somente as cores das extremidades desse lado.

Lema 2.3. Seja S um simplexo n-dimensional. Toda coloração própria de uma subdivisão simplicial de S contem uma célula completa.

Demonstração. Provaremos, por indução sobre n, que o número de células completas é ímpar. Nas seções anteriores, demonstramos o lema para n = 1 e n = 2. Suponhamos então que o resultado vale para algum inteiro positivo k e consideremos uma coloração própria de uma subdivisão simplicial de um simplexo S de dimensão k + 1. Note que k + 2 cores são usadas.

Vamos atribuir pesos as k-faces das células da subdivisão de modo que elas recebam peso 1 se seus vértices tiverem cores 1, 2, ..., k + 1 e recebam peso 0, caso contrário. Definimos o peso de uma célula como a soma dos pesos de suas k-faces. Assim, uma célula completa tem peso 1, pois ela possui exatamente uma k-face com vértices de cores 1, 2, ..., k, k + 1, enquanto uma célula que não é completa tem peso

- 0, se pelo menos uma das cores 1, 2, ..., k + 1 não for usada em seus vértices;
- 2, se exatamente uma das cores 1, 2, ..., k + 1 for usada duas vezes, enquanto as outras são usadas uma única vez.

Sejam F e I as somas dos pesos das k-faces de célula na fronteira e no interior de S, respectivamente, e C a soma dos pesos de todas as células. No cálculo de C, as k-faces de celula na fronteira contribuem uma vez com seu peso, pois pertencem a uma única célula, enquanto as k-faces de célula no interior de S contribuem duas vezes, já que pertencem a exatamente duas células. Daí, temos a seguinte igualdade

$$C = F + 2I.$$

Seja S' a única k-face de S com vértices de cores 1, 2, ..., k + 1. S' é um simplexo de dimensão k subdivido em células de dimensão k pelos vértices da subdivisão original. Pela hipótese de indução, S' possui um número ímpar de células de dimensão k completas, ou seja, com vértices de cores 1, 2, ..., k + 1. Logo F é ímpar e, consequentemente, C é ímpar. Portanto existe uma célula de dimensão k + 1 completa. □

2.5 Teorema do Ponto Fixo de Brouwer

Como aplicação do caso geral do Lema de Sperner, demonstraremos o teorema do ponto fixo enunciado no início do capítulo. Mas antes, precisamos ver alguns conceitos nescessários para o entendimento da prova.

Definição 2.5. Seja n um número natural. Dados $a \in \mathbb{R}^n$ e $r > 0$, uma *bola fechada* n-dimensional de centro a e raio r é o conjunto de todos os pontos do $\mathbb{R}^n$ que estão a uma distância menor do que ou igual a r de a, no sentido da definição 1. Em símbolos:

$$B^n[a,r] = \{x \in \mathbb{R}^n \mid d(x,a) \leq r\}.$$

Analogamente, definimos uma *bola aberta* n-dimensional de centro a e raio r como o conjunto

$$B^n(a,r) = \{x \in \mathbb{R}^n \mid d(x,a) < r\}.$$

Quando não houver dúvidas quanto ao centro, ao raior e ao fato da bola ser fechada ou aberta, escreveremos simplesmente B^n em vez de $B^n[a,r]$ ou $B^n(a,r)$.

Uma bola é a generalização da ideia de círculo ou de esfera para espaços de dimensão arbitrária: B^3 é uma esfera, B^2 é um círculo, e B^1 é um intervalo.

Definição 2.6. Sejam X um subconjunto não vazio do $\mathbb{R}^n$ e $a \in \mathbb{R}^n$. Dizemos que uma função $f : X \to \mathbb{R}^n$ é contínua em a se $a \in X$ e, para todo $\varepsilon > 0$, existe $\delta > 0$ tal que

$$\forall x \in X,\ d(x,a) < \delta \Rightarrow d(f(x),f(a)) < \varepsilon.$$

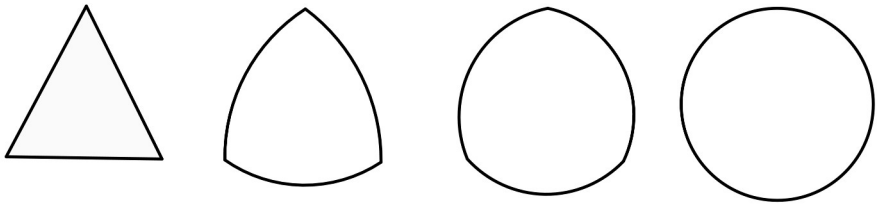
Dizemos que uma função é contínua se ela for contínua em todos os pontos do seu domínio.

Intuitivamente, uma função é contínua se pequenas variações nos elementos de seu domínio correspondem a pequenas variações nas imagens desses elementos.

Definição 2.7. Sejam M e N subconjuntos não vazios do $\mathbb{R}^n$. Um homeomorfismo é uma função $f : M \to N$, bijetiva, contínua e cuja inversa $f^{-1} : N \to M$ também é contínua. Se tal função existir, os conjuntos M e N são ditos homeomorfos.

Grosso modo, dois objetos são homeomorfos se um deles puder ser deformado continuamente (sem rasgos ou furos) transformando-se no outro. Um triângulo é homeomorfo a um círculo, como indica a figura abaixo, e mais geralmente um simplexo n-dimensional é homeomorfo a uma bola fechada n-dimensional. Fato que admitiremos sem prova.

Figura 11 – Homeomorfismo entre um triângulo e um círculo



Fonte: elaborada pelo autor.

Definição 2.8. Seja C um conjunto não vazio. Uma sequência de elementos de C é uma função $f : \mathbb{N} \to C$. O valor de f em n é chamado n-ésimo termo da sequência e denotado por x_n. A sequência passa então a ser representada por $(x_n) = (x_1, x_2, x_3, \ldots)$

Uma subsequência $(x_m)_{m\in A}$ de (x_n) é uma restrição de (x_n) a um subconjunto infinito $A = \{n_1 < n_2 < n_3 < \ldots\}$ de números naturais, ou seja, $(x_m)_{m\in A} = (x_{n_1}, x_{n_2}, x_{n_3}, \ldots)$

Uma sequência pode ser pensada como uma lista infinita e ordenada de elementos de um conjunto, enquanto uma subsequência é o que sobra quando apagamos alguns (ou até mesmo infinitos) termos de uma sequência, deixando ainda uma quantidade infinita dos mesmos.

Definição 2.9. Uma sequência (x_n) de elementos do $\mathbb{R}^n$ é dita convergente se os seus termos ficarem cada vez mais próximos de algum ponto do $\mathbb{R}^n$. Formalmente, se existe $a \in \mathbb{R}^n$ tal que, para todo $\varepsilon > 0$, existe um número natural n_0 de modo que

$$n > n_0 \Rightarrow d(x_n, a) < \varepsilon.$$

Se existir, o ponto a é chamado de limite da sequência e denotado por $\lim_{n\to\infty} x_n$ ou simplesmente $\lim x_n$.

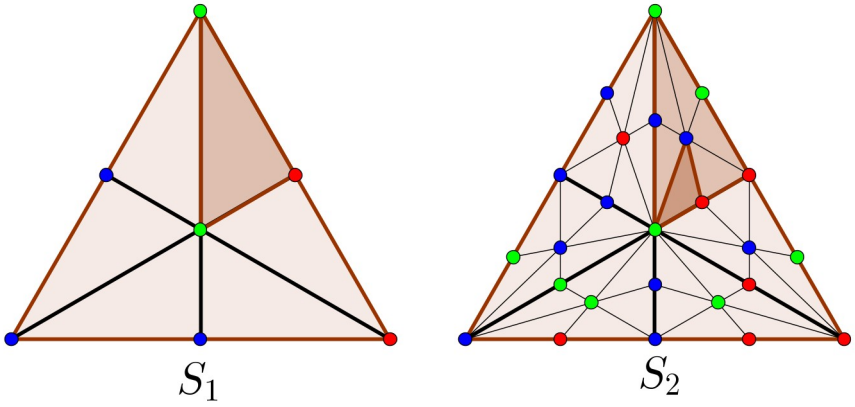
Teorema 2.1. Toda função contínua $f : B^n \to B^n$ de uma bola fechada n-dimensional nela mesma possui um ponto fixo, ou seja, um ponto $x \in B^n$ tal que $f(x) = x$.

Demonstração. Seja $S \subset \mathbb{R}^{n+1}$ o simplexo n-dimensional de vértices $v_1 = (1, 0, \ldots 0), v_2 = (0, 1, \ldots 0), \ldots v_{n+1} = (0, 0, \ldots 1)$. Sabemos que S é homeomorfo a B^n, ou seja, existe uma função $g : B^n \to S$, bijetiva, contínua e cuja inversa $g^{-1} : S \to B^n$ também é contínua. Logo a função $h = g \circ f \circ g^{-1} : S \to S$ é contínua. Além disso, f tem ponto fixo se, e somente se, h tem ponto fixo. De fato, suponhamos que x seja ponto fixo de f. Como g^{-1} é bijetiva, existe $y \in S$ tal que $g^{-1}(y) = x$. Daí, $h(y) = g(f(g^{-1}(y))) = g(f(x)) = g(x) = y$, isto é, y é ponto fixo de h. A prova da recíproca é análoga. Então basta provarmos que h possui ponto fixo.

Suponhamos, por absurdo, que h não tem ponto fixo. Vamos colorir os pontos de S com as cores $1, 2, \ldots, n+1$ da seguinte maneira: a cor de x, denotada por $c(x)$, é tal que $h(x)_{c(x)} < x_{c(x)}$, ou seja, a $c(x)$-ésima coordenada de $h(x)$ é menor do que a coordenada correspondente de x. Isso é possível porque, para todo $x \in S$, $\sum_{i=1}^{n+1} h(x)_i = \sum_{i=1}^{n+1} x_i = 1$ e $h(x) \neq x$, logo deve existir algum i tal que $h(x)_i < x_i$, caso contrário, $\sum_{i=1}^{n+1} h(x)_i > \sum_{i=1}^{n+1} x_i$. Se existir mais de uma coordenada com essa propriedade, peguemos a menor.

Nós podemos construir uma sequência $(S_1, S_2, \ldots)$ de subdivisões de S de modo que o "tamanho"das células de S_i converge para zero.

Figura 12 – Subdivisões de S



Fonte: elaborada pelo autor.

Mostremos que a coloração dos vértices de S_i é própria. Com efeito, a cor do vértice $v_i = (0, \ldots, 1, \ldots, 0)$ de S é i, pois só assim é possível $h(x)_i < x_i$. Analogamente, dado v pertencente a face de S determinada por todos os vértices menos v_i, temos que a i-ésima coordenada de v é zero. Logo as únicas cores possíveis para v são as cores dos vértices que determinam a face. Segue, do teorema de Sperner, que cada subdivisão S_i contem uma célula completa, isto é, uma célula de vértices $\{v_{(i,1)}, v_{(i,2)}, \ldots, v_{(i,n+1)}\}$ tais que $c(v_{(i,j)}) = j$. A sequência $(v_{(i,1)})_{i \in \mathbb{N}}$ pode não converjir, mas como S é limitado, essa sequência deve possuir uma subsequência convergente. Por simplicidade, vamos supor que $(v_{(i,1)})_{i \in \mathbb{N}}$ converge para algum x^*. Como o tamanho das subdivisões S_i tende a zero, todas as sequências $(v_{(i,2)}), (v_{(i,3)}), \ldots, (v_{(i,n+1)})$ também convergem para o mesmo x^*.

