UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

JOSÉ MARIO VIANA DA SILVA

COMPLETAMENTOS DOS RACIONAIS E O TEOREMA DE OSTROWSKI

FORTALEZA

2018

JOSÉ MARIO VIANA DA SILVA

COMPLETAMENTOS DOS RACIONAIS E O TEOREMA DE OSTROWSKI

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Alberto Duarte Maia

FORTALEZA
2018

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

S58c Silva, José Mário Viana da.
Completamentos dos racionais e o teorema de Ostrowski / José Mário Viana da Silva. – 2018.
57 f. : il.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2018.
Orientação: Prof. Dr. José Alberto Duarte Maia.

1. Completamentos. 2. Valores absolutos. 3. Teorema de Ostrowski. 4. Números p-ádicos. I. Título.
CDD 510

JOSÉ MARIO VIANA DA SILVA

COMPLETAMENTOS DOS RACIONAIS E O TEOREMA DE OSTROWSKI

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____

Prof. Dr. José Alberto Duarte Maia (Orientador)

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Jonatan Floriano da Silva

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Francisco Regis Vieira Alves

Instituto Federal de Educação do Ceará (IFCE)

Aos meus pais, Terezinha e Antônio.

AGRADECIMENTOS

Agradeço a energia consciente que rege a existência, o geômetra do universo, a quem chamamos de Deus.

Agradeço a minha família, em especial aos meus pais, Antônio e Terezinha, que me ensinaram o valor da educação.

A minha esposa Karyne, que me acompanha, incentiva com paciência e generosidade.

Agradeço meus irmãos Henrique e Patrícia pelo exemplo.

Agradeço a meu orientador Prof. Dr. José Alberto, pela disponibilidade e compreensão.

Agradeço a professora Aline Parente, pela generosidade e trabalho de revisão.

Agradeço a todos os professores do programa, a SBM e a CAPES pela oportunidade ofertada a tantos professores de matemática.

E por fim agradeço a todos que contribuíram com bons sentimentos e palavras carinhosas para esta conquista.

“A matemática prospera em simplicidades, e, se necessário, os matemáticos as inventam artificialmente para fornecer uma porta de entrada para problemas mais complexos.” (STEWART, 2013, p. 165)

RESUMO

É possível definir diferentes funções do tipo valor absoluto em um corpo K, o que influencia a maneira como se trabalham distâncias nesse corpo e, por conseguinte, a ideia de proximidade. Esse fato provoca consequências importantes nas condições de convergência das sequências de Cauchy, utilizadas na abordagem devida a Cantor para se alcançar o completamento de um corpo. O presente trabalho tem como objetivo mostrar quais os valores absolutos podem ser definidos em $\mathbb{Q}$, a fim de que sejam construídos diferentes completamentos do corpo dos racionais. Tal problema foi solucionado pelo matemático Alexander Markowich Ostrowski, em um dos teoremas que levam o seu nome. O Teorema de Ostrowski mostra que só existem três famílias de valores absolutos não equivalentes entre si em $\mathbb{Q}$. Assim, qualquer valor absoluto nos racionais ou é equivalente ao valor absoluto usual, ou é equivalente a algum valor absoluto p-ádico, ou é o próprio valor absoluto trivial.

Palavras-chave: Corpo. Teorema de Ostrowski. Valores absolutos. Completamento. Números p-ádicos.

ABSTRACT

It is possible to define different absolute value functions in a field K, which influences the way in which distances are worked in this body and hence the idea of proximity in this body. This fact has important consequences in the conditions of convergence of the Cauchy sequences, used in the approach due to Cantor to reach the completion of a body. The present work aims to show which absolute values can be defined in $\mathbb{Q}$, to construct different completions of the rational body. Such a problem was solved by the mathematician Alexander Markowich Ostrowski, in one of the theorems that bear his name. Ostrowski's Theorem shows that there are only three families of absolute values not equivalent to each other in Q. Thus, any absolute value in the rational is either equivalent to the usual absolute value or is equivalent to some absolute value p-adic or is itself trivial absolute value.

Keywords: Field. Ostrowski's theorem. Absolute values. Completions. P-adic numbers.

.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Desde a Antiguidade, os matemáticos conheciam diversos exemplos de segmentos incomensuráveis, apresentando medidas que não poderiam ser representadas pela razão de dois naturais. Na realidade, tratava-se de exemplos de números os irracionais. Tais exemplos refletem a carência dos números racionais em atender às necessidades exigidas na abordagem de diversos problemas. Essa constatação está nas antigas raízes da busca pela compreensão da passagem do conjunto dos números racionais $\mathbb{Q}$ para o conjunto $\mathbb{R}$ dos números reais. Esse problema não foi solucionado de forma linear e nem tão pouco célere. Mais de dois milênios se passaram até que, em meados do século XIX, a partir das pesquisas, em especial, de Augustin-Louis Cauchy, Karl Weierstrass, Richard Dedekind e Georg Cantor, se apresentassem caminhos rigorosos para a construção dos reais como extensão dos racionais.

Os resultados foram de tão profunda repercussão e influência, que não é exagero afirmar que o grosso da matemática conhecida se alicerça no sistema de números reais. Daí, percebemos a importância da construção formal de números de natureza tão intrigante.

Entretanto, números tão perturbadores quanto os irracionais ainda estavam por surgir. Em 1897, Kurt Hensel, interessado no estudo dos números algébricos, propôs uma analogia entre o estudo das funções racionais e o estudo dos números algébricos. Fixado um número inteiro positivo e primo p, existiria para cada número racional n uma expansão em série de potências da forma

$$n = \sum_{i=k}^{\infty} a_i \cdot p^i \text{, onde } k, a_i \in \mathbb{Z}, \text{ e } 0 \leq a_i < p.$$

Tais números foram chamados de p-ádicos e apresentavam um problema desconcertante: A argumentação envolvendo convergência, nos moldes como vinha sendo feito até então, a partir dos estudos da Análise, não fazia sentido para esses números. O motivo dessa inconsistência estava na necessidade de uma nova noção de distância, compatível com a natureza dos novos números de Hensel. O próprio conceito de limite necessita de uma estrutura que permita trabalhar com a noção de proximidade. Esta estrutura é o valor absoluto.

O interessante é que, a partir dessa estrutura, adequada para o trato com os números p-ádicos, podemos alcançar este novo conjunto numérico como uma extensão do conjunto $\mathbb{Q}$ dos números racionais, a exemplo do que fora feito com o conjunto $\mathbb{R}$ dos números reais. Esse processo é conhecido como completamento.

Ao associarmos cada número racional a um ponto de uma reta, perceberemos que, sobram pontos da reta. O processo de completamento “tapa esses buracos”, alcançando o

conjunto dos números reais de maneira a identificá-lo completamente com a reta. O mesmo pode ser feito para alcançarmos o conjunto $\mathbb{Q}_p$ dos números p-ádicos, partindo de um valor absoluto diferente do usualmente utilizado no conjunto dos racionais. Esse valor absoluto diferente do usual é o valor absoluto p-ádico e, a partir dele, chegamos em uma forma de medir distâncias bem conflitante com nosso senso, acostumado ao valor absoluto usual trazendo assim, como consequência propriedades interessantes ao conjunto $\mathbb{Q}_p$.

Uma dessas propriedades reside no caráter singular de sua topologia, em que por exemplo, as bolas são conjuntos abertos e fechados em que qualquer um de seus pontos pode ser o seu centro, e representa uma das grandes motivações para estudar o sistema numérico $\mathbb{Q}_p$.

Surge então a questão principal que perseguimos nesse trabalho: quais os valores absolutos que podem ser definidos em $\mathbb{Q}$ a fim de construirmos diferentes completamentos do corpo dos racionais? Essa questão foi respondida em 1916, pelo matemático ucraniano Alexander Markowich Ostrowski, um aluno de Hensel. Também buscamos apresentar o conceito de completamento e os caminhos para se alcançar os completamentos de $\mathbb{Q}$.

No capítulo inicial, apresentamos alguns conceitos e resultados que servirão de base para os capítulos seguintes. Escolhemos apenas os resultados e conceitos mais importantes, tendo em vista que muitos outros são apresentados também ao longo dos demais capítulos. No segundo capítulo, fazemos uma breve introdução à teoria dos valores absolutos, abordando os principais pontos necessários para atingirmos nosso objetivo. No terceiro capítulo discorremos sobre o conceito de completamento e sua relação com os valores absolutos. Já no quarto capítulo convidamos o leitor a se familiarizar com os p-ádicos e para isso, mostramos algumas propriedades e fatos interessantes a respeito desses números. E finalmente, no quinto capítulo caracterizamos valores absolutos equivalentes e demonstramos o teorema que responde nosso questionamento geral.

Procuramos construir um passeio agradável através do estudo das possibilidades de extensão dos números racionais para corpos completos. O tema já é intrigante pela sua natureza, mas além disso, mostra-se bastante frutífero para o desenvolvimento da ciência matemática possibilitando diversas aplicações em pesquisas modernas da Teoria dos Números, inclusive na demonstração do resultado conhecido como Último Teorema de Fermat.

2 PRELIMINARES

Neste capítulo, serão apresentadas definições, resultados e observações que sintetizam os principais conceitos e ideias que utilizaremos em nossos próximos passos.

Buscamos ser bastante sintéticos, relembrando o conceito de anel e de corpo como estruturas algébricas singulares, dotadas de propriedades com consequências interessantes. Finalizamos abordando o conceito de homomorfismo e subtipos especiais.

2.1 Corpos e suas propriedades

Um dos principais conceitos da álgebra moderna certamente é o de corpo. Essa estrutura sintetiza as propriedades mais interessantes e desejáveis a uma estrutura algébrica e desempenhará um papel central em nossa caminhada. Por isso iniciamos nossa explanação apresentando os conceitos relacionados e a definição de corpo.

Definição 2.1.1. *Um conjunto K, munido de duas operações chamadas de adição e multiplicação, e denotado por* $(K,\cdot,+)$, é *chamado de anel se atende às seguintes propriedades*:

A1. Associatividade da adição e da multiplicação:

$$(x+y)+z = x+(y+z) \text{ e } (xy)z = x(yz)$$

A2. Comutatividade da adição.

$$x+y = y+x$$

A3. Existência de elemento neutro da adição (comumente representado por 0) e da multiplicação (comumente representado por 1) distintos um do outro:

$$x+0 = 0+x = x \text{ e } x\cdot 1 = 1\cdot x = x$$

A4. Existência do inverso aditivo.

$$\forall x \in K, \exists -x \in K; x+(-x) = 0$$

A5. Distributividade da multiplicação em relação à adição à esquerda e à direita.

$$x(y+z) = (y+z)x = xy + xz$$

Se tomarmos apenas a operação de adição para os elementos do conjunto K, atendendo às propriedades acima, $(K,+)$ é um grupo abeliano (comutativo). Entretanto, se vale a comutatividade também para a multiplicação dizemos que $(K,\cdot,+)$ é um anel comutativo com unidade.

Definição 2.1.2. *Se K é um anel comutativo, e para todo $x,y \in K$ temos $x\cdot y = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que* $(K,\cdot,+)$ é *um domínio de integridade*.

Definição 2.1.3. *Se K é um dominio de integridade, e para todo $x \in K, x \neq 0$, $\exists\, x^{-1} \in K$ tal que $x \cdot (x^{-1}) = 1$, dizemos que $(K, \cdot, +)$ é um corpo.*

Um subconjunto S de um anel K é dito um subanel de K se S for um anel com as operações de K. Podemos demonstrar que S é um subanel de K se e somente se $0 \in S$ e para todos $a, b \in S$ temos $a - b$ e ab também pertencentes a S.

Vejamos agora algumas definições importantes para nossos próximos passos.

Definição 2.1.4. *Um subanel I de um anel K é chamado um ideal de K se para todo $a \in K$ e todo $x \in I$ temos $ax \in I$ e $xa \in I$.*

Definição 2.1.5. *Um ideal $I \neq K$ (equivalente a $1 \notin I$) do anel K é um ideal primo de K se para qualquer a e $b \in K$, o fato $ab \in I$ implica $a \in I$ ou $b \in I$.*

Definição 2.1.6. *Um ideal $M \neq K$ do anel K é um ideal maximal se, para qualquer ideal I de K, o fato $M \subseteq I$ implica $I = M$ ou $I = K$.*

Seja K um anel e I um ideal de K, pode-se mostrar que a relação definida por $x \sim y \Leftrightarrow x - y \in I$ para elementos de K é uma relação de equivalência em K. Seja $[x]$ a classe de equivalência dos elementos de K equivalentes a x por $\sim$, temos:

$$[x] = \{y \in K; y \sim x\} = \{y \in K; x - y \in I\} = \{y \in K; y \in x + I\}$$

Assim podemos usar a notação $[x] = x + I$ e definir o conjunto quociente de K por I como

$$K/I = \{x + I; x \in K\}.$$

Definindo as operações $(x + I) + (y + I) = (x + y + I)$ e $(x + I) \cdot (y + I) = (xy + I)$ em K/I, que independem dos representantes de cada classe (deve ser verificado), é possível demonstrar que K/I é um anel comutativo com unidade chamado de anel quociente.

A respeito do anel quociente, deixamos o resultado a seguir, que será de grande utilidade para nós.

Proposição 2.1.1. *Se K é uma anel comutativo com unidade e I um ideal de K, então*:

(i) *K/I é um dominio de integridade se e somente se I é primo.*

(ii) *K/I é um corpo se e somente se I é Maximal.*

(iii) *Todo ideal maximal de K é primo.*

Demonstração.

Para demonstrar (i), lembramos que K/I é um anel comutativo com unidade $[1] = 1 + I \neq 0 + I = [0]$ evidentemente, pois de outra forma teríamos $1 \in I$, o que é um absurdo, pois I é primo. Agora perceba que $[ab] = [a][b] = (a + I)(b + I) = 0 + I = [0] = I$ equivale

a dizer que $ab \in I$, que é primo e, portanto, $a \in I$ ou $b \in I$.

Para demonstrar a tese (ii), inicialmente, vamos assumir que K/I é um corpo e a existência de um ideal J tal que $I \subseteq J \subseteq K$. Vamos supor $I \neq J$. Então existe $a \in J \backslash I$, e assim $[a] \neq [0]$. Como K/I é um corpo, existe $[b] \in K/I$, tal que, $[b][a] = [1]$, de onde temos que $ab - 1 \in K$. Portanto, existe $i \in I \subseteq J$ tal que $1 = ab + i$. Como $a \in J$, temos que $ab \in J$. E consequentemente $1 \in J$, logo $J = K$. E assim inferimos que I é maximal.

Reciprocamente, como K/I é um anel comutativo com unidade, basta mostrar que se I é maximal, então cada elemento não nulo de K/I tem inverso. Seja $[a] \in K/I$, tal que $[a] \neq [0]$, ou seja $a \notin I$. Tomando o ideal aK, temos $I \subsetneq I + aK \subseteq K$, e como I é maximal temos $I + aK = K$. Logo, existem $i \in I$ e $k \in K$ tais que $1 = i + ak$. Daí concluímos que $[1] = [i] + [ak] = [ak]$. Logo a é invertível.

Para demonstrar a tese (iii), suponhamos a e $b \in I$ maximal de K, tais que $ab \in I$. Se $a \notin I$, e tomemos o ideal aK. A soma de ideais é um ideal então $I + aK$ é um ideal de K. Uma vez que $1 \in K$ temos $a = 0 + 1a \in I + aK$. Mas $a \notin I$ e, então $I \subsetneq I + aK \subseteq K$. Mas I é maximal, então $I + aK = K$. Logo podemos afirmar que $1 \in I + aK$. Assim existem $i \in I$ e $k \in K$ tais que $1 = i + ak$, que multiplicando por b encontramos $b = bi + (ab)k$. Sabemos $i \in I$, então $ib \in I$. Também $ab \in I$, então $abk \in I$. Logo $b = bi + (ab)k \in I$. Portanto I é ideal primo.

■

2.2 Funções entre corpos

Uma classe especial de funções entre estruturas algébricas (grupos, anéis ou espaços vetoriais) muito especial é o homomorfismo. Por definição, homomorfismo é uma função que respeita e preserva a propriedades dessas estruturas. Exibiremos aqui a definição relativa ao homomorfismo de anéis.

