Universidade Federal de Santa Catarina
Centro de Ciências Físicas e Matemáticas
Departamento de Matemática

MTM5263 - Introdução à Teoria de Galois **1º semestre de 2016**

Corpos p-ádicos

Professor: Eliezer Batista *Aluno: Vinícius Sousa Fazio - 13106219*

1 Introdução

Os números p-ádicos foram inicialmente introduzidos pelo matemático alemão Kurt Hensel por volta de 1897-1904, e se tornaram uma importante ferramenta para a Teoria dos Números. Foram usados inclusive na famosa prova do Último Teorema de Fermat(Boston 2003).

Os corpos p-ádicos são usados em alguns campos de física, como a teoria das cordas, e em outras áreas, como teoria de probabilidade e criptografia. (Rozikov 2013, Dragovich 2009).

Hensel queria usar corpos p-ádicos, entre outras coisas, para provar se alguns números eram transcendentes. E chegou a anunciar uma prova de que e é transcendente, mas com erros. Somente em 1987, Jean-Paul Bézivin e Philippe Robba obtiveram uma prova do Teorema Lindemann-Weierstrass usando corpos p-ádicos, mas admitiram que era completamente diferente da prova proposta por Hensel.

Este trabalho resume alguns dos principais resultados sobre corpos p-ádicos encontrados nas referências bibliográficas, listadas no final.

1.1 Motivação

Esta seção mostra apenas divagações, a fim de motivar, sem nenhum rigor matemático.

Considere a série

$$1 + 9 + 90 + 900 + 9000 + \dots$$

Essa série não converge em $\mathbb{R}$, mas podemos decompô-la em uma sequência de somas parciais:

$$\begin{aligned}
S_0 &= 1 &&= 1\\
S_1 &= 1 + 9 &&= 10\\
S_2 &= 1 + 9 + 90 &&= 100\\
S_3 &= 1 + 9 + 90 + 900 &&= 1000\\
&\vdots\\
S_k &= \dots &&= 10^k\\
&\vdots
\end{aligned}$$

Desta forma, verificamos que o k-ésimo elemento da sequência, S_k, possui k dígitos zeros a direita. Fazendo $k \to \infty$, teremos infinitos dígitos zeros a direita, portanto, podemos dizer que a série converge para zero? Se sim, existem implicações. Neste caso:

$$1 + 9 + 90 + 900 + \dots = 0$$

$$\implies 9 + 90 + 900 + \ldots = -1.$$

Até o final deste trabalho, o leitor estará familiarizado com estas divagações.

1.2 Introdução informal aos números p-ádicos

Nesta seção daremos uma ideia do que é um número p-ádicos, ainda sem um formalismo necessário.

Um número natural $m \in \mathbb{N}$ pode ser decomposto na soma

$$m = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \ldots + a_n 10^n, \quad \text{onde } a_k \in \{0, 1, 2, 3, \ldots, 9\}.$$

Ou seja, $m = \sum_{k=0}^{n} a_k \cdot 10^k$. A representação decimal de m é

$$m = a_n a_{n-1} \ldots a_3 a_2 a_1 a_0.$$

Definimos w como um número p-ádicos, onde p é um número primo, se

$$w = a_0 \cdot p^0 + a_1 \cdot p^1 + a_2 \cdot p^2 + \ldots, \quad \text{onde } a_k \in \{0, 1, 2, 3, \ldots, p\}.$$

Ou seja, $w = \sum_{k=0}^{\infty} a_k \cdot p^k$. A representação p-ádica de w é

$$w = \ldots a_3 a_2 a_1 a_0.$$

Ou seja, um número p-ádico pode ser entendido como um número com infinitos dígitos à esquerda.

Portanto, $\mathbb{N}$ está contido nos números p-ádicos, se considerarmos a representação de um número $\mathbb{N}$ na base p e onde $a_n = 0$ quando n é maior que um certo $n_0 \in \mathbb{N}$. A importância de estar na base p em vez da usual base decimal será observada mais adiante.

A soma e multiplicação de dois números p-ádicos podem ser definidas utilizando os mesmos algoritmos de soma e multiplicação dos números naturais. Por exemplo, supondo que estamos no conjunto 5-ádico, podemos fazer:

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

Um exemplo de multiplicação no conjunto 5-ádico:

$$\begin{array}{cccccc}
 & \ldots & 1 & 2 & 1 & 2 \\
\times & \ldots & 1 & 3 & 0 & 2 \\
\hline
 & \ldots & 2 & 4 & 2 & 4 \\
 & \ldots & 0 & 0 & 0 & \\
 & \ldots & 4 & 1 & & \\
+ & \ldots & 2 & & & \\
\hline
 & \ldots & 4 & 0 & 2 & 4
\end{array}$$

Agora considere a soma abaixo, ainda no conjunto 5-ádico:

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

Ou seja, $(\ldots 41231)$ é o inverso aditivo de $(\ldots 04214)$. Logo, existem inversos aditivos no conjunto 5-ádico. Outro exemplo:

$$\begin{array}{cccccc}
 & & 1 & 1 & 1 & \\
 & \ldots & 2 & 2 & 2 & 3 \\
\times & \ldots & 0 & 0 & 0 & 2 \\
\hline
 & \ldots & 0 & 0 & 0 & 1
\end{array}$$

Logo, $(\ldots 2223)$ é o inverso multiplicativo de 2, o que significa que existem números fracionários no conjunto 5-ádico.

É fácil ver que $(\ldots 4444) = -1$, pois somando 1, todos dígitos ficarão zerados.

Considere $x^2 = -1$, ou seja, $x = \sqrt{-1}$.

$$\begin{array}{cccccc} & & & 1 & & \\ & \ldots & 1 & 2 & 1 & 2 \\ \times & \ldots & 1 & 2 & 1 & 2 \\ \hline & \ldots & 4 & 4 & 4 & 4 \end{array}$$

Mais adiante teremos um teorema que garante que $\sqrt{-1}$ também é um número p-ádico.

2 Valores Absolutos

Antes de construir os corpos p-ádicos, precisaremos do conceito de valores absolutos, e algumas implicações.

Definição (Valor Absoluto)**.** Seja F um corpo. A função $\|\cdot\| : F \to \mathbb{R}_+$ é chamada de um *valor absoluto* de F se tiver as seguintes propriedades, $\forall x, y \in F$:

1. $\|x\| = 0 \iff x = 0$
2. $\|xy\| = \|x\|\|y\|$
3. $\|x + y\| \leq \|x\| + \|y\|$

Proposição (Propriedades Extras dos Valores Absolutos)**.** *Seja $\|\cdot\| : F \to \mathbb{R}_+$ um valor absoluto do corpo F. Então, $\forall x \in F$, $x \neq 0$ vale que:*

1. $\|1\| = 1$
2. $\|-x\| = \|x\|$
3. $\|x^{-1}\| = \|x\|^{-1}$

Demonstração. Seja $x \in F$, $x \neq 0$.

1. $\|1\| = \|1 \cdot 1\| = \|1\|\|1\| \implies \|1\| = \dfrac{\|1\|}{\|1\|} = 1$
2. $1 = \|1\| = \|-1 \cdot -1\| = \|-1\|\|-1\| \implies \sqrt{\|-1\|^2} = \sqrt{1} \implies \|-1\| = 1$
   Assim, $\|-x\| = \|-1 \cdot x\| = \|-1\|\|x\| = 1 \cdot \|x\| = \|x\|$
3. $1 = \|1\| = \|x \cdot x^{-1}\| = \|x\|\|x^{-1}\| \implies \|x^{-1}\| = \|x\|^{-1}$

□

Agora veremos alguns exemplos de valores absolutos.

Proposição (Valor Absoluto Trivial)**.** *A função $\|\cdot\| : \mathbb{Q} \to \mathbb{R}_+$ definida como*

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

é um valor absoluto de $\mathbb{Q}$ e é chamado valor absoluto trivial.

Demonstração. Sejam $x, y \in \mathbb{Q}$.

1. $\|x\| = 0 \implies x = 0$ pois $x \neq 0 \implies \|x\| = 1$.
2. Se $x = 0$ ou $y = 0$ então $\|xy\| = 0 = \|x\|\|y\|$
   Se $x \neq 0$ e $y \neq 0$ então $\|xy\| = 1 = \|x\|\|y\|$

3. Note que $\|x+y\| \leq 1$ por definição.
   Se $x \neq 0$ ou $y \neq 0$ então $\|x+y\| \leq 1 \leq \max\{\|x\|, \|y\|\} \leq \|x\| + \|y\|$.
   Se $x = 0 = y$ então $\|x+y\| = \|0\| = 0 = \|0\| + \|0\|$.
   Portanto $\|x+y\| \leq \|x\| + \|y\|$

□

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

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

é um valor absoluto de $\mathbb{Q}$ *e é chamado será chamado* valor absoluto real*. O símbolo* ∞ *é apenas notação, para identificar o valor absoluto real e distinguí-lo de outros valores absolutos.*

Demonstração. Sejam $x, y \in \mathbb{Q}$.

1. $\|x\|_\infty = 0 \implies x = 0$ pois x e $-x$ são diferentes de zero se $x \neq 0$.
2. Se $x \geq 0$ e $y \geq 0$ então $\|xy\|_\infty = xy = \|x\|_\infty \|y\|_\infty$
   Se $x < 0$ e $y < 0$ então $\|xy\|_\infty = xy = (-x)(-y) = \|x\|_\infty \|y\|_\infty$
   Se $x < 0 < y$ então $\|xy\|_\infty = -xy = (-x)y = \|x\|_\infty \|y\|_\infty$
   O caso $y < 0 < x$ é análogo. Portanto $\|xy\|_\infty = \|x\|_\infty \|y\|_\infty$.
3. Se $x \geq 0$ e $y \geq 0$ então $\|x+y\|_\infty = x + y = \|x\|_\infty + \|y\|_\infty$
   Se $x < 0$ e $y < 0$ então $\|x+y\|_\infty = -(x+y) = (-x) + (-y) = \|x\|_\infty + \|y\|_\infty$
   Se $x < 0 < y$ e $x + y < 0$ então $\|x+y\|_\infty = -(x+y) = -x - y = \|x\|_\infty - \|y\|_\infty < \|x\|_\infty + \|y\|_\infty$
   Se $x < 0 < y$ e $x + y \geq 0$ então $\|x+y\|_\infty = x + y = -\|x\|_\infty + \|y\|_\infty < \|x\|_\infty + \|y\|_\infty$
   Os casos $y < 0 < x$ são análogos. Portanto $\|x+y\|_\infty \leq \|x\|_\infty + \|y\|_\infty$.