Nós assumimos que não existe ponto fixo, logo $h(x^*) \neq x^*$. Isso significa que $h(x^*)_i > x_i^*$ para alguma coordenada i. Mas nós sabemos que $h(v_{(i,j)})_i < (v_{(i,j)})_i$ para todo j e $\lim_{j \to \infty} v_{(i,j)} = x^*$, o que implica $h(x^*) \leq x_i^*$, por continuidade. Um absurdo. □

3 VALORES ABSOLUTOS E NÚMEROS P-ÁDICOS

3.1 Motivação

Consideremos a seguinte equação

$$x = 1 + 2x. \tag{3.1}$$

É fácil ver que sua única solução é $x = -1$. Porém, usando um pouco mais de imaginação, percebemos que resolver a equação acima é equivalente a econtrar um ponto fixo da função $f(x) = 1 + 2x$, isto é, encontrar $x \in \mathbb{R}$ tal que $f(x) = x$. Da análise numérica, sabemos que uma forma de fazer isso é escolher um valor inicial, digamos $x_1 = 1$, e iterar f sucessivas vezes sobre ele. Ou seja, devemos considerar a sequência dada por $x_1 = 1$ e $x_{n+1} = f(x_n) = 1 + 2x_n$:

$$x_1 = 1$$
$$x_2 = 1 + 2$$
$$x_3 = 1 + 2(1 + 2) = 1 + 2 + 2^2$$
$$x_4 = 1 + 2(1 + 2 + 2^2) = 1 + 2 + 2^2 + 2^3$$
$$\dots$$
$$x_n = 1 + 2 + 2^2 + 2^3 + \dots + 2^n.$$

A sequência (x_n) acima obtida não converge para a solução de nossa equação (ela não é sequer convergente). De fato, podemos até mesmo calcular o quanto os termos de (x_n) se distanciam de $x = -1$ quando n cresce:

$$x = 1 + 2x$$
$$x = 1 + 2(1 + 2x) = 1 + 2 + 2^2 x$$
$$x = 1 + 2(1 + 2 + 2^2 x) = 1 + 2 + 2^2 + 2^3 x$$
$$\dots$$
$$x = 1 + 2 + \dots + 2^n + 2^{n+1} x = x_n + 2^{n+1} x.$$

Daí,

$$|x - x_n| = |2^{n+1}||x|.$$

Observe que o lado direito da igualdade pode ser tão grande quanto queiramos, já que, $|2^{n+1}| = 2^{n+1}$. Mas isso depende do que nós entedemos por $|\cdot|$. Pois, se nós definíssimos $|\cdot|$ de modo que $|2^{n+1}| \to 0$ quando $n \to \infty$, então a sequência (x_n) seria convergente.

Outro racicínio a sugerir que em algum contexto a sequência (x_n) converge é o seguinte: note que (x_n) é sequência de somas parciais da série geométrica

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^n + \ldots$$

e, dado $a \in \mathbb{R}$, $|a| < 1$, sabemos que vale a fórmula

$$1 + a + a^2 + \ldots + a^n + \ldots = \frac{1}{1-a}.$$

Se definíssimos de forma consistente $|\cdot|$ de modo que $|2| < 1$ e fizéssemos $a = 2$ na fórmula, consiguiriamos $\frac{1}{1-2} = -1$, solução da equação 3.1. Esse é um dos objetivos da próxima seção.

3.2 Valores Absolutos

Valores absolutos são funções que captam o que nós entendemos como o tamanho ou a magnitude de um objeto matemático (mais especificamente, um elemento de um corpo). O exemplo mais conhecido de tais funções é o módulo ou valor absoluto usual de um número real, definido como

$$|x| = \begin{cases} x, & \text{se } x \geq 0 \\ -x, & \text{se } x < 0. \end{cases} \tag{3.2}$$

O valor absoluto usual nos permite definir uma distância, ou métrica, entre números reais: basta pormos $d(x,y) = |x - y|$ (por exemplo, $d(-3,5) = |-3-5| = |-8| = 8$. Isso , por sua vez, nos permite falar em limite e convergência, conceitos que são a base do Cálculo e da Análise.

O objetivo dessa seção é estudar uma classe de valores absolutos definidos sobre os racionais e conhecidos como valores absolutos p-ádicos (pois estão relacionados com um número primo p). Essas novas formas de medir tamanho e distância podem ser usadas para construir, a partir de $\mathbb{Q}$, o conjunto dos racionais p-ádicos, $\mathbb{Q}_p$. O fato de que qualquer valor absoluto p-ádico pode ser estendido para $\mathbb{R}$ se mostrará grande importância na demonstração do Teorema de Monsky.

Sabemos que a função definida em (3.2) restrita ao conjunto dos números racionais satisfaz as seguintes propriedades:

1. $|x| = 0$ se, e somente se $x = 0$

2. $|xy| = |x||y|$ para todos $x,y \in \mathbb{Q}$
3. $|x+y| \leq |x| + |y|$ para todos $x,y \in \mathbb{Q}$ (Desigualdade Triangular).

Como sugerido no início da seção, existem outras funções que têm as mesmas propriedades. De fato, dado um número primo p, todo número racional não nulo pode ser escrito na forma

$$r = p^k \frac{a}{b},$$

onde $k,a,b \in \mathbb{Z}$ e p não divide a nem b. Consideremos a função $|\cdot| : \mathbb{Q} \to \mathbb{Q}_+$ definida por

$$|r|_p = p^{-k}, \quad |0|_p = 0.$$

Por exemplo,

$$|45|_3 = |3^2 \cdot 5|_3 = 3^{-2}$$
$$|24|_5 = |5^0 \cdot 24|_5 = 5^0 = 1$$
$$\frac{6}{20}_2 = \frac{2 \cdot 3}{2^2 \cdot 5}_2 = 2^{-1}\frac{3}{5}_2 = 2.$$

Claramente tal função satisfaz a primeira propriedade. Ademais, dados os números racionais $x = p^k \frac{a}{b}$ e $y = p^l \frac{c}{d}$, onde a, b, c e d não são divisíveis por p, temos

(2) $|xy|_p = p^k \frac{a}{b} \cdot p^l \frac{c}{d}_p = p^{k+l} \frac{ac}{bd}_p = p^{-(k+l)} = p^{-k} \cdot p^{-l} = |x||y|.$

(3) Podemos supor, sem perda de generalidade, que $k \geq l$. Daí,

$$|x+y|_p = p^k \frac{a}{b} + p^l \frac{c}{d}_p = p^l \quad \frac{p^{k-l} \cdot ad - cb}{bd} \quad _p.$$

O denominador da fração dentro do parênteses pode ser divisível por p (se $k = l$). Logo,

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

Se $k > l$ (particularmente, se $x \neq y$), então $m = 0$, ou seja, $|x+y|_p = max(|x|_p, |y|_p)$.

Portanto vale a segunda propriedade e uma condição mais forte do que a terceira. Devido a isso, a função $|\cdot|_p$ é chamada valor absoluto p-ádico. Mais geralmente temos a seguinte

Definição 3.1. Seja K um corpo. Um valor absoluto sobre K é uma função $|\cdot| : K \to \mathbb{R}_+$ satisfazendo as seguintes condições:

1. $|x| = 0$ se, e somente se $x = 0$

2. $|xy| = |x||y|$ para todos $x,y \in K$
3. $|x+y| \leq |x| + |y|$ para todos $x,y \in K$.

Nós dizemos que um valor absoluto $|\cdot|$ é não-arquimediano se ele satisfaz a seguinte condição mais forte, conhecida como desigualdade ultramétrica:

3'. $|x+y| \leq max(|x|, |y|)$,

caso contrário, dizemos que o valor absoluto é arquimediano.

Exemplo 3.1. Além dos já citados, outro exemplo de valor absoluto é o *valor absoluto trivial* que pode ser definido sobre qualquer corpo pondo $|x| = 1$, se $x \neq 0$, e $|0| = 0$.

Exemplo 3.2. Sejam K um corpo e $|\cdot|: K \to \mathbb{R}_+$ um valor absoluto não-arquimediano sobre K. Fixado um número real positivo α, a função $|\cdot|^0: K \to \mathbb{R}_+$ tal que $|x|^0 = |x|^\alpha$, para todo $x \in K$, também é um valor absoluto. De fato, é fácil ver que $|\cdot|^0$ satisfaz as condições (1) e (2). Além disso, dados $x,y \in K$, temos

$$|x+y|^0 = |x+y|^\alpha \leq max(|x|, |y|)^\alpha \leq max(|x|^\alpha, |y|^\alpha).$$

Logo, $|x+y|^0 \leq max(|x|^0, |y|^0)$.

O Teorema de Ostrowski, cuja prova poder ser encontrada em (SILVA, 2018), afirma que, de certa forma, o valor absoluto usual, os valores absolutos p-ádicos e suas potências são os únicos valores absolutos não triviais que podem ser definidos sobre $\mathbb{Q}$.

Lema 3.1. Para qualquer valor absoluto $|\cdot|$ sobre um corpo K, temos:

(i) $|1| = |-1| = 1$
(ii) Para todo $x \in K$, $|-x| = |x|$
(iii) Para todo $x \in K, x \neq 0$, $|x^{-1}| = |x|^{-1}$
(iv) Para todos $x,y \in K, y \neq 0$, $\frac{x}{y} = \frac{|x|}{|y|}$.

Demonstração.

(i) Observe que pela definição de valor absoluto tanto $|1|$ quanto $|-1|$ são diferentes de 0. Daí, $|1||1| = |1 \cdot 1| = |1| \Rightarrow |1| = \frac{|1|}{|1|} = 1$, e $|-1||-1| = |(-1)(-1)| = |1| = 1 \Rightarrow |-1| = 1$.
(ii) $|-x| = |(-1)x| = |-1||x| = 1|x| = |x|$.
(iii) $|x||x^{-1}| = |xx^{-1}| = |1| = 1 \Rightarrow |x^{-1}| = \frac{1}{|x|} = |x|^{-1}$.
(iv) $\frac{x}{y} = |xy^{-1}| = |x||y^{-1}| = |x||y|^{-1} = \frac{|x|}{|y|}$.

□

3.3 Extensões

Sabemos que o valor absoluto usual $|\cdot|$ sobre racionais pode ser estendido para o corpo dos números reais, isto é, existe um valor absoluto $|\cdot|^0 : \mathbb{R} \to \mathbb{R}_+$ tal que

$|x|^0 = |x|$, para todo $x \in \mathbb{Q}$.

Uma pergunta natural que podemos fazer é: Será que isso também vale para os outros valores absolutos definidos sobre $\mathbb{Q}$?

Consideremos o valor absoluto 2-ádico. Supondo que existe uma extensão desse valor absoluto para $\mathbb{R}$, podemos calcular a imagem de alguns números irracionais segundo essa extensão. Por exemplo,

$$(|\sqrt{2}|_2)^2 = |\sqrt{2}|_2 \cdot |\sqrt{2}|_2 = |\sqrt{2} \cdot \sqrt{2}|_2 = |2|_2 = \frac{1}{2}.$$

Logo $|\sqrt{2}|_2 = \sqrt{\frac{1}{2}}$.

Mais geralmente, dado $x \in \mathbb{Q}$ e $n \in \mathbb{N}$, temos

$$(|\sqrt[n]{x}|_2)^n = |\sqrt[n]{x}|_2 \cdot |\sqrt[n]{x}|_2 \cdot \ldots \cdot |\sqrt[n]{x}|_2 = |\sqrt[n]{x} \cdot \sqrt[n]{x} \cdot \ldots \cdot \sqrt[n]{x}|_2 = |x|_2.$$

Logo $|\sqrt[n]{x}|_2 = \sqrt[n]{|x|_2}$.

Porém não está claro como devemos definir $|\pi|_2$ ou $|e|_2$. E quanto aos outros valores absolutos definidos sobre $\mathbb{Q}$? Um teorema garante pelo menos a existência de tais extensões.

Teorema 3.1. (Chevalley) Seja $K \subset L$ uma extensão de corpos. Qualquer valor absoluto não-arquimediano definido sobre K pode ser estendido para L. Particularmente, podemos estender $|\cdot|_2$ para $\mathbb{R}$.

A demonstração desse teorema pode ser encontrado em (JACOBSON, 1975).

3.4 Completamentos

Começemos com algumas definições importantes vindas da Análise.

Definição 3.2. Seja K um corpo e seja $|\cdot|$ um valor absoluto sobre K. Uma sequência de elementos $x_n \in K$ é chamada uma sequência de Cauchy se para todo $\varepsilon > 0$ existir $n_0 \in \mathbb{N}$ tal que $|x_n - x_m| < \varepsilon$ sempre que $m, n \geq n_0$.

Definição 3.3. Um corpo K é dito completo com relação a um valor absoluto $|\cdot|$ se toda sequência de Cauchy de elementos de K for convergente.

Definição 3.4. Seja K um corpo. Um subconjunto $S \subset K$ é dito denso em K se toda bola aberta com centro em algum elemento de K contem um elemento de S, ou seja, se para todo $x \in K$ e todo $\varepsilon > 0$ nós temos

$$B(x, \varepsilon) \cap S \neq \emptyset.$$

Grosso modo, uma sequência é de Cauchy se seus termos ficam cada vez mais próximos uns do outros, ou seja, se a distância entre eles fica cada vez menor. Por exemplo, sabemos que a sequência (x_n) dada por $x_x = \frac{1}{n}$ converge para zero. Logo, dado $\varepsilon > 0$, podemos achar $n_0 \in \mathbb{N}$ tal que $\frac{1}{n_0} < \varepsilon$. Daí, se $m \geq n \geq n_0$, então $\frac{1}{m} \leq \frac{1}{n} \leq \frac{1}{n_0}$ e $\left|\frac{1}{n} - \frac{1}{m}\right| \leq \frac{1}{n_0} < \varepsilon$. Portanto, (x_n) é uma sequência de Cauchy.

