PRIMEIROS PASSOS P-ÁDICOS

Fernando Quadros Gouvêa

ISBN

85-244-0042-0

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

INSTITUTO DE MATEMÁTICA PURA E APLICADA

Estrada Dona Castorina, 110
22.460 – Rio de Janeiro – RJ

Introdução

Os números p-ádicos e a análise p-ádica são um dos aspectos mais divertidos e mais importantes da teoria de números moderna. Para o teorista de números, os vários valores absolutos que podem ser postos no corpo $\mathbf{Q}$ dos números racionais devem ser tratados em pé de igualdade. Quando se escolhe o valor absoluto clássico e se toma o completamento de $\mathbf{Q}$ em relação à métrica induzida, o resultado é o corpo $\mathbf{R}$ dos números reais; quando se faz o mesmo com um dos outros valores absolutos possíveis, obtém-se um dos corpos p-ádicos $\mathbf{Q}_p$. O propósito destes "primeiros passos" é apresentar o leitor a estes últimos corpos, desenvolvendo suas propriedades básicas e criando alguma familiariedade com eles. Não se pode esperar, num primeiro momento, que os números p-ádicos se tornem tão familiares quanto os reais (embora esse fosse o ideal!); nosso objetivo é torná-los parte do universo de trabalho do nosso leitor.

Já que esse é o nosso objetivo, o leitor não deverá procurar, nestas notas, muitos resultados profundos ou teoremas importantes. Estes são mencionados em vários momentos, mas de modo geral o leitor é enviado às várias referências básicas para maiores detalhes e aplicações mais sérias. Também por isso, o leitor encontrará, entremeados no texto, uma quantidade razoável de exercícios. A maioria destes são bastante fáceis, e procuram aumentar o envolvimento do leitor através do contato direto com a matemática que estamos discutindo. O autor gostaria de incentivar cada um dos seus leitores a fazerem os exercícios enquanto lêem o texto, completando, para si próprios, a exposição. (Em alguns casos, os exercícios se tornam triviais se forem atacados com a ajuda de material desenvolvido em seções subseqüentes.)

No último capítulo, o leitor encontrará algumas breves indicações de como continua a teoria que desenvolvemos aqui, em várias direções. Lá também são indicadas referências para estes segundos e terceiros passos no universo p-ádico. Nesta introdução queremos apenas comentar que aprendemos muito com os livros introdutórios de Koblitz e de Cassels, que recomendamos desde já aos nossos leitores.

Estas notas foram preparadas para um curso ministrado no 17º Colóquio Brasileiro de Matemática, realizado no Rio de Janeiro em julho de 1989. O autor gostaria de agradecer à Comissão Organizadora pelo convite.

São Paulo, 27 de abril de 1989

Fernando Q. Gouvêa

...τι ποιειτε, πάντα εις δόξαν Θεοῦ ποιειτε.

Sumário

Capítulo 1

Um Pouco de Motivação

A idéia de introduzir novas métricas no corpo $\mathbf{Q}$ dos números racionais e de considerar os completamentos correspondentes não surgiu de um mero anseio por generalidade, mas sim de várias situações concretas de caráter algébrico ou aritmético. Como estas métricas estarão cada uma delas ligada de perto a um primo p, elas "codificarão" muitas informações de interesse aritmético. O objetivo deste capítulo é fornecer uma introdução informal a estas idéias. Desta forma, vamos proceder sem muita preocupação com rigor ou precisão, enfatizando as idéias envolvidas. No próximo capítulo, passaremos ao desenvolvimento formal da teoria.

1.1 A analogia de Hensel

Os números p-ádicos foram introduzidos por K. Hensel, aparentemente a partir de uma analogia com o corpo de funções racionais $\mathbf{C}(X)$. A idéia é que dada uma função racional

$$f(X) = \frac{P(X)}{Q(X)},$$

com $P, Q \in \mathbf{C}[X]$, e dado um ponto $\alpha \in \mathbf{C}$, é sempre possível expandir f numa série de Laurent em torno de α, isto é, escrever

$$f(X) = \sum_{n \geq n_0} a_n (X - \alpha)^n,$$

pelo menos formalmente (embora a teoria das funções meromorfas garanta a convergência em alguma região, não vamo-nos preocupar com isso). Para obter a expansão, basta desenvolver

cada polinômio em potências de $(X-\alpha)$ e depois dividir formalmente. A série assim obtida reflete o comportamento da função quando X se aproxima de α, isto é, "localmente em α"; por exemplo:

- temos $n_0 \geq 0$ se e só se $Q(\alpha) \neq 0$, isto é, se e só se $f(X)$ é holomorfa em α;
- temos $n_0 > 0$ se e só se $f(\alpha) = 0$, e neste caso $a_1 = f'(\alpha)$.

Note que nem todas as possíveis séries de Laurent em $X-\alpha$ aparecem deste modo, já que qualquer função meromorfa numa região contendo α definirá uma tal série. Desta forma, o que a expansão em série de Laurent em torno de α dá é uma inclusão do corpo $\mathbf{C}(X)$ num corpo maior, o corpo das séries de Laurent em $X-\alpha$, que é às vezes denotado por $\mathbf{C}((X-\alpha))$.

A primeira observação que devemos fazer é que o corpo $\mathbf{C}(X)$ e o corpo $\mathbf{Q}$ têm muitas propriedades semelhantes. Cada um deles é o corpo de frações de um domínio a ideais principais (num caso, $\mathbf{C}[X]$, no outro, $\mathbf{Z}$) no qual todos os ideais primos não-nulos são maximais. É isto que sugeriu a Hensel procurar uma construção análoga para $\mathbf{Q}$. A chave é perceber que os elementos $X-\alpha$ são exatamente os *primos* do anel $\mathbf{C}[X]$. A versão para $\mathbf{Q}$, então, deverá envolver os primos $p \in \mathbf{Z}$.

Fixe, então, um primo $p \in \mathbf{Z}$. O análogo do desenvolvimento de um polinômio em potências de $X-\alpha$ é o desenvolvimento de um inteiro positivo $n \in \mathbf{Z}$ em potências de p, isto é, na forma

$$n = n_0 + n_1 p + n_2 p^2 + \cdots + n_k p^k,$$

com $0 \leq n_i \leq p-1$: trata-se da "expansão de n em base p", e é um fato bastante conhecido que ela sempre existe. Note que, como no caso de polinômios, esta é uma expansão finita[1].