□

Proposição (Valor Absoluto p-ádico)**.** *Seja* $\|\cdot\|_p : \mathbb{Q} \to \mathbb{R}_+$*, onde* p *é um número primo. Note que qualquer número* $x \in \mathbb{Q}$ *não nulo pode ser escrito da forma* $p^n \frac{a}{b}$*, onde* $a, n \in \mathbb{Z}, b \in \mathbb{N}, b \neq 0, p \nmid ab$*. A função* $\|\cdot\|_p$*, definida como*

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

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

Demonstração. Sejam $x, y \in \mathbb{Q}$.

1. $\|x\|_p = 0 \implies x = 0$ pois $p^{-n} > 0$
2. Se $x = 0$ ou $y = 0$ então $\|xy\|_p = 0$ e $\|x\|_p \|y\|_p = 0$, logo, vale a propriedade.
   Se $x \neq 0$ e $y \neq 0$, podemos escrever $x = p^n \frac{a}{b}$ e $y = p^m \frac{c}{d}$ onde $p \nmid abcd$.
   Então, $\|xy\|_p = \left\| p^{n+m} \frac{ac}{bd} \right\|_p = p^{-n-m} = p^{-n} p^{-m} = \|x\|_p \|y\|_p$.
3. Caso $x = 0$ ou $y = 0$ então $\|x+y\|_p = \|x\|_p + \|y\|_p$.
   Caso $x + y = 0$ então $\|x+y\|_p = \|0\|_p = 0 \leq \|x\|_p + \|y\|_p$ pois $\|\cdot\|_p$ é sempre maior ou igual a zero.
   Como último caso, assuma $x \neq 0$, $y \neq 0$ e $x + y \neq 0$. Assim, podemos escrever $x = p^n \frac{a}{b}$ e $y = p^m \frac{c}{d}$ onde $p \nmid abcd$.
   Suponha $n \leq m$. Note que, assim, $\|x\|_p \geq \|y\|_p$. Além disso,

$$\|x+y\|_p = \left\|p^n\frac{a}{b}+p^m\frac{c}{d}\right\|_p = \left\|\frac{p^n(ad+p^{m-n}bc)}{bd}\right\|_p \leq p^{-n} = \|x\|_p.$$

Analogamente, $m \leq n \implies \|y\|_p \geq \|x\|_p$ e $\|x+y\|_p \leq \|y\|_p$.

Logo, $\|x+y\|_p \leq \max\{\|x\|_p, \|y\|_p\} \leq \|x\|_p + \|y\|_p$

□

Os valores absolutos dão noção de distância. Veremos isso mais precisamente com o conceito de *métrica*.

Definição (Métrica)**.** Seja F um conjunto. A função $d : F \times F \to \mathbb{R}_+$ é dita ser uma *métrica* de F se tiver as seguintes propriedades, $\forall x, y, z \in F$:

1. $d(x,y) = 0 \iff x = y$
2. $d(x,y) = d(y,x)$
3. $d(x,z) \leq d(x,y) + d(y,z)$

Além disso, (F,d) é dito ser um *espaço métrico*.

Proposição (Métrica Induzida por Valor Absoluto)**.** *Seja F um corpo e $\|\cdot\|$ um valor absoluto de F. Então a função $d : F \times F \to \mathbb{R}_+$ definida por $d(x,y) = \|x-y\|$ é uma métrica de F.*

Demonstração. Seja $x, y, z \in F$.

1. $d(x,y) = 0 \iff \|x-y\| = 0 \iff x-y = 0 \iff x = y$
2. $d(x,y) = \|x-y\| = \|-(y-x)\| = \|y-x\| = d(y,x)$
3. $d(x,z) = \|x-z\| = \|x-y+y-z\| \leq \|x-y\| + \|y-z\| = d(x,y) + d(y,z)$

□

Definição (Métrica Arquimediana)**.** Seja (F,d) um espaço métrico. Se d tiver a propriedade, $\forall x, y, z \in F$, $d(x,y) \leq \max\{d(x,y), d(y,z)\}$, então d é dita *não-arquimediana*. Caso contrário, d é dita *arquimediana*.

Proposição (Valor Absoluto Arquimediano)**.** *Seja F um corpo e $\|\cdot\|$ um valor absoluto de F. Se $\|\cdot\|$ tiver a propriedade, $\forall x, y \in F$, $\|x+y\| \leq \max\{\|x\|, \|y\|\}$, então a métrica induzida $d(x,y) = \|x-y\|$ é* não-arquimediana *e o valor absoluto é dito ser* não-arquimediano*. Caso contrário, a métrica induzida é* arquimediana *e o valor absoluto é dito ser* arquimediano*.*

Demonstração. Suponha $\forall x, y \in F$, $\|x+y\| \leq \max\{\|x\|, \|y\|\}$. Neste caso, seja $x, y, z \in F$. Então:

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

onde se conclui que d é não-arquimediana. Agora suponha $\exists x_0, y_0 \in \mathbb{F}$ tais que $\|x_0+y_0\| > \max\{\|x_0\|, \|y_0\|\}$. Assim, vale que

$$d(x_0,y_0) = \|x_0-(-y_0)\| = \|x_0+y_0\| > \|x_0\| + \|y_0\| = d(x_0,0) + d(y_0,0) = d(x_0,0) + d(0,y_0).$$

Logo, d é arquimediana.

□

Exemplo. O valor absoluto trivial é não-arquimediano, como demonstrado.

Exemplo. O valor absoluto real é arquimediano pois $\|1+1\| = 2 \not\leq \max\{\|1\|, \|1\|\} = 1$.

Exemplo. O valor absoluto p-ádico é não-arquimediano, como demonstrado.

Um espaço métrica não-arquimediana não é muito intuitivo. Por exemplo, veremos agora a demonstração do princípio do triângulo isóceles, que implica que em um espaço métrico não-arquimediano todo triângulo possui pelo menos dois lados iguais.

Proposição (Princípio do Triângulo Isóceles)**.** *Seja F um corpo e $\|\cdot\|$ um valor absoluto de F não-arquimediano. Seja $x, y \in F$. Então ou $\|x\| = \|y\|$ ou $\|x - y\| = \|y\|$ ou $\|x - y\| = \|x\|$.*

Demonstração. Suponha $\|x\| < \|y\|$.
Como $\|x - y\| \leq \max\{\|x\|, \| - y\|\} = \max\{\|x\|, \|y\|\} \implies \|x - y\| \leq \|y\|$.
Por outro lado, temos que
$\|y\| = \|x - (x - y)\| \leq \max\{\|x\|, \| - (x - y)\|\} = \max\{\|x\|, \|x - y\|\} \implies \|y\| \leq \|x - y\|$.
Logo, $\|y\| = \|x - y\|$.
O resultado é análogo se $\|y\| < \|x\|$, que implicará $\|x\| = \|x - y\|$.
O último caso, $\|x\| = \|y\|$, já satisfaz a proposição.

□

Corolário (Princípio do Triângulo Isóceles)**.** *Seja F um corpo e $\|\cdot\|$ um valor absoluto de F não-arquimediano. Seja $x, y \in F$ tal que $\|x\| \neq \|y\|$. Então $\|x - y\| = \max\{\|x\|, \|y\|\}$.*
Ou seja, os dois lados iguais são maiores ou iguais ao terceiro lado.

Uma curiosidade sobre os valores absolutos não-arquimedianos é que todo elemento de uma bola aberta é centro da bola, como veremos com mais detalhes agora.

Definição (Bola Aberta)**.** Seja F um corpo e $\|\cdot\|$ um valor absoluto de F. Seja $x_0 \in F$ e $r \in \mathbb{R}$, $r > 0$. O conjunto $B(x_0, r) = \{x \in \mathbb{F} : \|x - x_0\| < r\}$ é dito uma *bola aberta* de centro x_0 e raio r.

Proposição (Centro da bola em valores absolutos não-arquimedianos)**.** *Seja F um corpo e $\|\cdot\|$ um valor absoluto de F não-arquimediano. Considere a bola $B(x_0, r)$ onde $x_0 \in F$ e $r \in \mathbb{R}$, $r > 0$. 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. Seja $x \in B(x_0, r)$. Logo, $\|x - x_0\| < r$. Sabemos que $y_0 \in B(x_0, r)$. Logo,
$\|x - y_0\| = \|x - x_0 + x_0 - y_0\| \leq \max\{\|x - x_0\|, \|x_0 - y_0\|\} < r$.
Portanto, $B(x_0, r) \subset B(y_0, r)$. Analogamente concluiremos que $B(y_0, r) \subset B(x_0, r)$.

□

3 Corpos p-ádicos

Nesta seção, os corpos p-ádicos serão definidos e construídos formalmente.

Precisaremos analisar convergência de sequências para gerar o corpo dos p-ádicos. Assim, vamos rever as sequências de Cauchy com valores absolutos.

Definição (Sequência de Cauchy)**.** Seja F um corpo com um valor absoluto $\|\cdot\|$. Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de F. A sequência (a_n) é dita *sequência de Cauchy* se, dado $\epsilon > 0, \exists n_0 \in \mathbb{N}$ tal que $\forall\, i, j \in \mathbb{N}$ onde $i > j > n_0$ então $\|a_i - a_j\| < \epsilon$.

Note que as sequências de Cauchy são definidas em espaços métricos. Mas como o valor absoluto induz uma métrica, podemos definí-la em termos de valores absolutos.

Proposição (Equivalência de Sequência de Cauchy)**.** *Sejam $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$ sequências de Cauchy com o valor absoluto $\|\cdot\|$. Então a relação $(a_n) \sim (b_n)$ definida por $\lim_{n\to\infty} \|a_n - b_n\| = 0$ forma uma classe de equivalência.*

Demonstração. Seja $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ e $(c_n)_{n\in\mathbb{N}}$ sequências de Cauchy.