Nossa intuição pode nos levar a pensar que sequências desse tipo são sempre convergentes. Veremos que isso não é verdade.

Proposição 3.1. $\mathbb{Q}$ não é completo com respeito ao valor absoluto usual $|\cdot|$, ou seja, existe uma sequência de Cauchy de elementos de $\mathbb{Q}$ que não converge para qualquer número racional.

Demonstração. Consideremos a sequência (a_n) dada por $a_1 = 1$ e $a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right)$. Tal sequência é de Cauchy. De fato:

(i) Para todo $x > 0$, $\left(x + \frac{2}{x}\right)^2 = x^2 + 4 + \frac{4}{x^2} > 4 \Rightarrow x + \frac{2}{x} > 2 \Rightarrow \frac{1}{2}\left(x + \frac{2}{x}\right) > 1$.

(ii) De (i) segue que, para todo $n > 1$, temos $a_n > 1$. Daí, $a_{n+1} \cdot a_n > 1$, ou seja,

$$\frac{1}{a_{n+1} \cdot a_n} < 1.$$

Usaremos esse fato para mostrar que

$$|a_{n+2} - a_{n+1}| \leq \frac{1}{2}|a_{n+1} - a_n|.$$

Com efeito,

$$a_{n+2} - a_{n+1} = \frac{1}{2}(a_{n+1} - a_n) + \left(\frac{1}{a_{n+1}} - \frac{1}{a_n}\right) = \frac{1}{2}(a_{n+1} - a_n) + \frac{a_n - a_{n+1}}{a_n \cdot a_{n+1}}.$$

Dividindo os dois lados por $a_{n+1} - a_n$ e tomando o módulo, temos

$$\left|\frac{a_{n+1} - a_{n+1}}{a_{n+1} - a_n}\right| = \left|\frac{1}{2} - \frac{1}{a_n \cdot a_{n+1}}\right| \leq \frac{1}{2}.$$

(iii) Façamos $\lambda = \frac{1}{2}$. Como $|a_{n+2} - a_{n+1}| \leq \lambda |a_{n+1} - a_n|$, para todo $n \in \mathbb{N}$, temos

$$|a_3 - a_2| \leq \lambda |a_2 - a_1|,$$
$$|a_4 - a_3| \leq \lambda |a_3 - a_2| \leq \lambda^2 |a_2 - a_1|.$$

Mais geralmente,

$$|a_{n+1} - a_n| \leq \lambda^{n-1} |a_2 - a_1|.$$

Segue que, para $n, p \in \mathbb{N}$, vale

$$\begin{aligned} |a_{n+p} - a_n| &= |a_{n+p} - a_{n+p-1} + a_{n+p-1} - \ldots - a_{n+1} + a_{n+1} - a_n| \\ &\leq |a_{n+p} - a_{n+p-1}| + \ldots + |a_{n+1} - a_n| \\ &\leq \lambda^{n+p-2} + \lambda^{n+p-3} + \ldots + \lambda^{n-1} \; |a_2 - a_1| \\ &= \lambda^{n-1} \; \lambda^{p-1} + \lambda 2^{p-2} + \ldots + \lambda + 1 \; |a_2 - a_1| \\ &= \lambda^{n-1} \cdot \frac{1 - \lambda^p}{1 - \lambda} \cdot |a_1 - a_0| \leq \frac{\lambda^{n-1}}{1 - \lambda} \cdot |a_2 - a_1|. \end{aligned}$$

Como $\lim_{n \to \infty} \frac{\lambda^{n-1}}{1 - \lambda} \cdot |a_2 - a_1| = 0$, segue que, dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que

$$n > n_0 \Rightarrow 0 < \frac{\lambda^{n-1}}{1 - \lambda} \cdot |a_2 - a_1| < \varepsilon.$$

Daí, $m, n > n_0 \Rightarrow |a_m - a_n| < \varepsilon$ (Pois podemos supor $m \geq n$ e tomar $m = n + p$).
Suponhamos que (a_n) converge para $a \in \mathbb{Q}$. Então,

$$\lim_{n \to \infty} a_{n+1} = \lim_{n \to \infty} \frac{1}{2} \left(a_n + \frac{2}{a_n} \right) \Rightarrow a = \frac{1}{2} \left(a + \frac{2}{a} \right) \Rightarrow 2a^2 = a^2 + 2 \Rightarrow a^2 = 2 \Rightarrow a = \sqrt{2}.$$

Um absurdo. □

Lema 3.2. Uma sequência (x_n) de números racionais é de Cauchy com respeito a um valor absoluto não-arquimediano $|\cdot|$ se, e somente se,

$$\lim_{n \to \infty} |x_{n+1} - x_n| = 0.$$

Demonstração. Tomemos $m, n \in \mathbb{N}$ tais que $m = n + p > n$. Como $|\cdot|$ é não-arquimediano, temos

$$\begin{aligned} |x_m - x_n| &= |x_{n+p} - x_{n+p-1} + x_{n+p-1} - x_{n+p-2} + \ldots + x_{n+1} - x_n| \\ &\leq \max(|x_{n+p} - x_{n+p-1}|, |x_{n+p-1} - x_{n+p-2}|, \ldots, |x_{n+1} - x_n|). \end{aligned}$$

$\Rightarrow$) Se (x_n) é uma sequência de Cauchy, então $\lim_{n\to\infty}|x_{n+p} - x_n| = 0$, para qualquer $p \in \mathbb{N}$, particularmente, $\lim_{n\to\infty}|x_{n+1} - x_n| = 0$.

$\Leftarrow$) Reciprocamente, se $\lim_{n\to\infty}|x_{n+1} - x_n| = 0$, então o lado direito da desigualdade acima tende a zero (observe que os pares de índices dentro dos módulos diferem por uma unidade). Logo $\lim_{n\to\infty}|x_{n+p} - x_n| = 0$ e, consequentemente, (x_n) é uma sequência de Cauchy. □

Definição 3.5. Sejam *a* e *b* números inteiros e *n* um número natural. Dizemos que *a* é congruente a *b* módulo n se *a* e *b* deixam o mesmo resto na divisão por *n*, ou seja, se *n* divide $a - b$. Se isso acontecer, escrevemos

$$a \equiv b \ (mod\ n).$$

Por exemplo, $14 \equiv 5\ (mod\ 3)$, pois 3 divide 14 - 5 = 9; $23 \equiv -2\ (mod\ 5)$, pois 5 divide 23 -(-2) = 25; para todo inteiro *a* e todo natural *n*, $a \equiv a\ (mod\ n)$, pois n divide a - a = 0.

Definição 3.6. Dado um número primo p, um sistema de congruências módulo p^n é o conjunto formado pelas congruências

$$x - a \equiv 0\ (mod\ p^i),$$

onde $1 \leq i \leq n$. Tal sistema será denotado simplesmente por

$$x - a \equiv 0\ (mod\ p^n).$$

Lema 3.3. Seja *p* um número primo. A congruência $bx \equiv a\ (mod\ p)$ possui solução se, e somente se, $mdc(b, p)$ divide *a*. Particularmente, se *p* não divide *b*, então a congruência tem solução.

Demonstração. Da definição de congruência, temos

$$bx \equiv a\ (mod\ p) \Leftrightarrow bx - a = pk \Leftrightarrow bx - pk = a.$$

Da teoria elementar dos números, segue que a *equação diofantina linear* acima possui solução se, e somente se, $mdc(b, p)$ divide *a*. □

Proposição 3.2. $\mathbb{Q}$ não é completo com relação a qualquer um de seus valores absolutos *p*-ádicos.

Demonstração.

Caso 1: $p \neq 2$. Tomemos $a = k^2 + p$, onde *k* é um número inteiro não divisível por *p*. Temos que

- $\sqrt{a} \notin \mathbb{Q}$. De fato, se $a = k^2 + p = l^2$, com $l \in \mathbb{Z}$, então $p = (l - k)(l + k)$, um absurdo. E como a não é um quadrado perfeito, segue que sua raiz quadrada não é racional.
- p não divide a.
- a é um resíduo quadrático módulo p, i.e, a congruência $x^2 \equiv a \pmod{p}$ possui solução. Com efeito, $k^2 \equiv a \pmod{p}$.

Olhemos agora para o sistema de congruências

$$x^2 \equiv a \pmod{p^n}.$$

Para $n = 1$, temos

$$x^2 \equiv a \pmod{p},$$

que, como já vimos, possui solução $x_1 = k^2$.

Mais geralmente, suponhamos que $x^2 \equiv a \pmod{p^n}$ possui solução x_n, onde p não divide x_n. Fazendo $x = x_n + p^n y$ na congruência

$$x^2 \equiv a \pmod{p^{n+1}}, \tag{3.3}$$

obtemos

$$(x_n + p^n y)^2 \equiv a \pmod{p^{n+1}}$$
$$x_n^2 + 2x_n p^n y + p^{2n} y^2 \equiv a \pmod{p^{n+1}}$$
$$2x_n p^n y \equiv a - x_n^2 \pmod{p^{n+1}}$$

Como $mdc(p^{n+1}, 2x_n p^n) = p^n$ divide $a - x_n^2$, segue que a congruência acima possui solução $y = y_n$ e, consequentemente, (3.3) possui solução $x_{n+1} = x_n + p^n y_n$.

A sequência (x_n) obtida é uma sequência de Cauchy. De fato, da última igualdade, temos que

$$x_{n+1} - x_n = p^n k \Rightarrow |x_{n+1} - x_n|_p = |p^n k|_p = \frac{|k|_p}{p^n} \to 0, \text{quando n} \to \infty.$$

Ademais,

$$x_n^2 \equiv a \pmod{p^n} \Rightarrow x_n^2 - a = p^n l \Rightarrow |x_n^2 - a|_p = \frac{|l|_p}{p^n} \to 0, \text{quando n} \to \infty.$$

Logo (x_n) converge para $\sqrt{a}$. Como $\sqrt{a} \notin \mathbb{Q}$, concluimos que $\mathbb{Q}$ não é completo com relação a $|\cdot_p|$, para $p \neq 2$.

Caso 2: $p = 2$. A congruência

$$x^3 \equiv 3 \ (mod\ 2)$$

possui solução $x_1 = 1$.

Mais geralmente, suponhamos que a congruência

$$x^3 \equiv 3 \ (mod\ 2^n)$$

possui solução $x = x_n$ ímpar e façamos $x = x_n + 2^n y$ na congruência

$$x^3 \equiv 3 \ (mod\ 2^{n+1}). \tag{3.4}$$

Daí,

$$(x_n + 2^n y)^3 \equiv 3 \ (mod\ 2^{n+1})$$
$$x_n^3 + 3x_n^2 2^n y + 3x_n 2^{2n} y^2 + 2^{3n} y^3 \equiv 3 \ (mod\ 2^{n+1})$$
$$x_n^3 + 3x_n^2 2^n y \equiv 3 \ (mod\ 2^{n+1})$$
$$3x_n^2 2^n y \equiv 3 - x_n^3 \ (mod\ 2^{n+1}).$$

Como $mdc(3x_n^2 2^n, 2^{n+1}) = 2^n$ divide $3 - x_n^3$, segue que a última congruência acima possui solução $y = y_n$. Logo (3.4) possui solução $x_{n+1} = x_n + 2^n y_n$.

Do lema 3.2, segue que a sequência (x_n) obtida é uma sequência de Cauchy. De fato, da última igualdade, temos que

$$x_{n+1} - x_n = 2^n y_n \Rightarrow |x_{n+1} - x_n|_2 = |2^n y_n|_2 = \frac{|y_n|_2}{2^n} \to 0 \text{ quando } n \to \infty.$$

Além disso,

$$x_n^3 \equiv 3 \ (mod\ 2^n) \Rightarrow x_n^3 - 3 = 2^n l \Rightarrow |x_n^3 - 3|_2 = |2^n l|_2 = \frac{|l|_2}{2^n} \to 0 \text{ quando } n \to \infty.$$

Logo (x_n) converge para $\sqrt[3]{3} \notin \mathbb{Q}$. Portanto, $\mathbb{Q}$ também não é completo com relação a $|\cdot_2|$ □

Da análise, sabemos que o corpo dos números racionais pode ser “completado"a fim de obtermos o corpo dos números reais. Analogamente, se considerarmos um valor absoluto p-ádico, podemos construir, a partir de $\mathbb{Q}$, um corpo completo chamado corpo dos racionais p-ádicos, $\mathbb{Q}_p$. Essa construção, encontrada com detalhes em (GOUVêA, 1997), pode ser resumida da seguinte maneira:

(i) Consideramos o conjunto C de todas as sequências de Cauchy de números racionais (com relação ao valor absoluto escolhido) e definimos sobre C uma adição e uma multiplicação "naturais":

$$(x_n) + (y_n) = (x_n + y_n)$$
$$(x_n) \cdot (y_n) = (x_n y_n).$$

É possível provar que C junto com essas operações é um domínio de integridade, mas não é um corpo.