Agora passamos dos inteiros positivos para os racionais positivos como no caso dos polinômios, isto é, dividindo formalmente: dados $a, b \in \mathbf{Z}$ positivos, expandimos ambos na base p e dividimos formalmente para obter uma série. O único cuidado é notar que (ao

[1] A condição $0 \leq n_i \leq p-1$ pode parecer não ter analogia no caso de $\mathbf{C}[X]$; a questão é que o quociente de $\mathbf{C}[X]$ pelo ideal gerado por $X-\alpha$ é isomorfo a $\mathbf{C}$, e as constantes em $\mathbf{C}[X]$ são um sistema de representantes. Da mesma forma, os números entre 0 e $p-1$ são um sistema de representantes do quociente de $\mathbf{Z}$ pelo ideal gerado por p.

contrário do caso de $\mathbf{C}[X]$), a soma de dois coeficientes da expansão pode ser maior que p, e deve então ser re-escrita de acordo. O mais fácil é ver um exemplo: tomemos $p = 3$, $a = 24$ e $b = 17$. Então

$$a = 0 + 2 \times 3 + 2 \times 3^2 = 2p + 2p^2$$

e

$$b = 2 + 2 \times 3 + 1 \times 3^2 = 2 + 2p + p^2,$$

o que dá (lembre que $p = 3$!)

$$\frac{a}{b} = \frac{24}{17} = \frac{2p + 2p^2}{2 + 2p + p^2} = p + p^3 + 2p^5 + p^7 + p^8 + \dots$$

Para verificar que isto dá certo, lembre que $p = 3$ e faça a conta:

$$(2 + 2p + p^2)(p + p^3 + 2p^5 + p^7 + p^8 + \dots) =$$

$$= 2p + 2p^2 + p^3 + 2p^3 + 2p^4 + p^5 + 4p^5 + 4p^6 + 2p^7 + 2p^7 + 2p^8 + p^9 + 2p^8 + 2p^9 + \dots$$

$$= 2p + 2p^2 + p^4 + 2p^4 + p^5 + 4p^5 + 4p^6 + 2p^7 + 2p^7 + 2p^8 + p^9 + 2p^8 + 2p^9 + \dots$$

$$= 2p + 2p^2 + p^5 + p^5 + 4p^5 + 4p^6 + 2p^7 + 2p^7 + 2p^8 + p^9 + 2p^8 + 2p^9 + \dots$$

$$= 2p + 2p^2 + 2p^6 + 4p^6 + 2p^7 + 2p^7 + 2p^8 + p^9 + 2p^8 + 2p^9 + \dots$$

$$= 2p + 2p^2 + 2p^7 + 2p^7 + 2p^7 + 2p^8 + p^9 + 2p^8 + 2p^9 + \dots$$

$$= 2p + 2p^2 + 2p^8 + 2p^8 + p^9 + 2p^8 + 2p^9 + \dots$$

$$= \dots$$

$$= 2p + 2p^2$$

de modo que os termos em p^n vão desaparecendo "para a direita".

É claro que isto é formal, mas é bastante fácil ver que sempre dá certo, e que a série assim obtida reflete as propriedades do número racional $x = a/b$ "localmente em p", isto é as propriedades que só envolvem o primo p. Por exemplo, se

$$x = \frac{a}{b} = \sum_{n \geq n_0} a_n p^n,$$

temos que

- $n_0 \geq 0$ se e só se $p \not| b$, isto é, se e só se x é p-inteiro[2];
- $n_0 > 0$ se e só se $p \not| b$ e $p|a$.

Mais ainda, n_0 é caracterizado pela igualdade

$$x = p^{n_0}\frac{a_1}{b_1} \qquad \text{com} \quad p \not| a_1 b_1.$$

Resta ver como obter os racionais negativos. Mantendo em mente que estamos trabalhando formalmente, e com um pouco de imaginação, achamos logo

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots,$$

já que

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

A conclusão é que, pelo menos formalmente, todo número racional pode ser escrito como uma série de Laurent em p, e que esta "expansão p-ádica" coincide com a expansão em base p para os inteiros positivos.

É fácil ver que o conjunto de todas as séries de Laurent em p forma um corpo, que contém $\mathbf{Q}$ mas é estritamente maior (vamos provar isto na próxima seção). Este corpo se chama *corpo dos números p-ádicos*, e é denotado por $\mathbf{Q}_p$. É claro, entretanto, que esta versão da sua definição não está "au gôut du jour"; no Capítulo 2, daremos uma definição formal e rigorosa. De qualquer forma, é fácil ver desde já o que a definição rigorosa requer: é preciso pôr uma topologia em $\mathbf{Q}$ na qual tenhamos que a seqüência p^n tenda a zero quando $n \to \infty$, para que as séries de potências em p^n tenham alguma chance de convergir, e depois definir $\mathbf{Q}_p$ como um completamento de $\mathbf{Q}$ em relação a essa topologia. Antes de procurar cumprir este programa, entretanto, vamos explorar um pouco mais o corpo que acabamos de construir.

[2]Para tornar a analogia com o caso de $\mathbf{C}(X)$ mais forte, seria interessante interpretar isto como alguma forma de holomorficidade. A idéia então é definir o "valor de x em p" como sendo x reduzido módulo p. Aí, temos que $n_0 \geq 0$ se e só se x módulo p está definido, já que se $p|b$ estaríamos dividindo por zero em $\mathbf{F}_p$.

Exercício 1 *Considere um número p-ádico*

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots.$$

Qual é a expansão p-ádica de $-x$?

Exercício 2 *Mostre que $\mathbf{Q}_p$ é um corpo.*

Exercício 3 *O fato de que os inteiros negativos têm expansões p-ádicas infinitas é um tanto desagradável em face da analogia com o caso de polinômios. Mostre que se fizermos as nossas expansões em potências de $-p$ (em vez de em potências de p) este problema desaparece, isto é, que todo $n \in \mathbf{Z}$ tem uma expansão finita em potências de $-p$.*

Exercício 4 *É natural, à luz de nossa experiência com os números reais, conjeturar que a expansão p-ádica de um racional deve ser periódica a partir de certo ponto, e que reciprocamente toda expansão p-ádica deste tipo representa um número racional. Prove que é de fato assim (sem se preocupar com questões de convergência).*

1.2 Resolvendo congruências módulo p^n

A construção de Hensel se relaciona de perto ao problema de resolver congruências módulo potências de p. Vamos considerar alguns exemplos.