1. $\lim_{n\to\infty} \|a_n - a_n\| = \lim_{n\to\infty} \|0\| = 0 \implies (a_n) \sim (a_n)$
2. $(a_n) \sim (b_n) \iff \lim_{n\to\infty} \|a_n - b_n\| = 0 \iff \lim_{n\to\infty} \| - (b_n - a_n)\| = 0 \iff (b_n) \sim (a_n)$
3. Seja $(a_n) \sim (b_n)$ e $(b_n) \sim (c_n)$.
   Então, por hipótese, $\lim_{n\to\infty} \|a_n - b_n\| = 0$ e $\lim_{n\to\infty} \|b_n - c_n\| = 0$.
   Desta forma, para qualquer $\epsilon > 0$, $\exists n_0, m_0 \in \mathbb{N}$ tal que $\forall n > n_0$ e $\forall m > m_0$ valem que:
   $\|a_n - b_n\| < \dfrac{\epsilon}{2}$ e $\|b_m - c_m\| < \dfrac{\epsilon}{2}$.

Assim, $\forall n > \max\{n_0, m_0\}$ vale que

$\|a_n - c_n\| = \|a_n - b_n + b_n - c_n\| \leq \|a_n - b_n\| + \|b_n - c_n\| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon,$

o que implica que $\lim_{n\to\infty} \|a_n - c_n\| = 0 \implies (a_n) \sim (c_n)$.

□

Definição (Corpo Completo)**.** Um corpo F é dito *completo* se toda sequência de Cauchy de F, usando valor absoluto $\|\cdot\|$, converge.

Se quisermos completar um corpo A, que não é completo, precisaremos de um novo corpo, B, que seja completo, tal que de certa forma $A \subset B$, e os valores absolutos dos elementos de A se mantenham iguais aplicados ao valor absoluto de B. Além disso, queremos o menor corpo completo que contenha A.

Por isso, definiremos o que é um completamento de um corpo.

Definição (Completamento de um Corpo com Valor Absoluto)**.** O conjunto $\widetilde{F}$ é dito *completamento* de um corpo F pelo valor absoluto $\|\cdot\|$ se as seguintes condições forem satisfeitas:

1. $\widetilde{F}$ é completo
2. Existe uma isometria $f : F \to \widetilde{F}$, ou seja, o valor absoluto estendido para $\widetilde{F}$, denotado $\|\cdot\|_{\widetilde{F}}$, é tal que $\|f(x)\|_{\widetilde{F}} = \|x\|$, para todo $x \in F$
3. Para todo $x \in \widetilde{F}$ existe $(a_n)_{n\in\mathbb{N}}$ sequência de Cauchy de F tal que $x = \lim_{n\to\infty} a_n$

A isometria f é necessária para inserir os elementos de F em $\widetilde{F}$. Agora analisaremos alguns corpos completos.

Proposição (Corpo $\mathbb{Q}$)**.** *O corpo dos números racionais $\mathbb{Q}$ é completo quando o valor absoluto trivial é usado.*

Demonstração. Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy de $\mathbb{Q}$.

Então, para $\exists n_0 \in \mathbb{N}$ tal que se $i > j > n_0$ então $\|a_i - a_j\| < 1/2$.

Mas no valor absoluto trivial, $\|x\| \neq 1 \iff x = 0$. Assim, $a_i - a_j = 0 \implies a_i = a_j$.

Portanto, a sequência (a_n) é constante a partir de um determinado índice, logo, converge para algum elemento de $\mathbb{Q}$, o que faz com que $\mathbb{Q}$ seja completo. □

Proposição (Corpo $\mathbb{R}$)**.** *O completamento dos números racionais $\mathbb{Q}$ usando o valor absoluto real é o conjunto dos $\mathbb{R}$. Este resultado não será demonstrado.*

Proposição (Corpo $\mathbb{Q}_p$)**.** *O completamento dos números racionais $\mathbb{Q}$ usando o valor absoluto* p*-ádico, para algum p primo, forma um corpo, denominado corpo* p*-ádico, e denotado $\mathbb{Q}_p$.*

Demonstração. Seja $\mathbb{Q}_p$ o conjunto das classes de equivalências das sequências de Cauchy de $\mathbb{Q}$ usando o valor absoluto p-ádico.

Seja $\|\cdot\|_p : \mathbb{Q}_p \to \mathbb{R}$ uma extensão do valor absoluto p-ádico, para poder ser aplicado em valores de $\mathbb{Q}_p$ em vez de $\mathbb{Q}$. Seja $a \in \mathbb{Q}_p$ a classe de equivalência da sequência $(a_n)_{n\in\mathbb{N}}$, onde $a_n \in \mathbb{Q}$. Então definiremos $\|a\|_p = \lim_{n\to\infty} \|a_n\|_p$, onde $\|a_n\|_p$ tem a definição de valor absoluto p-ádico dos $\mathbb{Q}$. Tal limite existe pois:

1. Caso $a = 0$.

   Então $\lim_{n\to\infty} a_n = 0 \iff \lim_{n\to\infty} \|a_n - 0\|_p = 0 \iff \lim_{n\to\infty} \|a_n\|_p = 0$

2. Caso $a \neq 0$.

   Sabemos que $a \neq 0 \implies \lim_{n\to\infty} a_n \neq 0$. Assim, seja $\epsilon > 0$ tal que exista a subsequência $(b_n)_{n\in\mathbb{N}}$ de (a_n) onde $\|b_n\|_p > \epsilon, \forall n \in \mathbb{N}$. Caso não exista tal ϵ então todas subsequências de (a_n) convergem para 0, o que implica que $\lim_{n\to\infty} a_n = 0$. Portanto, tal ϵ existe.

   Como $(a_n)_{n\in\mathbb{N}}$ é de Cauchy, $\exists n_0 \in \mathbb{N}$ tal que $\forall i > j \geq n_0$ vale que $\|a_i - a_j\|_p < \epsilon$.

   Como (b_n) é subsequência, $\exists n_1 \geq n_0$ tal que $b_{n_0} = a_{n_1}$. Logo, $\|a_{n_1}\| > \epsilon$.

Em particular, vale que $\forall i > n_0$, $\|a_i - a_{n_1}\|_p < \epsilon$.

Sendo o valor absoluto p-ádico não-arquimediano, o princípio do triângulo isóceles se aplica.

Pelo princípio, se $\|a_i\|_p \neq \|a_{n_1}\|_p \implies \|a_i - a_{n_1}\|_p = \max\{\|a_i\|_p, \|a_{n_1}\|_p\} \geq \|a_{n_1}\|_p > \epsilon$, contradição. Logo, $\|a_i\|_p = \|a_{n_1}\|_p$, $\forall i > n_0$. Portanto, $\lim_{n\to\infty} \|a_n\|_p = \|a_{n_1}\|_p$.

Note que o fato das sequências $(\|a_n\|_p)_{n\in\mathbb{N}}$ serem constante a partir de um determinado índice, como visto na demonstração, faz com que o valor absoluto de $a \in \mathbb{Q}_p$ seja igual ao valor absoluto de um $x \in \mathbb{Q}$, logo, o conjunto imagem da função valor absoluto estendido para $\mathbb{Q}_p$ não mudou.

Agora, definiremos a soma e a multiplicação de dois elementos distintos de $\mathbb{Q}_p$.

Sejam $(a_n)_{n\in\mathbb{N}}$ e $(a'_n)_{n\in\mathbb{N}}$ dois representantes da classe de equivalência $a \in \mathbb{Q}_p$. Analogamente, sejam $(b_n)_{n\in\mathbb{N}}$ e $(b'_n)_{n\in\mathbb{N}}$ representantes de $b \in \mathbb{Q}_p$.

Definiremos $a + b = (a_n + b_n)_{n\in\mathbb{N}}$.

Considere $\|(a_n + b_n) - (a'_n + b'_n)\|_p = \|(a_n - a'_n) + (b_n - b'_n)\|_p \leq \|a_n - a'_n\|_p + \|b_n - b'_n\|_p$.

Assim, $\lim_{n\to\infty} \|(a_n+b_n)-(a'_n+b'_n)\|_p \leq \lim_{n\to\infty} \|a_n-a'_n\|_p+\|b_n-b'_n\|_p = 0$ pois $(a_n) \sim (a'_n)$ e $(b_n) \sim (b'_n)$.

Concluímos então que $(a_n + b_n) \sim (a'_n + b'_n)$.

O inverso aditivo é análogo a demonstração acima.

Definiremos $ab = (a_n b_n)_{n\in\mathbb{N}}$.

Considere $\|a_n b_n - a'_n b'_n\|_p = \|a_n b_n - a_n b'_n + a_n b'_n - a'_n b'_n\|_p = \|a_n(b_n - b'_n) + b'_n(a_n - a'_n)\|_p$
$\leq \max\{\|a_n(b_n - b'_n)\|_p, \|b'_n(a_n - a'_n)\|_p\}$.

Assim, $\lim_{n\to\infty} \|a_n b_n - a'_n b'_n\|_p \leq \lim_{n\to\infty} \max\{\|a_n\|_p \cdot \|b_n - b'_n\|_p, \|b'_n\|_p \cdot \|a_n - a'_n\|_p\}$.

Sabemos que $\lim_{n\to\infty} \|a_n\|_p$ existe e é finito, e que $\lim_{n\to\infty} \|b_n - b'_n\|_p = 0$ porque $(b_n) \sim (b'_n)$.

Analogamente, $\lim_{n\to\infty} \|b'_n\|_p$ existe e é finito, e $\lim_{n\to\infty} \|a_n - a'_n\|_p = 0$ porque $(a_n) \sim (a'_n)$.

Portanto, $\lim_{n\to\infty} \|a_n b_n - a'_n b'_n\|_p = 0$, logo, $(a_n b_n) \sim (a'_n b'_n)$.