Definição 2.2.7. *Sejam A e A' anéis, uma função $f: A \to A'$ é dita um homomorfismo se valem as propriedades*:

i. $f(x + y) = f(x) + f(y)$

ii. $f(xy) = f(x)f(y)$

Seja f um homomorfismo, chamamos de núcleo de f o conjunto representado por $Ker(f) = \{a \in A; f(a) = 0 \in A'\}$.

Abaixo citamos algumas propriedades importantes de um homomorfismo.

Proposição 2.2.2. *Se* $f: A \to A'$ é *um homomorfismo de anéis, então*:

i. $0 \in Ker(f)$, ou seja, $f(0) = 0$;

ii. $f(-a) = -f(a)$;

iii. $f(a - b) = f(a) - f(b)$

iv. f é injetivo, se e somente se, $Ker(f) = \{0\}$;

v. $Ker(f)$ é um ideal de A;

vi. $Im(f)$ é um subanel de A'

Um homomorfismo bijetivo é chamado de isomorfismo e cumpre o papel de ser uma ferramenta singular que possibilita a análise de uma estrutura por meio de outra. Chamamos de endomorfismo um homomorfismo $f: A \to A$. E um endomorfismo bijetor de automorfismo.

Finalizamos esse capítulo com um conceito que será útil logo a frente.

Definição 2.2.8. *Uma função* $f: K \to K'$, *onde* K *e* K' *são corpos,* é *dita uma imersão se* f $satisfaz$.

i. $f(x + y) = f(x) + f(y)$

ii. $f(xx) = f(x)f(y)$

iii. $Ker(f) = \{0\}$.

Perceba que a definição acima, em suas duas primeiras exigências, estabelece primeiramente que uma imersão entre corpos se trata de um homomorfismo. Já a terceira exigência garante que uma imersão é sempre injetiva.

3 VALORES ABSOLUTOS

No presente capítulo, apresentaremos uma breve introdução à teoria geral dos valores absolutos em corpos. O valor absoluto usual do conjunto $\mathbb{R}$ dos reais é definido a partir da ordem usual. No entanto, ao tomarmos o conjunto $\mathbb{C}$ dos números complexos, percebemos um exemplo da possibilidade de extensão do valor absoluto sem a extensão da ordem. Assim, estudar os valores absolutos aplicados em corpos diversos mostra-se uma abordagem bastante interessante.

Uma utilidade importante dos valores absolutos é que, através deles, podemos estabelecer a ideia de distância e, desse modo, a noção de proximidade. Tal noção é uma peça chave para a definição do conceito de limite, influenciando o conceito de convergência de sequências e a definição de uma topologia em um corpo.

3.1 Valores absolutos em um corpo

É possível definir um valor absoluto como uma função em um corpo ordenado qualquer. Entretanto, para os nossos objetivos nesse trabalho, podemos nos restringir à definição de valor absoluto como uma função que associa cada elemento de um corpo K a um número real não negativo.

Definição 3.1.9. *Seja K um corpo, uma função* $|\ \ |: K \to \mathbb{R}_+$ *é dita um valor absoluto de K se atender às seguintes propriedades, para todo $x, y \in K$:*

P1. $|x| = 0 \Leftrightarrow x = 0$

P2. $|x \cdot y| = |x| \cdot |y|$

P3. $|x + y| \leq |x| + |y|$ $(Desigualdade\ triangular)$

As propriedades exigidas na definição são bastante naturais a partir da nossa experiência com o valor absoluto usual. Esse valor absoluto (citado na introdução do capítulo), com $K = \mathbb{R}$, é definido da seguinte forma:

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

Pode ser dito que esse valor absoluto induz um valor absoluto em $\mathbb{Q}$, pela inclusão do corpo dos racionais em $\mathbb{R}$. E o mesmo também pode ser dito do valor absoluto usual do conjunto dos números complexos $\mathbb{C}$ (para $(a, b) \in \mathbb{C}$, temos $|(a, b)| := \sqrt{a^2 + b^2}$), em relação ao conjunto dos números reais $\mathbb{R}$. Assim os três casos são compreendidos como o valor absoluto usual. A partir de agora usaremos a notação $|\ \ |_\infty$ para representá-lo. O símbolo ∞ é comum para diferenciá-lo de outros valores absolutos. Aqui esse costume também será adotado.

Um fato interessante é que para um valor absoluto qualquer $|\ \ |$ em um corpo K arbitrário, para todo $r \in \mathbb{R}$ com $0 < r \leq 1$ a função definida por $|\ \ |^r$ também é um valor absoluto em K. Com efeito, $|\ \ |^r$ satisfaz as propriedades P1 e P2, já que $|\ \ |$ é um valor absoluto. Já a propriedade P3 é consequência do fato de para a e b reais positivos vale $(a+b)^r \leq a^r + b^r$ [1]. Fazendo $a = |x|$ e $b = |y|$ segue que $|x+y|^r \leq (|x| + |y|)^r \leq |x|^r + |y|^r$ provando a validade de P3 para $|\ \ |^r$.

A proposição abaixo mostra algumas propriedades dos valores absolutos.

Proposição 3.1.3. *Seja a função* $|\ \ |: K \to \mathbb{R}_+$ *um valor absoluto do corpo* K, *então são válidas as propriedades abaixo* :

i. $|1| = 1$;

ii. $|-x| = |x|$, *para todo* $x \in K$;

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

iv. $|x| - |y| \leq |x - y| \leq |x| + |y|$ *para todo* $x, y \in K$;

v. $|x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|$, *para todo* $x_1, x_2, \ldots, x_n \in K$.

Demonstração.

Para demonstrar i, basta perceber que $|1| = |1 \cdot 1| = |1| \cdot |1|$, e dividindo ambos os lados por $|1|$ obtemos que $|1| = 1$.

Para demonstrar ii, primeiramente é necessário mostrar que $1 = |1| = |(-1) \cdot (-1)| = |-1| \cdot |-1| = |-1|^2$, e aplicando a raiz quadrada, obtemos $|-1| = 1$. Portanto $|-x| = |(-1)x| = |(-1)| \cdot |x| = 1 \cdot |x| = |x|$.

Já para provar iii. basta observar que $1 = |1| = |x \cdot x^{-1}| = |x| \cdot |x^{-1}|$, e dividindo ambos os membros por $|x|$, obtemos $|x^{-1}| = |x|^{-1}$.

A propriedade iv. é consequência da desigualdade triangular. Primeiro veja que $|x| = |x - y + y| \leq |x - y| + |y|$, e somando $-|y|$ a ambos os lados da desigualdade segue a primeira desigualdade. A segunda desigualdade é imediata a partir da desigualdade triangular, combinada com a propriedade ii.

Finalmente a propriedade v é obtida por indução sobre n. Para $n = 1$, a afirmação é verdadeira. Assumindo válida para $n - 1$, temos:

$$|x_1 + x_2 + \cdots + x_n| \leq |x_1 + x_2 + \cdots + x_{n-1}| + |x_n| \leq |x_1| + |x_2| + \cdots + |x_n|$$

■

[1] De fato $f(x) = \frac{(a+b)^x}{a^x + b^x}$, com a e b reais positivos, é estritamente crescente no intervalo]0,1], e para valores de x nesse intervalo temos $\frac{1}{2} < f(x) \leq 1$.

Um exemplo bem simples, mas que pode ser definido para qualquer corpo K, é o valor absoluto definido da forma abaixo, que é chamado de valor absoluto trivial.

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

Seja K um corpo qualquer, a validade de P1 para esse valor absoluto é diretamente verificada pela definição. Para x e $y \in K$, se $x = 0$ ou $y = 0$, tem-se $|x \cdot y| = 0 = |x| \cdot |y|$. Já se ambos forem não nulos temos $|x \cdot y| = 1 = |x| \cdot |y|$. E assim está provada P2. Se $x = y = 0$ a propriedade P3 é evidente. Se $x \neq 0$ ou $y \neq 0$ basta observar que $|x + y| \leq 1 = \max\{|x|, |y|\} \leq |x| + |y|$.

Podemos observar que todo valor absoluto de um corpo K determina um homomorfismo do grupo multiplicativo K^* no grupo $\mathbb{R}_+^*$ dos reais estritamente positivos. Também é possível mostrar que o único valor absoluto que podemos definir em um corpo finito é o valor absoluto trivial.

Um conceito que possui uma relação interessante com um tipo especial de valores absolutos que trataremos daqui a pouco é o conceito de valorizações de um corpo. Não nos aprofundaremos no estudo das valorizações, pois isso extrapolaria os objetivos deste trabalho, mas citaremos sua definição formal no intuito de enfatizar a importância deste conceito.

Definição 3.1.10. *Uma valorização v em um corpo K é uma função $v: K \to \mathbb{R} \cup \{\infty\}$ que* satisfaz as seguintes condições:

V1. $v(x) = \infty \Leftrightarrow x = 0$;

V2. $v(x + y) \geq \min\{v(x), v(y)\}, para\ todo\ x, y \in K$;

V3. $v(xy) = v(x) + v(y), para\ todo\ x, y \in K$.

Onde convencionamos $x + \infty = \infty$, $\infty + \infty = \infty$ e $a < \infty, para\ todo\ a \in \mathbb{R}$.

Note que a valorização se comporta de forma semelhante ao logaritmo, transformando produtos em somas. Tomaremos aqui um exemplo de valorização que será de grande importância para o desenvolvimento de nosso trabalho: a valorização p-ádica.

Definição 3.1.11. (Valorização p-ádica) *Dado um p primo, a valorização $p-$ádica* de *um número racional* é *definida como o inteiro dado por*:

$$\begin{cases} v_p(x) = \max\{n \in \mathbb{Z}_+ : p^n | x\} \text{ se } x \in \mathbb{Z}^* \\ v_p(q) = v_p(a) - v_p(b) \text{ se } q = \dfrac{a}{b} \in \mathbb{Q} \\ v_p(0) = \infty \end{cases}$$

Perceba que a valorização p-ádica é uma função $v_p: \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Podemos observar que para um inteiro x tem-se que, $x = p^{v_p(x)} \cdot x'$ onde $p \nmid x'$, e claramente $p|x \Leftrightarrow$

$v_p(x) > 0$. Por exemplo $v_5(40) = 1$ e $v_2(40) = 3$ já que $40 = 2^3 \cdot 5$, e ainda $v_3\left(\frac{2}{9}\right) = -2$. Na verdade, sendo $\mathcal{P}$ o conjunto dos números primos, pelo teorema fundamental da aritmética todo inteiro positivo x (para os negativos basta acrescentar o sinal) pode ser escrito da forma:

$$x = \prod_{p \in \mathcal{P}} p^{v_p(x)}$$

A proposição abaixo mostra que a valorização p-ádica atende a definição geral de valorização de um corpo.

Proposição 3.1.4. *Para $m, n \in \mathbb{Q}$ são validas as seguintes propriedades da valorização $p-$ádica*:

(i). $v_p(m \cdot n) = v_p(m) + v_p(n)$

(ii). $v_p(m + n) \geq \min\{v_p(m), v_p(n)\}$

Demonstração.

Para o caso de $m = 0$ ou $n = 0$, basta observar as convenções $x + \infty = \infty$, $\infty + \infty = \infty$, onde $\infty > x$ para todo $x \in \mathbb{Z}$.

Excluindo-se os casos anteriores, sendo $m = \frac{a}{b}$ e $n = \frac{c}{d}$ pode-se afirmar que:

$$v_p(m \cdot n) = v_p\left(\frac{ac}{bd}\right) = v_p\left(\frac{\prod_{q \in \mathcal{P}} q^{v_q(ac)}}{\prod_{q \in \mathcal{P}} q^{v_q(bd)}}\right) = v_p\left(\prod_{q \in \mathcal{P}} q^{v_q(ac)}\right) - v_p\left(\prod_{q \in \mathcal{P}} q^{v_q(bd)}\right)$$

No entanto $ac = \prod_{q \in \mathcal{P}} q^{v_q(a) + v_q(c)}$, logo:

$$v_p(m \cdot n) = v_p(a) + v_p(c) - v_p(b) - v_p(d) = v_p\left(\frac{a}{b}\right) + v_p\left(\frac{c}{d}\right) = v_p(m) + v_p(n)$$

E assim fica demonstrada (i).

Para demonstrar (ii) inicialmente para $m, n \in \mathbb{Z}$, pode-se afirmar que $p^{v_p(m)} | m$ e $p^{v_p(n)} | n$. Seja $l = \min\{v_p(m), v_p(n)\}$ sabe-se que $p^l | m$ e $p^l | n$, logo $p^l | m + n$. O que garante que $v_p(m + n) \geq l = \min\{v_p(m), v_p(n)\}$.

Para $m, n \in \mathbb{Q}$ tem-se:

$$v_p(m + n) = v_p\left(\frac{a}{b} + \frac{c}{d}\right) = v_p\left(\frac{ad + bc}{bd}\right) = v_p(ad + bc) - v_p(bd)$$

Como $ad, cb \in \mathbb{Z}$, e já provamos que (ii) vale para inteiros, podemos afirmar que:

$$\begin{aligned} v_p(m + n) &= v_p(ad + bc) - v_p(bd) \\ &\geq \min\{v_p(ad), v_p(bc)\} - v_p(bd) \\ &= \min\{v_p(ad) - v_p(bd), v_p(bc) - v_p(bd)\} \end{aligned}$$

$$= \min\left\{v_p\left(\frac{a}{d}\right), v_p\left(\frac{c}{d}\right)\right\}$$
$$= \min\{v_p(m), v_p(n)\}$$

E assim fica demonstrado (ii).

■

Em analogia ao que vimos para inteiros, para um racional $x = \frac{a}{b}$, também podemos representá-lo por $x = p^{v_p(x)}\frac{a'}{b'}$, tal que $p \nmid a' \cdot b'$. Outro fato importante é que a valorização p-ádica independe da representação em forma de fração, pois $v_p\left(\frac{ac}{bc}\right) = v_p(ac) - v_p(bc) = v_p(a) + v_p(c) - v_p(b) - v_p(c) = v_p\left(\frac{a}{b}\right)$.

Definição 3.1.12. (Valor Absoluto p-ádico) *A função* $|\ |_p: \mathbb{Q} \to \mathbb{R}_+$, *onde* p *é um número primo, e definida por*:

$$|x|_p = \begin{cases} p^{-v_p(x)}, se\ x = p^{v_p(x)}\dfrac{a}{b} \neq 0 \text{ tal que } p \nmid a \cdot b \\ 0, se\ x = 0 \end{cases}.$$

é um valor absoluto em $\mathbb{Q}$, *e é chamado de valor absoluto* $p-$ *ádico.*

De fato $|\ \ |_p$ satisfaz as propriedades de valor absoluto. Como para todo $x \neq 0$, $|x|_p = p^{-v_p(x)} > 0$, tem-se que $|x|_p = 0$ se, e somente se, $x = 0$. Se $x = 0$ ou $y = 0$ então $|x \cdot y|_p = 0 = |x|_p \cdot |y|_p$. Agora se $x \neq 0$ e $y \neq 0$ pode-se escrever $x = p^{v_p(x)}\frac{a}{b}$ e $y = p^{v_p(y)}\frac{c}{d}$, com $p \nmid abcd$. Portanto $|x \cdot y|_p = \left|p^{v_p(x)}\frac{a}{b} \cdot p^{v_p(y)}\frac{c}{d}\right|_p = p^{-v_p(x)-v_p(y)} = |x|_p \cdot |y|_p$. Finalmente basta mostrar que $|\cdot|_p$ atende a desigualdade triangular. Para isso é conveniente dividir a argumentação em casos:

Caso 1. Se $x = 0$ ou $y = 0$, então $|x + y|_p = |x|_p + |y|_p$.

Caso 2. Se $x + y = 0$, então $|x + y|_p = |0|_p = 0 \leq |x|_p + |y|_p$.

Caso 3. Se nenhum dos casos anteriores ocorrem, então é possível escrever $x = p^{v_p(x)}\frac{a}{b}$ e $y = p^{v_p(y)}\frac{c}{d}$ com $p \nmid abcd$. Sem perda de generalidade, supondo $v_p(x) \leq v_p(y)$ tem-se:

$$|x + y|_p = \left|\frac{p^{v_p(x)}\left(ad + p^{v_p(y)-v_p(x)}bc\right)}{bd}\right|_p \leq p^{-v_p(x)} = |x|_p < |x|_p + |y|_p$$

3.2 Métrica induzida por um Valor Absoluto

Mostraremos aqui como os valores absolutos possibilitam uma noção de distância em um corpo K. Assim apresentamos a seguir o conceito matemático relacionado à ideia de distância.