Vamos começar com uma equação que tenha soluções em $\mathbf{Q}$, como por exemplo

$$X^2 = 25,$$

e vamos considerá-la módulo p^n para $p = 3$ e todos os n. Como a equação tem soluções $X = \pm 5$ em $\mathbf{Q}$, é claro que $X \equiv \pm 5 \pmod{3^n}$ é um sistema de soluções módulo 3^n.

Exercício 5 *Deixamos ao leitor a verificação (fácil) de que estas são as únicas soluções (a menos de congruências).*

Para entender melhor estas soluções em termos p-ádicos, vamos escrever cada uma das soluções usando representantes entre 0 e $3^n - 1$. Para $X = 5$, obtemos

$$\begin{aligned} X &\equiv 2 \pmod 3 \\ X &\equiv 5 = 2 + 3 \pmod 9 \\ X &\equiv 5 = 2 + 3 \pmod{27} \\ &\text{etc.} \end{aligned}$$

o que dá a expansão p-ádica da solução:

$$X = 5 = 2 + 1 \times 3.$$

Para $X = -5$, o resultado é mais interessante; os representantes são

$$\begin{aligned} X &\equiv -5 \equiv 1 \pmod 3 \\ X &\equiv -5 \equiv 4 = 1 + 3 \pmod 9 \\ X &\equiv -5 \equiv 22 = 1 + 3 + 2 \times 9 \pmod{27} \\ X &\equiv -5 \equiv 76 = 1 + 3 + 2 \times 9 + 2 \times 27 \pmod{81} \\ &\text{etc.} \end{aligned}$$

o que dá a expansão p-ádica da solução:

$$X = -5 = 1 + 3 + 2 \times 3^2 + 2 \times 3^3 + 2 \times 3^4 + \cdots$$

Note ainda que os dois sistemas de soluções são "coerentes", no seguinte sentido:

Definição 1 *Uma seqüência α_n de inteiros satisfazendo $0 \leq \alpha_n \leq p^n - 1$ se diz coerente se, para todo $n \geq 1$, $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$.*

É claro que o fato de nossas seqüências de soluções serem coerentes é uma conseqüência imediata do fato de que elas "são" soluções em $\mathbf{Q}$. Para nós, o mais importante é notar que há uma ligação entre sistemas coerentes de soluções de congruências e a expansão p-ádica da solução racional correspondente.

Exercício 6 *Faça um ou dois exemplos deste tipo. Por exemplo, tome a equação $X^2 = 49$ e $p = 5$. O que acontece se tomarmos a equação $X^2 = 81$ e $p = 2$? Este último caso é especialmente interessante.*

1.2. Resolvendo congruências módulo p^n

A coisa se torna muito mais interessante se tomarmos uma equação que *não* tem soluções em $\mathbf{Q}$. Por exemplo, considere o sistema de congruências

$$X^2 \equiv 2 \pmod{7^n}$$

para $n = 1, 2, 3, \ldots$ Para $n = 1$, as soluções são $X \equiv 3 \pmod 7$ ou $X \equiv 4 \equiv -3 \pmod 7$. Para $n = 2$, pomos $X = 3 + 7k$ ou $X = 4 + 7k$ e resolvemos:

$$\begin{aligned}(3+7k)^2 &\equiv 2 \pmod{49}\\ 9 + 42k &\equiv 2 \pmod{49}\\ 7 + 42k &\equiv 0 \pmod{49}\\ 1 + 6k &\equiv 0 \pmod 7\\ k &\equiv 1 \pmod 7\end{aligned}$$

o que dá a solução $X \equiv 10 \pmod{49}$. Pondo $X = 4 + 7k$ dá a solução $X \equiv 39 \equiv -10 \pmod{49}$.

Exercício 7 *Prove que este processo pode ser continuado indefinidamente, isto é, que dada uma solução α_n de $X^2 \equiv 2 \pmod{7^n}$, existe uma e uma só solução α_{n+1} de $x^2 \equiv 2 \pmod{7^{n+1}}$ tal que $\alpha_{n+1} \equiv \alpha_n \pmod{7^n}$. Ache os próximos termos de cada uma das seqüências coerentes começadas acima.*

Já que o processo pode ser continuado indefinidamente, ele nos dá duas seqüências coerentes de soluções:

$$x_1 = (3, 10, 108, \ldots)$$

e

$$x_2 = (4, 39, 235, \ldots) = (-3, -10, -108, \ldots) = -x_1,$$

que por sua vez dão duas expansões 7-ádicas:

$$x_1 = 3 + 1 \times 7 + 2 \times 49 + \cdots$$

e

$$x_2 = 4 + 5 \times 7 + 4 \times 49 + \cdots = -x_1.$$

O fato é que estes números 7-ádicos são de fato soluções da equação:

Exercício 8 *Mostre que se x_1 é obtido como acima, então $x_1^2 = 2$ em $\mathbf{Q}_7$. Conclua que $\mathbf{Q}_7$ é estritamente maior que $\mathbf{Q}$.*

Exercício 9 *Verifique que $X^2 = 2$ não tem solução em $\mathbf{Q}_5$. Note que isto seria uma maneira (extremamente complicada) de provar que não há soluções em $\mathbf{Q}$, já que qualquer solução em $\mathbf{Q}$ é automaticamente uma solução em $\mathbf{Q}_5$.*

Exercício 10 *Verifique que $X^2 + 1 = 0$ tem solução em $\mathbf{Q}_5$, mas não em $\mathbf{Q}_7$.*

Exercício 11 *Mostre que um número p-ádico*

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

é uma solução de uma equação $X^2 = m$ em $\mathbf{Q}_p$ se e só se

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

é uma seqüência coerente de soluções de $X^2 \equiv m \pmod{p^n}$.

Exercício 12 *Suponha que $X^2 \equiv m \pmod{p}$ tenha solução; mostre que se $p \neq 2$ é sempre possível "continuar" essa solução para obter uma seqüência coerente. Use este fato para obter uma condição necessária e suficiente para que $X^2 = m$ tenha solução em $\mathbf{Q}_p$ para $p \neq 2$. Por que $p = 2$ é especial?*

Exercício 13 *Mostre que para todo p, a inclusão $\mathbf{Q} \subset \mathbf{Q}_p$ é estrita. Mostre também que $\mathbf{Q}_p$ nunca é algebricamente fechado. (Para $p \neq 2$, use as idéias acima; para $p = 2$, um pouco de criatividade deve resolver.)*

1.3 Outros exemplos

A idéia de trabalhar com $\mathbf{Q}_p$ é bastante útil em muitos outros contextos. O objetivo desta seção é citar dois exemplos divertidos.