Para o inverso multiplicativo, considere $1/a = (1/a_n)_{n\in\mathbb{N}}, a \neq 0$. Para estar bem definido, é necessário pegar representantes sem valores nulos na sequência. É sempre possível obter tal representante. Por exemplo, pode-se remover todos primeiros elementos nulos da sequência. Depois, basta substituir cada elemento nulo restante pelo elemento não nulo anterior a ele da sequência. Assim a sequência continuará de Cauchy, pois se era de Cauchy até o último elemento não nulo, continuará sendo com o valor repetido. Sendo assim, considere:

$$\left\| \frac{1}{a_n} - \frac{1}{a'_n} \right\|_p = \left\| \frac{a'_n - a_n}{a_n a'_n} \right\|_p = \|a'_n - a_n\|_p \left\| \frac{1}{a'_n} \right\|_p \left\| \frac{1}{a_n} \right\|_p .$$

Como $\lim_{n\to\infty} \|1/a_n\|$ e $\lim_{n\to\infty} \|1/a'_n\|$ são finitos e $\lim_{n\to\infty} \|a'_n - a_n\| = 0$ pois $(a_n) \sim (a'_n)$,

$$\lim_{n\to\infty} \left\| \frac{1}{a_n} - \frac{1}{a'_n} \right\|_p = \lim_{n\to\infty} \|a'_n - a_n\|_p \left\| \frac{1}{a'_n} \right\|_p \left\| \frac{1}{a_n} \right\|_p = 0.$$

Podemos concluir então que $(1/a_n) \sim (1/a'_n)$.

Da forma como foi definido, é direto mostrar que a multiplicação e soma de $\mathbb{Q}_p$ possuem elementos neutros, inversos, e são comutativas e associativas, além de respeitarem a distributividade, apenas referenciando $\mathbb{Q}$, que possui estas propriedades. Portanto, $\mathbb{Q}_p$ é um corpo.

Para $\mathbb{Q}_p$ ser completamento de $\mathbb{Q}$ precisa satisfazer:

1. $\mathbb{Q}_p$ ser completo: falta mostrar.

2. Existe uma isometria $f : \mathbb{Q} \to \mathbb{Q}_p$ tal que $\|f(x)\|_p = \|x\|_p$, $\forall x \in \mathbb{Q}$: pode-se afirmar que sim. Primeiramente, o valor absoluto foi estendido para $\mathbb{Q}_p$. Além disso, tomando a isometria $f(x) = [x]$ onde $[x]$ é a classe de equivalência das sequências constantes $(x)_{n\in\mathbb{N}}$, temos que as distâncias $\|f(x)\|_p = \|x\|_p$ pois toda sequência constante converge para o elemento constante, que faz parte de $\mathbb{Q}$.

3. Para todo $x \in \mathbb{Q}_p$ deve existir $(a_n)_{n\in\mathbb{N}}$ sequência de Cauchy de $\mathbb{Q}$ tal que $x = \lim_{n\to\infty} a_n$: é válido pois o conjunto $\mathbb{Q}_p$ foi definido assim.

Assim, basta mostrar que $\mathbb{Q}_p$ é completo.

Seja $(A_k)_{k\in\mathbb{N}}$ uma sequência de Cauchy de $\mathbb{Q}_p$. Temos que motrar que $\lim_{k\to\infty} A_k$ é um representante de um elemento de $\mathbb{Q}_p$.

Sabemos que o elemento A_k, para um k fixo, é a classe de equivalência de sequências de Cauchy em $\mathbb{Q}$. Vamos denotar um representante dessa classe de equivalência por $(a_{k,n})_{n\in\mathbb{N}}$. Essa sequência é de Cauchy em $\mathbb{Q}$, então existe um $n(k) \in \mathbb{N}$ tal que se $i > j \geq n(k)$ então $\|a_{k,i} - a_{k,j}\|_p < p^{-k}$. Estamos fixando um p^{-k} para facilitar as contas. Considere a sequência $(a_{k,n(k)})_{k\in\mathbb{N}}$. Vamos mostrar que essa sequência é o representante do limite procurado.

Note que para um k qualquer, vale que $\|A_k - a_{k,n(k)}\|_p < p^{-k}$, pois $\|a_{k,i} - a_{k,n(k)}\|_p < p^{-k}$ para qualquer $i > k$, como visto acima. Assim, $\|A_k - a_{k,n(k)}\|_p = \lim_{i\to\infty} \|a_{k,i} - a_{k,n(k)}\|_p \leq p^{-k}$.

Portanto, $\lim_{k\to\infty} \|A_k - a_{k,n(k)}\|_p \leq \lim_{k\to\infty} p^{-k} = 0$. Assim, a sequência $(a_{k,n(k)})_{k\in\mathbb{N}}$ é um representante para o limite de A_k.

Agora basta mostrar que $(a_{k,n(k)})_{k\in\mathbb{N}}$ é de Cauchy para garantir que ela está em $\mathbb{Q}_p$.

Considere $\|a_{i,n(i)} - a_{j,n(j)}\|_p = \|a_{i,n(i)} - A_i + A_i - A_j + A_j - a_{j,n(j)}\|_p$.

Assim, $\|a_{i,n(i)} - a_{j,n(j)}\|_p \leq \max\{\|a_{i,n(i)} - A_i\|_p, \|A_i - A_j\|_p, \|A_j - a_{j,n(j)}\|_p\}$.

Fixe um $\epsilon > 0$.

Já sabemos que $\|a_{i,n(i)} - A_i\|_p < p^{-i}$, pois acabamos de demonstrar. Em particular, existe um n_0 tal que se $i > n_0$, $\|a_{i,n(i)} - A_i\|_p < \epsilon$

Além disso, existe um n_1 tal que se $i > j > n_1$ então $\|A_i - A_j\|_p < \epsilon$, pois (A_k) é de Cauchy.

Por fim, existe um n_2 tal que se $j > n_2$ então $\|A_j - a_{j,n(j)}\|_p < \epsilon$, que é análogo ao primeiro caso.

Logo, concluimos que se $i > j > \max\{n_0, n_1, n_2\}$ então

$$\|a_{i,n(i)} - a_{j,n(j)}\|_p \leq \max\{\|a_{i,n(i)} - A_i\|_p, \|A_i - A_j\|_p, \|A_j - a_{j,n(j)}\|_p\} < \max\{\epsilon,\epsilon,\epsilon\} = \epsilon.$$

Logo, a sequência é um representante de uma classe de equivalência de $\mathbb{Q}_p$, portanto, $\mathbb{Q}_p$ é completo! □

4 Outros completamentos de $\mathbb{Q}$

Antes de analisarmos os corpos p-ádicos, vamos investigar se existem outros completamentos dos $\mathbb{Q}$ utilizando outros valores absolutos.

Definição (Equivalência de Valores Absolutos)**.** Dois valores absolutos $\|\cdot\|_a$ e $\|\cdot\|_b$ são ditos *equivalentes* quando uma sequência é de Cauchy em $\|\cdot\|_a$ se e somente se é de Cauchy em $\|\cdot\|_b$.

Vamos mostrar agora que basta analisar o valor absoluto em $\mathbb{N} \subset \mathbb{Q}$ para encontrar todos valores absolutos possíveis de $\mathbb{Q}$.

Proposição (Igualdade de valores absolutos $\mathbb{Q}$)**.** *Sejam $\|\cdot\|_a$ e $\|\cdot\|_b$ valores absolutos de $\mathbb{Q}$. Se $\forall n \in \mathbb{N}$ vale que $\|n\|_a = \|n\|_b$ então $\forall x \in \mathbb{Q}$ vale que $\|n\|_a = \|n\|_b$.*

Demonstração. Já sabemos que $\|0\|_a = \|0\|_b = 0$. Assim, seja $\frac{a}{b} \in \mathbb{Q}$ tal que $a, b \in \mathbb{N}$.

Então, usando as propriedades dos valores absolutos, verificamos que

$$\left\|-\frac{a}{b}\right\|_a = \left\|\frac{a}{b}\right\|_a = \|a\| \left\|\frac{1}{b}\right\|_a = \|a\|_a \|b\|_a^{-1} = \|a\|_b \|b\|_b^{-1} = \|a\| \left\|\frac{1}{b}\right\|_b = \left\|\frac{a}{b}\right\|_b = \left\|-\frac{a}{b}\right\|_b$$ □

O teorema abaixo irá mostrar que existem somente três valores absolutos não equivalentes entre si nos $\mathbb{Q}$.

Teorema (Ostrowski)**.** *Todo valor absoluto em $\mathbb{Q}$ é equivalente ao valor absoluto trivial, ou ao valor absoluto* p*-ádico ou ao valor absoluto real.*

Demonstração. Seja $\|\cdot\|$ um valor absoluto de $\mathbb{Q}$. Pela proposição anterior, basta analisar os possíveis valores absolutos em $\mathbb{N}$.

Caso 1: suponha que $\forall n \in \mathbb{N}$, se $n \neq 0$ então $\|n\| = 1$. Assim, $\|\cdot\|$ é o valor absoluto trivial.

Caso 2: suponha $\exists n \in \mathbb{N}$ tal que $\|n\| > 1$. Assim, o conjunto $A = \{n \in \mathbb{N} : \|n\| > 1\} \neq \emptyset$.

Como $A \subset \mathbb{N}$ então $\exists m = \min A$.