Definição 3.2.13. (Métrica) *Seja A um conjunto não vazio, uma métrica ou distância sobre A é uma função $d: A \times A \to R_+$ tal que para todo x, y e $z \in A$ valem as seguintes propriedades*:

D1. $d(x, y) = 0 \Leftrightarrow x = y$

D2. $d(x, y) = d(y, x)$

D3. $d(x, y) \leq d(x, z) + d(z, y)$

Um par (K, d) com K um conjunto não vazio e d uma métrica em K é denominado de espaço métrico. No conjunto dos números reais, a distância entre dois de seus elementos é dada por $d(x, y) = |y - x|_\infty$. É a métrica chamada de usual. Esse é o exemplo mais familiar, que é compatível com a reta como representação geométrica do conjunto $\mathbb{R}$ dos números reais. Na verdade, se (K, d) é um espaço métrico e A um subconjunto de K, (A, d), é também um espaço métrico. Assim a métrica de A se diz induzida por K, o que permite determinar diversos exemplos de espaços métricos. Para isso basta considerar diversos subconjuntos de um espaço métrico, como por exemplo $(\mathbb{Q}, |\quad|_\infty)$.

Proposição 3.2.5. (Métrica induzida por valor absoluto). *Seja K um corpo* e $|\quad|$ *um valor absoluto em K, a função $d: K \times K \to R_+$ definida por $d(x, y) = |y - x|$ é uma métrica de K.*

Demonstração.

A propriedade D1 de fato é válida pois:

$$d(x, y) = 0 \Leftrightarrow |y - x| = 0 \Leftrightarrow y - x = 0 \Leftrightarrow y = x$$

Uma vez que $d(x, y) = |y - x| = |x - y| = d(y, x)$ fica demonstrada D2.

Finalmente para mostrar a propriedade D3, basta perceber que:

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

■

Evidentemente diferentes valores absolutos podem gerar noções diferentes de distância, e algumas diferem bastante da noção usual vista anteriormente. Uma característica importante para analisar as possibilidades desse comportamento diferenciado é registrada na definição a seguir que define o tipo especial de valor absoluto que citamos anteriormente.

Definição 3.2.14. (Valor Absoluto Arquimediano) *Um valor absoluto de um corpo* K é *dito* não $-$ *arquimediano se para todo* $x, y \in K$ *vale a versão forte da desigualdade triangular*:

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

Do contrário, dizemos que o valor absoluto é arquimediano.

Pelo que foi mostrado anteriormente um exemplo de valor absoluto não-arquimediano é o valor absoluto trivial, enquanto o valor absoluto usual é arquimediano, pois $|1 + 2| = 3 > \max\{|1|, |2|\} = 2$.

Perceba que essa exigência realmente é mais forte que a desigualdade triangular. Com efeito, veja que $|x + y| \leq \max\{|x|, |y|\} < \max\{|x|, |y|\} + \min\{|x|, |y|\} = |x| + |y|$.

Proposição 3.2.6. *Para todo* p *primo,* $|\ \ |_p$ *é um valor absoluto não* $-$ *arquimediano sobre* $\mathbb{Q}$.

Demonstração.

Pela proposição 2.1.4. (ii), pode-se afirmar que: $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Portanto:

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

■

O resultado a seguir ilustra o quanto a noção de métrica induzida por um valor absoluto não-arquimediano pode se afastar da ideia intuitiva a respeito de distância. Também há consequências importantes na noção de topologia em um corpo que apresentaremos logo adiante.

Proposição 3.2.7. (Princípio do triângulo isósceles). *Seja* K *um corpo e* $|\ \ |$ *um valor absoluto não* $-$ *arquimediano em* K. *Sejam* $x, y \in K$, *então ou* $|x| = |y|$ *ou* $|x - y| = |x|$ *ou* $|x - y| = |y|$.

Demonstração.

Como $|x - y| \leq \max\{|x|, |-y|\} = \max\{|x|, |y|\}$, supondo $|x| < |y|$ infere-se que $|x - y| \leq |y|$. Por outro lado $|y| = |y - x + x| \leq \max\{|y - x|, |x|\}$. Como por hipótese $|x| < |y|$, segue $|y| \leq |y - x| = |x - y|$. E portanto $|y| = |x - y|$.

Caso a hipótese assumida for $|y| < |x|$, analogamente infere-se que $|x| = |x - y|$.

Ou seja, se $|x| \neq |y|$ então $|x - y| = \max\{|y|, |x|\}$.

Para o último caso $|x| = |y|$ é imediato.

■

Uma métrica d induzida por um valor absoluto não-arquimediano é chamada de métrica não-arquimediana, e um conjunto K com uma métrica assim é dito espaço métrico não arquimediano. Desta forma, tomando a desigualdade triangular para x, y e $z \in K$, assumindo $|y| < |x| < |z|$, tem-se que:

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

A ilustração acima esclarece o motivo da designação de "Princípio do triângulo isósceles", já que, a partir dessa análise, percebe-se que, geometricamente, todo triângulo em um espaço métrico com uma métrica não-arquimediana é isósceles e, se não for equilátero, o lado de medida diferente é o menor dos três.

Conforme o que foi dito, fica demonstrado que seja (K, d) um espaço métrico, em que d é uma métrica não-arquimediana vale a seguinte propriedade:

$$\forall\, x, y \in K, d(x,z) \leq \max\{d(x,y), d(y,z)\}.$$

Outra curiosidade sobre valores absolutos não-arquimedianos, que vale a pena ser citada, é o fato de que todo elemento de uma bola aberta é centro dessa bola.

Definição 3.2.15. (Bola Aberta). *Sejam K um corpo e $|\cdot|$ um valor absoluto em K, $x_0 \in K$ e $r \in \mathbb{R}_+^*$. O conjunto $B(x_0, r) = \{x \in K : |x - x_0| < r\}$ é chamado de bola aberta de centro x_0 e raio r.*

Proposição 3.2.8. Seja K um corpo, $|\cdot|$ um valor absoluto não-arquimediano em K e $B(x_0, r)$ uma bola aberta em K. Então qualquer $y_0 \in B(x_0, r)$ é centro de $B(x_0, r)$. Ou seja $B(x_0, r) = B(y_0, r)$.

Demonstração.

Como estamos tratando com um valor absoluto não-arquimediano, temos:

$$|y_0 - x| = |y_0 - x_0 + x_0 - x| = \max\{|y_0 - x_0|, |x - x_0|\}$$

Logo, se $x \in B(x_0, r)$ e sabendo que $y_0 \in B(x_0, r)$, pode-se afirmar que:

$$|y_0 - x| < r$$

O que mostra que $B(y_0, r) \supset B(x_0, r)$.

Analogamente, mostra-se que $B(x_0, r) \supset B(y_0, r)$, e assim que $B(y_0, r) = B(x_0, r)$.

■

A proposição a seguir estabelece uma relação entre as valorizações em um corpo K

e os valores absolutos não-arquimedianos desse mesmo corpo K.

Proposição 3.2.9. *Existe uma correspondência bijetora entre as valorizações v de um corpo K e os valores absolutos não − arquimedianos em K*

Demonstração.

Seja v uma valorização em K. Vamos considerar a função $|\ \ |: K \to \mathbb{R}$ definida por $|x| = e^{-v(x)}$, convencionando que $e^{-\infty} = 0$.

Agora provaremos que $|\ \ |$ é um valor absoluto não-arquimediano em K. Primeiro observamos que $|x| = 0 \Leftrightarrow e^{-v(x)} = 0 \Leftrightarrow v(x) = \infty \Leftrightarrow x = 0$. A propriedade P2 dos valores absolutos é evidenciada, pois $|xy| = e^{-v(xy)} = e^{-[v(x)+v(x)]} = e^{-v(x)-v(x)} = e^{-v(x)}e^{-v(y)} = |x||y|$. Finalmente basta provar a desigualdade triangular forte. Para isso, vamos observar que:

$$\begin{aligned} |x+y| &= e^{-v(x+y)} \\ &\leq e^{-\min\{v(x),v(y)\}} \\ &= e^{\max\{-v(x),-v(y)\}} \\ &= \max\{e^{-v(x)}, e^{-v(y)}\} \\ &= \max\{|x|,|y|\} \end{aligned}$$

Assim mostramos que, para cada valorização em K, existe um valor absoluto não-arquimediano em K.

Agora seja $|\ \ |$ um valor absoluto não-arquimediano em K. Convencionando que $-\ln 0 = \infty$, considere a função $v: K \to \mathbb{R} \cup \{\infty\}$, definida por $v(x) = -\ln|x|$.

Vamos mostrar que v é uma valorização em K. De fato $v(x) = \infty \Leftrightarrow -\ln x = \infty \Leftrightarrow x = 0$. Agora sejam $x, y \in K$ tais $xy \neq 0$, então $v(xy) = -\ln|xy| = -\ln|x||y| = -\ln|x| - \ln|y| = v(x) + v(y)$. Pelas convenções adotadas, o resultado também é valido para o caso $xy = 0$. Finalmente se $x + y = 0$, temos $v(x+y) = v(0) = \infty \geq \min\{v(x), v(y)\}$. Se $x = 0$ e $y \neq 0$ temos $v(0+y) = v(y) = \min\{\infty, v(y)\} \geq \min\{v(0), v(y)\}$. Agora se $x \neq 0$, $y \neq 0$ e $x + y \neq 0$, então:

$$\begin{aligned} v(x+y) &= -\ln|x+y| \\ &= \ln|x+y|^{-1} \\ &\geq \ln(\max\{|x|,|y|\})^{-1} \\ &= \ln(\min\{|x|^{-1}, |y|^{-1}\}) \\ &= \min\{\ln|x|^{-1}, \ln|y|^{-1}\} \\ &= \min\{-\ln|x|, -\ln|y|\} \end{aligned}$$

$$= \min\{v(x), v(y)\}$$

Logo para cada valor absoluto não-arquimediano em K existe uma valorização em K, de onde segue o resultado.

■

Encerramos essa seção com o resultado a seguir. Nesta proposição, oferecemos uma caracterização dos valores absolutos não-arquimedianos.

Proposição 3.2.10. *Seja K um corpo e $A \subset K$ o subanel gerado por* 1 *(onde* 1 *é o elemento neutro da multiplicação em K) e $|\ \ |$ é um valor absoluto em K, então as afirmações seguintes são equivalentes*:

(i). $|a| \leq 1$ *para cada* $a \in A$.

(ii). *O conjunto* $\{|a|: a \in A\}$ é *limitado*.

(iii). $|\ \ |$ é *um valor absoluto não arquimediano*.

(iv). *Para todo número real* $n > 0$, *a função* $|\ \ |^n$ é *um valor absoluto em* K.

Demonstração.

Primeiramente percebe-se que a implicação (i) ⇒ (ii) é imediata.

Agora suponha (ii) e tome $C > 0$ em $\mathbb{R}$ de tal modo que

$$|a| \leq C \text{ para todo } a \in A.$$

Sejam x, y elementos de K. Para cada $n \in \mathbb{N}$, vale expansão $(x+y)^n = \sum \binom{n}{i} x^i y^{n-i}$, logo:

$$\begin{aligned}
|x+y|^n &= |x|^n \left|1 + \frac{y}{x}\right|^n \\
&= |x|^n \left|\sum_{i=0}^{n} \binom{n}{i} \left(\frac{y}{x}\right)^i\right| \\
&\leq |x|^n \sum_{i=0}^{n} \left|\binom{n}{i}\right| \left|\left(\frac{y}{x}\right)^i\right| \\
&\leq |x|^n \sum_{i=0}^{n} C \left|\left(\frac{y}{x}\right)^i\right|, \text{ pois } \left|\binom{n}{i}\right| \leq C \\
&\leq |x|^n C(n+1) \max\left\{|1|, \left|\frac{y}{x}\right|, \left|\frac{y}{x}\right|^2, \ldots, \left|\frac{y}{x}\right|^n\right\} \\
&= |x|^n C(n+1) \max\left\{|1|, \left|\frac{y}{x}\right|^n\right\} \\
&= C(n+1) \max\{|x|^n, |y|^n\}
\end{aligned}$$

Agora extraindo a raiz n-ésima e fazendo $n \to \infty$:

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

De onde fica provada (iii).

Agora, supondo (iii) pode-se escrever

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

De onde infere-se que a desigualdade triangular forte vale para $|\ \ |^n$. Já as duas primeiras propriedades dos valores absolutos são diretas.

Finalmente a implicação (iv) ⇒(i) será provada por indução. Suponha (iv), ou seja, que $|\ \ |^n$ é um valor absoluto para qualquer $n \in \mathbb{R}$. A implicação é válida para $a = 1$ pois $|1| = |1|^n = 1 \leq 1$. Agora assumindo que para algum $a \in A$ temos $|a| \leq 1$, consequentemente $|a|^n \leq 1$. Pela desigualdade triangular, para $a + 1$ infere-se que $|a + 1|^n \leq |a|^n + |1|^n$. E pela hipótese de indução

$$|a + 1|^n \leq 1 + 1 = 2$$

Tomando a raiz n-ésima e o limite com $n \to \infty$ obtém-se o resultado $|a + 1| \leq 1$. Logo para todo $a \in A$ tem-se que $|a| \leq 1$ e assim está provado (i).

■

4 COMPLETAMENTOS

Nesse capítulo apresentaremos o conceito de completamento de um corpo com valor absoluto. Esse conceito é extremamente relevante para nosso objetivo uma vez que o Teorema de Ostrowski guarda uma relação importante com os completamentos do conjunto $\mathbb{Q}$ dos números racionais.

Definiremos corpo ordenado e corpo completo e explicaremos o debate que ocorreu ao longo da história do desenvolvimento da matemática envolvendo esses conceitos. Apresentaremos dois caminhos para completar um espaço métrico: cortes de Dedekind e o completamento canônico de Cantor. Nesse sentido, faz-se necessário, discorrermos sobre as sequências de Cauchy, que representam importante ferramenta para alcançarmos e compreendermos nosso objetivo.

4.1 O corpo ordenado completo

Afirmamos que um corpo K é um corpo ordenado quando existe um subconjunto $P \subset K$ que apresenta as seguintes propriedades:

P1. Se $x \in P$ e $y \in P$, então $x + y \in P$ e $xy \in P$;

P2. Se $x \in K$, então ocorre apenas uma das três opções: ou $x \in P$, ou $-x \in P$, ou $x = 0$.

O conjunto P é chamado de conjunto dos elementos positivos de K. Representando por $-P$ o conjunto $\{-x: x \in P\}$, percebemos que $K = P \cup (-P) \cup \{0\}$, em que claramente os três conjuntos são dois a dois disjuntos. A partir dessa propriedade, podemos definir uma relação de ordem total em um corpo ordenado K, afirmando que $x \geq y$ sempre que $x - y \in P \cup \{0\}$. E usamos a notação $x > y$ sempre que $x - y \in P$.

Proposição 4.1.11. *O corpo* $(\mathbb{Q}, +, \cdot)$ *é ordenado.*

Demonstração.

De fato, basta tomar $P = \left\{\frac{p}{q} \in \mathbb{Q}; p \cdot q \in \mathbb{N}\right\}$. Para mostrar P1, tomemos $x, y \in P$.

$$x + y = \frac{p}{q} + \frac{p'}{q'} = \frac{pq' + qp'}{qq'}$$

Como $qq'(pq' + qp') \in \mathbb{N}$, temos que $x + y \in P$.

Para demonstrar P2, basta perceber que, se $p/q \in \mathbb{Q}$, temos três opções: ou $p \cdot q \in \mathbb{N}$ (o que implica que $p/q \in P$), ou $p \cdot q = 0$ (o que implica em $p = 0$ e $p/q = 0$), ou $p \cdot q \notin \mathbb{N}$ (o que implica em $-p/q \in P$).

■

Proposição 4.1.12. *Para todo corpo ordenado* K, *se* $a \in K$ *e* $a \neq 0$, *então* $a^2 \in P$.

Demonstração.

Só restam duas opções. Se $a \in P$, então $a \cdot a = a^2 \in P$. Se $-a \in P$, então $a^2 = (-a) \cdot (-a) \in P$.