Tomemos a equação $X = 1 + 3X$; vamos tentar resolvê-la por recorrência:

$$\begin{aligned} a_0 &= 1 \\ a_1 &= 1 + 3a_0 = 1 + 3 \\ a_2 &= 1 + 3a_1 = 1 + 3 + 3^2 \\ &\cdots \\ a_n &= 1 + 3 + 3^2 + \cdots + 3^n. \end{aligned}$$

Em $\mathbf{R}$, é claro que a seqüência dos a_n é divergente. Entretanto, como os a_n são racionais, podemos pensar neles como elementos de $\mathbf{Q}_3$. É claro, então, que o limite é o número 3-ádico

$$1 + 3 + 3^2 + \cdots + 3^n + \cdots,$$

que, pelo argumento usual, é a expansão 3-ádica de $-1/2$, que é a solução da equação.

É claro que tanta sofisticação para resolver uma equação linear é um pouco de exagero, mas o fato notável é que um argumento que, pensado em $\mathbf{R}$, envolve manipulações duvidosas com séries divergentes se torna respeitável pensado em $\mathbf{Q}_3$. De fato, a série geométrica acima vai ser *convergente* na topologia 3-ádica que vamos introduzir no próximo capítulo, e a moral da estória é que ela só parece divergente porque temos em mente a topologia errada. Uma das razões para trabalhar com os números p-ádicos é esta possibilidade de tornar alguns problemas mais simples.

O seguinte exemplo é talvez ainda mais interessante. Considere a expansão em série de potências clássica do logaritmo:

$$\log(1 + X) = X - \frac{X^2}{2} + \frac{X^3}{3} - \frac{X^4}{4} + \cdots.$$

Queremos usar esta série para calcular o logaritmo de -1. É claro que a série resultante é divergente em $\mathbf{R}$, mas é mais ou menos fácil ver que ela converge em $\mathbf{Q}_2$ (há uns denominadores preocupantes, mas não é difícil lidar com eles—veja adiante!). É claro também que o limite tem que ser 0, porque

$$2\log(-1) = \log(1) = 0.$$

Logo, temos

$$0 = \log(1 - 2) = -(2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \cdots),$$

isto é, a seqüência

$$a_n = 2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \cdots + \frac{2^n}{n}$$

tende a zero em $\mathbf{Q}_2$. Como "tender a zero em $\mathbf{Q}_2$" significa ficar muito divisível por 2, concluímos que para qualquer $M > 0$ existe um n tal que a_n é divisível por 2^M. O leitor fica desafiado a dar uma demonstração elementar deste fato.

A relevância deste exemplo é destacar, outra vez, uma das principais razões para o uso dos métodos p-ádicos: como a topologia p-ádica está ligada de perto à divisibilidade por p ela permite obter resultados sobre divisibilidade por métodos analíticos que são mais simples e mais conceituais que os métodos clássicos.

Capítulo 2

Fundamentos

A topologia p-ádica em $\mathbf{Q}$ é definida a partir de um valor absoluto. Neste capítulo, vamos desenvolver a teoria geral que inclui esta situação, isto é, vamos tentar construir uma teoria geral de valores absolutos em corpos. É claro que o exemplo principal que teremos em mente é o corpo $\mathbf{Q}$, mas os enunciados (neste capítulo) serão gerais, já que essa generalidade não dificulta muito as coisas (e além disso ajuda o leitor que quiser se aprofundar mais depois).

2.1 Valores absolutos em um corpo

Seja k um corpo qualquer. Vamos começar definindo o que é um valor absoluto em k e explorando um pouco as possibilidades implícitas na definição.

Definição 2 *Um valor absoluto em* k *é uma função*

$$|\ |: \mathsf{k} \longrightarrow \mathbf{R}_+$$

satisfazendo as seguintes condições:

i) $|x| = 0$ *se e só se* $x = 0$

ii) $|xy| = |x|\,|y|$ *para todos os* $x, y \in \mathsf{k}$

iii) $|x + y| \leq |x| + |y|$ *para todos os* $x, y \in \mathsf{k}$.

Um valor absoluto se diz não-arquimediano *se satisfaz a condição adicional*

iv) $|x+y| \leq \max\{|x|,|y|\}$ *para todos os* $x, y \in \mathsf{k}$;

caso contrário, o valor absoluto se diz arquimediano.

Note que a condição (*iv*) implica a (*iii*). Vamos considerar alguns exemplos.

EXEMPLOS: 1. Se tomarmos $\mathsf{k} = \mathbf{Q}$, é claro que o valor absoluto usual (que é obtido a partir da inclusão $\mathbf{Q} \hookrightarrow \mathbf{R}$) é um valor absoluto em $\mathbf{Q}$; é imediato verificar que ele é arquimediano. (Tome $x = y = 1$ para ver que a condição (*iv*) não está satisfeita.) Por razões que devem ficar claras adiante, este valor absoluto é às vezes chamado de *valor absoluto infinito* em $\mathbf{Q}$, e denotado por $|\ |_\infty$.

2. Um exemplo pouco interessante é o valor absoluto dado por $|x| = 1$ se $x \neq 0$ e $|0| = 0$. É imediato que isto define um valor absoluto não-arquimediano em qualquer corpo, conhecido, por razões óbvias, como *valor absoluto trivial.*

3. O exemplo que nos ocupará na maior parte deste livro é o seguinte. Tome $\mathsf{k} = \mathbf{Q}$, e escolha um primo $p \in \mathbf{Z}$ qualquer. Dado qualquer inteiro $n \in \mathbf{Z}$, podemos escrever $n = p^v n'$, com $p \nmid n'$, de forma única. Como v fica determinado por p e n, escrevemos $v_p(n) = v$. Formalmente:

Definição 3 *Dado* $n \in \mathbf{Z}$, $n \neq 0$, *definimos a valorização p-ádica de* n *como sendo o inteiro positivo* $v_p(n)$ *definido pela condição*

$$n = p^{v_p(n)} n' \qquad com \quad p \nmid n'.$$

Se $x = a/b \in \mathbf{Q}^\times$, *definimos a valorização p-ádica de* x *pondo*

$$v_p(x) = v_p(a) - v_p(b).$$

Finalmente, escrevemos $v_p(0) = +\infty$.