Como $\|m\| > 1$, $\exists \alpha \in \mathbb{R}$, $\alpha > 0$, tal que $\|m\| = m^\alpha$.
Seja $n \in \mathbb{N}$ um número natural qualquer. Ele pode ser escrito como:

$$n = a_0 + a_1 m + a_2 m^2 + \ldots + a_k m^k \text{ onde } a_j \in \{0, 1, 2, \ldots, m-1\},\ 0 \leq j \leq k$$

Assim, pelas propriedades de valor absoluto,

$$\|n\| \leq \|a_0\| + \|a_1 m\| + \|a_2 m^2\| + \|a_3 m^3\| + \ldots + \|a_k m^k\|$$

$$= \|a_0\| + \|a_1\| m^\alpha + \|a_2\| m^{2\alpha} + \|a_3\| m^{3\alpha} + \ldots + \|a_k\| m^{k\alpha}$$

Note que $0 \leq a_j < m$, $\forall j \in \{0, 1, \ldots, k\}$. Como m é o menor número natural cujo valor absoluto é maior que 1, temos que $\|a_j\| \leq 1$. Assim, podemos continuar a desigualdade como

$$\|n\| \leq 1 + m^\alpha + m^{2\alpha} + \ldots + m^{k\alpha}$$

$$= m^{k\alpha}(1 + m^{-\alpha} + m^{-2\alpha} + \ldots + m^{-k\alpha})$$

$$\leq m^{k\alpha} \sum_{j=0}^{\infty} m^{-j\alpha}$$

$$\leq n^\alpha \sum_{j=0}^{\infty} m^{-j\alpha},$$

pois $m^k \leq n \implies m^{k\alpha} \leq n^\alpha$. A série acima é a série geométrica, que converge para um número real L. Assim, $\|n\| \leq L n^\alpha$. Note que isso vale para um $n \in \mathbb{N}$ qualquer, e L e α são independentes da escolha de n. Considere

$$\left\|n^N\right\| \leq L n^{N\alpha} \implies \|n\|^N \leq L n^{N\alpha} \implies \|n\| \leq L^{1/N} n^\alpha$$

$$\implies \|n\| \leq \lim_{N \to \infty} L^{1/N} n^\alpha = n^\alpha.$$

Por outro lado, $m^{k+1} > n \geq m^k$. Assim,

$$\|m^{k+1}\| = \|n + m^{k+1} - n\| \leq \|n\| + \|m^{k+1} - n\|$$

Note que $\|m^{k+1}\| = \|m\|^{k+1} = m^{(k+1)\alpha}$.
Além disso, $\|m^{k+1} - n\| \leq (m^{k+1} - n)^\alpha \implies -\|m^{k+1} - n\| \geq -(m^{k+1} - n)^\alpha$.
Assim,

$$\|n\| \geq \|m^{k+1}\| - \|m^{k+1} - n\| = m^{(k+1)\alpha} - \|m^{k+1} - n\| \geq m^{(k+1)\alpha} - (m^{k+1} - n)^\alpha$$

Como $n \geq m^k$ então $(m^{k+1} - n) \leq (m^{k+1} - m^k) \implies -(m^{k+1} - n) \geq -(m^{k+1} - m^k)$.
Aplicando isso na desigualdade anterior, temos

$$\|n\| \geq m^{(k+1)\alpha} - (m^{k+1} - n)^\alpha \geq m^{(k+1)\alpha} - (m^{k+1} - m^k)^\alpha$$

$$= m^{(k+1)\alpha} - m^{(k+1)\alpha}(1 - m^{-1})^\alpha = m^{(k+1)\alpha}\left[1 - \left(1 - \frac{1}{m}\right)^\alpha\right]$$

$$\geq n^\alpha \left[1 - \left(1 - \frac{1}{m}\right)^\alpha\right] = n^\alpha L',$$

para algum $L' \in \mathbb{R}$ que depende somente de m e α, portanto, independente de n.
Assim,

$$\|n\|^N = \|n^N\| \geq n^{N\alpha} L' \implies \|n\| \geq n^\alpha L'^{1/N}$$

$$\implies \|n\| \geq \lim_{N\to\infty} n^{\alpha} L'^{1/N} = n^{\alpha}.$$

Portanto, $\|n\| = n^{\alpha}$.

Assim, $\|x\| = |x|^{\alpha}$ para qualquer $x \in \mathbb{Q}$.

Agora iremos mostrar que o valor absoluto encontrado, onde $\|x\| = |x|^{\alpha}$, é equivalente ao valor absoluto real, onde $\|p\|_{\infty} = |x|$

Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy usando o valor absoluto $\|x\| = |x|^{\alpha}$, com $\alpha > 0$. Assim, dado $\epsilon > 0, \exists n_0 \in \mathbb{N}$ tal que $i > j > n_0 \implies \|a_i - a_j\| < \epsilon^{\alpha} \implies |a_i - a_j|^{\alpha} < \epsilon^{\alpha} \implies |a_i - a_j| < \epsilon \implies \|a_i - a_j\|_{\infty} < \epsilon$.

Por outro lado, seja $(b_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy usando o valor absoluto real $\|x\|_{\infty}$. Assim, dado $\epsilon > 0, \exists m_0 \in \mathbb{N}$ tal que $i > j > m_0 \implies \|b_i - b_j\|_{\infty} < \epsilon^{1/\alpha} \implies |b_i - b_j| < \epsilon^{1/\alpha} \implies |b_i - b_j|^{\alpha} < \epsilon^{\alpha/\alpha} \implies \|b_i - b_j\| < \epsilon$.

Portanto, se uma sequência é de Cauchy usando o valor absoluto $\|x\| = |x|^{\alpha}$ se e somente se é uma sequência de Cauchy usando o valor absoluto real $\|x\|_{\infty}$, o que significa que estes valores absolutos são equivalentes.

Conclusão: se $\exists n \in \mathbb{N}$ tal que $\|n\| > 1$ então o $\|\cdot\|$ é equivalente ao valor absoluto real $\|\cdot\|_{\infty}$.

Caso 3: suponha $\|n\| \leq 1$, $\forall n \in \mathbb{N}$, $n > 0$, e que o valor absoluto não é o trivial.

Assim, o conjunto $B = \{n \in \mathbb{N} : n > 0 \text{ e } \|n\| < 1\} \neq \emptyset$. E como $B \subset \mathbb{N}$ então $\exists p = \min B$.

Sabemos que $p > 1$ pois $\|1\| = 1$. Suponha que p não é primo. Assim, $\exists a, b \in \mathbb{N}$, $1 < a \leq b$ tais que $p = ab$. Assim, $\|p\| = \|ab\| = \|a\|\|b\|$. Mas p é o menor número natural não nulo cujo valor absoluto é menor que 1, e todos números naturais tem o valor absoluto menor ou igual a 1. Assim, $\|a\|\|b\| = 1 \cdot 1 = 1$, o que é uma contradição, pois $\|p\| < 1$. Assim, p é primo.

Além disso, seja q primo, $q \neq p$. Suponha $\|q\| < 1$. Então, $\exists N \in \mathbb{N}$ tal que $\|q^N\| = \|q\|^N \leq 1/4$. Da mesma forma, $\exists M \in \mathbb{N}$ tal que $\|p^M\| = \|p\|^M \leq 1/4$. Como $\text{mdc}(p^M, q^N) = 1$ então existem $a, b \in \mathbb{Z}$ tais que $ap^M + bq^N = 1$. Assim,

$$1 = \|1\| = \|ap^M + bq^N\| \leq \|ap^M\| + \|bq^N\| = \|a\|\|p^M\| + \|b\|\|q^N\|$$

Como, por hipótese, $\|a\| = \|-a\| \leq 1$ e $\|b\| = \|-b\| \leq 1$, temos que

$$1 \leq \|a\|\|p^M\| + \|b\|\|q^N\| \leq \|p^M\| + \|q^N\| \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2},$$

contradição. Logo, $\|q\| = 1$ já que neste caso o valor absoluto de todos números naturais são menores ou iguais a 1.

Assim, dado $n \in \mathbb{N}$ tal que $n > 0$. Então ele pode ser decomposto unicamente em $n = p_0^{\beta_0} p_1^{\beta_1} \dots p_s^{\beta_s}$, onde p_j são números primos distintos e $\beta_j \in \mathbb{N}$. Assim,

$$\|n\| = \|p_0^{\beta_0}\|\|p_1^{\beta_1}\| \dots \|p_s^{\beta_s}\|.$$

Como apenas o valor absoluto de p é diferente de 1, podemos reescrever $n = p^{\beta} r$ onde $p \nmid r$, e assim temos que

$$\|n\| = \|p^{\beta} r\| = \|p^{\beta}\|\|r\| = \|p^{\beta}\| \cdot 1 = \|p\|^{\beta}$$

.

Como $\|p\| < 1$, suponha $\|p\| = p^{-\alpha}$, para algum $\alpha > 0 \in \mathbb{R}$.

Agora iremos mostrar que o valor absoluto encontrado, onde $\|p\| = p^{-\alpha}$, é equivalente ao valor absoluto p-ádico, onde $\|p\|_p = p^{-1}$

Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy usando o valor absoluto $\|x\| = \left\|p^{\beta}\frac{a}{b}\right\| = \|p\|^{\beta} = p^{-\alpha\beta}$, para $\alpha > 0$.

Assim, dado $\epsilon > 0, \exists n_0 \in \mathbb{N}$ tal que $i > j > n_0 \implies \|a_i - a_j\| < \epsilon^{\alpha}$.

Seja $a_i - a_j = p^{\beta_0}\frac{c}{d}$ tal que $p \nmid cd$.

Assim, $\|a_i - a_j\| < \epsilon^{\alpha} \implies p^{-\alpha\beta_0} < \epsilon^{\alpha} \implies p^{-\beta_0} < \epsilon \implies \|a_i - a_j\|_p < \epsilon$, pois $\alpha > 0$.

Por outro lado, seja $(b_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy usando o valor absoluto p-ádico $\|x\|_p$. Assim, dado $\epsilon > 0, \exists m_0 \in \mathbb{N}$ tal que $i > j > m_0 \implies \|b_i - b_j\|_p < \epsilon^{1/\alpha}$.

Seja $b_i - b_j = p^{\beta_1}\frac{c'}{d'}$ tal que $p \nmid c'd'$.

Assim, $\|b_i - b_j\| < \epsilon^{1/\alpha} \implies p^{-\beta_1} < \epsilon^{1/\alpha} \implies p^{-\alpha\beta_1} < \epsilon^{\alpha/\alpha} \implies \|a_i - a_j\| < \epsilon$.

Portanto, se uma sequência é de Cauchy usando o valor absoluto $\|x\| = \left\|p^\beta \frac{a}{b}\right\| = \|p\|^\beta$ se e somente se é uma sequência de Cauchy usando o valor absoluto p-ádico $\|x\|_p$, o que significa que estes valores absolutos são equivalentes.

Conclusão: se $\|n\| \leq 1\ \forall n \in \mathbb{N}$ e $\|\cdot\|$ não é o valor absoluto trivial então $\|\cdot\|$ é equivalente ao valor absoluto p-ádico $\|\cdot\|_p$.