(ii) Definimos o conjunto $N = \{(x_n) \in C \mid lim|x_n|_p = 0\}$, ou seja, formado por todos os elementos de C que convergem para 0.

(iii) O conjunto C é formado por sequências que não convergem em $\mathbb{Q}$ e também por sequências que convergem para o mesmo número racional - por exemplo, $(1,1,1, \ldots)$ e $(0,1,1,1, \ldots)$. O próximo passo de nossa construção é reunir tais sequências em *classes de equivalência*. Fazemos isso definindo

$$(x_n) \equiv (y_n), \text{ se } (x_n) - (y_n) \in N \text{ e}$$
$$\overline{(x_n)} = \{(a_n) \in C \,/\, (a_n) \equiv (x_n)\}.$$

Depois, reunimos todas essas classes de equivalência no conjunto $C/N = \{\overline{(x_n)} \,/\, (x_n) \in C\}$.

(iv) Definimos sobre C/N uma adição e uma multiplicação:

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

(v) Podemos estender para C/N o valor absoluto p-ádico. Dado $\lambda = \overline{(x_n)} \in C/N$, basta pormos:

$$|\lambda|_p = \lim_{n \to \infty} |x_n|_p.$$

Essa definição faz sentido, pois, para n suficientemente grande, $(|x_n|_p)$ é constante. Isso é demonstrado nas próximas três proposições.

Proposição 3.3. $(|x_n|_p)$ também é de Cauchy com respeito a $|\cdot\,|$

Demonstração.

$$|x_m|_p = |x_m - x_n + x_n|_p \leq |x_m - x_n|_p + |x_n|_p \Rightarrow |x_m| - |x_n|_p \leq |x_m - x_n|_p.$$

Analogamente,

$$|x_n|_p - |x_m|_p \leq |x_m - x_n|_p.$$

Logo, $||x_n|_p - |x_m|_p| \leq |x_m - x_n|_p$. □

Proposição 3.4. Existe $c > 0$ e $N \in \mathbb{N}$ tal que $n \geq N \Rightarrow |x_n|_p \geq c$.

Demonstração. Como (x_n) não tende a zero, existe $\varepsilon > 0$ tal que, para todo $n_0 \in \mathbb{N}$, existe $n > n_0$ de modo que

$$|x_n|_p > \varepsilon.$$

Tomemos $0 < c < \varepsilon$. Como $(|x_n|_p)$ é de Cauchy, existe $N \in \mathbb{N}$ tal que

$$m,n \geq N \Rightarrow ||x_m|_p - |x_n|_p| < \varepsilon - c.$$

Podemos sempre tomar n de modo que $|x_n|_p > \varepsilon$. Daí, se $|x_m|_p \geq |x_n|_p$, então $|x_m| > c$. Caso contrário, ou seja, se $|x_m|_p < |x_n|_p$, então $||x_m|_p - |x_n|_p| = |x_n|_p - |x_m|_p < \varepsilon - c \Rightarrow |x_m|_p - |x_n|_p > c - \varepsilon \Rightarrow |x_m|_p > c$. □

Proposição 3.5. Seja $(x_n) \in C$ uma sequência que não converge para zero com relação a $|\cdot_p|$. A sequência $(|x_n|_p)$ se torna eventualmente estacionária, ou seja, existe $N \in \mathbb{N}$ tal que $|x_n|_p = |x_m|_p$ para todos $m,n \geq N$.

Demonstração. Existem $c > 0$ e $N_1 \in \mathbb{N}$ tais que

$$n \geq N_1 \Rightarrow |x_n|_p \geq c > 0.$$

Como (x_n) é de Cauchy, existe $N_2 \in \mathbb{N}$ tal que

$$m,n \geq N_2 \Rightarrow |x_m - x_n|_p < c.$$

Tomemos $N = max(N_1, N_2)$. Daí,

$$m,n \geq N \Rightarrow |x_m - x_n|_p < |x_n|_p \Rightarrow |x_n|_p = |x_m|_p.$$

□

(vi) É possível identificar os elementos de $\mathbb{Q}$ com elementos de C/N através da aplicação:

$$x \to \overline{(x,x,x,\ \ldots)}.$$

Além disso, é possível demonstrar que C/N junto com a adição e a multiplicação definidas acima é um corpo completo (com relação ao valor absoluto p-ádico estendido). Ou seja, C/N tem todas as propriedades que nós esperávamos. Encerramos a construção definindo

$$\mathbb{Q}_p := C/N.$$

(GOUVêA, 1997) comenta que pode soar meio artificial dizer que um número p-ádico é uma classe de equivalência de sequências de Cauchy. Inspirados nele, buscaremos então uma caracterização mais explícita. A saber, mostraremos que todo número p-ádico pode ser representado por uma soma infinita da forma

$$a_{-r}\frac{1}{p^r} + a_{-r+1}\frac{1}{p^{r-1}} + \ \dots\ + a_{-1}\frac{1}{p} + a_0 + a_1 p + a_2 p^2 + \ \dots$$

onde r e a_i são números inteiros e $0 \leq a_i \leq p - 1$.

O primeiro passo nessa busca é a formalização do conceito de soma infinita.

Definição 3.7. Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de elementos de um corpo K. Para atribuir um significado a soma infinita, ou série,

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + \ \dots\ + a_n + \ \dots$$

olhamos para sua *sequência de somas parciais*

$$s_1 = a_1,$$

$$s_2 = a_1 + a_2,$$

$$\dots$$

$$s_n = a_1 + a_2 + \ \dots\ + a_n.$$

$$\dots$$

Se essa sequência possuir limite s (com relação a um valor absoluto $|\ \cdot\ |$), dizemos que a série $\sum_{n=1}^{\infty} a_n$ é convergente (com relação a $|\ \cdot\ |$) e escrevemos

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + \ .a_n + \ \dots\ = s.$$

Caso contrário, ou seja, caso $\lim_{n\to\infty} s_n$ não exista, dizemos que a série é divergente.

O limite s e a expressão a_n são chamados de soma e termo geral da série, respectivamente. As vezes é conveniente pensar na série com n variando a partir de algum inteiro $r \leq 0$.

A próxima proposição traz uma propriedade importante das séries em $\mathbb{Q}_p$.

Proposição 3.6. Uma série $\sum_{n=1}^{\infty} a_n$ de elementos de $\mathbb{Q}_p$ é convergente se, e somente se, $lim_{n\to\infty} a_n = 0$.

Demonstração. Consideremos a sequência de somas parciais da série cujo termo geral é $s_n = a_1 + a_2 + \ldots + a_n$. Oberve que

$$s_n - s_{n-1} = a_1 + \ldots + a_{n-1} + a_n - (a_1 + \ldots + a_{n-2} + a_{n-1}) = a_n.$$

Do lema 3.2, segue que s_n é de Cauchy (logo convergente) se, e somente se,

$$\lim_{n\to\infty} |a_n|_p = \lim_{n\to\infty} |s_n - s_{n-1}|_p = 0.$$

□

Da proposição 3.6, temos que a série

$$\sum_{n=0}^{\infty} a_n p^n = a_0 + a_1 p + a_2 p^2 + \ldots,$$

onde $a_i \in \mathbb{Z}$, $0 \leq a_i < p$, é convergente. De fato, $lim\ |a_n p^n|_p = lim\ \frac{1}{p^n} = 0$.

Logo a seguinte definição faz sentido

Definição 3.8. Um inteiro p-ádico é um série da forma

$$\sum_{n=0}^{\infty} a_n p^n = a_0 + a_1 p + a_2 p^2 + \ldots,$$

onde $a_i \in \mathbb{Z}$ e $0 \leq a_i < p$. Denotamos por $\mathbb{Z}_{(p)}$ o conjunto de todos os inteiros p-ádicos.

Sabemos que, para todo $0 \neq x \in \mathbb{Q}_p$, existe $n \in \mathbb{Z}$ tal que $|x|_p = p^{-n}$. Será conveniente nas próximas demonstrações se considerarmos apenas o inteiro $n = -\log_p |x|_p$.

Definição 3.9. Seja p um número primo. *A valoração p-ádica* é a função $v_p : \mathbb{Q}_p \to \mathbb{R}_+$ dada por

$$v_p(0) = +\infty \text{ e } v_p(x) = -\log_p |x|_p, \text{ se } x \neq 0.$$

Observe que, da discussão do parágrafo anterior, $v_p(x) \in \mathbb{Z}$, para todo $x \neq 0$.

O lema a seguir apresenta algumas propriedades básicas da valoração p-ádica.

Lema 3.4. Para todos x e $y \in \mathbb{Q}_p$, temos

(i) $v_p(xy) = v_p(x) + v_p(y)$.

(ii) $v_p(x+y) \geq \min(v_p(x), v_p(y))$.

(iii) Dado $n \in \mathbb{Z}$, $v_p(p^n) = n$.

Demonstração. (i) $v_p(xy) = -\log_p |xy|_p = -\log_p(|x|_p|y|_p) = -\log_p |x|_p - \log_p |y|_p$
$= v_p(x) + v_p(y)$.

(ii) $v_p(x+y) = -\log |x+y|_p \geq -\log_p[\max(|x|_p, |y|_p)] = \min(-\log_p |x|_p, -\log_p |y|_p) =$
$\min(v_p(x), v_p(y))$.

(iii) $v_p(p^n) = -\log_p |p^n|_p = -\log_p(p^{-n}) = -(-n) = n$.

Se $xy = 0$, basta convencionarmos $\infty + \infty = \infty$ e, para $r \in \mathbb{R}$, $r + \infty = \infty$ que os resultados continuam válidos. □

Definição 3.10. Uma sequência (x_n) de números inteiros é dita coerente se, para todo $n \in \mathbb{N}$, vale

$0 \leq x_n \leq p^n - 1$ e

$x_{n+1} \equiv x_n \pmod{p^n}$.

Lema 3.5. Dado $x \in \mathbb{Q}_p$, temos que $x \in \mathbb{Z}_{(p)}$ se, e somente se, existe uma sequência coerente (x_n) que converge para x com relação a $|\cdot_p|$.

Demonstração. $\Rightarrow$) Seja (x_n) uma sequência coerente que converge para x. Como $x_{n+1} \equiv x_n \pmod{p^n}$, segue $x_{n+1} = x_n + p^n y_n$. Temos que $0 \leq y_n \leq p-1$, pois, se $y_n \geq p$, então

$$x_{n+1} = x_n + p^n y_n \geq x_n + p^n p \geq p^{n+1}.$$

O que é absurdo.

Assim,

$x_2 = x_1 + y_1 p$

$x_3 = x_2 + y_2 p^2 = x_1 + y_1 p + y_2 p^2$

…

$x_n = x_{n-1} + y_{n-1} p^{n-1} = x_1 + y_1 p + y_2 p^2 + \ldots + y_{n-1} p^{n-1}$,

onde $0 \leq y_i \leq p$.

Portanto,

$x = x_1 + y_1 p + y_2 p^2 + \ldots + y_n p^n + \ldots \in \mathbb{Z}_{(p)}$.

$\Leftarrow$) Reciprocamente, dado

$$x = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots \in \mathbb{Z}_{(p)},$$

consideremos a sequência (x_n) tal que $x_n = a_0 + a_1 p + \ldots + a_{n-1} p^{n-1}$. Temos que $x_{n+1} - x_n = a_n p^n$. Logo $x_{n+1} \equiv x_n \ (mod\ p^n)$. Ademais

$$x_n \leq (p-1) + (p^2 - p) + (p^3 - p^2) + \ldots + (p^n - p^{n-1}) = p^n - 1.$$

Portanto (x_n) é uma sequência coerente. □

Proposição 3.7. Seja $\frac{a}{b} \in \mathbb{Q}$, com $mdc(a,b) = 1$. Temos que $\frac{a}{b} \in \mathbb{Z}_{(p)}$ se, e somente se, p não divide b.

Demonstração. $\Rightarrow$) Suponhamos que p não divide b. Mostraremos que existe uma sequência (x_n) coerente que converge para $\frac{a}{b}$, ou seja:

$0 \leq x_n \leq p^n - 1$

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

$\lim_{n\to\infty} \left| \frac{a}{b} - x_n \right|_p = 0.$

Com efeito, como $mdc(a,b) = 1$, sabemos da teoria dos números que a congruência

$$bx \equiv a \ (mod\ p^n)$$

possui solução para todo $n \in \mathbb{N}$, ou seja, existe $x_n \in \mathbb{Z}$ tal que

$$bx_n - a \equiv 0 \ (mod\ p^n).$$

Ademais, podemos tomar $0 \leq x_n \leq p^n - 1$.