Exercício 14 *Verifique que a definição da valorização p-ádica de um número racional dada acima independe da representação como quociente de inteiros.*

É fácil ver que a valorização p-ádica de um $x \in \mathbf{Q}$ fica determinada pela condição

$$x = p^{v_p(x)} \cdot \frac{a}{b}$$

com $p \nmid ab$.

Exercício 15 *Calcule alguns exemplos para sentir como funciona a coisa. Por exemplo, determine* $v_5(400)$, $v_7(902)$, $v_2(621)$, $v_3(123/48)$, $v_5(180/3)$.

As propriedades básicas da função v_p são fáceis de determinar:

Lema 2.1.1 *Para todos os* x *e* $y \in \mathbf{Q}$, *temos*

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

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

com as convenções óbvias em relação a $v_p(0) = +\infty$.

Exercício 16 *Prove o Lema 2.1.1.*

O Lema mostra que v_p se comporta como o logaritmo de um valor absoluto, exceto pelo fato que a desigualdade está na direção errada. Isto sugere:

Definição 4 *Para qualquer* $x \in \mathbf{Q}$, *definimos o* valor absoluto p-ádico *de* x *por*

$$|x|_p = p^{-v_p(x)},$$

com a convenção natural no caso em que $x = 0$, *de modo que* $|0|_p = 0$.

Proposição 2.1.2 *A função* $|\ |_p$ *é um valor absoluto não-arquimediano em* $\mathbf{Q}$.

DEMONSTRAÇÃO: Dado o Lema 2.1.1, todas as condições são imediatas. □

Vale notar que a associação entre um valor absoluto não-arquimediano e uma função com a propriedades de v_p (uma "valorização") é um fato geral, e a teoria pode ser desenvolvida tomando um ou outro objeto como primitivo. Nestas notas, fizemos a opção pelos valores absolutos. As propriedades específicas do valor absoluto p-ádico serão um de nossos temas centrais no que segue. Por hora, entretanto, é preferível manter um enfoque geral.

Exercício 17 *Verifique que* $|p^n|_p \to 0$ *quando* $n \to \infty$.

Exercício 18 *Mostre que se escolhermos um número* $c \in \mathbf{R}$, $c > 1$ *qualquer, é possível definir um valor absoluto não-arquimediano pondo* $|x| = c^{-v_p(x)}$. *Faça uma conjetura sobre a relação entre este valor absoluto e* $|\ |_p$. *Faça uma conjetura quanto à razão para a escolha* $c = p$.

3. Um terceiro exemplo é útil para enfatizar o alcance da teoria, e para confirmar a intuição de Hensel quanto à analogia entre $\mathbf{Q}$ e corpos de funções racionais. Sejam k um corpo qualquer (por exemplo: finito), $\mathsf{k}[t]$ o anel dos polinômios sobre k e $\mathsf{k}(t)$ o corpo de frações de $\mathsf{k}[t]$. Vamos definir várias valorizações (e portanto vários valores absolutos não-arquimedianos) diferentes em $\mathsf{k}(t)$.

a) Para todo polinômio $f \in \mathsf{k}[t]$, $f \neq 0$, ponhamos $v_\infty(f) = -\operatorname{grau}(f)$, e estendamos v_∞ a $\mathsf{k}(t)$ como antes, pondo $v_\infty(0) = +\infty$ e

$$v_\infty(\frac{f}{g}) = v_\infty(f) - v_\infty(g) = \operatorname{grau}(g) - \operatorname{grau}(f).$$

É imediato verificar que v_∞ satisfaz às mesmas condições que a valorização p-ádica:

Exercício 19 *Verifique que para quaisquer* $x, y \in \mathsf{k}(t)$ *temos* $v_\infty(xy) = v_\infty(x) + v_\infty(y)$ *e também* $v_\infty(x+y) \geq \min v_\infty(x), v_\infty(y)$.

Logo, obtemos um valor absoluto não-arquimediano pondo

$$|x|_\infty = c^{-v_\infty(x)}$$

para todo $x \in \mathsf{k}(t)$, onde c é um número real qualquer satisfazendo $c > 1$. (Veremos adiante que mudar c produz valores absolutos equivalentes; por isso, não é necessário escrever algo como $|\ |_{\infty,c}$.)

b) As outras valorizações em $\mathsf{k}(t)$ podem ser obtidas imitando a definição da valorização p-ádica, já que $\mathsf{k}[t]$ é um domínio a ideais principais. Basta escolher um polinômio irredutível $p = p(t) \in \mathsf{k}[t]$ e imitar o que foi feito acima para obter um valor absoluto não-arquimediano. Vale notar, por sinal, que todos os valores absolutos que construímos para $\mathsf{k}(t)$ são não-arquimedianos e induzem o valor absoluto trivial no corpo de constantes k.

Exercício 20 *Dado um polinômio irredutível $p \in \mathsf{k}[t]$, defina o valor absoluto p-ádico em $\mathsf{k}(t)$, e verifique que ele é um valor absoluto não-arquimediano.*

Exercício 21 *Mostre que a mudança de variável $t \to 1/t$ é um automorfismo de $\mathsf{k}(t)$ (que não preserva o "anel de inteiros" $\mathsf{k}[t]$, é claro). Verifique que a valorização "v_∞" definida acima corresponde ao polinômio irredutível $1/t \in \mathsf{k}[1/t]$, de modo que todas as valorizações de $\mathsf{k}(t)$ são "p-ádicas" se pensadas corretamente.*

Tendo em mente este conjunto de exemplos, queremos passar a um exame mais cuidadoso das propriedades dos valores absolutos.

2.2 Propriedades Básicas

Nesta seção, k é um corpo qualquer e $|\ |$ é um valor absoluto (não-trivial) em k, que pode ou não ser arquimediano. As primeiras propriedades são simples:

Lema 2.2.1 *i)* $|1| = 1$

ii) Se $x \in \mathsf{k}$ e $|x^n| = 1$, então $|x| = 1$.

iii) $|-1| = 1$

iv) Para todo $x \in \mathsf{k}$, $|-x| = |x|$.

v) Se k é um corpo finito, $|\ |$ é trivial.