■

Assim percebemos que o conjunto $\mathbb{C}$ dos números complexos não é ordenado, uma vez que, pela proposição acima, $i^2 \in P \subset \mathbb{C}$, em que P é o conjunto dos complexos positivos. Mas $i^2 = -1$, e assim teríamos $-1 \in P$. Por outro lado, pela mesma proposição, $(-1)^2 = 1 \in P$ também, o que é um absurdo, pois teríamos 1 e $-1 \in P$, contrariando a propriedade P2 de P.

Outra consequência imediata é que, para $1 \in K$, sempre teremos $1 \in P$ pois $1 = 1^2$. Logo $1 > 0$, pois $1 - 0 = 1$. Também podemos afirmar que $1+\ldots+1 > 0$, ou seja, K apresenta característica 0[2]. Daí percebemos que, em um corpo ordenado K, tem-se, $1 > 0$, $1 + 1 > 1$, $1 + 1 + 1 > 1 + 1$, e assim sucessivamente. Assim identificamos uma cópia isomorfa de $\mathbb{N}$ em qualquer corpo ordenado K. Para isso, seja $1'$ a unidade de K, basta tomar $f: \mathbb{N} \to K$, definida por $f(1) = 1'$ e $f(n+1) = f(n) + 1'$. O conjunto $\mathbb{N}' = f(\mathbb{N})$ será essa cópia (observe que $\mathbb{N}' \subset P$). Considerando o conjunto $-\mathbb{N}' = \{-n; n \in \mathbb{N}'\}$, o conjunto $(-\mathbb{N}') \cup \{0\} \cup \mathbb{N}'$ é uma cópia isomorfa de $\mathbb{Z}$. Dadas essas identificações, costuma-se convencionar $\mathbb{N} \subset \mathbb{Z} \subset K$. Desta forma sejam $m, n \in \mathbb{Z}$, com $n \neq 0$, existe $n^{-1} \in K$, e tomando o conjunto formado por $m \cdot n^{-1} = \frac{m}{n} \in K$, identificamos uma cópia de $\mathbb{Q}$ em K. É fácil perceber que essa última cópia é um subcorpo de K. Graças aos isomorfismos citados, dado um corpo ordenado K, é comum convencionar as inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset K$.

Resta então alcançarmos um corpo muito especial: o corpo $\mathbb{R}$ dos números reais. As definições abaixo nos ajudam nessa missão se optarmos por um caminho inspirado nas ideias de Richard Dedekind (1831-1916).

Seja $X \subset K$, onde K é um corpo ordenado. Dizemos que $y \in K$ é uma cota superior de X se para todo $x \in X$ temos $y \geq x$ e afirmamos que X é limitado superiormente. Analogamente, se $y \leq x$ para todo $x \in X$, y é dita cota inferior e X é dito limitado inferiormente.

Definição 4.1.16. *Seja K um corpo ordenado, e $X \subset K$, é um subconjunto limitado superiormente de K. O elemento $x \in K$ é o supremo de X, e é designado por* $\sup X$ *se*:

S1. x *é cota superior de* X

S2. y *é uma cota superior de* X, *então* $x \leq y$

[2] Um corpo em que qualquer soma sucessiva do elemento neutro da multiplicação $(1 + 1 + \cdots + 1)$ não tem como resultado o elemento neutro da adição (0).

Definição 4.1.17. *Seja K um corpo ordenado, e $X \subset K$ é um subconjunto limitado inferiormente de K. O elemento $x \in K$ é o ínfimo de X, e é designado por* $\inf X$ *se*:

I1. *x é cota inferior de X*

I2. *y é uma cota inferior de X, então $x \geq y$.*

Inspirado na matemática da Grécia antiga, Dedekind assume a reta como modelo de conjunto com as propriedades desejáveis ao conjunto dos reais. Assumindo uma associação entre os racionais e os pontos de uma reta, ele percebeu que sobram pontos da reta. Para "completar" esse conjunto, Dedekind concebe o conceito de "corte". Por esse conceito, estabelece-se que o conjunto dos números racionais pode ser "cortado" em duas partes não vazias, disjuntas e complementares do conjunto $\mathbb{Q}$ dos números racionais.

Definição 4.1.18. *Entenderemos por corte todo par (A_1, A_2) de conjuntos não vazios dos números racionais, cuja união é o próprio $\mathbb{Q}$, e tais que todo elemento de A_1 é menor que todo elemento de A_2.*

Como exemplo, tomemos $A_1 = \{x \in \mathbb{Q}; x > 1\}$ e $A_2 = \mathbb{Q} \backslash A_1$. Evidentemente o número racional que define o corte é o número racional 1, mas também existem cortes que não são determinados por números racionais. O exemplo mais comum é $A_2 = \{x \in \mathbb{Q}_+^*; x^2 > 2\}$ e $A_1 = \mathbb{Q} \backslash A_2$. A rigor, devemos mostrar que, se existe um número racional que define este corte, ele dever ser tal, que seu quadrado é igual a 2. Entretanto pelo lema abaixo, vemos que tal elemento não existe nos racionais.

Proposição 4.1.13. (Lema de Pitágoras) *Não existe um racional x, tal que $x^2 = 2$.*

Demonstração.

Tomando $z \in \mathbb{Q}$, sabemos que existe a representação irredutível de $z = \frac{m}{n}$, onde m e n são primos entre si e $n \neq 0$. Assumindo que $z^2 = 2$ temos $m^2 = 2n^2$.

De onde podemos afirmar que m^2 é par e consequentemente m é par. Fazendo $m = 2k$, temos:

$$4k^2 = 2n^2 \Leftrightarrow 2k^2 = n^2.$$

Logo, percebemos que n^2 também é par, e consequentemente n também é par. O que é um absurdo, pois m e n são primos entre si.

■

Dedekind estabelece que sempre que encontrarmos um corte como o último apresentado, devemos assumir a existência de um número não racional que determina esse corte, e inclui-lo sempre como maior elemento de A_1 (ou de forma equivalente, como menor

elemento de A_2). Esse processo "completaria" o conjunto $\mathbb{Q}$ dos racionais, criando o conjunto $\mathbb{R}$ dos números reais. É possível provar que, a partir dessa abordagem, o novo conjunto conserva a ordem e as operações do corpo dos racionais e portanto $\mathbb{R}$ é um corpo ordenado "completo".

Uma forma de estabelecer a completude dos números reais é expressa pelo postulado que segue.

Postulado 4.1.19. *Existe um corpo ordenado completo* $\mathbb{R}$*, chamado corpo dos números reais, no qual, todo subconjunto não vazio e limitado superiormente de* $\mathbb{R}$*, possui supremo em* $\mathbb{R}$.

Finalizaremos esta seção com a demonstração de uma importante propriedade de um corpo ordenado completo, a propriedade arquimediana.

Definição 4.1.20. *Um corpo ordenado* K *é dito arquimediano quando a ordem definida em* K *satisfaz a propriedade de Arquimedes*: "*Quaisquer que sejam* $a > 0$ *e* $b > 0$ *em* K*, então existe um número natural* n *tal que* $b < n \cdot a$"

Proposição 4.1.14. *Todo corpo ordenado completo é arquimediano.*

Demonstração.

Seja K um corpo ordenado completo. Vamos tomar o conjunto $S = \{na \in K; n \in \mathbb{N}\}$, onde $0 < a < b,$ e $a, b \in K$.

Como K possui característica 0, o produto na faz sentido, e S é não vazio, pois para $n = 1$ temos $1 \cdot a = a \in S$. Por absurdo, vamos assumir que $b \geq na$, para todo n natural. Dessa forma b é uma cota superior de S e assim S admite $s = \sup S$. Evidentemente $s - a < s$, e como s é a menor das cotas superiores de S, existe $n' \in \mathbb{N}$, tal que $s - a < n' \cdot a < s$, o que implica em $s < a(n' + 1)$, o que é um absurdo, pois $(n' + 1) \in \mathbb{N}$ e $a(n' + 1) \in S$. Logo K é arquimediano.

■

4.2 Sequências

Uma sequência, ou sucessão $\{x_1, x_2, \ldots\}$, em um corpo K é uma função $x: \mathbb{N} \longrightarrow K$. É comum representarmos o valor de $x(n) \in K$, para $n \in \mathbb{N}$, por x_n que chamamos de *n-ésimo termo* da sequência e representar a sequência por $(x_n)_n$.

Se o corpo K é dotado de um valor absoluto, podemos definir uma métrica em K, e assim tratar da convergência de sequências de elementos de K.

Definição 4.2.21. *Seja* K *um corpo com valor absoluto* $|\ \ |$*, uma sequência* $(a_n)_n$ *de*

$elementos\ de\ K$, é $dita\ convergente\ para\ um\ elemento\ a \in K, se\ para\ todo\ \epsilon > 0$ $existe\ n_0 \in \mathbb{N}\ tal\ que\ |a_n - a| < \epsilon, para\ todo\ n > n_0$.

Nesse caso dizemos que o elemento a é o limite da sequência e representamos por $a = \lim a_n$.

4.3 Sequências de Cauchy

Uma família especial de sequências, que desempenhará papel singular em nossa jornada, é definida abaixo.

Definição 4.3.22. $A\ sequência\ (a_n)_n\ em\ K$, é $dita\ uma\ sequência\ de\ Cauchy\ (com\ respeito\ a\ |\ \ |, definido\ em\ K)\ se\ para\ todo\ número\ real\ \epsilon > 0$, $existe\ n_0 \in \mathbb{N}\ tal\ que\ |a_n - a_m| < \epsilon, para\ todo\ n > n_0\ e\ m > n_0\ naturais.$

Evidentemente toda sequência convergente é uma sequência de Cauchy. Com efeito basta perceber que, se $a = \lim a_n$, existe um natural n_0 para o qual $|a_n - a| < \frac{\epsilon}{2}$ para todo $n > n_0$. Assim, se tomarmos n e m maiores que n_0, temos $|a_n - a_m| = |a_n - a - (a_m - a)| \leq |a_n - a| + |a_m - a| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$. Já a recíproca dessa afirmação é um fato que merece uma discussão mais aprofundada, pois define o conceito de corpo completo.

Definição 4.3.23. $Um\ corpo\ K, com\ valor\ absoluto\ |\ \ |, é\ dito\ completo\ se\ toda\ sequencia\ de\ Cauchy\ em\ K\ \ converge\ para\ um\ elemento\ de\ K.$

Pode ser mostrado que, no caso de K ser um corpo ordenado, assumindo os conceitos de cotas superiores, cotas inferiores, supremo e ínfimo para sequências, nos termos dos conjuntos de elementos que formam essas sequências, a definição acima é equivalente ao postulado de completeza.

Representaremos por $S(K)$ o conjunto de todas as sequências de elementos de K e definimos a soma de sequências $(a_n)_n + (b_n)_n = (a_n + b_n)_n$ e o produto de sequências $(a_n)_n \cdot (b_n)_n = (a_n b_n)_n$ para toda $(a_n)_n, (b_n)_n \in S(K)$. Definimos também o conjunto $S_C(K)$ de todas as sequências de Cauchy em K. Dizemos que a sequência $(a_n)_n \in S_C(K)$ é uma sequência nula se $\lim a_n = 0 \in K$.

Relembramos abaixo alguns resultados interessantes da Análise Real relacionados às sequências de Cauchy no conjunto $\mathbb{Q}$ dos números racionais, mas são resultados válidos também para um corpo K qualquer, com valor absoluto $|\ \ |$.

Proposição 4.3.15. $Toda\ sequência\ de\ Cauchy,\ com\ respeito\ a\ |\ \ |, em\ K$ é $limitada.$

Proposição 4.3.16. $Se\ (a_n)_n$ é $uma\ sequência\ de\ Cauchy\ em\ K,\ com\ respeito\ a\ |\ \ |,$

então $(|a_n|)_n$ é *um sequência de Cauchy em* $\mathbb{R}$.

Proposição 4.3.17. *As sequências de Cauchy em* K, *com respeito a* $|\ \ |$, *formam um anel comutativo com unidade*.

Proposição 4.3.18.*O conjunto* $S_0(K)$ *das sequências nulas de* K *formam um ideal no anel* $S_c(K)$ *das sequências de Cauchy*.

Ao analisarmos as condições de convergência de uma sequência, em um espaço métrico completo, basta testar se a sequência é de Cauchy. O que em alguns casos é vantajoso, pois trabalhamos apenas com os termos da própria sequência. Evidentemente a condição de convergência depende da métrica utilizada.

Abaixo definimos uma relação em $S_C(K)$ importante para nossos próximos passos.

Definição 4.3.24. *Se* $(a_n)_n$ *e* $(b_n)_n$ *são duas sequências de Cauchy quaisquer, então* $(a_n)_n \sim (b_n)_n$ *se, e somente se,* $(a_n - b_n)_n$ é *uma sequência nula.*

Proposição 4.3.19. *A relação* $\sim$ *definida acima* é *uma relação de equivalência em* $S_C(K)$ *compatível com as operações de adição e multiplicação em* $S_C(K)$.

Demonstração.

De fato, a relação definida é reflexiva. Com efeito, para toda $(a_n)_n$ em $S_C(K)$ podemos definir a sequência $(a_n - a_n) = (0)$, que é uma sequência nula. Logo $(a_n)_n \sim (a_n)_n$.

Para $(a_n)_n$ e $(b_n)_n$ sequências de Cauchy tais que $(a_n)_n \sim (b_n)_n$ temos $(a_n - b_n)_n$ nula. Assim temos $\lim(a_n - b_n) = 0 \Rightarrow \lim -(b_n - a_n) = 0 \Rightarrow \lim(b_n - a_n) = 0$, e portanto $(b_n)_n \sim (a_n)_n$. O que mostra que $\sim$ é simétrica.

Dadas $(a_n)_n$, $(b_n)_n$ e $(c_n)_n$ sequências de Cauchy, tais que $(a_n)_n \sim (b_n)_n$ e $(b_n)_n \sim (c_n)_n$ e portanto $\lim(a_n - b_n) = 0$ e $\lim(b_n - c_n) = 0$. Como as sequências nulas formam um ideal no anel das sequências de Cauchy, temos $(a_n - c_n) = \big((a_n - b_n) + (b_n - c_n)\big)_n$ é uma sequência nula. E assim fica evidente que $\sim$ é transitiva.

Pelo exposto acima, evidenciamos que $\sim$ é uma relação de equivalência em $S_C(K)$.

Finalmente, sejam $(a_n)_n$, $(b_n)_n$ e $(c_n)_n$ sequências de Cauchy, tais que $(a_n)_n \sim (b_n)_n$. Primeiramente $(a_n)_n \sim (b_n)_n$ implica em $(a_n - b_n)_n = (a_n - b_n + c_n - c_n)_n = (a_n - c_n)_n - (b_n - c_n)_n$ ser uma sequência nula e assim temos $(a_n - c_n)_n \sim (b_n - c_n)_n$. Analogamente temos $\big((a_n - b_n)(c_n)\big)_n = (a_n c_n - b_n c_n)$ uma sequência nula e portanto $(a_n c_n)_n \sim (b_n c_n)_n$.

■

4.4 Completamentos

Começaremos por definir o conceito de completamento de um corpo com valor absoluto.

Definição 4.4.25. (Completamento) *Um completamento de K, com respeito ao valor absoluto* $|\ \ |$ *é o par* $(\widehat{K}, |\widehat{\ }|)$, *consistindo em uma extensão* $\widehat{K}$ *de* K, *e o valor absoluto* $|\widehat{\ }|$ *em* $\widehat{K}$, *satisfazendo as seguintes propriedades.*

(i). $|\widehat{\ }|$ é uma extensão de $|\ \ |$

(ii). K é denso em $\widehat{K}$, com respeito a $|\widehat{\ }|$.

(iii). $\widehat{K}$ é completo com relação a $|\widehat{\ }|$.

Por exemplo, o conjunto $\mathbb{R}$ dos reais é um completamento do conjunto $\mathbb{Q}$ dos racionais. Não vamos nos deter na demonstração desse fato que já nos é familiar. No entanto, no teorema seguinte, generalizamos a construção de um completamento de um espaço métrico, pois na verdade todo corpo com valor absoluto pode ser completado, seguindo passos gerais.

Proposição 4.4.20. (Teorema do completamento) *Todo corpo com valor absoluto pode ser completado.*

Demonstração.