Olhemos agora para a congruência

$$bx \equiv a \ (mod\ p^{n+1})$$

e façamos $x = x_n + p^n y$:

$$b(x_n + p^n y) \equiv a \ (mod\ p^{n+1})$$

$$bp^n y \equiv a - bx_n \ (mod\ p^{n+1}).$$

Como $mdc(bp^n, p^{n+1}) = p$ divide $a - bx_n$, segue que existe $x_{n+1} = x_n + p^n y_n$, ou seja, $x_{n+1} \equiv x_n \ (mod\ p^n)$.

Além disso,

$$\lim_{n\to\infty} \frac{a}{b} - x_n \Big|_p = \lim_{n\to\infty} \frac{a - bx_n}{b} \Big|_p = \lim_{n\to\infty} p^{-n} = 0.$$

$\Leftarrow$) Por outro lado, se p divide b, então a congruência

$$bx \equiv a \pmod{p} \Leftrightarrow 0 \equiv a \pmod{p}$$

não tem solução, já que, $a \neq 0$.

Suponhamos que $mdc(a,b) = 1$ e que $\frac{a}{b} \in \mathbb{Z}_p$, ou seja, existe uma sequência coerente (x_n) que converge para $\frac{a}{b}$. Então, existe $m \in \mathbb{N}$ tal que

$$\frac{a}{b} - x_m \Big| = \frac{a - x_m b}{b} \Big| < \frac{1}{p}.$$

Logo p divide $a - x_m b$ e, consequentemente, p divide a. Um absurdo. □

Proposição 3.8. Dado $x \in \mathbb{Q}_p$, $x \in \mathbb{Z}_{(p)}$ se, e somente se, $|x|_p \leq 1$.

Demonstração. $\Rightarrow$) Seja $x = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots$ um inteiro p-ádico. Então,

$$\begin{aligned} |x|_p &= \lim_{n\to\infty} |a_0 + a_1 p + \ldots + a_n p^n|_p \\ &\leq \lim_{n\to\infty} max(|a_0|, |a_1 p|_p, \ldots, |a_n p^n|_p) \\ &\leq \lim_{n\to\infty} max(1, p^{-1}, \ldots, p^{-n}) = 1, \end{aligned}$$

ou seja, $|x|_p \leq 1$.

$\Leftarrow$) Suponhamos que $|x|_p \leq 1$. Como $\mathbb{Q}$ é denso em $\mathbb{Q}_p$, segue que $\mathbb{Q}$ também é denso em $\mathbb{Z}_p$. Logo, para todo $n \in \mathbb{N}$, existe $\frac{a}{b} \in \mathbb{Q}$, $mdc(a,b) = 1$ tal que

$$x - \frac{a}{b} \Big|_p \leq p^{-n} < 1.$$

Observe que

$$\frac{a}{b} \Big|_p = \frac{a}{b} - x + x \Big|_p \leq max(x - \frac{a}{b} \Big|_p, |x|_p) \leq 1.$$

Portanto $\frac{a}{b} \Big|_p \leq 1$. Daí p não divide b. Segue que existe $b^0 \in \mathbb{Z}$ tal que $bb^0 \equiv 1 \pmod{p^n}$. Daí,

$$\left|\frac{a}{b} - ab^0\right|_p = \left|\frac{a(1-bb^0)}{b}\right|_p \leq p^{-n}.$$

Tomemos $\alpha \in \mathbb{Z}$ de modo que

$0 \leq \alpha \leq p^n - 1$ e

$\alpha \equiv ab^0 \pmod{p^n}$.

Temos

$$\left|\frac{a}{b} - \alpha\right|_p = \left|\frac{a}{b} - ab^0 - (\alpha - ab^0)\right|_p \leq \max\left(\left|\frac{a}{b} - ab^0\right|_p, |\alpha - ab^0|_p\right) \leq p^{-n}.$$

Logo,

$$|x - \alpha| = \left|x - \frac{a}{b} - \alpha - \frac{a}{b}\right|_p \leq \max\left(\left|x - \frac{a}{b}\right|_p, \left|\frac{a}{b} - \alpha\right|_p\right) \leq p^{-n}.$$

Resumindo: Dado $x \in \mathbb{Q}_p$, $|x|_p \leq 1$, temos que, para todo $n \in \mathbb{N}$, existe $\alpha_n \in \mathbb{Z}$ com as seguintes propriedades

$0 \leq \alpha_n \leq p^n - 1$ e

$|x - \alpha_n|_p \leq p^{-n}$.

Mostraremos que

$\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$,

ou seja, $|\alpha_{n+1} - \alpha_n|_p \leq p^{-n}$.

Com efeito,

$$|\alpha_{n+1} - \alpha_n|_p = |\alpha_{n+1} - x + x - \alpha_n|_p \leq \max(|\alpha_{n+1} - x|_p, |x - \alpha_n|_p) \leq p^{-n}.$$

Segue, do lema 3.2, que $x \in \mathbb{Z}_p$. □

Usando a ideia de valoração p-ádica, a proposição 3.8 pode ser reescrita da seguinte forma: dado $x \in \mathbb{Q}_p$, $x \in \mathbb{Z}_p$ se, e somente se, $v_p(x) \geq 0$. De fato,

$$|x|_p \leq 1 \Leftrightarrow \log_p |x|_p \leq 0 \Leftrightarrow -\log_p |x|_p \geq 0 \Leftrightarrow v_p(x) \geq 0.$$

Proposição 3.9. Para todo $x \in \mathbb{Q}_p$ existe $n \geq 0$ tal que $p^n x \in \mathbb{Z}_p$.

Demonstração. Se $v_p(x) \geq 0$, então x já é um elemento de $\mathbb{Z}_p$. Caso contrário, ou seja, se $v_p(x) < 0$, então nós temos

$$v_p(p^{-v_p(x)}x) = v_p(p^{-v_p}(x)) + v_p(x) = -v_p(x) + v_p(x) = 0.$$

Logo, $p^{-v_p(x)}x \in \mathbb{Z}_p$. □

Da proposição anterior, segue que, dado $y \in \mathbb{Q}_p$, existem $n \in \mathbb{Z}$ e $x \in \mathbb{Z}_p$ tais que $y = \frac{x}{p^n}$. Escrevendo x como uma série, temos

$$\begin{aligned} y &= \frac{1}{p^n}(a_0 + a_1 p + a_2 p^2 + \ \ldots\ + a_n p^n + a_{n+1}p^{n+1} + \ \ldots) \\ &= a_0 \frac{1}{p^n} + a_1 \frac{1}{p^{n-1}} + a_2 \frac{1}{p^{n-2}} + \ \ldots\ + a_n + a_{n+1}p + a_{n+2}p^2 + \ \ldots \end{aligned}$$

Isso motiva a notação na qual enxergamos um número p-ádico como um número com uma quantidade infinita de algarismos antes da vírgula e uma quantidade finita de algarismo depois da vírgula:

$$(\ldots a_2 a_1 a_0, a_{-1}a_{-2}\ldots a_{-r})_p := a_{-r}\frac{1}{p^r} + a_{-r+1}\frac{1}{p^{r-1}} + \ \ldots\ + a_{-1}\frac{1}{p} + a_0 + a_1 p + a_2 p^2 + \ \ldots$$

Quando não houver dúvida quanto ao número primo p considerado, escreveremos simplesmente $\ldots a_2 a_1 a_0, a_{-1}a_{-2}\ldots a_{-r}$. Se $a_l = 0$ para todo $l > k$, escreveremos $a_k a_{k-1}\ldots a_0, a_{-1}a_{-2}\ldots a_{-r}$ em vez de $\ldots 000 a_k a_{k-1}\ldots a_0, a_{-1}a_{-2}\ldots a_{-r}$ Por exemplo, para $p = 5$, temos os seguintes números 5-ádicos:

$$\begin{aligned} &\ldots 2222,1234 = 4\cdot\frac{1}{5^4} + 3\cdot\frac{1}{5^3} + 2\cdot\frac{1}{5^2} + 3\cdot\frac{1}{5} + 2 + 2\cdot 5 + 2\cdot 5^2 + \ \ldots \\ &4,2 = \ \ldots 004,2 = 2\cdot\frac{1}{5} + 4 + 0\cdot 5 + 0\cdot 5^2 + \ \ldots = \frac{22}{5}. \end{aligned}$$

3.5 Representação p-ádica de Inteiros

Na seção anterior, vimos que existe uma função que identifica cada número racional com um número racional p-ádico. Veremos agora como encontrar os representantes p-ádicos de números inteiros. A ideia é encontrar uma sequência coerente de soluções do sistema $x - a \equiv 0 \ (mod\ p^n)$.

Exemplo 3.3. Determinar o representante 3-ádico de 7.

Solução: Devemos encontrar uma sequência coerente de soluções do sistema

$$x - 7 \equiv 0 \ (mod\ 3^n).$$

Com efeito,

$$x - 7 \equiv 0 \ (mod\ 3) \Rightarrow x_1 = 1 = 1 \cdot 3^0$$
$$x - 7 \equiv 0 \ (mod\ 3^2) \Rightarrow x_2 = 7 = 1 \cdot 3^0 + 2 \cdot 3^1$$
$$x - 7 \equiv 0 \ (mod\ 3^3) \Rightarrow x_3 = 7 = 1 \cdot 3^0 + 2 \cdot 3^1 + 0 \cdot 3^2$$
$$\ldots$$
$$x - 7 \equiv 0 \ (mod\ 3^n) \Rightarrow x_n = 7 = 1 \cdot 3^0 + 2 \cdot 3^1 + 0 \cdot 3^2 + \ \ldots \ + 0 \cdot 3^{n-1}.$$

Logo o representante 3-ádico de 7 é $1 \cdot 3^0 + 2 \cdot 3^1 + 0 \cdot 3^2 + \ \ldots \ + 0 \cdot 3^n + \ \ldots = (\ldots 0021)_3 = 21$. Nada mais que 7 escrito na base 3. É fácil ver que isso vale para qualquer outro número primo p e inteiro positivo a, ou seja, o inteiro p-ádico associado ao inteiro a é sua representação na base p.

Exemplo 3.4. Determinar representante 2-ádico de -1.

Solução: Devemos encontrar uma sequência coerente de soluções do sistema

$$x + 1 \equiv 0 \ (mod\ 2^n).$$

Com efeito,

$$x + 1 \equiv 0 \ (mod\ 2) \Rightarrow x_1 = 1$$
$$x + 1 \equiv 0 \ (mod\ 2^2) \Rightarrow x_2 = 3 = 1 + 2$$
$$x + 1 \equiv 0 \ (mod\ 2^3) \Rightarrow x_3 = 7 = 1 + 2 + 2^2$$
$$\ldots$$
$$x + 1 \equiv 0 \ (mod\ 2^n) \Rightarrow x_n = 2^n - 1 = 1 + 2 + 2^2 + \ \ldots \ + 2^{n-1}.$$

Logo o inteiro 2-ádico associado a -1 é $1 + 2 + 2^2 + \ \ldots \ + 2^n + \ \ldots = (1.11)_2$. A série que aparece no início do capítulo.

3.6 Adição em $Z_{(p)}$

Veremos agora como somar inteiros *p*-ádicos. Sejam *a* e *b* inteiros *p*-ádicos para algum número primo *p*, ou seja,

$$a = \sum_{i=0}^{\infty} a_i p^i \text{ e } b = \sum_{i=0}^{\infty} b_i p^i.$$

A adição sobre $\mathbb{Z}_{(p)}$ é a operação que leva a e b no inteiro p-ádico

$$a+b=\sum_{i=0}^{\infty} c_i p^i$$

de modo que $c_k = a_k + b_k$, se $a_k + b_k \leq p-1$, caso contrário, $c_k = a_k + b_k - p$, "levando 1"para o próximo coeficiente, a_{k+1}. Tal inteiro p-ádico é chamado *soma de a e b*.

Exemplo 3.5. Determinar a soma $(12021)_3 + (110)_3$.

Solução:

$$\begin{array}{cccccc} & & & 1 & & \\ & 1 & 2 & 0 & 2 & 1 \\ + & & & 1 & 1 & 0 \\ \hline & 1 & 2 & 2 & 0 & 1 \end{array}$$

De fato, $(12201)_3 = 1\cdot 3^4 + 2\cdot 3^3 + 2\cdot 3^2 + 0\cdot 3^1 + 1 = 154 = 142 + 12 = (12021)_3 + (110)_3$.