□

5 Elementos dos Corpos p-Ádicos

Uma vez construído o corpo p-ádico, é conveniente saber representar seus elementos. Demonstraremos agora que o corpo p-ádico possui uma representação na base p unicamente determinada. Isso o difere dos $\mathbb{R}$, onde, por exemplo, $0{,}9999\ldots = 1$.

Mas antes, mostraremos o resultado onde qualquer número racional pode ser aproximado por um inteiro nos corpos p-ádicos.

Lema (Representação p-ádica de um elemento de $\mathbb{Q}$)**.** *Seja $x \in \mathbb{Q}$ tal que $\|x\|_p \leq 1$. Então, para qualquer $k \in \mathbb{N}$ existe um $m \in \mathbb{N}$, $m < p^k$ tal que $\|m - x\|_p \leq p^{-k}$.*

Demonstração. Seja $x = p^n \frac{a}{b}$ tal que $p \nmid ab$ e $\|x\|_p =\leq 1$. Então existem $r, s \in \mathbb{Z}$ e $k \in \mathbb{N}$ tais que $rb + sp^k = 1$, assim, $rb - 1 = -sp^k \implies \|rb - 1\|_p = \|sp^k\|_p$. Seja $m = rp^n a + tp^k$, para um $t \in \mathbb{Z}$ de forma que $0 \leq m < p^k$. Assim,

$$\|m - x\|_p = \left\|rp^n a + tp^k - \frac{p^n a}{b}\right\|_p \leq \max\left\{\left\|rp^n a - \frac{p^n a}{b}\right\|_p, \|tp^k\|_p\right\}$$

$$= \max\left\{\|p^n a\|_p \left\|r - \frac{1}{b}\right\|_p, \|tp^k\|_p\right\} = \max\left\{\|x\|_p \|rb - 1\|_p, \|tp^k\|_p\right\}$$

$$\leq \max\left\{\|rb - 1\|_p, \|tp^k\|_p\right\} \leq \max\left\{\|sp^k\|_p, \|tp^k\|_p\right\} \leq p^{-k}.$$

Portanto, o inteiro existe. □

Proposição (Representação p-ádica Única)**.** *Seja $a \in \mathbb{Q}_p$ tal que $\|a\|_p \leq 1$. Então a tem exatamente um representante $(a_n)_{n\in\mathbb{N}}$ que satisfaz as condições, $\forall\, k \in \mathbb{N}, k > 0$:*

1. $0 \leq a_k < p^k$
2. $a_k \equiv a_{k+1} \pmod{p^k}$

Demonstração. Seja (b_n) um representante de uma classe de equivalência de um elemento de $\mathbb{Q}_p$. Seja (c_n) uma subsequência de (b_n) onde para todo $i > j \geq n$, $\|c_i - c_j\|_p < p^{-n}$. Isso é possível pois (b_n) é uma sequência de Cauchy.

Assim, criaremos a sequência (a_n) formada pelos inteiros $0 \leq a_n < p^n$ de tal forma que $\|a_n - c_n\|_p < p^{-n}$. Isso é possível pelo lema anterior, pois $\|c_n\|_p \leq 1$. Logo, (a_n) tem a primeira propriedade necessária.

Como $\lim\limits_{n\to\infty} \|a_n - c_n\|_p = \lim\limits_{n\to\infty} p^{-n} = 0$ então $(a_n) \sim (c_n) \sim (b_n)$.

Por fim, se $a_k \equiv a_{k+1} \pmod{p^k} \iff a_k - a_{k+1} = rp^k \iff \|a_k - a_{k+1}\|_p \leq p^{-k}$.

Consideremos então $\|a_k - a_{k+1}\|_p = \|a_k - c_k + c_k - c_{k+1} + c_{k+1} - a_{k+1}\|_p$

$\leq \max\{\|a_k - c_k\|, \|c_k - c_{k+1}\|, \|c_{k+1} - a_{k+1}\|\} \leq \max\{p^{-k}, p^{-k}, p^{-k-1} = p^{-k}$.

Existe tal representação. Suponha que existe $(a'_n)_{n\in\mathbb{N}}$ tal que $(a'_n) \sim (a_n)$ e com as propriedades da representação proposta, mas que existe um $n_0 \in \mathbb{N}$ tal que $a_{n_0} \neq a'_{n_0}$.

Logo, $a_{n_0} \not\equiv a'_{n_0} \pmod{p^{n_0}}$. Mas para todo $n > n_0$, $a_n \equiv a_{n_0} \pmod{p^{n_0}}$ e $a'_n \equiv a'_{n_0} \pmod{p^{n_0}}$.

Portanto, $\forall n > n_0, a_n \not\equiv a'_n \pmod{p^{n_0}}$, logo, $p^{n_0} \nmid (a_n - a'_n)$, portanto, $\|a_n - a'_n\|_p > p^{-n_0}$.

Assim, $(a_n) \nsim (a'_n)$, o que é uma contradição. Portanto, (a_n) é único.

□

Caso $a \in \mathbb{Q}_p$ seja tal que $\|a\|_p > 1 = p^m$, podemos criar um $b = p^m a$. Assim, $\|b\| = 1$, e pode ser representado unicamente. Logo, a pode ser representado unicamente por $p^{-m}b$.

Ou seja, suponha

$$b = b_0p^0 + b_1p^1 + b_2p^2 + b_3p^3 + \dots$$

Assim,

$$a = b_0p^{-m} + b_1p^{-m+1} + b_2p^{-m+2} + \dots + b_{m-1}p^{-1} + b_mp^0 + b_{m+1}p^1 + b_{m+2}p^2 + \dots$$

Neste caso, supondo $m = 3$, a representação p-ádica ficaria:

$$a = (\dots b_5b_4b_3{,}b_2b_1b_0).$$

Ou seja, os elementos dos corpos p-ádicos podem ser representados como um número com finitos dígitos à direita da vírgula mas infinitos dígitos à esquerda da vírgula.

As séries nos corpos p-ádicos são mais bem comportadas que as séries dos $\mathbb{R}$. É possível determinar a convergência da série verificando apenas se os termos da série convergem para zero.

Proposição (Convergência de séries)**.** *Seja $(A_n)_{n\in\mathbb{N}}$ uma sequência de $\mathbb{Q}_p$.*

Então a série $\sum_{n\in\mathbb{N}} A_n$ converge $\iff \lim_{n\to\infty} A_n = 0$.

Demonstração. Suponha que $\lim_{n\to\infty} A_n = 0$.

Assim, para $\epsilon > 0$ existe $n_0 \in \mathbb{N}$ tal que se $n > n_0$, $\|A_n\|_p < \epsilon$.

Seja a sequência de somas parciais $(S_n)_{n\in\mathbb{N}}$, definida por $S_n = \sum_{k=0}^{n} A_k$. Para $i > j > n_0$, vale que

$$\|S_i - S_j\|_p = \left\| \sum_{k=j+1}^{i} A_k \right\|_p \leq \max\{\|A_{j+1}\|_p, \|A_{j+2}\|_p, \dots, \|A_i\|_p\} < \epsilon.$$

.

Assim, (S_n) é sequência de Cauchy em um espaço completo, portanto, convergente.

Agora suponha que $\sum_{n\in\mathbb{N}} A_n$ converge. Suponha que $\lim_{n\to\infty} A_n \neq 0$, podendo inclusive não existir. Então existe $\epsilon > 0$ e uma subsequência (B_n) de (A_n) onde $\|B_n\|_p > \epsilon \ \forall n \in \mathbb{N}$. Se tal ϵ não existir, então $\lim_{n\to\infty} A_n = 0$.

Considere a sequência das somas parciais (S_n). Como é convergente por hipótese, também vale que é de Cauchy. Assim, existe $n_0 \in \mathbb{N}$ tal que se $j \geq n_0$ então $\|S_j - S_{j-1}\|_p < \epsilon$.

Note que $\exists n_1 \geq n_0$ tal que $A_{n_1} = B_{n_0}$, pois (B_n) é subsequência de (A_n).

Assim, sabemos que $\|S_{n_1} - S_{n_1-1}\|_p < \epsilon \implies \|A_{n_1}\|_p < \epsilon$, o que é uma contradição, pois $\|A_{n_1}\|_p > \epsilon$. Pontanto, $\lim_{n\to\infty} A_n = 0$. □

Corolário. *Seja $\sum_{n=n_0}^{\infty} a_n p^n$, sendo $0 \leq a_n < p$ e $n_0 \in \mathbb{Z}$. Então a série converge e pertence a $\mathbb{Q}_p$.*

6 Polinômios p-ádicos

O Lema de Hensel é um resultado importante dos corpos p-ádicos, e é usado em demonstrações de outros teoremas. Pelo lema afirma que, para determinados polinômios, é possível encontrar facilmente uma raiz, construíndo-a dígito a dígito. A raiz é encontrada de forma semelhante a encontrar uma raiz real usando o método de Newton, porém com a vantagem do método ser mais bem comportado nos números p-ádicos.

Mas antes de chegar nele, veremos um pequeno resultado.

Proposição. $\sqrt{2}$ *é irracional.*

Demonstração. Seja o polinômio $x^2 = 2$. Tentaremos encontrar $x \in \mathbb{Q}_2$ tal que $x^2 = 2$. Podemos verificar o valor absoluto dos dois lados da equação, obtendo $\|x^2\|_2 = \|2\|_2 \implies 2^{2k} = 2^{-1}$, para algum $k \in \mathbb{Z}$. Logo, $2k = -1$, o que é uma contradição. Portanto, $x^2 = 2$ não tem solução em $\mathbb{Q}_2$. Como $\mathbb{Q} \subset \mathbb{Q}_2$ concluímos que $\sqrt{2} \notin \mathbb{Q}$. □

Definição (Inteiro p-ádico)**.** Seja $a \in \mathbb{Q}_p$ tal que $\|a\|_p \leq 1$. Então a é denominado *inteiro* p*-ádico.*

A condição $\|a\|_p \leq 1$ faz com que a representação p-ádica de a não tenha nenhum coeficiente em bases negativas de p, ou seja, a representação dele não tem dígitos à direita da virgula. Isso se assemelha aos inteiros dos reais.