Já vimos que o conjunto das sequências nulas em K, $S_0(K)$ é um ideal no anel das sequências de Cauchy, assim, vamos considerar o anel quociente

$$\widehat{K} \coloneqq S_c(K)/S_0(K).$$

Afirmamos que $\widehat{K}$ é um corpo. Tomando um elemento não nulo $[a_n] \in \widehat{K}$ (lembre-se que $[a_n]$ é uma classe de equivalência das sequências de Cauchy, cuja diferença resulta em uma sequência nula) e $(a_n)_n \in S_c(K)$ um representante de $[a_n]$ podemos afirmar que existe $\epsilon > 0$ e $n_0 \in \mathbb{N}$ tais que

$$|a_n| \geq \epsilon, \forall\ n > n_0.$$

Caso contrário haveria uma subsequência de $(a_n)_n$ convergindo para zero e, consequentemente, a própria $(a_n)_n$ seria convergente para zero, o que sabemos não ser verdade. Assim $a_n \neq 0$ para todo $n > n_0$. Portanto, existe uma sequência de elementos $b_n \in K$ tais que

$$b_n = \frac{1}{a_n}\ , \forall\ n > n_0.$$

Como para $m, n > n_0$ temos

$$|b_n - b_m| = \left|\frac{a_m - a_n}{a_n a_m}\right| = \frac{|a_m - a_n|}{|a_n||a_m|} \leq \frac{|a_m - a_n|}{\epsilon \cdot \epsilon} = \frac{|a_m - a_n|}{\epsilon^2}$$

podemos afirmar que $(b_n)_n$ é uma sequência de Cauchy. Tomando $[b_n] \in \widehat{K}$ como a classe de equivalência de $(b_n)_n$, temos $(a_n b_n - 1)_n \in S_0(K)$, ou seja $(a_n b_n)_n \sim (1)_n$ onde $1 \in K$ e portanto $[a_n][b_n] = 1 \in \widehat{K}$.

Agora devemos mostrar que $|\widehat{\ }|$ é uma extensão de $|\ \ |$. Para isso precisamos definir $|\widehat{\ }|$. Sejam $(a_n)_n \in S_c(K)$ um representante da classe $[(a_n)_n] \in \widehat{K}$, como a sequência $(|a_n|)_n$ é de Cauchy em $\mathbb{R}$ então ela converge para um número real (pois $\mathbb{R}$ é completo). Definimos

$$|\widehat{[(a_n)_n]}| = \lim |a_n|$$

Se $(b_n)_n$ é outro representante da classe $[(a_n)_n]$, temos que $(a_n - b_n)_n$ é uma sequência nula e assim $(|a_n - b_n|)_n$ é uma sequência nula em $\mathbb{R}$, da mesma forma que $(|a_n| - |b_n|)_n$. Isso garante que $\lim|a_n| = \lim|b_n|$, e que $|\widehat{\ }|$ independe do representante da classe. Claramente a função $|\widehat{\ }|: \widehat{K} \to \mathbb{R}$ definida acima é um valor absoluto em $\widehat{K}$.

Podemos definir uma imersão de K em $\widehat{K}$ com o homomorfismo $\iota: K \to \widehat{K}$ que associa $a \in K$ a classe de equivalência da sequência constante $\iota(a) = [(a_n = a)_n]$(que é de Cauchy). Claramente ι é injetivo, um vez que $\iota(a) = \iota(b) \Rightarrow [(a_n = a)_n] = [(b_n = b)_n]$, que por sua vez implica em $\big((a_n = a) - (b_n = b)\big)_n$ ser uma sequência nula, que só acontece se $a = b$. Assim $|\widehat{\ }|$ é claramente uma extensão de $|\ \ |$, onde

$$|\widehat{[a_n]}| = \lim|a_n = a| = |a|.$$

Agora vamos mostrar que K (ou na verdade $\iota(K)$) é denso em $\widehat{K}$ com respeito a $|\widehat{\ }|$. Precisamos mostrar que um elemento de $\widehat{K}$ pode ser aproximado arbitrariamente por um elemento de K com respeito a $|\widehat{\ }|$. Com efeito seja $[(a_n)_n] \in \widehat{K}$ e $(a_n)_n$ um representante de $[(a_n)_n]$. Como $(a_n)_n$ é de Cauchy, para cada $\epsilon > 0$ arbitrário existe n_0, tal que para $m, n > n_0$ naturais temos $|a_n - a_m| < \epsilon$. Tomemos a_{n_0+1} fixo, e a classe de equivalência $[(a_n)_n] - \iota(a_{n_0+1})$. Pela definição de $|\widehat{\ }|$ apresentada anteriormente, temos

$$\left|\widehat{[(a_n)_n] - \iota(a_{n_0+1})}\right| = \lim_{n\to\infty} |a_n - a_{n_0+1}| < \epsilon,$$

pois $(a_n)_n$ é de Cauchy. E assim se se $n_0 \to \infty$, o lado direito da igualdade acima vai para zero, mostrando que podemos aproximar $\iota(a_{n_0+1})$ de $[(a_n)_n]$ tanto quanto quisermos, ou seja

$$[(a_n)_n] = \lim_{n_0\to\infty} \iota(a_{n_0+1}).$$

Isso, pelo homomorfismo ι é o mesmo que

$$[(a_n)_n] = \lim_{n_0 \to \infty} a_{n_0+1}.$$

Agora só nos resta provar que $\widehat{K}$ é completo em relação a $|\widehat{\ }|$. Seja $([(a_n)_n])_n$ uma sequência de Cauchy em $\widehat{K}$ (agora tratamos com sequências de classes de equivalência, de sequências de Cauchy em K) com respeito a $|\widehat{\ }|$, devemos mostrar que ela converge com respeito a $|\widehat{\ }|$ para algum elemento de $\widehat{K}$. No intuito de evitar possíveis confusões e facilitar o acompanhamento do raciocínio, vamos inserir a notação da classe de equivalência de sequências de Cauchy $[(a_n)_n] = \hat{a}$, de sequências equivalentes a $(a_n)_n$. Assim a sequência de Cauchy em $\widehat{K}$ $([(a_n)_n])_n = (\hat{a}_n)_n$. Atenção para o fato de que os termos de $(\hat{a}_n)_n$ são classes de equivalência $\hat{a}_K = [(a_n^k)_n]$. Podemos entender da seguinte forma

$$\hat{a}_1 = [\{a_1^1, a_2^1, a_3^1, a_4^1, a_5^1, \dots\}]$$
$$\hat{a}_2 = [\{a_1^2, a_2^2, a_3^2, a_4^2, a_5^2, \dots\}]$$
$$\hat{a}_3 = [\{a_1^3, a_2^3, a_3^3, a_4^3, a_5^3, \dots\}]$$
$$\vdots$$
$$\hat{a}_k = [\{a_1^k, a_2^k, a_3^k, a_4^k, a_5^k, \dots\}]$$
$$\vdots$$

Como para todo k a sequência $(a_n^k)_n$ é de Cauchy, podemos afirmar que para cada uma das sequências (ou para todo k), dado $\epsilon = 1/k$, existe um $n_k \in \mathbb{N}$ de forma que para todos os naturais $m, n > n_k$ temos $|a_n^k - a_m^k| < 1/k$.

Mostraremos que a sequência $\left(a_{n_k}^k\right)_k$ é de Cauchy em K. Para isso, dado $\epsilon > 0$, basta escolhermos k natural tal que $\frac{3}{k_\epsilon} < \epsilon$.

Sabendo que a sequência de classes $(\hat{a}_n)_n$ em $\widehat{K}$ é de Cauchy existe $k_0 > k_\epsilon$ tal que para todo $p, q > k_0$ temos

$$\widehat{|\hat{a}_p - \hat{a}_q|} < \frac{1}{k_\epsilon}.$$

Mas por definição temos

$$\widehat{|\hat{a}_p - \hat{a}_q|} = \lim_{n \to \infty} |a_n^p - a_n^q| < \frac{1}{k_\epsilon}.$$

A partir desse limite, podemos afirmar que para $n > n^*$ suficientemente grande temos $\left|a_n^p - a_n^q\right| \leq 1/k_\epsilon$. Assim para p, q maiores que k_0 e $n > \max\{n^*, n_p, n_q\}$, temos

$$\left|a_{n_p}^p - a_{n_q}^q\right| \leq \left|a_{n_p}^p - a_n^p\right| + \left|a_n^p - a_n^q\right| + \left|a_n^q - a_{n_q}^q\right| < \tfrac{1}{p} + \tfrac{1}{k_\epsilon} + \tfrac{1}{q} < \tfrac{3}{k_\epsilon} < \epsilon.$$

Logo a sequência $\left(a_{n_k}^k\right)_k$ é de Cauchy em K.

Agora mostraremos que a classe da sequência $\left(a_{n_k}^k\right)_k$ de Cauchy é o limite da sequência $(\hat{a}_n)_n$ em $\widehat{K}$. Representando $\left[\left(a_{n_k}^k\right)_k\right] = \hat{\alpha}$, afirmamos que $\lim_{n\to\infty} |\widehat{\hat{a}_n - \hat{\alpha}}| = 0$. Com efeito temos

$$\lim_{n\to\infty} |\widehat{\hat{a}_n - \hat{\alpha}}| = \lim_{n\to\infty} \lim_{k\to\infty} \left|a_k^n - a_{n_k}^k\right| \leq \lim_{n\to\infty} \lim_{k\to\infty} \left(\left|a_k^n - a_{n_n}^n\right| + \left|a_{n_n}^n - a_{n_k}^k\right|\right).$$

Como as sequências $(a_k^n)_k$ e $\left(a_{n_k}^n\right)_k$ são de Cauchy, temos que

$$\lim_{n\to\infty} |\widehat{\hat{a}_n - \hat{\alpha}}| \leq \lim_{n\to\infty} \lim_{k\to\infty} \left|a_k^n - a_{n_n}^n\right| + \lim_{n\to\infty} \lim_{k\to\infty} \left|a_{n_n}^n - a_{n_k}^k\right| = 0 + 0 = 0.$$

Assim finalizamos a demonstração do teorema.

■

Nos termos da demonstração anterior, podemos afirmar que $\widehat{K}$ é um completamento de K, o que representamos pelo par $\left(\widehat{K}, \iota\right)$, onde, como vimos, $\iota: K \to \widehat{K}$ é uma transformação isométrica[3] de K em $\widehat{K}$.

A demonstração apresentada exibe as etapas gerais para alcançarmos um completamento de qualquer corpo com valor absoluto. No caso dos números reais, estabelecemos que duas sequências $(a_n)_n$ e $(b_n)_n$ de Cauchy em $\mathbb{Q}$ são equivalentes, se a sequência $(a_n - b_n)_n$ for nula, o que define uma relação de equivalência $\sim$ no anel das sequências de Cauchy em $\mathbb{Q}$. Em seguida provamos que $\mathbb{R} = \mathbb{Q}/\sim$ é um completamento de $\mathbb{Q}$. Vale observar que a completude de $\mathbb{R}$ é utilizada na demonstração do teorema geral anterior.

Provada a existência, uma questão que segue naturalmente é se o completamento é único. Para analisarmos essa questão, vejamos os resultados seguintes.

Proposição 4.4.21. *Seja (K_1, d_1) um espaço métrico, $X \subset K_1$ denso em K_1 e uma isometria $f: X \to K_2$, onde (K_2, d_2) é um espaço métrico completo, f estende-se de forma única para uma isometria $g: K_1 \to K_2$.*

Demonstração.

Como X é denso em K_1, para todo $x \in K_1$ existe uma sequência $(x_n)_n$ em X convergindo para x. Como $(x_n)_n$ é convergente, podemos afirmar que é de Cauchy em K_1, o que por sua vez, já que f é uma isometria, implica em $\left(f(x_n)\right)_n$ ser uma sequência de Cauchy em K_2. E como, por hipótese, K_2 é completo, podemos afirmar que $\left(f(x_n)\right)_n$ converge para um $g(x) \in K_2$. Mesmo que $(y_n)_n$ seja outra sequência em X convergindo para o mesmo x em K_1,

[3] Uma função que preserva distâncias, ou seja, $|x - y| = \left|\iota(x) - \iota(y)\right|$, para todos $x, y \in K$.

sabemos que $\lim_{n\to\infty} d_1(x_n, y_n) = 0 = d_2\left(\lim_{n\to\infty} f(x_n), \lim_{n\to\infty} f(y_n)\right)$, pois f é uma isometria. Isso implica em $\lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} f(y_n)$. Assim temos uma função $g: K_1 \to K_2$ bem definida, tal que

$$g(x) = \lim_{n\to\infty} f(x_n).$$

Evidentemente para $x \in X$ basta tomar a sequência constante $(x_n = x)_n$ e assim temos $g(x) = \lim_{n\to\infty} f(x_n = x) = f(x)$.

Afirmamos também que g é uma isometria, pois tomando $x, y \in K_1$, duas sequências $(x_n)_n$, $(y_n)_n$ em X convergindo respectivamente para x e y, temos

$$\begin{aligned} d_2\big(g(x), g(y)\big) &= d_2\left(\lim_{n\to\infty} f(x_n), \lim_{n\to\infty} f(y_n)\right) \\ &= \lim_{n\to\infty} d_2\big(f(x_n), f(y_n)\big) \\ &= \lim_{n\to\infty} d_1(x_n, y_n) \\ &= d_1(\lim x_n, \lim y_n) \\ &= d_1(x, y) \end{aligned}$$

Para finalizar a demonstração, vamos assumir que exista outra isometria h com as mesmas propriedades mostradas para g, mas aí teríamos

$$h(x) = h(\lim x_n) = \lim h(x_n) = \lim f(x_n) = g(x),$$

o que mostra que g é uma extensão de f e finaliza a demonstração.

■

Proposição 4.4.22. *Seja $(\widehat{K}, \imath)$ um completamento do espaço métrico K, seja $\imath'$ uma isometria de K em um outro espaço métrico completo K', então há uma única isometria $j: \widehat{K} \to K'$ tal que $j \circ \imath = \imath'$.*

Demonstração.

Afirmamos que essa isometria é a extensão de $\imath' \circ \imath^{-1}$. De fato $\imath' \circ \imath^{-1}$ é uma isometria por ser a composição de duas isometrias. Entretanto, pela proposição anterior $\imath' \circ \imath^{-1}$, estende-se de forma única para uma isometria $j: \widehat{K} \to K'$, que satisfaz $j \circ \imath = \imath'$.

■

Assim, supondo a existência de $(\widehat{K}, \imath)$ e $(K', \imath')$, dois completamentos de um mesmo espaço métrico K, é imediato pela proposição anterior que existe uma única isometria $j: \widehat{K} \to K'$ tal que $j \circ \imath = \imath'$ (analogamente existe uma única isometria $j: K' \to \widehat{K}$ tal que $j' \circ \imath' = \imath$). Isso nos diz que a menos de isometrias (que são homomorfismos) o completamento de um

espaço métrico é único.

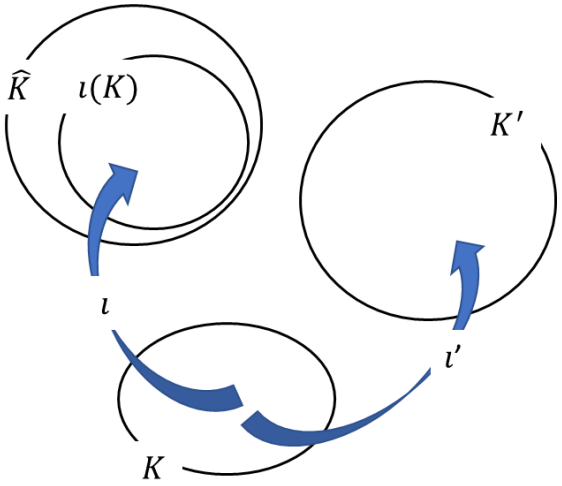

Figura 1 - Proposição 4.4.22.

No entanto, há ainda um aspecto a ser contemplado na discussão sobre completamentos. Vimos que a convergência das sequências de Cauchy, em um espaço métrico, define as classes de equivalência que compõem seu completamento. No entanto, a convergência dessas sequências depende de como trabalhamos distâncias nesse espaço métrico. Ou seja, depende das condições impostas pelo valor absoluto considerado nesse espaço métrico. Assim, para o próximo capítulo, apresentaremos um exemplo de um completamento de $\mathbb{Q}$ utilizando um valor absoluto diferente do usual, o valor absoluto p-ádico, apresentado no capítulo anterior.