Exemplo 3.6. Vamos determinar a soma de $(\ldots 111)_2$ com $(\ldots 001)_2$, o representante 2-ádico de 1. Com efeito,

$$\begin{array}{cccccc} & & 1 & 1 & 1 & \\ & \ldots & 1 & 1 & 1 & 1 \\ + & \ldots & 0 & 0 & 0 & 1 \\ \hline & \ldots & 0 & 0 & 0 & 0 \end{array}$$

Assim, $(\ldots 111)_2 + (\ldots 001)_2 = (\ldots 000)_2$, a representação 2-ádica do zero. Isso mostra que $(\ldots 001)_2$ tem que ser a representação 2-ádica de -1.

3.7 Multiplicação em $\mathbb{Z}_{(p)}$

De maneira análoga a realizada com números inteiros, podemos multiplicar inteiros p-ádicos. Só precisamos tomar cuidado quando o resultado de uma operação com dígitos é maior do que p. Se isso acontecer, "levamos"o quociente da divissão por p desse resultado e "deixamos"o resto. Mais precisamente:

Seja p um número primo. Dados os inteiros p-ádicos

$$a=\sum_{i=0}^{\infty} a_i p^i \text{ e } b=\sum_{i=0}^{\infty} b_i p^i.$$

A multiplicação sobre $\mathbb{Z}_{(p)}$ é a operação que associa a e b ao inteiro p-ádico

$$a \cdot b = \sum_{i=0}^{\infty} c_i p^i,$$

onde os coeficientes c_k são obtidos da seguinte maneira: Tomamos $d_k = \sum_{i=0}^{k} a_i b_{k-i}$. Depois definimos c_0 como o resto da divisão de d_0 por p e, para $k > 0$, definimos c_k como o resto da divisão de $d_k + q$ por p, onde q é quociente da divisão de d_{k-1} por p.

Exemplo 3.7. Encontrar os representantes 3-ádicos de 758 e 8 e efetuar a multiplicação desses inteiros 3-ádicos.

Solução:

$38 = 3^3 + 3^2 + 2 = (1102)_3$,

$8 = 2 \cdot 3^1 + 2 = (2,2)_3$.

					1	
			1	1	0	2
		x			2	2
			2	2	1	1
	+	2	2	1	1	
	1	0	2	0	2	1

De fato, $(102021)_3 = 304 = 38 \cdot 8$.

Exemplo 3.8. Efetuar a multiplicação dos representantes 5-ádicos dos números 98 e 73.

Solução: Primeiro observe que $98 = (343)_5$ e $73 = (243)_5$. Daí,

					2	1	
					3	4	3
				x	2	4	3
				2	1	3	4
			3	0	3	2	
	+	1	2	4	1		
		2	1	2	1	0	4

Na conta acima, note que $3 \cdot 3 = 9 = 5 \cdot 1 + 4$. Daí, “levamos" 1 e “deixamos" 4. Continuando, $3 \cdot 4 + 1 = 13 = 5 \cdot 2 + 3$. Então, “levamos" 2 e “deixamos" 3 e assim por diante.

3.8 Representação p-ádica de Inteiros Negativos

Vimos na seção 3.5 que a representação 2-ádica de -1 é infinita. Mostraremos agora que isso vale para qualquer número primo p. Consequentemente, a representação p-ádica de qualquer inteiro negativo também será infinita, pois todo inteiro negativo é da forma $-k = (-1) \cdot k$, onde $k \in \mathbb{Z}^+$.

Com efeito, seja p um número primo. Consideremos o sistema de congruências $x + 1 \equiv 0 \ (mod\, p^n)$. Temos

$$x \equiv -1 \ (mod\, p) \rightarrow x_1 = p - 1$$
$$x \equiv -1 \ (mod\, p^2) \rightarrow x_2 = p^2 - 1$$
$$x \equiv -1 \ (mod\, p^3) \rightarrow x_3 = p^3 - 1$$
$$\dots$$

A sequência $(p-1, p^2-1, p^3-1, \dots p^n-1, \dots)$ obtida é coerente. De fato, $p^{n+1} - 1 - (p^n - 1) = p^n(p-1)$ é divisível por p^n.

Agora observe que,

$$\begin{aligned} p^n - 1 &= p^{n-1} + (p-1) \cdot p^{n-1} \\ &= p^{n-2} + (p-1) \cdot p^{n-2} + (p-1) \cdot p^{n-1} \\ &= p^{n-3} + (p-1) \cdot p^{n-3} + (p-1) \cdot p^{n-2} + (p-1) \cdot p^{n-1} \\ &\dots \\ &= (p-1) \cdot p^0 + (p-1) \cdot p^1 + \dots + p(-1) \cdot p^{n-2} + (p-1) \cdot p^{n-1}. \end{aligned}$$

Logo o representante p-ádico de -1 será

$$(\dots(p-1)(p-1)(p-1)(p-1))_p.$$

Dado $k \in \mathbb{Z}^+$, para determinarmos a representação p-ádica de $-k$, basta multiplicarmos a representação p-ádica de k pela de -1. Ou seja, se $k = (a_n \dots a_2 a_1)_p$, então

$$-k = (a_n \dots a_2 a_1)_p \cdot (\dots(p-1)(p-1)(p-1)(p-1))_p.$$

Logo a representação de $-k$ será infinita, pois a representação de -1 é infinita.

Exemplo 3.9. Determinar a representação 3-ádica de -17.

Solução: Temos

$-1 = (\dots 222)_3$ e $17 = (122)_3$. Daí

$$\begin{array}{cccccccc} & \ldots & 2 & 2 & 2 & 2 & 2 \\ & x & & & 1 & 2 & 2 \\ \hline & \ldots & 2 & 2 & 2 & 2 & 1 \\ & \ldots & 2 & 2 & 2 & 1 & \\ + & \ldots & 2 & 2 & 2 & & \\ \hline & \ldots & 2 & 2 & 1 & 0 & 1 \end{array}$$

Logo $-17 = (..222101)_3$.

3.9 Representação p-ádica de Números Racionais

Sejam $r = \frac{a}{b}$ um número racional escrito na forma de fração irredutível e p um número primo. Se p não divide b, então sabemos, da proposição 3.7, que r possui um inteiro p-ádico correspondente. Tal inteiro p-ádico pode ser determinado achando uma sequência de soluções coerente do sistema de congruências

$$bx \equiv a \ (mod\, p^n).$$

Por outro lado, se p divide b, então, de acordo com proposição 3.7, $p^m r \in \mathbb{Z}_{(p)}$, onde p^m é a maior potência de p que divide b. Daí, para encontrarmos a representação p-ádica de r, basta dividir o inteiro p-ádico associado a $p^m r$ por p^m.

Exemplo 3.10. Determinar o representante 5-ádico do número $\frac{2}{3}$.
Solução: Devemos olhar para o sistema de congruências

$$3x \equiv 2 \ (mod\, 5^n). \tag{3.5}$$

Para $n = 1$, temos

$$3x \equiv 2 \ (mod\, 5) \ \rightarrow x_1 = 4.$$

Agora, façamos $x = x_n + 5^n y$ na congruência

$$3x \equiv 2 \ (mod\, 5^{n+1}).$$

Obtemos

$$3(x_n + 5^n y) \equiv 2 \ (mod\, 5^{n+1}) \tag{3.6}$$

$$3 \cdot 5^n y \equiv 2 - 3x_n \ (mod\, 5^{n+1}). \tag{3.7}$$

Daí,

$$n = 1 \rightarrow 15y \equiv -10 \ (mod\ 5^2) \rightarrow y = 1 \rightarrow x_2 = 9$$

$$n = 2 \rightarrow 75y \equiv -25 \ (mod\ 5^3) \rightarrow y = 3 \rightarrow x_3 = 84$$

$$n = 3 \rightarrow 375y \equiv -250 \ (mod\ 5^4) \rightarrow y = 1 \rightarrow x_4 = 209$$

$$n = 4 \rightarrow 1875y \equiv -625 \ (mod\ 5^5) \rightarrow y = 3 \rightarrow x_3 = 2084$$

$\ldots$

Como $5^n = mdc(3 \cdot 5^n, 5^{n+1})$ divide $2 - 3x_n$ a congruência (3.7) sempre terá solução. Isso garante a existência de uma sequência coerente de soluções do sistema de congruências (3.5):

$$x = (4, 9, 84, 209, 2084, 5209, \ \ldots).$$

Escrevendo cada termo dessa sequência na base 5, obtemos

$$x_1 = 4 = 4 \cdot 5^0$$

$$x_2 = 9 = 4 \cdot 5^0 + 1 \cdot 5^1$$

$$x_3 = 84 = 4 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2$$

$$x_4 = 209 = 4 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 1 \cdot 5^3$$

$$x_5 = 2084 = 4 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4$$

$$x_6 = 5209 = 4 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + 1 \cdot 5^5.$$

Portanto o representante 5-ádico de $\frac{2}{3}$ é

$$4 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + 1 \cdot 5^5 + \ \ldots = (\ldots 131314)_5.$$

Podemos verificar esse resultado multiplicando-o pelo representante 5-ádico de 3 e constando que o produto é o representante de 2:

$$\begin{array}{cccccccc} & & & 1 & 2 & 1 & 2 & \\ & \ldots & 1 & 3 & 1 & 3 & 1 & 4 \\ \text{x} & \ldots & 0 & 0 & 0 & 0 & 0 & 3 \\ \hline & \ldots & 0 & 0 & 0 & 0 & 0 & 2 \end{array}$$

Exemplo 3.11. Determinar o representante 3-ádico do número $\frac{5}{18}$.

Solução: Vamos atrás do representante 3-ádico de $3^2 \cdot \frac{5}{18} = \frac{5}{2}$. Para encontra-lo, devemos achar

uma sequência coerente de soluções dos sistema de congruências $2x \equiv 5 \ (mod\ 3^n)$. Com efeito, para $n = 1$, temos

$$2x \equiv 5 \ (mod\ 3) \ \rightarrow x_1 = 1 = 1 \cdot 5^0.$$

Façamos $x = x_n + 3^n y$ na congruência

$$2x \equiv 5 \ (mod\ 3^{n+1}).$$

Obtemos,

$$2(x_n + 3^n y) \equiv 5 \ (mod\ 3^{n+1})$$
$$2 \cdot 3^n y \equiv 5 - 2x_n \ (mod\ 3^{n+1}).$$

Daí,

$$n = 1 \rightarrow 6y \equiv 3 \ (mod\ 3^2) \ \rightarrow y = 2 \rightarrow x_2 = 7 = 1 \cdot 3^0 + 2 \cdot 3$$
$$n = 2 \rightarrow 18y \equiv -9 \ (mod\ 3^3) \ \rightarrow y = 1 \rightarrow x_3 = 16 = 1 \cdot 3^0 + 2 \cdot 3 + 1 \cdot 3^2$$
$$n = 3 \rightarrow 54y \equiv -27 \ (mod\ 3^2) \ \rightarrow y = 1 \rightarrow x_3 = 43 = 1 \cdot 3^0 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3$$
$$\ldots$$

Logo,

$$\frac{5}{18} = \frac{1}{3^2} \ 1 \cdot 3^0 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \ \ldots = \frac{1}{3^2} + \frac{2}{3} + 1 + 1 \cdot 3 + 1 \cdot 3^2 + \ \ldots$$
$$= (..111,21)_3.$$

3.10 Representação p-ádica de Números Irracionais Algébricos e Imaginários

Veremos nessa seção que alguns números irracionais e até mesmo alguns números imaginários possuem representantes p-ádicos. Mas antes precisamos introduzir uma definição importante.

Definição 3.11. Seja p um número primo. Dizemos que $d \in \mathbb{Z}$ é um *resíduo quadrático* módulo p se a congruência

$$X^2 \equiv d \ (mod\ p)$$

possuir solução.

Por exemplo, $0^2 \equiv 0\ (mod\ 5), 1^2 \equiv 1\ (mod\ 5), 2^2 \equiv 4\ (mod\ 5), 3^2 \equiv 4\ (mod\ 5), 4^2 \equiv 1\ (mod\ 5)$. Não é difícil provar que todos os resíduos quadráticos módulo 5 são congruentes a 0, 1 e 4.

Exemplo 3.12. Encontre, se existir, o representante 7-ádico de $\sqrt{2}$.

Solução: Devemos olhar para o sistema de congruências

$$x^2 \equiv 2\ (mod\ 7^n)$$

cuja a equação correspondente tem como soluções $\pm\sqrt{2}$.