DEMONSTRAÇÃO: A primeira afirmação segue de $1^2 = 1$ e $|1| \in \mathbf{R}_+^\times$; o resto segue imediatamente.□

Nosso primeiro resultado sério é uma caraterização dos valores absolutos não-arquimedianos.

Proposição 2.2.2 *Seja $A \subset \mathsf{k}$ a imagem de $\mathbf{Z}$ em k (isto é, o subanel gerado por $1 \in \mathsf{k}$). Então $|\ |$ é não-arquimediano se e só se $|a| \leq 1$ para todo $a \in A$.*

DEMONSTRAÇÃO: Se $|\ |$ é não arquimediano, temos $|\pm 1| = 1$ e portanto

$$|a \pm 1| \leq \max\{|a|, 1\}.$$

Por indução, $|a| \leq 1$.

Reciprocamente, suponhamos que $|a| \leq 1$ para todo $a \in A$. Dados $x, y \in \mathsf{k}$ quaisquer, queremos provar que $|x + y| \leq \max\{|x|, |y|\}$. Dividindo por $|y|$, isto é equivalente a

$$|\frac{x}{y} + 1| \leq \max\{|\frac{x}{y}|, 1\},$$

de modo que podemos supor que $y = 1$.

Seja m um inteiro positivo qualquer. Então

$$\begin{aligned} |x+1|^m &= |\sum_k \binom{m}{k} x^k| \\ &\leq \sum_k \left|\binom{m}{k}\right| |x^k| \\ &\leq \sum_k |x^k| \qquad \text{porque } \left|\binom{m}{k}\right| \leq 1 \\ &\leq (m+1)\max\{1, |x|^m\}. \end{aligned}$$

Agora, extraindo a raiz m-ésima dos dois lados, sai

$$|x+1| \leq \sqrt[m]{m+1}\ \max\{1, |x|\};$$

fazendo $m \to \infty$ dá o resultado.□

Este resultado ajuda a entender a nomenclatura: um valor absoluto é *arquimediano* se tem a seguinte propriedade:

Dados $x, y \in \mathbf{k}$, $x \neq 0$, existe um inteiro positivo n tal que $|nx| > |y|$.

Dadas as propriedades dos valores absolutos, isto é equivalente a

$$\sup\{|n| : n \in \mathbf{Z}\} = +\infty.$$

Nestes termos, a proposição acima diz que

$|\ |$ é não-arquimediano se e só se $\sup\{|n| : n \in \mathbf{Z}\} = 1$.

Para "fechar o círculo" deixamos ao leitor mostrar que:

Exercício 22 *Se* $\sup\{|n| : n \in \mathbf{Z}\} = C < +\infty$, *então* $|\ |$ *é não-arquimediano, e* $C = 1$.

2.3 Topologia

Como sempre, um valor absoluto determina uma métrica e portanto uma topologia.

Definição 5 *Seja* $\mathbf{k}$ *um corpo e* $|\ |$ *um valor absoluto em* $\mathbf{k}$. *Definimos uma métrica em* $\mathbf{k}$ *pondo*

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

Deixamos ao leitor as verificações naturais:

Exercício 23 *Verifique que* $d(x, y)$ *é de fato uma métrica, em relação à qual o corpo* $\mathbf{k}$ *é um corpo topológico (isto é, todas as operações em* $\mathbf{k}$ *são contínuas na toipologia induzida pela métrica d).*

A condição de não-arquimedianidade se traduz facilmente:

Lema 2.3.1 *Se o valor absoluto* $|\ |$ *for não-arquimediano e* $d(x, y) = |x - y|$, *então, para quaisquer* $x, y, z \in \mathbf{k}$,

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

DEMONSTRAÇÃO: Claro. □

Esta desigualdade é conhecida como "desigualdade ultramétrica"; um espaço métrico que a satisfaz é às vezes chamado um "espaço ultramétrico". A topologia induzida por uma métrica deste tipo tem, como não poderia deixar de ser, uma série de propriedades especiais. Vamos explorar algumas delas.

Proposição 2.3.2 *Sejam* $\mathbf{k}$ *um corpo e* $|\ |$ *um valor absoluto não-arquimediuano em* $\mathbf{k}$. *Se* $x, y \in \mathbf{k}$ *e* $|x| \neq |y|$, *então*

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

DEMONSTRAÇÃO: Trocando x e y se necessário, podemos supor que $|x| > |y|$. Já sabemos, então, que $|x + y| \leq |x| = \max\{|x|, |y|\}$.

Por outro lado, $x = (x + y) - y$, donde

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

Como $|x| > |y|$, esta desigualdade só pode valer se $\max\{|x+y|, |y|\} = |x+y|$; logo $|x| \leq |x+y|$, donde $|x| = |x + y|$. □

Corolário 2.3.3 *Em um espaço ultramétrico, todos os triângulos são isósceles.*

Estes resultados são um tanto surpreendentes; assim, talvez valha a pena olhar o exemplo específico dos valores absolutos p-ádicos em $\mathbf{Q}$: pomos $|x| = p^{-v_p(x)}$ como acima. Considere primeiro o caso de $x, y \in \mathbf{Z}$. Suponhamos $v_p(x) = n$ e $v_p(y) = m$, de modo que

$$x = p^n x' \qquad y = p^m y' \qquad p \nmid x'y'.$$

Em termos de valores absolutos,

$$|x| = p^{-n} \qquad \text{e} \qquad |y| = p^{-m}.$$

Teremos $|x| > |y|$ quando $n < m$; digamos que $m = n + \varepsilon$. Então

$$x + y = p^n x' + p^{n+\varepsilon} y' = p^n (x' + p^\varepsilon y').$$

Agora, como $p \nmid x'$ temos $p \nmid (x' + p^\varepsilon y')$, donde $v_p(x + y) = n$ e $|x + y| = p^{-n} = |x|$, confirmando a proposição.

Por outro lado, se $|x| = |y|$, isto é, $n = m$, temos

$$x + y = p^n (x' + y')$$

com $p \nmid x'$ e $p \nmid y'$, mas pode bem ser que $p|(x' + y')$. Neste caso, então, o máximo que se pode dizer é que $v_p(x + y) \geq n = \min\{v_p(x), v_p(y)\}$, isto é,

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

Note que em qualquer caso dois dentre $|x|$, $|y|$ e $|x + y|$ são iguais.