5 UMA INICIAÇÃO AOS NÚMEROS p-ÁDICOS

O presente capítulo apresenta uma introdução ao mundo dos números p-ádicos. Para aquele leitor que está sendo iniciado no trato com esse sistema numérico, será aproveitada a sua familiarização com expansões de um número por potências de uma inteiro positivo $p \geq 2$, ou seja, expansões em base p. Esse ponto de partida cumpre o papel de ser bastante intuitivo, considerando que um número p-ádico x pode ser representado pela sequência de dígitos $[\dots a_4 a_3 a_2 a_1 a_0 a_{-1} a_{-2} \dots a_k]_p$, e que, para os números inteiros não negativos, essa sequência coincide com os coeficientes da expansão de n em base p, com p primo. Assim o conjunto $\mathbb{Q}_p$ dos números p-ádicos é constituído pelos números da forma

$$x = \sum_{i=k}^{\infty} a_i \cdot p^i \text{, onde } k, a_i \in \mathbb{Z}, \text{ e } 0 \leq a_i < p.$$

Os resultados apresentados aqui podem ser encontrados com maior detalhamento em GOUVÊA, 1993, KOBLITZ, 1984 e BACHMAN, 1964.

5.1 O conjunto dos números p-ádicos

Uma função racional $f(X)$ sobre um corpo K é o quociente entre dois polinômios sobre esse mesmo corpo. Assim, uma função racional sobre o corpo $\mathbb{C}$ dos números complexos é definida como:

$$f(X) = \frac{P(X)}{Q(x)}, \text{ com } P, Q \in \mathbb{C}[X]$$

Uma função racional sobre $\mathbb{C}$ sempre pode ser expandida em torno de um complexo α através das chamadas séries de Laurent

$$f(X) = \sum_{k}^{\infty} a_i (X - \alpha)^i.$$

Sendo k um inteiro e a convergência garantida em uma região do plano complexo. A série assim obtida reflete o comportamento da função f quando X se aproxima de α, isto é, localmente em α.

O corpo das funções racionais $\mathbb{C}(X)$ e o corpo $\mathbb{Q}$ dos números racionais guardam entre si muitas semelhanças. Ambos são um *corpo de frações* de um *domínio de ideias principais*, no qual todos os *ideais primos e não nulos* são *maximais*. Em 1897 Kurt Hensel propôs uma analogia entre o estudo das funções racionais e o estudo dos números algébricos. Hensel percebeu que os elementos $(X - \alpha)$ são elementos irredutíveis (como os primos em $\mathbb{Z}$)

no anel de polinômios complexos $\mathbb{C}[X]$ e dessa forma, fixado um número inteiro positivo e primo p, existiria para cada número racional x uma expansão em série de potências da forma

$$x = \sum_{i=k}^{\infty} a_i \cdot p^i \text{, onde } k, a_i \in \mathbb{Z}, \text{ e } 0 \leq a_i < p$$

Hensel denominou os números definidos da forma acima de números p-ádicos. Inicialmente esses números não foram bem aceitos, pois apresentavam uma natureza duvidosa em relação à convergência. Por exemplo, tomemos o problema simplório de determinar o conjunto solução da equação $x = 1 + 3x$, inspirado em uma ilustração de OLIVEIRA, 2009. Percebendo que essa expressão nos aponta que o valor de x é o mesmo que $1 + 3x$, seria até natural que um estudante propenso a experimentar novos caminhos de resolução imaginasse a possibilidade de substituir uma expressão por outra, e assim encontrar $x = 1 + 3(1 + 3x)$. Seguindo despretensiosamente esse método iterativo, após $k - 1$ substituições, ficaria com:

$$x = 1 + 3 + 3^2 + 3^3 + \cdots + 3^k x.$$

Perceba que na prática, esse estudante está buscando a solução desejada, enxergando equação da forma $x_{n+1} = 1 + 3x_n$, ou seja, aplicando-lhe um olhar recursivo. Se é assim, observando o padrão, seria compreensível que se experimente $x_0 = 1$, obtendo

$$x_1 = 1 + 3$$

$$x_2 = 1 + 3 + 3^2$$

...

$$x_n = \sum_{i=0}^{n} 3^i.$$

Esse processo poderia ser repetido indefinidamente. Tomando então o limite, a solução encontrada seria $x = \sum_{i=0}^{\infty} 3^i$. Em seguida, lembrando que, para determinadas séries, temos $\sum_{i=0}^{\infty} a^i = \frac{1}{1-a}$, e substituindo $a = 3$, esse mesmo estudante determinaria a solução $x = \frac{1}{1-3} = -\frac{1}{2}$.

É evidente que a soma da série geométrica utilizada é válida apenas para um número positivo $a < 1$. Então teria havido uma confusão, por parte do matemático aventureiro que pensou em resolver o problema de uma forma diferente da usual? O espantoso é que, apesar da abordagem, um tanto singular, a resposta está correta.

A compreensão da situação acima passa por avaliar como podemos medir distâncias. Ao considerar a convergência da série geométrica, assumimos que estamos somando um número cada vez menor a medida que caminhamos infinitamente. Assim nossa caminhada

está tendendo a alcançar algum ponto específico, que é o limite da série. Mas se a razão for um número maior que 1, estamos dando passos cada vez maiores. No entanto, essa percepção depende de como enxergamos distâncias. Por exemplo, na situação descrita anteriormente, se assumirmos o valor absoluto 3-ádico, percebemos que cada parcela somada possui um valor absoluto menor que a parcela anterior pois $|3^n|_3 = 1/3^n$. Desta forma o "tamanho" das parcelas tende a zero.

Assim, para reestabelecer uma noção de convergência de forma adequada para os números p-ádicos, precisamos adotar o valor absoluto p-ádico. Foi o que fez o matemático húngaro Josef Kurschák, em 1993, dando aos números de Hensel o mesmo tratamento rigoroso dado aos reais por Cantor, construindo, a partir dos números racionais, o corpo $\mathbb{Q}_p$ dos números p-ádicos.

A definição de sequências de Cauchy e de convergência de sequências apresentadas no capítulo anterior continuam valendo aqui. O resultado abaixo nos traz uma observação interessante no caso de um valor absoluto arquimediano.

Proposição 5.1.23. *Uma sequência $(x_n)_n$ em $\mathbb{Q}$ em relação a um valor absoluto não arquimediano $|\ \ |$, é uma sequência de Cauchy, se e somente se,* $\lim|x_{n+1} - x_n| = 0$.

Demonstração.

A implicação é imediata, pois se assumirmos $(x_n)_n$ de Cauchy, então para todo $\epsilon > 0$ existe um natural n_0 tal que, para todos os naturais $n > n_0$ e $m > n_0$, temos $|x_n - x_m| < \epsilon$. Em particular basta tomar $m = n + 1$, de onde segue a tese.

Reciprocamente basta notarmos que, para $m = n + r > n$, temos:

$|x_m - x_n| = |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \cdots + x_{n+1} - x_n|$.

E assim, como $|\ \ |$ é não arquimediano temos

$$|x_m - x_n| \leq \max\{|x_{n+r} - x_{n+r-1}|, \dots, |x_{n+1} - x_n|\}.$$

■

Para um dado primo p, definimos também o conjunto $\mathbb{Z}_p$ dos inteiros p-ádicos como sendo o conjunto dos elementos de $x \in \mathbb{Q}_p$ tais que, $x = \sum_{i=0}^{\infty} a_i \cdot p^i$, onde $a_i \in \mathbb{Z}$ e $0 \leq a_i < p$. Isso significa que, na expansão de base p de inteiros p-ádicos, só aparecem potências de p com expoentes positivos ou nulos. Perceba que para $x \in \mathbb{Z}$, a representação de $x = \sum_0^n a_i p^i$, para $n \in \mathbb{N}$ e p primo é exatamente a expansão de x pela base p, assim como usualmente fazemos no sistema de numeração decimal, cuja base é 10. Se assumirmos que para $i > n$ temos $a_{i>n} = 0$, temos $x = \sum_0^{\infty} a_i p^i$, e assim podemos considerar todo $\mathbb{Z} \subset \mathbb{Z}_p$.

Agora observe que para $x \in \mathbb{Z}_p$ temos

$$|x|_p = \left|\sum_{i=0}^{\infty} a_i \cdot p^i\right|_p \leq \max\{|a_0|_p, |a_1 \cdot p|_p, |a_2 \cdot p^2|_p, \dots, \} = 1.$$

E como para $x \in \mathbb{Q}_p$, temos $x = \sum_{i=k}^{\infty} a_i \cdot p^i$, onde k e $a_i \in \mathbb{Z}$, e $0 \leq a_i < p$, só acontece de $|x|_p \leq 1$ se tivermos $a_i = 0$, para todo $i < 0$, podemos afirmar que $|x|_p \leq 1$ implica em $x \in \mathbb{Z}_p$. Assim também podemos definir $\mathbb{Z}_p = \{x \in \mathbb{Q}_p; |x|_p \leq 1\}$. É possível verificar que $\mathbb{Z}_p$ é um subanel de $\mathbb{Q}_p$.

A definição de números p-ádicos dada, nos termos apresentados anteriormente, estabelece que $x \in \mathbb{Z}_p$ é o limite da sequência $(x_n)_n$, onde essa sequência é dada pelas soluções do sistema de congruências $x_{i+1} \equiv x_i \pmod{p^{i+1}}$, para $i = 0, 1, 2, 3, \dots$ com $x_n = a_0 + a_1 p + \cdots + a_n p^n$ como é ilustrado abaixo:

$$x_1 \equiv x_0 \pmod{p}$$
$$x_2 \equiv x_1 \pmod{p^2}$$
$$\vdots$$
$$x_n \equiv x_{n-1} \pmod{p^i}$$
$$\vdots$$

Afirmamos que $(x_n)_n$ é de Cauchy em relação ao valor absoluto $|\ \ |_p$. De fato $|x_{n+1} - x_n|_p = |\gamma p^{n+1}|_p \leq p^{-(n+1)}$ que converge para zero quando $n \to \infty$. Logo pela proposição **5.1.23** temos que $(x_n)_n$ é uma sequência de Cauchy em $\mathbb{Q}$.

5.2 O lema de Hensel

A proposição abaixo, conhecida como Lema de Hensel, estabelece como podemos determinar uma sequência como a apresentada na seção anterior para cada número racional, como mostraremos em seguida.

Proposição 5.2.24. (Lema de Hensel) *Seja $f(x) \in \mathbb{Z}_p[x]$ e seja $f'(x) \in \mathbb{Z}_p[x]$ sua derivada formal com p primo. Seja $a \in \mathbb{Z}_p$* e *r_0 tal que*:

I. $f(a) \equiv 0 \pmod{p^{r_0}}$

II. p^s é *a maior potência de p que divide $f'(a)$, com $0 \leq 2s < r_0$*

Então existe uma sequência $(a_r)_{r \geq r_0}$, tal que:

$$a_{r_0} = a, \text{ e } a_{r+1} \equiv a_r \pmod{p^{r-s}}$$

$$f(a_r) \equiv 0(\text{mod}\, p^r)\ para\ todo\ r \geq r_0$$

Em particular, se existe um inteiro a *tal que* $f(a) \equiv 0(\text{mod}\, p)$ *mas* $f'(a) \not\equiv 0(\text{mod}\, p)$ *então* $f(x) \equiv 0(mod\ p^k)$ *admite solução para todo* $k \in \mathbb{N}$.

Demonstração.

Seja um $r' > r$, por indução, vamos assumir o resultado válido para todo r tal que $r_o \leq r \leq r'$. Será provado que também é válido para $r' + 1$.

Pela hipótese de indução, podemos afirmar que $p^{r'} | f(a_{r'})$, o que equivale a dizer que existe $k \in \mathbb{Z}$ tal que $f(a_{r'}) = k \cdot p^{r'}$ e que $f'(a_{r'}) = qp^s$, com q inteiro não divisível por p.

Precisa-se determinar $a_{r'+1} = a_{r'} + t \cdot p^{r'-s}$, para t inteiro, que satisfaça:

i. $f(a_{r'+1}) \equiv 0\left(\text{mod}\, p^{r'+1}\right)$

ii. $f'(a_{r'+1}) \equiv 0(\text{mod}\, p^s)$

iii. $f'(a_{r'+1}) \not\equiv 0(\text{mod}\, p^{s+1})$

Assim temos:

$$\begin{aligned}
f(a_{r'+1}) &= \sum_{i=0}^{n} b_i (a_{r'+1})^i \\
&= \sum_{i=0}^{n} b_i \left(a_{r'} + t \cdot p^{r'-s}\right)^i \\
&= \sum_{i=0}^{n} b_i \left(\sum_{j=0}^{i} \binom{i}{j} (a_{r'})^{i-j} t^j \cdot p^{j(r'-s)} \right) \\
&= \sum_{i=0}^{n} b_i \, (a_{r'})^i + \sum_{i=1}^{n} b_i \cdot i \cdot (a_{r'})^{i-1} \cdot t \cdot p^{(r'-s)} \\
&\qquad + \sum_{i=2}^{n} b_i \left(\sum_{j=2}^{i} \binom{i}{j} (a_{r'})^{i-j} t^j \cdot p^{j(r'-s)} \right) \\
&= f(a_{r'}) + f'(a_{r'}) t p^{(r'-s)} + \sum_{i=2}^{n} b_i \left(\sum_{j=0}^{i} \binom{i}{j} (a_{r'})^{i-j} t^j \cdot p^{j(r'-s)} \right)
\end{aligned}$$

Pela hipótese de $0 \leq 2s < r_0 < r'$ tem-se que $2(r' - s) \geq r' + 1$, o que garante que a terceira parcela acima é múltipla de $p^{r'+1}$. Logo:

$$\begin{aligned}
f(a_{r'+1}) &\equiv f(a_{r'}) + f'(a_{r'}) \cdot t \cdot p^{(r'-s)} (mod\ p^{r'+1}) \\
&\equiv k \cdot p^{r'} + q \cdot p^s \cdot t \cdot p^{(r'-s)} \left(mod\ p^{r'+1}\right) \\
&\equiv k \cdot p^{r'} + qt \cdot p^{r'} \left(mod\ p^{r'+1}\right) \\
&\equiv p^{r'} (k + qt) \left(mod\ p^{r'+1}\right)
\end{aligned}$$

Assim basta determinar t para o qual $k + qt \equiv 0(\text{mod}\, p)$. O que é possível já que q é invertível (mod p).

Para fechar a demonstração, da mesma forma mostrada acima, basta perceber que $f'(a_{r+1}) \equiv f'(a_r) = q \cdot p^s (\text{mod}\, p^s)$.

$$f'(a_{r+1}) \equiv 0(\text{mod}\, p^s)$$
$$f'(a_{r+1}) \not\equiv 0(\text{mod}\, p^{s+1})$$

Para finalizar, basta observar que se $r_0 = 1$ a única possibilidade é $s = 0$, que garante o caso particular.

■

Observe que a constante $a \in \mathbb{Z}_p$, exigida nas hipóteses do lema, consiste em uma aproximação p-ádica de uma das raízes do polinômio f. Já a sequência (a_r) é constituída por aproximações cada vez melhores desta raiz. Seja x_0 esta raiz, como se pode suspeitar, $\lim a_n = x_0$.

Como exemplo, vamos expressar $-1/2$ em sua forma 3-ádica. Para isso vamos tomar o polinômio $f(x) = 2x + 1$, pois $f(1) \equiv 0(\text{mod } 3)$ e $f'(1) \not\equiv 0(\text{mod } 3)$ de acordo com o Lema de Hensel, e buscar a sequência $(x_n)_n$.

$$2x \equiv -1(\text{mod } 3) \Rightarrow x_0 = 1$$
$$2x \equiv -1(\text{mod } 3^2) \Rightarrow x_1 = 4 = 1 + 3$$
$$2x \equiv -1(\text{mod } 3^3) \Rightarrow x_2 = 13 = 1 + 3 + 3^2$$
$$2x \equiv -1(\text{mod } 3^4) \Rightarrow x_3 = 40 = 1 + 3 + 3^2 + 3^3$$

Portanto $-1/2$ é um inteiro 3-ádico da forma $1 + 3 + 3^2 + 3^4 + \cdots$ que representaremos por $[\ldots 111]_3$ como uma expansão pela base 3. Compare com o resultado do início do capítulo.