Para $n = 1$, temos

$$x^2 \equiv 2\ (mod\ 7). \tag{3.8}$$

Essa congruência possui duas soluções positivas menores do que 7, $x_1 = 3$ e $x_1^0 = 4 \equiv -3\ (mod\ 7)$. Façamos $x = x_n + 7^n y$ na congruência

$$x^2 \equiv 2\ (mod\ 7^{n+1}).$$

Obtemos,

$$(x_n + 7^n y)^2 \equiv 2\ (mod\ 7^{n+1})$$
$$x_n^2 + 2 \cdot x_n \cdot 7^n y + 7^{2n} y^2 \equiv 2\ (mod\ 7^{n+1})$$
$$2 \cdot x_n \cdot 7^n y \equiv 2 - x_n^2\ (mod\ 7^{n+1}).$$

Para $n = 1$, temos

$x_1 = 3$	$x_1 = 4$
$42y \equiv -7\ (mod\ 7^2)$	$56y \equiv -14\ (mod\ 7^2)$
$y = 1 \rightarrow x_2 = 10$	$56y = 5 \rightarrow x_2^0 = 39$

Para $n = 2$, temos

$x_2 = 10$	$x_2 = 39$
$980y \equiv -98\ (mod\ 7^3)$	$3822y \equiv -1519\ (mod\ 7^3)$
$980y \equiv 245\ (mod\ 7^3)$	$3822y \equiv 196\ (mod\ 7^3)$
$y = 2 \rightarrow x_3 = 108$	$y = 4 \rightarrow x_3 = 235$

Como $7^n = mdc(2 \cdot x_n \cdot 7^n, 7^{n+1})$ divide $2 - x_n^2$, segue que a congruência

$$2 \cdot x_n \cdot 7^n y \equiv 2 - x_n^2 \ (mod\ 7^{n+1})$$

sempre terá solução. Assim, obtemos duas sequências coerentes de soluções do sistema de congruências:

$$(3, 10, 108, \ldots) = 3(3 + 1 \cdot 7, 3 + 1 \cdot 7 + 2 \cdot 7^2, \ldots)$$
$$(4, 39, 235, \ldots) = 4(4 + 5 \cdot 7, 4 + 5 \cdot 7 + 4 \cdot 7^2, \ldots)$$

Portanto os representantes 7-ádicos das soluções da equação $x^2 - 2 = 0$ são $(\ldots, 213)_7$ e $(\ldots 454)_7$. De fato, o resultado da multiplicação de qualquer um desses números por ele mesmo é 2:

$$\begin{array}{rccccc} & & & & 1 & \\ & & \ldots & 2 & 1 & 3 \\ & \text{x} & \ldots & 2 & 1 & 3 \\ \hline & & \ldots & 6 & 4 & 2 \\ & & \ldots & 1 & 3 & \\ + & & \ldots & 6 & & \\ \hline & & \ldots & 0 & 0 & 2 \end{array} \qquad \begin{array}{rccccc} & & & & 3 & 2 \\ & & \ldots & 4 & 5 & 4 \\ & \text{x} & \ldots & 4 & 5 & 4 \\ \hline & & \ldots & 5 & 1 & 2 \\ & & \ldots & 6 & 6 & \\ + & & \ldots & 2 & & \\ \hline & & \ldots & 0 & 0 & 2 \end{array}$$

Note que a congruência (3.5) só tem solução porque 2 é um resíduo quadrático módulo 7. Analogamente, $\sqrt{a}$, onde $a \in \mathbb{Z}_+$, terá representante p-ádico se, e somente se, a for resíduo quadrático módulo p. Outra coisa interessante de se notar é que, diferente das representações dos dois exemplos anteriores, as representação acima não aparentam ter algum tipo de periodicidade.

Exemplo 3.13. Determine, se existir, o representante 5-ádico de *i*, a unidade imaginária.
Solução: Lembremos que *i* é raiz da equação

$$x^2 + 1 = 0$$

cujo sistema de congruências correspondente é

$$x^2 + 1 \equiv 0 \ (mod\ 5^n). \tag{3.9}$$

Para $n = 1$, temos

$$x^2 + 1 \equiv 0 \ (mod\ 5).$$

A congruência acima possui duas soluções positivas menores do que 5, a saber $x_1 = 2$ e $x_1^0 = 3$. Fazendo $x = x_n + 5^n y$ na congruência

$$x^2 + 1 \equiv 0 \ (mod\ 5^{n+1})$$

obtemos

$$(x_n + 5^n y)^2 + 1 \equiv 0 \ (mod\ 5^{n+1})$$
$$x_n^2 + 2x_n 5^n y + 5^{2n} y^2 + 1 \equiv 0 \ (mod\ 5^{n+1})$$
$$2x_n 5^n y \equiv -1 - x_n^2 \ (mod\ 5^{n+1}).$$

Fazendo novamente $n = 1$, conseguimos

$$x_1 = 2 \qquad\qquad x_1 = 3$$
$$20y \equiv -5 \ (mod\ 5^2) \qquad\qquad 30y \equiv -10 \ (mod\ 5^2)$$
$$y = 1 \rightarrow x_2 = 7 \qquad\qquad y = 3 \rightarrow x_2^0 = 18.$$

Para $n = 2$, temos

$$x_2 = 7 \qquad\qquad x_2 = 18$$
$$350y \equiv -50 \ (mod\ 5^3) \qquad\qquad 900y \equiv -325 \ (mod\ 5^3)$$
$$y = 2 \rightarrow x_3 = 57 \qquad\qquad y = 2 \rightarrow x_3^0 = 68.$$

Do mesmo modo que no exemplo anterior, a congruência

$$2x_n 5^n y \equiv -1 - x_n^2 \ (mod\ 5^{n+1})$$

sempre terá solução. Obtemos assim duas sequências coerentes de soluções do sistema de congruências (3.6):

$$(2, 7, 57, \ldots) = 2(2 + 1 \cdot 5, 2 + 1 \cdot 5 + 2 \cdot 5^2, \ldots)$$
$$(3, 18, 68, \ldots) = 3(3 + 3 \cdot 5, 3 + 3 \cdot 5 + 2 \cdot 5^2, \ldots).$$

Logo os inteiros p-ádicos $(\ldots 212)_5$ e $(\ldots 233)_5$ correspondem aos números complexos $\pm i$. Sendo que o cálculo feito não nos permite saber se existe alguma periodicidade na representação, nem qual inteiro p-ádico corresponde a qual número complexo.

Novamente podemos verificar que multiplicando os inteiros p-ádicos obtidos por eles mesmos conseguimos os três primeiros dígitos do resultado esperado, $(\ldots 444)_5 = -1$:

		1			
		...	2	1	2
	x	...	2	1	2
		...	4	2	4
		...	1	2	
+		...	4		
		...	4	4	4

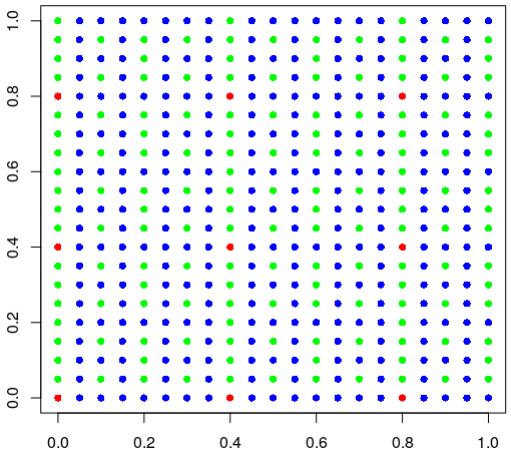
		1	2	1	
		...	2	3	3
	x	...	2	3	3
		...	3	0	4
		...	0	4	
+		...	1		
		...	4	4	4

4 O TEOREMA DE MONSKY

O teorema 3.1 (Chevalley) garante que existe uma extensão do valor absoluto2-ádico para o corpo dos números reais. Por comodidade, denotaremos essa extensão por $|\cdot|$ em vez de $|\cdot_2|$. Vamos colorir os pontos do plano cartesiano com as cores 1, 2 e 3 de modo que o ponto $P = (x,y)$ receba a cor

$$\begin{cases} 1, \text{ se } |x| < 1 \text{ e } |y| < 1; \\ 2, \text{ se } |x| \geq 1 \text{ e } |x| \geq |y|; \\ 3, \text{ se } |y| \geq 1 \text{ e } |y| > |x|. \end{cases}$$

Figura 13 – Coloração dos pontos $(0,05n; 0,05n)$, com $0 \leq n \leq 20$. As cores 1, 2 e 3 são vermelho, azul e verde, respectivamente. Observer que Q tem um único lado com extremidades de cores 1 e 2

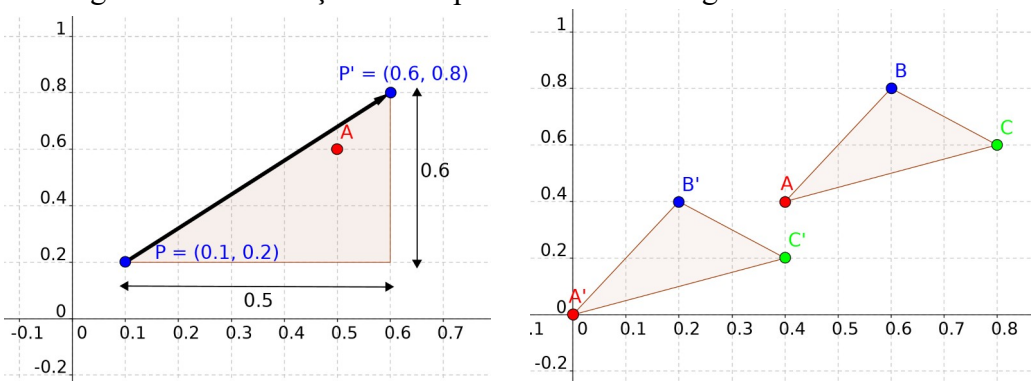


Fonte: elaborada pelo autor.

Definição 4.1. Seja A o ponto de coordenadas (a,b), fixo. A translação por A é a transformação que leva um ponto $P = (x,y)$ no ponto $P^0 = (x+a, y+b)$.

Intuitivamente, transladar uma figura geométrica corresponde a desloca-la em determinado direção sem gira-la. É possível provar que esse tipo de transformação leva retas em retas e leva triângulos em triângulos de mesma área.

Figura 14 – Translação de um ponto e de um triângulo



Fonte: elaborada pelo autor.

Lema 4.1. A translação por um ponto de cor 1 não altera a cor do ponto transladado. Em outras palavras, se o ponto $A = (a,b)$ tem cor 1, então o ponto $P^0 = (x+a, y+b)$ tem a mesma cor que $P = (x,y)$.

Demonstração. Lembremos que o valor absoluto 2-ádico é não-arquimediano, isto é, $|x+y| \leq max(|x|, |y|)$. Logo

(i) Se P tem cor 1, então $|x| < 1$ e $|y| < 1$. Daí, $|x+a| \leq max(|x|, |a|)$ e $|y+b| \leq max(|y|, |b|)$, ou seja, $|x+a| < 1$ e $|y+b| < 1$.

(ii) Se P tem cor 2, então $1 \leq |x| = |x+a-a| \leq max(|x+a|, |a|)$. Mas, se $max(|x+a|, |a|) = |a|$, então $|x| \leq |a| < 1$, um absurdo. Logo $max(|x+a|, |a|) = |x+a|$ e, consequentemente $|x+a| \geq 1$. Ademais, $|y+b| \leq \max(|y|, |b|) \leq \max(|x|, |b|) \leq |x| \leq |x+a|$.

(iii) Se P tem cor 3, então a prova é análoga a (ii).

□

Lema 4.2. Qualquer reta no plano contem pontos de no máximo duas cores.

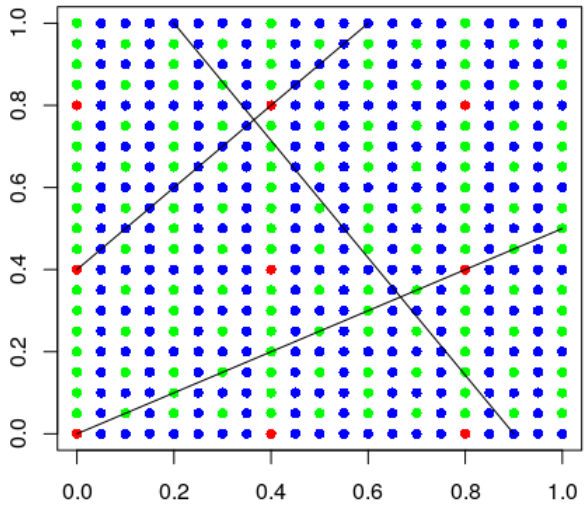
Demonstração. Suponhamos que exista uma reta r com pontos das três cores. Então r possui um ponto $A = (a,b)$ de cor 1. Denotemos por $-A$ o ponto de coordenadas $(-a, -b)$. Como $|-a| = |a|$ e $|-b| = |b|$, segue $-A$ também tem cor 1. Seja r' a translação de r por $-A$. Temos que

(i) pelo lema 4.1, r' também possui pontos das três cores.