A propriedade de que "todo triângulo é isósceles" é característica dos espaços ultramétricos, e influencia profundamente sua topologia. Por exemplo:

Definição 6 *Sejam* k *um corpo munido de um valor absoluto* $|\ |$, $a \in \mathsf{k}$ *e* $r \in \mathbf{R}_+$. *Definimos as bolas "aberta" e "fechada"de centro* a *e raio* r *por*

$$B(a, r) = \{x \in \mathsf{k} : |x - a| < r\}$$

$$\overline{B}(a, r) = \{x \in \mathsf{k} : |x - a| \leq r\}.$$

As aspas são explicadas pelo que acontece no caso não-arquimediano:

Proposição 2.3.4 *Seja* k *um corpo munido de um valor absoluto não-arquimediano. Então:*

i) se $b \in B(a, r)$, *então* $B(a, r) = B(b, r)$;

ii) se $b \in \overline{B}(a, r)$, *então* $\overline{B}(a, r) = \overline{B}(b, r)$;

iii) o conjunto $B(a, r)$ *é aberto e fechado na topologia induzida por* $|\ |$;

iv) se $r \neq 0$, *o conjunto* $\overline{B}(a, r)$ *é aberto e fechado na topologia induzida por* $|\ |$;

v) *se* $a, b \in \mathbf{k}$ *e* $r, s \in \mathbf{R}_+^\times$, *temos* $B(a,r) \cap B(b,s) \neq \emptyset$ *se e só se* $B(a,r) \subset B(b,s)$ *ou* $B(a,r) \supset B(b,s)$;

vi) *se* $a, b \in \mathbf{k}$ *e* $r, s \in \mathbf{R}_+^\times$, *temos* $\overline{B}(a,r) \cap \overline{B}(b,s) \neq \emptyset$ *se e só se* $\overline{B}(a,r) \subset \overline{B}(b,s)$ *ou* $\overline{B}(a,r) \supset \overline{B}(b,s)$.

DEMONSTRAÇÃO: *i)* Temos $b \in B(a,r)$ se e só se $|b-a| < r$. Agora, se $|x-a| < r$, temos

$$|x-b| \leq \max\{|x-a|, |b-a|\} < r,$$

donde $B(a,r) \subset B(b,r)$. Trocando a e b, a igualdade segue.

ii) Troque $<$ por $\leq$ no argumento *(i)*.

iii) Em qualquer espaço métrico, $B(a,r)$ é um aberto. Para ver que neste caso $B(a,r)$ é também um fechado, lembre que $x \in \overline{B(a,r)}$ se e só se toda bola aberta em torno de x intercepta $B(a,r)$. Escolha $s \leq r$; como $B(a,r) \cap B(x,s) \neq \emptyset$, existe

$$b \in B(a,r) \cap B(x,s).$$

Mas então $|b-a| < r$ e $|b \dot{-} x| < s \leq r$, donde

$$|x-a| \leq \max\{|x-b|, |b-a|\} < r,$$

de modo que $x \in B(a,r)$.

iv) Análogo a *(iii)*.

v) Podemos supor $r \leq s$. Se existe $c \in B(a,r) \cap B(b,s)$, temos, por *(iii)*, que $B(a,r) = B(c,r)$ e $B(b,s) = B(c,s)$. Logo

$$B(a,r) = B(c,r) \subset B(c,s) = B(b,s),$$

como queríamos.

vi) Idêntico ao anterior, usando *(iv)*. □

Exercício 24 *Sob as mesmas hipóteses da proposição, mostre que para* $a \in \mathsf{k}$ *e* $r \in \mathbf{R}_+$, $r \neq 0$, *o conjunto* $\{x \in \mathsf{k} : |x - a| = r\}$ *é simultaneamente aberto e fechado.*

Conjuntos que são simultaneamente abertos e fechados são bastante comuns na teoria dos corpos munidos de valores absolutos não-arquimedianos. Tanto assim que recebem um nome especial:

Definição 7 *Seja* k *um corpo munido de um valor absoluto. Dizemos que um conjunto* $X \subset \mathsf{k}$ *é* fechaberto *se* X *é simultaneamente aberto e fechado na topologia induzida pelo valor absoluto de* k.

Em inglês, o termo usado é "clopen". O fato das bolas serem fechabertas faz que as propriedades de conexão da topologia induzida por um valor absoluto não-arquimediano sejam bastante ruins:

Proposição 2.3.5 *A topologia induzida por um valor absoluto não-arquimediano é totalmente desconexa, isto é, a componente conexa de qualquer ponto* $x \in \mathsf{k}$ *é o conjunto unitário* $\{x\}$.

DEMONSTRAÇÃO: Claro, porque qualquer x tem um sistema fundamental de vizinhanças fechabertas. □

Note, entretanto, que o conjunto $\{x\}$ não é aberto, de modo que a topologia em questão não é discreta.

Exercício 25 *Considere a topologia induzida pelo valor absoluto* arquimediano *de* $\mathbf{Q}$. *Existem conjuntos fechabertos não triviais nessa topologia? Existem conjuntos fechabertos em* $\mathbf{R}$?

Exercício 26 *Considere a topologia p-ádica em* $\mathbf{Q}$. *Mostre que toda bola aberta é uma reunião* disjunta *de bolas abertas. Isto é verdade para qualquer corpo munido de um valor absoluto não-arquimediano?*

2.4 Álgebra

Até aqui, nós usamos muito pouco o lado algébrico da teoria, isto é, o fato de que k é um corpo. Na realidade, a estrutura de corpo de k tem relações fortes com as valorizações de k (e portanto com os valores absolutos não-arquimedianos). Começamos com a seguinte definição:

Definição 8 *Seja* k *um corpo munido de um valor absoluto não-arquimediano* $|\ |$. *O* anel de valorização *de* $|\ |$ *é o subanel*

$$\mathcal{O} = \overline{B}(0,1) = \{x \in \mathsf{k} : |x| \leq 1\}.$$

O ideal de valorização *de* $|\ |$ *é o ideal*

$$\wp = B(0,1) = \{x \in \mathsf{k} : |x| < 1\}.$$

Deixamos ao leitor a verificação de que os nomes estão certos:

Exercício 27 *Seja* k *um corpo munido de um valor absoluto não-arquimediano.*

i) Mostre que $\mathcal{O}$ *é um subanel de* k, *e que* k *é o corpo de frações de* $\mathcal{O}$.

ii) Mostre que $\wp$ *é um ideal de* $\mathcal{O}$.

iii) Mostre que se $x \in \mathcal{O}$ *e* $x \notin \wp$, *então* x *é inversível em* $\mathcal{O}$, *de modo que* $\mathcal{O}$ *é um anel local com ideal maximal* $\wp$.