Em geral, tomando o polinômio $f(x) = bx + a$ com $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}_+^*$ e $(a, b) = 1$, a congruência $bx + a \equiv 0(mod\ p)$ possui solução se, e somente se, $(b, p) = 1$. Assumindo que p seja primo, basta que b não seja múltiplo de p. Dessa forma temos $f'(x) = b \not\equiv 0(mod\ p)$. Logo, nessas condições, a raiz de f, $x_0 = -a/b$ possui uma representação p-ádica que pode ser alcançada da forma garantida pelo lema de Hensel.

Caso seja de nosso interesse determinar o p-ádico correspondente a um racional que não atenda as exigências anteriores, ainda é possível fazê-lo. Por exemplo, a fim de determinarmos o correspondente ao racional 5/9 em $\mathbb{Q}_3$, de fato $9x - 5 \not\equiv 0(mod\ 3)$. Entretanto perceba que 9 é uma potência da base de nosso interesse, e dividir pela potência da

base é muito simples. Como o representante 3-ádico de $5 = [12]_3$ e de $9 = [100]_3$ por analogia a nossa experiência no sistema decimal podemos inferir que $\frac{5}{9} = \frac{2}{9} + \frac{1}{3} = 2 \cdot 3^{-2} + 3^{-1} = [0{,}12]_3$, que não é um inteiro 3-ádico, mas um racional 3-ádico.

Tomemos agora, como exemplo, o polinômio $f(x) = x^2 - 7$, para determinar a representação 3-ádica de uma de suas raízes. As exigências do lema são satisfeitas, pois $f(1) = -6 \equiv 0 (\text{mod } 3)$ e $f'(1) = 2 \not\equiv 0 (\text{mod } 3)$.

$$x^2 \equiv 7 (\text{mod } 3) \Rightarrow x_0 = 1$$

$$x^2 \equiv 7 (\text{mod } 3^2) \Rightarrow x_1 = 4 = 1 + 3$$

$$x^2 \equiv 7 (\text{mod } 3^3) \Rightarrow x_2 = 13 = 1 + 3 + 3^2$$

$$x^2 \equiv 7 (\text{mod } 3^4) \Rightarrow x_3 = 13 = 1 + 3 + 3^2 + 0 \cdot 3^3$$

$$x^2 \equiv 7 (\text{mod } 3^5) \Rightarrow x_4 = 175 = 1 + 3 + 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4$$

$$\vdots$$

$$x^2 \equiv 7 (\text{mod } 3^{11}) \Rightarrow x_{10} = 148.891$$

$$= 1 + 3 + 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^7 + 3^8 + 3^9 + 2 \cdot 3^{10}$$

Ou seja, 7 é um quadrado perfeito em $\mathbb{Z}_3$, e assim:

$$\sqrt{7} = [\ldots 21120020111]_3$$

As operações de adição e multiplicação entre números p-ádicos funcionarão de forma análoga às operações usuais com expansões de base 10 já conhecidas. Podemos inclusive verificar o resultado anterior.

								...	2	1	1	2	0	0	2	0	1	1	1
×								...	2	1	1	2	0	0	2	0	1	1	1
								...	2	1	1	2	0	0	2	0	1	1	1
							...	2	1	1	2	0	0	2	0	1	1	1		
						...	2	1	1	2	0	0	2	0	1	1	1			
					...	0	0	0	0	0	0	0	0	0	0	0	0			
				...	1	2	0	0	1	0	1	1	0	2	2	2				
			...	0	0	0	0	0	0	0	0	0	0	0	0					
		...	0	0	0	0	0	0	0	0	0	0	0	0						
	...	1	2	0	0	1	0	1	1	0	2	2	2							
							⋮													
...	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1

Como $\sqrt{7}$ não é racional, percebemos que $\mathbb{Q}$ é uma parte própria de $\mathbb{Q}_3$. Em geral

seja a um inteiro que não é um quadrado perfeito em $\mathbb{Q}$ e $p \neq 2$ (para $p = 2$ a condição da derivada no Lema de Hensel não seria atendida) um primo que não divide a. Se a congruência $x^2 \equiv a(\mathrm{mod}\, p)$ possui solução, tomando a sequência $(x_n)_n$ definida por $x_n^2 \equiv a(\mathrm{mod}\, p^{n+1})$, que já vimos ser de Cauchy, teríamos $|x_n^2 - a|_p = |\gamma p^{n+1}|_p \leq p^{-(n+1)}$ que converge para zero quando $n \to \infty$. O que nos mostra que, caso exista, $\lim x_n = \sqrt{a}$, que por hipótese não é racional. Outro exemplo interessante é que, através do polinômio $f(x) = x^2 + 1$, para $p = 5$, podemos determinar a raiz quadrada de -1 em $\mathbb{Q}_5$.

Para $p = 2$ podemos buscar o 2-ádico correspondente à raiz cúbica de 3. De acordo com o Lema de Hensel, podemos tomar o polinômio $f(x) = x^3 - 3$, pois $f(1) \equiv 0(\mathrm{mod}\ 2)$ e $f'(1) \not\equiv 0(\mathrm{mod}\ 2)$, assim temos a seguinte sequência

$$x^3 \equiv 3(\mathrm{mod}\ 2) \Rightarrow x_0 = 1$$
$$x^3 \equiv 3(\mathrm{mod}\ 2^2) \Rightarrow x_1 = 3 = 1 + 2$$
$$x^3 \equiv 3(\mathrm{mod}\ 2^3) \Rightarrow x_2 = 3 = 1 + 2 + 0$$
$$x^3 \equiv 3(\mathrm{mod}\ 2^4) \Rightarrow x_3 = 11 = 1 + 2 + 0 + 2^3$$
$$x^3 \equiv 3(\mathrm{mod}\ 2^5) \Rightarrow x_4 = 27 = 1 + 2 + 0 + 2^3 + 2^4$$
$$x^3 \equiv 3(\mathrm{mod}\ 2^6) \Rightarrow x_5 = 59 = 1 + 2 + 0 + 2^3 + 2^4 + 2^5$$
$$x^3 \equiv 3(\mathrm{mod}\ 2^7) \Rightarrow x_7 = 123 = 1 + 2 + 0 + 2^3 + 2^4 + 2^5 + 2^6$$

...

De onde temos que 3 é um cubo perfeito em $\mathbb{Q}_2$ e uma de suas raízes é representada por $[\ldots 1111011]_2$.

Diante do que foi apresentado aqui, percebemos que $\mathbb{Q}$ é incompleto em relação ao valor absoluto p-ádico, já que encontramos sequências de Cauchy de racionais convergentes a elementos que não pertencem a $\mathbb{Q}$ com respeito a $|\quad|_p$.

Denotemos $S_{C_p}(\mathbb{Q})$ o anel das sequências de Cauchy com elementos em $\mathbb{Q}$ em relação ao valor absoluto p-ádico $|\quad|_p$ e por $S_{0_p}(\mathbb{Q})$, o ideal das sequência nulas com relação a $|\quad|_p$.

Proposição 5.2.25. *O ideal* $S_{0_p}(\mathbb{Q})$ *é um ideal maxial de* $S_{C_p}(\mathbb{Q})$.

Demonstração.

Seja $(a_n)_n \in S_{C_p}(\mathbb{Q})$ não nula e I o ideal gerado por $(a_n)_n$. Precisamos mostrar que I é necessariamente o próprio anel $S_{C_p}(\mathbb{Q})$. Para isso basta mostrar que a sequência constante $(a_n = 1)_n$, correspondente ao elemento neutro da multiplicação em $S_{C_p}(\mathbb{Q})$.

Como $(a_n)_n$ é de Cauchy, existem $\epsilon > 0$ e um natural n_0, tais que $|a_n|_p \geq \epsilon$ para todo $n \geq n_0$. Em particular temos $a_n \neq 0$ para todo $n > n_0$, o que nos permite definir a sequência $(b_n)_n$ tal que $b_n = 1/a_n$ se $n > n_0$.

Afirmamos que $(b_n)_n$ é de Cauchy já que $(a_n)_n$ é de Cauchy e

$$|b_{n+1} - b_n| = \left|\frac{1}{a_{n+1}} - \frac{1}{a_n}\right| \leq \frac{|a_n - a_{n-1}|}{|a_n||a_{n+1}|} \leq \frac{|a_{n-1} - a_n|}{\epsilon^2}.$$

Assim $(a_n b_n - 1)_n \in S_{0_p}(\mathbb{Q})$, e portanto $1 \sim [(a_n b_n)_n] \in I$, o que encerra a prova.

■

Podemos construir o completamento de $\mathbb{Q}$ em relação a $|\ \ |_p$ definindo $\mathbb{Q}_p = S_{C_p}(\mathbb{Q})/S_{0_p}(\mathbb{Q})$. O resultado anterior garante que $\mathbb{Q}_p = S_{C_p}(\mathbb{Q})/S_{0_p}(\mathbb{Q})$ é um corpo. Perceba que podemos definir (como feito anteriormente) uma imersão ι de $\mathbb{Q}$ em $\mathbb{Q}_p$ de forma que para $x \in \mathbb{Q}$ temos associada a classe de equivalência $\iota(x) = [(a_n = x)_n] \in \mathbb{Q}_p$ onde $\iota(\mathbb{Q})$ é denso em $\mathbb{Q}_p$. Para $[(a_n)_n] \in \mathbb{Q}_p$ é possível mostrar que $|[\widehat{(a_n)_n}]| = \lim|a_n|_p$ é uma extensão do valor absoluto p-ádico em $\mathbb{Q}_p$. Assim podemos mostrar que $\mathbb{Q}_p$ é um completamento de $\mathbb{Q}$, usando os mesmos moldes da demonstração do completamento canônico de Cantor.

6 O TEOREMA DE OSTROWSKI

No segundo capítulo, apresentamos uma introdução à teoria dos valores absolutos. Agora, compreendido o que significa completamento e a relação desse conceito com os valores absolutos, iniciamos a etapa final de nossa caminhada, em que apresentamos a resposta à questão central deste trabalho: quais os valores absolutos que podem ser definidos em $\mathbb{Q}$ a fim de construirmos diferentes completamentos para o corpo dos racionais?

Começaremos por definir equivalência entre valores absolutos, conceito de grande importância para a introdução do resultado que fecha nosso trabalho, o teorema de Ostrowski.

6.1 Valores absolutos equivalentes

No segundo capítulo, vimos que todo valor absoluto $|\ \ |$ de um corpo K define uma métrica $d(x,y) = |x-y|$ em K, e desta forma definimos bola aberta como todo conjunto do tipo $B(x_0, r) = \{x \in K : |x - x_0| < r\}$ com $r \in \mathbb{R}_+^*$. Entenderemos um subconjunto aberto de K como qualquer reunião de bolas abertas em K. Dois valores absolutos distintos em K definem métricas diferentes de K.[4] No entanto, valores absolutos distintos podem determinar a mesma família de subconjuntos abertos de K, ou seja, a mesma topologia em K.

Representaremos a topologia induzida pelo valor absoluto $|\ \ |$ por $T_{|\ \ |}$.

Definição 6.1.26. *Dois valores absolutos* $|\ \ |_1$ *e* $|\ \ |_2$ *em* K*, são ditos equivalentes se, e somente se, definem os mesmos subconjuntos abertos em* K*, ou seja, as mesmas topologias e assim temos* $T_{|\ \ |_1} = T_{|\ \ |_2}$.

Como exemplo tomemos o valor absoluto usual $|\ \ |_\infty$ em $\mathbb{R}$ e o valor absoluto $|\ \ |_* = \sqrt{|\ \ |_\infty}$. Já vimos no segundo capítulo que $|\ \ |_*$ é um valor absoluto, então só nos resta testar a condição $T_{|\ \ |_\infty} = T_{|\ \ |_*}$. De fato $|x-a|_* < r$ é quivalente a $|x-a|_\infty < r^2$, logo o $|\ \ |_\infty$ e $|\ \ |_*$ determinam as mesmas bolas abertas, portanto a mesma topologia.

Lembramos agora o conceito de topologia discreta que se refere à topologia de um conjunto K em que todo subconjunto de K são abertos, e K é dito espaço topológico discreto.

Proposição 6.1.26. *Seja* $T_{|\ \ |}$ *a topologia induzida pelo valor absoluto* $|\ \ |$ *em* K*,* $T_{|\ \ |}$ *é discreta em* K *se, e somente se,* $|\ \ |$ *é o valor absoluto trivial.*

Demonstração.

Se $T_{|\ \ |}$ é discreta, então o conjunto $\{0\}$ é aberto. Logo existe $\epsilon > 0$ tal que, $B(0,\epsilon) = \{0\}$, ou seja $|a| < \epsilon$ se, e somente se, $a = 0$. Agora seja $x \in K^*$, então existe x^{-1} tal

[4] O valor absoluto pode ser resgatado da métrica, já que $|x| = d(x,0)$.

que $x \cdot x^{-1} = 1 = |x||x^{-1}|$. Vamos supor que $|x| \neq 1$, então $|x| < 1$ ou $|x| > 1$. Se $|x| < 1$, para algum $n \in \mathbb{N}$ temos $|x|^n < \epsilon$, então $x^n = 0$, o que é um absurdo. Agora se $|x| > 1$, temos $|x^{-1}| < 1$ e assim temos para algum $n \in \mathbb{N}$ temos $(x^{-1})^n = 0$, outro absurdo. Portanto, para todo $x \in K^*$ temos $|x| = 1$, e assim $|\ \ |$ só pode ser o valor absoluto trivial.

Reciprocamente se $|\ \ |$ é o valor absoluto trivial de K então $|x - y| = \begin{cases} 0 \ se \ x = y \\ 1 \ se \ x \neq y \end{cases}$ para todo $x, y \in K$. Logo, para todo $x \in K$, temos $\{x\} = B(x, \epsilon)$ que é aberto. E para qualquer $E \subseteq K$ temos $E = \bigcup_{x \in E}\{x\}$ aberto, ou seja, todo subconjunto de K é aberto, e assim podemos afirmar que $T_{|\ \ |}$ é discreta.

■

Uma consequência direta do resultado acima é que o valor absoluto trivial não é equivalente a qualquer outro valor absoluto, uma vez que apenas ele determina a topologia discreta.

Finalizamos esta seção com o resultado abaixo, que traz a caracterização de valores absolutos equivalentes.

Proposição 6.1.27. *Sejam* $|\ \ |_1$ *e* $|\ \ |_2$ *dois valores absolutos em* K, *não triviais, as seguintes afirmações são equivalentes.*

(i). $Existe \ \rho \in \mathbb{R}_+^*, tal \ que, |\ \ |_1 = |\ \ |_2^\rho$;

(ii). $T_{|\ \ |_1} = T_{|\ \ |_2}$, *e portanto* $|\ \ |_1$ *e* $|\ \ |_2$, *são equivalentes*;

(iii). $Seja \ (a_n)_n \ em \ K, então \ \lim a_n = 0, com \ respeito \ a \ |\ \ |_1, se \ e \ somente \ se, \lim a_n = 0 \ com \ respeito \ a \ |\ \ |_2$;

(iv). $|x|_1 < 1 \ se \ e \ somente \ se \ |x|_2 < 1, para \ todo \ x \in K$;

Demonstração.

Primeiramente vamos supor (i) e provar (ii). Assumindo que $|\ \ |_1 = |\ \ |_2^\rho$, para algum real positivo ρ, temos que para qualquer bola aberta $B(x_0, r)$, por $|\ \ |_1$

$$\begin{aligned} B(x_0, r) &= \{x \in K; |x - x_0|_1 < r\} \\ &= \left\{x \in K; |x - x_0|_2^\rho < r\right\} \\ &= \left\{x \in K; |x - x_0|_2 < r^{\frac{1}{\rho}}\right\} \end{aligned}$$

O que garante (ii).

Agora vamos assumir (ii) e demonstrar (iii). Se $\lim a_n = 0$ com respeito a $|\ \ |_1$, é porque dado $\epsilon > 0$, existe n_0 tal que para todo $n > n_0$ temos $|a_n|_1 < \epsilon$. Tomemos a bola aberta

$B(0,\epsilon)$ por $|\quad|_1$

$$B(0,\epsilon) = \{x \in K; |x|_1 < \epsilon\}.$$

Lembramos que $B(0,\epsilon) \subset A$ aberto de $T_{|\quad|_1}$. Como $|\quad|_1$ e $|\quad|_2$ são equivalentes A também é aberto de $T_{|\quad|_2}$. Logo para algum $\epsilon' > \max_{n>n_0}\{|a_n|_2\}$, para todo, $n > n_0$ temos $a_n \in B(0,\epsilon') = \{x \in K; |x|_2 < \epsilon'\} \subset A$. Assim como ϵ é arbitrário (mas guarda uma relação com ϵ') podemos concluir que $\lim a_n = 0$ com respeito a $|\quad|_2$. Como a recíproca é análoga, basta substituir $|\quad|_1$ por $|\quad|_2$, de onde segue a tese (iii).