Definição (Congruência em $\mathbb{Q}_p$)**.** Seja $a, b \in \mathbb{Q}_p$. A relação $a \equiv b \pmod{p^k}, k \in \mathbb{Z}$ existe se $\|a-b\|_p \leq p^{-k}$, ou equivalentemente, $\dfrac{a-b}{p^k}$ é um inteiro p-ádico.

Se considerarmos $a, b \in \mathbb{Z}$, essa relação é idêntica à relação de congruência de $\mathbb{Z}$.

Teorema (Lema de Hensel)**.** *Seja $f(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n$ um polinômio com os coeficientes inteiros* p*-ádicos.*
Seja $f'(x)$ a derivada formal de $f(x)$, isto é, $f'(x) = c_1 + 2c_2x + \ldots + nc_nx^{n-1}$.
Seja a_0 inteiro p*-ádico tal que $f(a_0) \equiv 0 \pmod{p}$ e $f'(a_0) \not\equiv 0 \pmod{p}$.*
Então existe um único $a \in \mathbb{Q}_p$, $\|a\|_p \leq 1$, tal que $f(a) = 0$ e $a \equiv a_0 \pmod{p}$.

Demonstração. Primeiro, criaremos uma sequêcia $(a_n)_{n\in\mathbb{N}}$ em que a_0 é o elemento que satisfaz a hipótese. Todos os demais elementos da sequência devem satisfazer as condições:

1. $f(a_n) \equiv 0 \pmod{p^{n+1}}$
2. $a_n \equiv a_{n-1} \pmod{p^n}$
3. $0 \leq a_n < p^{n+1}$

Precisamos provar que essa sequência existe. Provaremos por indução. Para $n = 1$, seja $0 \leq b_0 < p$ tal que $b_0 \equiv a_0 \pmod{p}$. Logo, b_0 é unicamente determinado.

Para a_1 satisfazer as duas últimas condições, é necessário que seja da forma $a_1 = b_0 + b_1p$, onde $0 \leq b_1 < p$. Considere $a_0 = b_0 + ps$, com s inteiro p-ádico. Então

$$f(a_0) = f(b_0 + ps) = \sum_{k=0}^{n} c_k(b_0 + ps)^k = \sum_{k=0}^{n} c_k b_0^k + \sum_{k=0}^{n} pr(k),$$

em que $r(k)$ são os termos restantes. Assim, Como $r(k)$ é multiplicação e soma de inteiro p-ádicos. Logo

$$f(a_0) = \sum_{k=0}^{n} c_k b_0^k + p\sum_{k=0}^{n} r(k) = f(b_0) + p\sum_{k=0}^{n} r(k) \equiv f(b_0) \pmod{p}$$

Assim, $f(a_0) \equiv f(b_0) \equiv 0 \pmod{p}$.
De forma semelhante, considere:

$$f'(a_0) = f'(b_0 + ps) = \sum_{k=1}^{n} kc_k(b_0 + ps)^{k-1} = \sum_{k=0}^{n} kc_k b_0^{k-1} + p\sum_{k=0}^{n} r(k) = f'(b_0) + p\sum_{k=0}^{n} r(k),$$

em que $r(k)$ são os termos restantes. Concluimos que $f'(a_0) \equiv f'(b_0) \equiv 0 \pmod{p}$.
Agora, analisaremos de forma semelhante a condição $f(a_1) \equiv 0 \pmod{p^2}$.

$$f(a_1) = f(b_0 + b_1p) = \sum_{k=0}^{n} c_k(b_0 + b_1p)^k = \sum_{k=0}^{n} c_k b_0^k + \sum_{k=0}^{n} nc_k b_0^{k-1} b_1 p + \sum_{k=0}^{n} c_k p^2 r(k),$$

Logo,

$$f(a_1) = \left(\sum_{k=0}^{n} c_k b_0^k\right) + \left(\sum_{k=0}^{n} nc_k b_0^{k-1}\right) b_1 p + \sum_{k=0}^{n} c_k p^2 r(k) = f(b_0) + f'(b_0)b_1 p + p^2 \sum_{k=0}^{n} c_k r(k).$$

Concluimos então que

$$f(a_1) \equiv f(b_0) + f'(b_0)b_1 p \pmod{p^2}$$

Como já sabemos que $f(b_0) \equiv 0 \pmod{p}$, podemos dizer que $f(b_0) \equiv \alpha p \pmod{p^2}$, com algum $0 \leq \alpha < p$.

Assim, para satisafazer $f(a_1) \equiv 0 \pmod{p^2}$ então precisamos que

$$f(b_0) + f'(b_0)b_1 p \equiv \alpha p + f'(b_0)b_1 p \equiv 0 \pmod{p^2}$$

Note que

$$(\alpha + f'(b_0)b_1)p \equiv 0 \pmod{p^2} \implies \alpha + f'(b_0)b_1 \equiv 0 \pmod{p}$$

.

Sabemos que $f'(b_0) \equiv f'(a_0) \not\equiv 0 \pmod{p}$. Portanto, como estamos em um módulo p primo (que forma um corpo em $\mathbb{Z}/p\mathbb{Z}$), então $0 \leq b_1 < p$ pode ser unicamente determinado, para qualquer valor de α, que já foi também unicamente determinado.

Vamos mostrar agora que $f'(a_1) \equiv f'(a_0)$.

$f'(a_1) = f'(b_0 + b_1 p) = \sum_{k=1}^{n} k c_k (b_0 + b_1 p)^{k-1} = \sum_{k=0}^{n} k c_k b_0^{k-1} + p \sum_{k=0}^{n} r(k) = f'(b_0) + p \sum_{k=0}^{n} r(k)$

$\implies f'(a_1) \equiv f'(b_0) \equiv f'(a_0) \pmod{p}$.

Iremos usar este resultado na indução.

Agora, voltando à indução, considere que $(a_k)_{k=1}^{n-1}$ satisfazem as condições. a_n terá n dígitos na base p pela terceira condição, mas pela segunda condição, os $n-1$ primeiros dígitos já estão determinados. Assim, podemos escrever $a_n = a_{n-1} + b_n p^n$, bastando encontrar b_n que satisfaça a primeira condição para determinar a_n.

De modo análogo ao caso a_1, expandindo $f(a_n)$ como $f(a_{n-1} + b_n p^n)$, podemos concluir que:

$$f(a_n) \equiv f(a_{n-1}) + f'(a_{n-1})b_n p^n \pmod{p^{n+1}}.$$

Como $f(a_{n-1}) \equiv 0 \pmod{p^n}$ pela hipótese de indução, então $f(a_{n-1}) \equiv \beta p^n \pmod{p^{n+1}}$, para algum $0 \leq \beta < p$ unicamente determinado.

Assim, para satisfazer $f(a_n) \equiv 0 \pmod{p^{n+1}}$ temos que

$$f(a_n) \equiv f(a_{n-1}) + f'(a_{n-1})b_n p^n \equiv (\beta + f'(a_{n-1})b_n)p^n \equiv 0 \pmod{p^{n+1}},$$

$$\implies \beta + f'(a_{n-1})b_n \equiv 0 \pmod{p}.$$

Podemos mostrar que $f'(a_k) \equiv f'(a_{k-1})$ para qualquer $1 < k < n$, de forma semelhante a mostrada para $k = 1$. Assim, $f'(a_{n-1}) \equiv f'(a_{n-2}) \ldots \equiv f'(a_0) \not\equiv 0 \pmod{p}$. Assim, $0 \leq b_n < p$ pode ser unicamente determinado, o que completa a prova da indução, mostrando a existência e unicidade de (a_n) e (b_n).

Seja então $a = b_0 + b_1 p + b_2 p^2 + \ldots$. Logo, $f(a) \equiv f(a_n) \equiv 0 \pmod{p^{n+1}}$, logo, $f(a) = 0$.

□

7 Exemplos de como encontrar raízes p-ádicas

Nesta seção apenas veremos alguns exemplos para ficar mais habituado com os teoremas demonstrados anteriormente.

Exemplo ($x^2 - 6$ em $\mathbb{Q}_5$). Tentaremos agora encontrar a raiz de $x^2 - 6$ em $\mathbb{Q}_5$. Na base p, 6 é representado por 11_5 pois é $1 \cdot 5^1 + 1 \cdot 5^0$.

Queremos resolver então

$$\begin{array}{cccccc} & \ldots & b_3 & b_2 & b_1 & \textcircled{b_0} \\ \times & \ldots & b_3 & b_2 & b_1 & \textcircled{b_0} \\ \hline & \ldots & 0 & 0 & 1 & \triangle 1 \end{array}$$

Assim, temos que $b_0 b_0 \equiv 1 \pmod 5$. Um candidato é 1. Existe outro candidato, 4, pois $4 \cdot 4 = 16 \equiv 1 \pmod 5$. Estas duas escolhas existem porque as duas raízes do polinômio ($\sqrt{6}$ e $-\sqrt{6}$) estão em $\mathbb{Q}_5$, e cada escolha leva a uma raiz.

Vamos escolher $b_0 = 1$. Assim,

$$\begin{array}{cccccc} & \ldots & b_3 & b_2 & b_1 & 1 \\ \times & \ldots & b_3 & b_2 & b_1 & 1 \\ \hline & \ldots & 0 & 0 & 1 & 1 \end{array}$$

Precisamos que $b_1 1 + b_1 1 = 2b_1 \equiv 1 \pmod 5$. Como $3 \cdot 2 = 6 = 11_5$ na base 5, e como $11_5 \equiv 1 \pmod 5$ então $b_1 = 3$. Como o resultado é maior que 5, passa 1 para o próximo dígito, como no algoritmo de multiplicação usual.

$$\begin{array}{cccccc} & & & +1 & & \\ & \ldots & b_3 & b_2 & 3 & 1 \\ \times & \ldots & b_3 & b_2 & 3 & 1 \\ \hline & \ldots & 0 & 0 & 1 & 1 \end{array}$$

Agora precisamos que $b_2 1 + 3\,3 + b_2 1 + 1 = 2b_2 + 10 \equiv 0 \pmod 5$. Com $b_2 = 0$ essa equação já é satisfeita, assim, o resultado será 10, que é 20_5 na base 5, então 2 passa para frente.

$$\begin{array}{cccccc} & & & +2 & & \\ & \ldots & b_3 & 0 & 3 & 1 \\ \times & \ldots & b_3 & 0 & 3 & 1 \\ \hline & \ldots & 0 & 0 & 1 & 1 \end{array}$$

Para calcular este último dígito, precisamos que $b_3 \cdot 1 + 3 \cdot 0 + 3 \cdot 0 + b_3 \cdot 1 + 2 = 2b_3 + 2 \equiv 0 \pmod 5$. Com $b_3 = 4$ essa equação resulta em $10 \equiv 0 \pmod 5$, assim, o resultado será 10, que é 20_5 na base 5, então 2 passa para frente.