(ii) r' passa pela origem do plano cartesiano, pois $A = (a,b)$ é levado pela translação em $(a-a, b-b) = (0,0)$.

(iii) r' não é o eixo y, já que, todos os pontos do eixo y têm cor 1 ou 3 e, por (i), r' tem pontos de cor 2.

Figura 15 – Retas contêm pontos com no máximo duas cores



Fonte: elaborada pelo autor.

Logo r' tem equação da forma $y = mx$. Sejam $B = (c,d)$ e $C = (e,f)$ pontos de r' com as cores 2 e 3, respectivamente. Então, $\frac{d}{c} = \frac{f}{e} = m$ e, consequentemente, $|de| = |cf|$. Porém, $|c| \geq |c|$ e $|f| > |e|$. Daí, $|cf| = |c||f| > |c||e| = |ce|$. Um absurdo. □

Lema 4.3. Qualquer triângulo completo, isto é, com vértices de cores diferentes, tem área com valor absoluto 2-ádico maior do que 1.

Demonstração. Sejam T um triângulo completo e V seu vértice de cor 1. Seja T' o triângulo obtido pela translação de T por -V. Do lema 4.1, segue que T' também é completo. Assim, T' tem um vértice na origem do plano cartesiano e os outros dois vértices, digamos (x,y) e (x^0,y^0), com as cores 2 e 3, respectivamente.

Denotemos por $|\cdot|_0$ o valor absoluto usual. Da Geometria Analítica, sabemos que

$$\text{Área de T'} = \frac{1}{2}\det\begin{pmatrix} 0 & 0 & 1 \\ x & y & 1 \\ x^0 & y^0 & 1 \end{pmatrix}\Bigg|_0 = \frac{1}{2}|(xy^0 - x^0y)|_0,$$

Daí,

$$|\text{Área de T'}| = \frac{1}{2}|xy^0 - x^0y|_0 = \frac{1}{2}\cdot|xy^0 - x^0y| = 2\cdot|xy^0 - x^0y|.$$

Por hipótese, $|x| \geq 1$, $|x| \geq |y|$, $|y|_0 > 1$ e $|y^0| > |x|_0$. Daí $|xy^0| > 1$ e $|xy^0| > |x^0y|$. Ademais,

$$|xy^0| = |xy^0 - x^0y + x^0y| \leq \max(|xy^0 - x^0y|, |x^0y|).$$

Logo $\max(|xy^0 - x^0y|, |x^0y|) = |xy^0 - x^0y|$ e, consequentemente, $|xy^0 - x^0y| > 1$.

Portanto, $|\text{Área de T}| = |\text{Área de T'}| > 1$. □

Teorema 4.1. (Monsky) Um quadrado não pode ser dividido em um número ímpar de triângulos de mesma área.

Demonstração. Considerando o lado do quadrado como unidade de medida, podemos supor que seus vértices são $(0,0)$, $(1,0)$, $(1,1)$ e $(0,1)$. Suponhamos também que esse quadrado foi subdivido em n triângulos T_i de área $\frac{1}{n}$.

Do lema 4.2, segue que nenhum lado (do quadrado ou de algum triângulo T_i) contem pontos das três cores. Como Q tem exatamente um lado cujas extremidades têm as cores 1 e 2, segue, do lema 2.2 (Sperner), que existe um triângulo T_i completo. Do lema 4.3, temos que $|\text{Área de } T_i| = \frac{1}{n} > 1$. Portanto n tem que ser par. □

4.1 Generalizações

O problema de Richman e a solução dada por Monsky inspiraram vários outros problemas semelhantes que passaram a ser chamados **problemas de equidissecção**.

Uma *dissecção* de um polígono P é um conjunto de triângulos não sobrepostos cuja união é P. Uma dissecção com n triângulos é chamada de *n-dissecção* e pode ser classificada em ímpar ou par de acordo com a paridade de *n*. Uma *equidissecção* é uma dissecção com triângulos de mesma área.

As definições anteriores podem ser generalizadas para dimensões arbitrárias usando polítopos, simplexos e volume em vez de polígonos, triângulos e área, respectivamente.

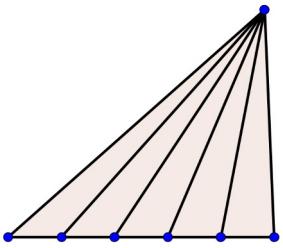
O problema geral que podemos enunciar é: **Dado um polígono (ou polítopo), determinar quais n-equidissecções são possíveis.**

Começemos com polígonos de três lados. É fácil ver que um triângulo pode ser particionado em qualquer número *n* de triângulos não sobrepostos e de mesma área. Basta dividir um de seus lados em *n* segmentos congruentes usando $n-1$ pontos e traçar segmentos de reta unindo esses pontos ao vértice oposto ao lado.

Segue do resultado acima que, se um polígono possui uma *n*-equidissecção, então ele também possui uma *mn*-equidissecção, para todo $m \in \mathbb{N}$. De fato, podemos subidivir cada triângulo de sua *n*-equidissecção em *m* triângulos de mesma área.

Definição 4.2. Fixados $a,b > 0$. Uma dilatação é uma função $d : \mathbb{R}^2 \to \mathbb{R}^2$ que leva o ponto $A(x,y)$ no ponto $A'(ax,by)$.

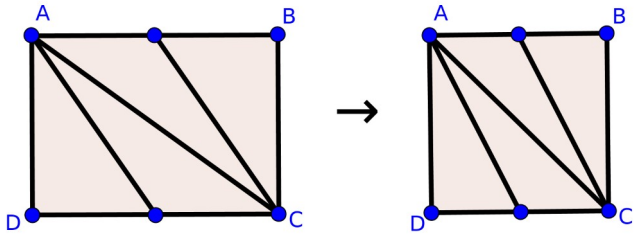
Figura 16 – 5-equidissecção de um triângulo



Fonte: elaborada pelo autor.

Informalmente, dilatar uma figura equivale a estica-la ou contrai-la na direção dos eixos do plano cartesiano. É possível provar que esse tipo de transformação leva equidissecções em equidissecções. Logo retângulos também só podem ser particionados em um número par de triângulos de mesma área. Pois, se um retângulo possuisse equidissecção ímpar, ele poderia ser transformado por uma dilatação num quadrado com equidissecção ímpar. O que é um absurdo, segundo o teorema de Monsky.

Figura 17 – 4-equidissecção de um retângulo levada numa 4-equidissecção de um quadrado por uma dilatação



Fonte: elaborada pelo autor.

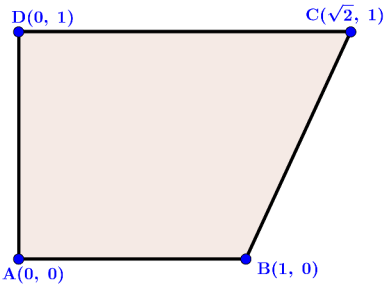
Para quadriláteros em geral o problema é mais complicado. Por exemplo, o trapézio de vértices $(0,0)$, $(0,1)$, $(1,0)$ e $(a,1)$ não possui equidissecções se a for um número transcendente (resultado devido ao matemático americano Sherman Stein). Mas para $a = \sqrt{2}$ não se sabe se existem equidissecções.

Quanto a polígonos com um número arbitrário de lados, temos os seguintes resultados.

Definição 4.3. Dizemos que um polígono P é centralmente simétrico se existe um ponto C tal que, para todo ponto $A \in P$, existe um ponto $A^0 \in P$ de modo que C é o ponto médio do segmento AA^0.

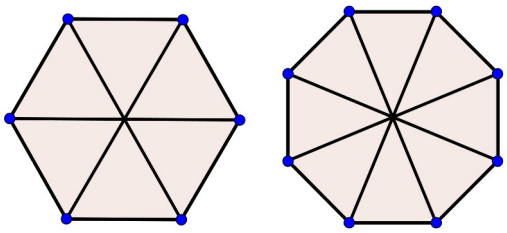
Teorema 4.2. (Monsky, 1990) Toda equidissecção de um polígono centralmente simétrico é par. Particularmente, toda equidissecção de um polígono com o número par de lados é par.

Figura 18 – O trapézio acima pode ser dividido em triângulos de mesma área?



Fonte: elaborada pelo autor.

Figura 19 – Equidissecção de um pentágono e de um hexágono



Fonte: elaborada pelo autor.

Teorema 4.3. Seja P um polígono de n lados, $n > 4$. Se P possui uma m-equidissecção, então n divide m.

Para dimensões arbitrárias, temos o seguinte teorema devido a David Mead:

Teorema 4.4. Se um cubo n-dimensional for particionado em simplexos de mesmo n-volume, então o número de simplexos é divisível por $n!$. Particularmente, se um cubo for particionado em tetraedros de mesmo volume, então o número de tais tetraedros é múltiplo de 6.

Aqui mais um problema em aberto: Um poliedro n-dimensional centralmente simétrico pode ser particionado em um número ímpar de simplexos de mesma área?

As demonstrações dos teoremas anteriores seguem a mesma ideia usado no teorema de Monsky e podem ser encontradas em (STEIN *et al.*, 1994) junto com outros resultados semelhantes.

5 CONSIDERAÇÕES FINAIS

Estudando a demonstração do Teorema de Monsky aprendemos conceitos e métodos importantes de várias áreas da matemática como o lema de Sperner (Combinatória), congruência (Teoria de Números), valores absolutos (Análise), etc. Muitos desses conceitos podem ser trabalhados no ensino básico.

O lema de Sperner, por exemplo, pode ser apresentado como uma ferramenta para resolução de outros problemas combinatórios ou através de jogos como o "Impacto"(AZAMBUJA, 2014).

Problemas de dissecção (dos quais o problema de Richman é um exemplo) existem nos mais diversos níveis de dificuldade e podem ser trabalhados como motivação para o estudo de área de figuras planas e outros tópicos da Geometria. O professor até mesmo a questão resolvida com o teorema de Monsky como um desafio e, posteriormente, como um tema de pesquisa.

REFERÊNCIAS

AIGNER, M.; ZIEGLER, G. M.; HOFMANN, K. H.; ERDOS, P. **Proofs from the book**. [*S. l.*]: Springer, 2010. v. 274.

AMORIM, E. F. d. **Números p-ádicos e o teorema de Monsky**. São Paulo: ICMC, 2015. Disponível em: http://legal.icmc.usp.br/lib/exe/fetch.php?media=slides:monsky.pdf. Acesso em: 08 jan. 2019.

AZAMBUJA, T. A. R. d. **Os lemas de Sperner no ensino médio e uma modesta introdução à topologia.** São Paulo: Universidade Estadual Paulista (UNESP), 2014.

COXETER, H. S. M. **Regular polytopes.** [*S. l.*]: Courier Corporation, 1973.

GOUVÊA, F. **p-adic numbers**: an introduction. [*S. l.*]: Springer-Verlag Berlin Heidelberg, 1997.

JACOBSON, N. **Lectures in abstract algebra**: part III, theory of fields and Galois theory. [*S. l.*]: Springer, New York, 1975.(Graduate texts in mathematics, 32).

LANG, S. **Álgebra para graduação.** [*S. l.*]: Ed. Ciência Moderna, 2008.

LIMA, E. L. **Curso de análise, vol. 2**. [*S. l.: s. n.*], 2008. v. 2.

LIMA, E. L. **Curso de análise, v. 1**. Rio de Janeiro: Projeto Euclides, 2010.

MONSKY, P. On dividing a square into triangles. **The American Mathematical Monthly**, United States, v. 77, n. 2, p. 161–164, 1970.

SANTOS, J. P. D. O. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, v. 3, 2000.

SILVA, J. M. V. da. **Completamentos dos racionais e o teorema de Ostrowski**. 2018. 58 p. Dissertação (Mestrado) – Universidade Federal do Ceará, Fortaleza, 2018.

STEIN, S.; SZABÓ, S. **Algebra and tiling**: homomorphisms in the service of geometry. [*S. l.*]: Cambridge University Press, 1994.

THOMAS, J. A dissection problem. **Mathematics Magazine,** United States, v. 41, n. 4, p. 187–190, 1968.

XU, M. **Sperner's lemma**. United States: University of California (Berkeley), 2012. Disponível em: https://math.berkeley.edu/~moorxu/misc/equiareal.pdf. Acesso em: 01 jan. 2019.