Agora vamos assumir (iii) e provar (iv). Seja $a \in K$, para o qual $|a|_1 < 1$, temos que $|a^n|_1 \to 0$, logo, por hipótese temos que $|a^n|_1 \to 0 \Leftrightarrow |a^n|_2 \to 0 \Rightarrow |a|_2 < 1$.

Finalmente vamos assumir (iv) e demonstrar (i). Se existir $\rho \in \mathbb{R}_+^*$, tal que para todo $x \in K$ tenhamos $|x|_1 = |x|_2^{\rho}$, único valor possível de ρ, que não pode depender do valor de x, é

$$\rho = \frac{\log|x|_1}{\log|x|_2}.$$

Assim, sem perda de generalidade, tomemos $x, y \in K$, com $|x|_1 > 1$ e $|y|_1 > 1$, e por absurdo vamos assumir que $\frac{\log|x|_1}{\log|x|_2} < \frac{\log|y|_1}{\log|y|_2}$, e como os logaritmos são números reais positivos podemos escrever $\frac{\log|x|_1}{\log|y|_1} < \frac{\log|x|_2}{\log|y|_2}$. Podemos assumir que existe um racional m/n, tal que

$$\frac{\log|x|_1}{\log|y|_1} < \frac{m}{n} < \frac{\log|x|_2}{\log|y|_2}.$$

Assim podemos fazer duas inferências:

$$\frac{\log|x|_1}{\log|y|_1} < \frac{m}{n} \Rightarrow \log|x|_1^n < \log|y|_1^m \Rightarrow |x|_1^n < |y|_1^m \Rightarrow \left|\frac{x^n}{y^m}\right|_1 < 1$$

e

$$\frac{m}{n} < \frac{\log|x|_2}{\log|y|_2} <\Rightarrow \log|y|_2^m < \log|x|_2^n \Rightarrow |y|_2^m < |x|_2^n <\Rightarrow 1 < \left|\frac{x^n}{y^m}\right|_2$$

O que é um absurdo, pois contraria nossa hipótese. Logo segue a tese.

■

Outra consequência do ponto (iv) desse teorema é estabelecida no resultado seguinte.

Proposição 6.1.28. *Sejam* $|\quad|_1$ *e* $|\quad|_2$ *dois valores absolutos em* K*, não triviais, equivalentes, então* $|a|_1 = 1$ *se e somente se* $|a|_2 = 1$*, para todo* $x \in K$.

Demonstração.

Para $a \in K$ temos por (iv) que $|a|_1 > 1 \Leftrightarrow |a|_2 > 1$. E se $|a|_1 < 1$ temos $|1/a|_1 > 1 \Leftrightarrow |1/a|_2 > 1$ o que garante que $|a|_2 < 1$. Logo chegamos à conclusão de que

$$|a|_1 > 1 \Leftrightarrow |a|_2 > 1 \text{ e } |a|_1 < 1 \Leftrightarrow |a|_2 < 1$$

De onde, fica demonstrado que $|a|_1 = 1 \Leftrightarrow |a|_2 = 1$.

■

A partir desse resultado temos um exemplo de valores absolutos não equivalentes. Quaisquer valores absolutos p-ádicos $|\ \ |_p$ e $|\ \ |_q$ em $\mathbb{Q}$ com $p \neq q$ primos, não serão equivalentes, pois $|p|_p = p^{-1} \neq 1 = |p|_q$.

6.2 O teorema de Ostrowski

Quase vinte anos depois de Hensel apresentar os números p-ádicos, em 1916, Alexander Markowich Ostrowski, um aluno de Hensel, lança luz sobre as bases por traz desta ideia. Em um de seus teoremas mais conhecidos, o matemático ucraniano demonstra que todo valor absoluto não trivial em $\mathbb{Q}$ ou é uma potência do valor absoluto trivial, ou é uma potência de um valor absoluto p-ádico, para algum primo p. Portanto, um completamento de $\mathbb{Q}$ com respeito a algum valor absoluto não trivial, ou é $\mathbb{R}$ ou é $\mathbb{Q}_p$ para algum primo p. A seguir apresentamos o Teorema de Ostrowski, de acordo com CONRAD.

Proposição 6.2.29. (Teorema de Ostrowski) *Todo valor absoluto não trivial em* $\mathbb{Q}$ é *equivalente a um dos valores absolutos* $|\ \ |_p$, *onde p é um número primo ou* $p = \infty$.

Demonstração.

Lembramos que um valor absoluto em $\mathbb{Q}$, dadas as propriedades do valor absoluto, é completamente determinado pelos valores que assumem para $n \in \mathbb{Z}_+$. Assim, precisamos mostrar que dado um valor absoluto $|\ \ |$ qualquer em $\mathbb{Q}$, temos $t > 0$ tal que $|n| = |n|_\infty^t$ ou $|n| = |n|_p^t$ para algum primo p, com $n \in \mathbb{Z}_+$. No entanto basta mostrar isso para $n \in \mathbb{Z}_+$.

Se $|\ \ |$ é não trivial, certamente para algum $n \in \mathbb{Z}_+$ temos $|n| > 1$ para algum $n \geq 2$ (se for arquimediano) ou $|n| \leq 1$ para todo $n \geq 2$ (se for não arquimediano pela proposição **3.2.10**). Assim vamos dividir a demonstração em duas partes, referentes a esses dois casos.

Para demonstrar o primeiro caso, primeiramente vamos mostrar que se $|n| > 1$ para algum $n \geq 2$ então $|n| > 1$ para todo $n \geq 2$. Faremos isso provando a contrapositiva desta afirmação: se $|n_0| \leq 1$ para algum $n_0 \geq 2$ então $|n| \leq 1$ para todo $n \geq 2$. Com esse fim, vamos escrever n na base n_0:

$$n = a_0 + a_1 n_0 + \cdots + a_k n_0^k,$$

onde $a_k \neq 0$ e $0 \leq a_i < n_0$, de onde $n_0^d \leq n < n_0^{d+1}$. Certamente também temos que $|a_i| = |1 + 1 + \cdots + 1| \leq |1| + |1| + \cdots + |1| = a_i < n_0$. Então aplicando o valor absoluto, e usando o fato de que $|n_0| \leq 1$ temos

$$\begin{aligned} |n| &= |a_0 + a_1 n_0 + a_2 {n_0}^2 + \cdots + a_k {n_0}^k| \\ &\leq |a_0| + |a_1||n_0| + \cdots + |a_k||n_0|^k \\ &< n_0 + n_0|n_0| + \cdots + n_0|n_0|^k \\ &= n_0(1 + |n_0| + \cdots + |n_0|^k) \\ &\leq n_0(\underbrace{1 + 1 + \cdots + 1}_{d+1\ vezes}) \\ &= n_0(d+1). \end{aligned}$$

Mas de $n_0^d \leq n < n_0^{d+1}$ temos $\log_{n_0} n_0^d \leq \log_{n_0} n$ que é equivalente a $d \leq \log_{n_0} n$ e $d + 1 \leq \log_{n_0}(n) + 1$ que combinando com o resultado anterior nos diz que $|n| < n_0(d+1) \leq n_0[\log_{n_0}(n) + 1]$. Substituindo n por n^d na última inequação, encontramos $|n|^d \leq n_0[d \cdot \log_{n_0}(n) + 1]$. Finalmente aplicando raiz ficamos com

$$|n| \leq \sqrt[d]{n_0[d \cdot \log_{n_0}(n) + 1]}$$

Como $n, n_0 > 1$, temos $\log_{n_0}(n) > 0$ e fazendo $d \to \infty$ percebe-se que $|n| \leq 1$ para todo n.

Agora podemos voltar para a demonstração do primeiro caso de que se $|n| > 1$ para algum $n \geq 2$ então $|\quad| = |\quad|_\infty^t$ em $\mathbb{Q}$. E podemos supor m e n inteiros maiores do que 2, e, portanto $|m| > 1$ e $|n| > 1$. Sempre podemos escolher $k > 0$, tal que $m^k \leq n < m^{k+1}$ onde k é a parte inteira de $\log_m n$. Assim escrevendo n na base m e repetindo o processo da etapa anterior, e usando o fato $|m| > 1$, encontramos

$$\begin{aligned} |n| &\leq m(1 + |m| + \cdots + |m|^k) \\ &= m\frac{|m|^{k+1} - 1}{|m| - 1} \\ &< m\frac{|m|^{k+1}}{|m| - 1} = |m|^k \frac{m|m|}{|m| - 1} \end{aligned}$$

Como $k \leq \log_m n$ temos

$$|n| < \frac{m|m|}{|m| - 1} |m|^{\log_m n},$$

que é válida para n arbitrário, logo podemos substituir n por um n^j, e ficar com

$$|n|^j < \frac{m|m|}{|m|-1}|m|^{j\log_m n}.$$

Tomando a j-ésima raiz em ambos os lados, e fazendo $j \to \infty$ temos

$$|n| < \sqrt[j]{\frac{m|m|}{|m|-1}}|M|^{\log_m n} \overset{j\to\infty}{\Longrightarrow} |n| \leq 1 \cdot |m|^{\log_m n}.$$

Como $|n|$ e $|m|$ são números reais, sabemos que existem $s = \log_{\mathrm{m}}|m|$ e $t = \log_{\mathrm{n}}|n|$ positivos (pois n e m são maiores do que 1) e assim $|n| = n^t$ e $|m| = m^s$. Fazendo a substituição na expressão acima, temos $n^t \leq m^{s\log_m n} = n^s$. Logo $t \leq s$

Mas os papéis de m e n em toda a argumentação são simétricos, então poderíamos trocar as posições de m e n, fazermos as mesmas substituições que fizemos por último e encontrarmos $|m| \leq |n|^{\log_n m} \Rightarrow m^s \leq n^{t\log_m n} = m^t \Rightarrow s \leq t$.

Portanto $s = t$ e $|n| = n^t$ e $|m| = m^t$. O que demonstra que

$$|n| = n^t = |n|_\infty^t, \text{ para todo } n \in \mathbb{Z}_+.$$

Agora iniciamos a segunda parte da demonstração, em que afirmamos que se $|n| \leq 1$ para todo $n \geq 2$ então $|\quad| = |\quad|_p^t$ em $\mathbb{Q}$, para algum p primo.

Para algum inteiro $n \geq 2$ temos $|n| \neq 1$ e assim $0 < |n| < 1$. Tomemos p o menor desses números. Sendo assim temos $0 < |p| < 1$ e, $0 < 1/p < 1$ e podemos escrever $|p| = (1/p)^t$ onde $t = \log_{1/p}|p| > 0$. Vamos mostrar que $|n| = |n|_p^t$ para todo $n > 1$.

Certamente que p é primo, pois se por contradição assumimos $p = a \cdot b$, com a e b inteiros positivos menores do que p, pela minimalidade de p teríamos $|a| = |b| = 1$, e assim $|p| = |a||b| = 1 \cdot 1 = 1$, o que é absurdo.

Mostraremos agora que para cada inteiro positivo m não divisível por p tem-se $|m| = 1$. Usando a divisão euclidiana, vamos supor $m = pq + r$, com $0 \leq r < p$. De onde temos $r = m - pq$. Aplicando o módulo temos $|r| = |m - pq| \leq \max\{(|m| \leq 1), (\,|p| < 1)(|q| \leq 1)\} = \max\{(|m| \leq 1), (\,|p||q| < 1)\} \leq 1$. Entretanto, como p é o menor tal que $|p| < 1$, temos $|r| = 1$ e, portanto, só nos resta que $|m| = 1$.

Agora, se n é um inteiro divisível por p, então existe $\alpha \geq 1$ tal que $n = p^\alpha n'$, onde n' não é divisível por p (portanto, $|n'| = 1$). E lembrando que $|p| = (1/p)^t$, temos

$$|n| = |p^\alpha n'| = |p^\alpha||n'| = |p^\alpha| = |p|^\alpha = \left[\left(\frac{1}{p}\right)^t\right]^\alpha = \left[\left(\frac{1}{p}\right)^\alpha\right]^t$$

E como $|n|_p = \left(\frac{1}{p}\right)^\alpha$, temos $|n| = |n|_p^t$.

■

7 CONSIDERAÇÕES FINAIS

Na demonstração do Teorema de Ostrowski, claramente usamos a separação complementar e disjunta de valores absolutos em arquimedianos e não arquimedianos, o que pela definição apresentada no segundo capítulo percebemos ser possível. Utilizamos também algumas propriedades da caracterização dos valores absolutos não arquimedianos de uma forma sucinta.

Pelas proposições **2.1.28** (iv) e **2.1.29** percebemos que se dois valores absolutos $|\ \ |'$ e $|\ \ |^*$ em $\mathbb{Q}$ são equivalentes, e um deles é não arquimediano, digamos $|\ \ |'$, então para $x \in \mathbb{Z}_+^*$ temos o $|x|' \leq 1$. Mas, pela equivalência dos dois, isto implica $|x|^* \leq 1$, o que pela proposição **3.2.10** (i) garante que $|\ \ |^*$ é também não arquimediano. Assim dois valores absolutos equivalentes, ou são ambos arquimedianos, ou são ambos não arquimedianos.

Assim temos a resposta de Ostrowski para questionamento central que motiva esse trabalho: quais os valores absolutos que podem ser definidos em $\mathbb{Q}$ a fim de construirmos diferentes completamentos do corpo dos racionais? O Teorema de Ostrowski nos mostra que só existem três famílias de valores absolutos não equivalentes entre si em $\mathbb{Q}$. Assim qualquer valor absoluto nos racionais ou é equivalente ao valor absoluto usual, ou é equivalente a algum valor absoluto p-ádico, ou é o valor absoluto trivial.

REFERÊNCIAS

BACHMAN, G. **Introduction to p-Adic Numbers and Valuation Theory**. new york: Academic Press, 1964.

CONRAD, K. **OSTROWSKI'S THEOREM FOR Q**. Disponivel em: <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/ostrowskiQ.pdf>. Acesso em: 25 março 2018.

DOMINGUES, H. H. **Espaços métricos e introdução à topologia**. São Paulo: Atual, 1982.

GOUVÊA, F. Q. **Primeiros passos p-ádicos**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1989.

GOUVÊA, F. Q. **p-adic Numbers:** An Introduction. Weterville: Springer-Verlag, 1993.

HERSTEIN, I. N. **Abstract Algebra**. New Jersey: Prentice-Hall, 1996.

KATOK, S. **p-adic Analysis Compared with Real**. Providence: American Mathematical Society, 2007.

KOBLITZ, N. **p-adic Numbers, p-adic Analysis, and Zeta- Functions**. 2ª. ed. New York: Springer-Verlag , 1984.

LANG, S. **Estruturas Algébrica**. Rio de Janeiro: Ao Livro Técnico S.A., 1972.

LIMA, E. L. **Curso de Análise**. Rio de Janeiro: Institutuo de Matemática Pura e Aplicada, v. I, 1976.

LIMA, E. L. **Espaços Métricos**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2011.

LORENZ, F. **Fields with Structure, Algebras and Advanced Topics**. New York: Springer Science+Business Media, v. II, 2008.

MARTINEZ, B. et al. **Teoria dos Números:** Um Passeio com Primos e Outros Números Familiares Pelo Mundo Inteiro. Rio de Janeiro: IMPA, 2015.

MONTEIRO, L. H. J. **Elementos de Algebra**. 1ª. ed. Rio de Janeiro: Livros Técnicos e Científicos Editora S.A., 1974.

OLIVEIRA, G. D. O Corpo dos p-ádicos. **Gazeta de Matemática**, Lisboa, v. 159, n. 1, p. 7-18, dezembro 2009. ISSN 0373-2681.

ROQUE, T.; CARVALHO, J. B. P. **Tópicos de História da Matemática**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

SCHNEIDER, A. A. **Completameto de Espaços Métricos**, 2015. Disponivel em: <https://www.researchgate.net/publication/281626457_Completamento_de_Espacos_Metricos>. Acesso em: 24 setembro 2018.

STEWART, I. **17 Equações que Mudaram o Mundo**. Rio de Janeiro: Zahar, 2013.