Vamos parar por aqui mesmo. Sabemos o número p-ádico, na base 5, $(\ldots 4031)_p^2 = 11_5 = 6$. Logo, $\sqrt{6} \in \mathbb{Q}_5$.

Exemplo ($x^2 - a$ em $\mathbb{Q}_5$). Nem todas raízes pertencem a um corpo p-ádico. Considere encontrar as raízes de $x^2 - 3$ na base $\mathbb{Q}_5$. Repetindo o procedimento, o primeiro dígito deve satisfazer $b_0 b_0 = 3$. Porém:

$0 \cdot 0 = 0$,
$0 \cdot 1 = 1$,
$2 \cdot 2 = 4$,
$3 \cdot 3 = 9 \equiv 4 \pmod 5$,
$4 \cdot 4 = 16 \equiv 1 \pmod 5$.

Assim, não é possível encontrar nem o primeiro dígito, e pelo teorema demonstrado, qualquer número p-ádico possui representação única. Por isso, concluimos que $\sqrt{a}$ não existe em $\mathbb{Q}_5$ se $a \equiv 3 \pmod 5$ ou se $a \equiv 2 \pmod 5$. Portanto, não existirá raiz de $2, 3, 7, 8, 12, 13, 17, 18, \ldots$.

Exemplo ($x^3 - 6$ em $\mathbb{Q}_5$). Para um polinômio simples como $x^2 - a$, calcular manualmente é relativamente fácil, mas para polinômios um pouco mais complexo, como $x^3 - a$, se torna muito trabalhoso. Assim, é preferível utilizar o Lema de Hensel.

Agora encontraremos a raiz em $\mathbb{Q}_5$ do polinômio abaixo utilizando o Lema de Hensel:

$$f(x) = x^3 - 6$$
$$f'(x) = 3x^2$$

Precisamos encontrar os valores da sequência (a_n). Vamos considerar o número a_0 com um só dígito, ou seja, $a_0 = b_0$, onde $0 \leq b_0 < 5$, para facilitar as contas. Assim, precisamos primeiro encontrar a_0 tal que $f(a_0) \equiv 0 \mod 5$ e $f'(a_0) \not\equiv 0 \mod 5$. A condição falha para $b_0 \in \{0,2,3,4\}$ mas é satisfeita para $b_0 = 1$. Portanto, já sabemos pelo lema que existe uma raiz unicamente determinada em $\mathbb{Q}_5$.

Agora para o próximo número da sequêcia, temos que $a_1 = b_1 \cdot 5 + b_0 = b_1 \cdot 5 + 1$. Assim, a_1 já satisfaz as duas últimas condições da demonstração e basta que b_1 seja tal que

$$f(a_1) = (5b_1 + 1)^3 - 6 \equiv 0 \pmod{5^2}.$$

Temos:
$b_1 = 0 \implies 1^3 - 6 = -5 \not\equiv 0 \pmod{25}$,
$b_1 = 1 \implies 6^3 - 6 = 210 \not\equiv 0 \pmod{25}$,
$b_1 = 2 \implies 11^3 - 6 = 1325 \equiv 0 \pmod{25}$,
assim, $b_1 = 2$. Logo, $a_1 = 21_5$ na base 5.
Agora, $a_2 = b_2 \cdot 5^2 + 2 \cdot 5 + 1$ precisa satisfazer

$$f(a_2) = (5^2 b_2 + 2 \cdot 5 + 1)^3 - 6 = (25b_2 + 11)^3 - 6 \equiv 0 \pmod{5^3}.$$

Temos:
$b_2 = 0 \implies 11^3 - 6 = 1.325 \not\equiv 0 \pmod{125}$,
$b_2 = 1 \implies 36^3 - 6 = 46.650 \not\equiv 0 \pmod{125}$,
$b_2 = 2 \implies 61^3 - 6 = 226.975 \not\equiv 0 \pmod{125}$,
$b_2 = 3 \implies 86^3 - 6 = 636.050 \not\equiv 0 \pmod{125}$,
$b_2 = 4 \implies 111^3 - 6 = 1.367.625 = 125 \cdot 10.941 \equiv 0 \pmod{125}$,
logo, $b_2 = 4$.
Iremos parar por aqui, sabendo que $(\ldots 421)^3 = 11_5 = 6$.

Exemplo (polinômios mais complexos). Considere encontrar uma raiz do polinômio abaixo em $\mathbb{Q}_5$, onde os coeficientes são números p-ádicos:

$$f(x) = x^3 + 2x^2 + (\ldots 133101123)x + 2$$

$$f'(x) = 3x^2 + 4x + (\ldots 133101123)$$

Pelo método descrito, precisamos encontrar um $0 \leq a_0 < 5$ tal que $f(a_0) \equiv 0 \pmod 5$ e $f'(a_0) \not\equiv 0 \pmod 5$.

Falha com $a_0 \in \{0, 1, 2, 3\}$ mas $f(4) \equiv 0 \pmod 5$ e $f'(4) \not\equiv 0 \pmod 5$, portanto, o polinômio tem garantidamente uma raiz em $\mathbb{Q}_5$, e todos os dígitos podem ser construídos seguindo o algoritmo.

Exemplo ($x^2 + 1$ em $\mathbb{Q}_5$). Considere o polinômio

$$f(x) = x^2 + 1$$

$$f'(x) = 2x$$

Ou seja, vamos verificar se $\sqrt{-1} \in \mathbb{Q}_5$.
Note que para $a_0 = 2$ temos que $f(2) = 2^2 + 1 = 5 \equiv 0 \pmod 5$ e que $f'(2) = 4 \not\equiv 0 \pmod 5$.
Para $a_0 = 3$ temos que $f(3) = 3^2 + 1 = 10 \equiv 0 \pmod 5$ e que $f'(3) = 6 \not\equiv 0 \pmod 5$.
Logo, pelo Lema de Hensel, duas raízes distintas de $x^2 + 1$ pertencem a $\mathbb{Q}_5$, ou seja, $\pm\sqrt{-1} \in \mathbb{Q}_5$.

Exemplo ($x^2 - 2$ em $\mathbb{Q}_7$). Vimos anteriormente que $\sqrt{2} \notin \mathbb{Q}_5$. Tentaremos agora encontrar uma solução em $\mathbb{Q}_7$.

$$f(x) = x^2 - 2$$

$$f'(x) = 2x$$

Precisamos então encontrar um $0 \leq a_0 < 7$ tal que
$f(a_0) \equiv 0 \pmod 7$ e

$f'(a_0) \not\equiv 0 \pmod 7$.
Veja que para $a_0 = 3$ temos que:
$f(a_0) = f(3) = 3^2 - 2 = 7 \equiv 0 \pmod 7$ e
$f'(a_0) = f'(3) = 2 \cdot 3 = 6 \not\equiv 0 \pmod 7$.
Além disso, para $a_0 = 4$ vale que:
$f(a_0) = f(4) = 4^2 - 2 = 14 \equiv 0 \pmod 7$ e
$f'(a_0) = f'(4) = 2 \cdot 4 = 8 \not\equiv 0 \pmod 7$.
Então o Lema de Hensel garante existir duas raízes distintas para o polinômio, logo, $\pm\sqrt{2} \in \mathbb{Q}_7$.

8 Outros Resultados

Nesta seção serão citados alguns resultados que não serão demonstrados, apenas para dar uma ideia melhor sobre corpos p-ádicos.

1. Para cada extensão finita de corpos dos p-ádicos existe um único valor absoluto possível de ser estendido . Além disso, o corpo estendido é completo com relação a esta novo valor absoluto.

2. Existe o fechamento algébrico de $\mathbb{Q}_p$, é para isso é necessário fazer extensões de corpos infinitas de $\mathbb{Q}_p$, e o seu fechamento não é completo em relação a métrica estendida.

3. O completamento do fecho algébrico de $\mathbb{Q}_p$, denotado $\mathbb{C}_p$, ou ainda por Ω, é fechado algebricamente. Ou seja, $\mathbb{C}_p$ possui a mesma propriedade de $\mathbb{C}$, de ser completo e fechado algebricamente.

4. O Teorema Hasse-Minkowski diz que qualquer forma quadrática com coeficientes racioanais tem raiz racional se e somente se tem raiz nos reais e em todos corpos $\mathbb{Q}_p$. O 11^o Problema de Hilbert, que consiste em classificar formas quadráticas em corpos de números algébricos, foi resolvido graças ao Teorema Hasse-Minkowski.

Referências

Baker 2011 BAKER, A. An introduction to p-adic numbers and p-adic analysis. 2011.

Boston 2003 BOSTON, N. The proof of fermat's last theorem. University of Wisconsin - Madison, 2003.

Dragovich 2009 DRAGOVICH, B. On p-adic mathematical physics. 2009.

Evertse 2011 EVERTSE, J.-H. P-adic numbers. 2011.

Gouvea 1989 GOUVEA, F. Q. *Primeiros Passos p-ádicos*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1989.

Koblitz 1984 KOBLITZ, N. *P-adic numbers, p-adic analysis and zeta-functions*. 2. ed. New York: Springer-Verlag, 1984.

Rozikov 2013 ROZIKOV, U. A. What are p-adic numbers? what are they used for? *Asia Pacific Mathematics Newsletter*, 2013.

Schinck 2011 SCHINCK, A. *The Local-Global Principle in Number Theory*. Tese (Doutorado) — Concordia University, 2011.