O último item do exercício sugere a seguinte definição:

Definição 9 *Sob as mesmas condições da definição precedente, o* corpo residual *de* k *é o corpo quociente*

$$\kappa = \mathcal{O}/\wp.$$

É instrutivo olhar o caso dos valores absolutos p-ádicos:

Proposição 2.4.1 *Se* $\mathsf{k} = \mathbf{Q}$ *e* $|\ | = |\ |_p$ *é o valor absoluto p-ádico, então*

i) $\mathcal{O} = \mathbf{Z}_{(p)} = \{a/b \in \mathbf{Q} : p \not| b\}$

ii) $\wp = p\mathbf{Z}_{(p)} = \{a/b \in \mathbf{Q} : p \not| b \text{ e } p|a\}$

iii) $\kappa = \mathbf{F}_p$ *é o corpo de* p *elementos.*

DEMONSTRAÇÃO: Claro. □

Exercício 28 *Verifique que tanto para* $|\ |_p$ *quanto para os outros exemplos acima, o ideal* $\wp$ *é principal. Tente achar um exemplo em que isto não acontece.*

Exercício 29 *Seja* k *um corpo, e seja* $\mathcal{O} \subset$ k *um subanel satisfazendo*

- k *é o corpo de frações de* $\mathcal{O}$*;*
- $\mathcal{O}$ *é um anel local noetheriano.*

Mostre que existe um valor absoluto em k *cujo anel de valorização é* $\mathcal{O}$.

Exercício 30 *Seja* k *um corpo, e seja* $|\ |$ *um valor absoluto em* k. *A valorização associada a* $|\ |$ *é a função definida por*

$$v(x) = -\log|x|.$$

Mostre que o ideal de valorização de $|\ |$ *é principal se e só se a imagem de* v *é um subgrupo discreto de* $\mathbf{R}^\times$. *Mostre que se a imagem de* v *for um subgrupo discreto de* $\mathbf{R}^\times$ *então o anel* $\mathcal{O}$ *é um domínio a ideais principais cujos únicos ideais primos são* $\wp$ *e* 0.

Capítulo 3

Números p-ádicos

Passamos agora a aplicar a teoria geral ao caso específico do corpo dos números racionais. A extensão dos nossos resultados aos corpos de números algébricos (e mesmo aos "corpos globais" em geral) não seria particularmente difícil, mas preferimos optar pelo exemplo mais concreto possível nesta introdução. O leitor encontrará detalhes do caso geral nas referências (veja, por exemplo, [5]).

3.1 Valores absolutos em Q

Nosso primeiro passo é mostrar que os exemplos que já obtivemos esgotam todos os possíveis valores absolutos em $\mathbf{Q}$ (a menos de equivalência). Vamos primeiro lembrar quais são eles:

- o valor absoluto trivial
- o valor absoluto real $|\ | = |\ |_\infty$
- para cada primo p, o valor absoluto p-ádico $|\ |_p$.

Repare que exceto pelo valor absoluto trivial, todos estes valores absolutos "são" da forma $|\ |_p$, onde p ou é um primo ou é ∞. Esta é uma das razões pelas quais se fala no "primo infinito" de $\mathbf{Q}$. Em alguns contextos, falaremos em "os primos $p \leq \infty$" para indicar este conjunto de valores absolutos[1].

[1] É importante enfatizar que se trata de um nome, apenas: não é muito claro o que há de tão "infinito" no valor absoluto real. De qualquer forma, esta nomenclatura parece estar definitivamente consagrada pelo

Para podermos enunciar o teorema central desta seção, precisamos primeiro de um bom conceito de equivalência de valores absolutos.

Definição 10 *Dois valores absolutos* $|\ |_1$ *e* $|\ |_2$ *em um corpo* $\mathbf{k}$ *se dizem equivalentes se induzem a mesma topologia em* $\mathbf{k}$.

É fácil caracterizar quando é que dois valores absolutos são equivalentes:

Lema 3.1.1 *Dois valores absolutos* $|\ |_1$ *e* $|\ |_2$ *em um corpo* $\mathbf{k}$ *são equivalentes se e só se existe um número real* α *tal que* $|\ |_1 = |\ |_2^{\alpha}$.

Exercício 31 *Prove o lema. Pode ser útil notar também que* $|\ |_1$ *e* $|\ |_2$ *são equivalentes se e só se tivermos*

$$|x|_1 < 1 \Longleftrightarrow |x|_2 < 1.$$

Por exemplo, se tomarmos um número real $c > 1$ e definirmos

$$|x| = c^{-v_p(x)},$$

o resultado é um valor absoluto equivalente ao valor absoluto p-ádico. A escolha de $c = p$ é conveniente porque queremos que a "fórmula do produto" (veja adiante) seja válida.

Teorema 3.1.2 (Ostrowski) *Todo valor absoluto não-trivial em* $\mathbf{Q}$ *é equivalente a um dos valores absolutos* $|\ |_p$, *para* p *primo ou* $p = \infty$.

DEMONSTRAÇÃO: Seja $|\ |$ um valor absoluto não-trivial em $\mathbf{Q}$. Vamos considerar os casos possíveis.

a) Se $|\ |$ for *arquimediano*, seja n_0 o menor inteiro positivo tal que $|n_0| > 1$. É claro que temos

$$|n_0| = n_0^{\alpha}$$

para algum $\alpha \in \mathbf{R}$. Para provar que este α serve, isto é, que para todo $x \in \mathbf{Q}$ temos $|x| = |x|_{\infty}^{\alpha}$, é claro que basta provar que $|n| = n^{\alpha}$ para todo inteiro positivo n.

uso, apesar de haver quem defenda (notadamente J. H. Conway) que se deveria chamar o "primo infinito" de "-1" e o valor absoluto real de "-1-ádico"...

Considere, então, um inteiro positivo n, e escreva n "na base n_0", isto é, na forma

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k,$$

com $0 \leq a_i \leq n_0 - 1$ e $a_k \neq 0$. Note que k é determinado pela desigualdade $n_0^k \leq n < n_0^{k+1}$, que dá

$$k = \left\lfloor \frac{\log n}{\log n_0} \right\rfloor,$$

onde $\lfloor x \rfloor$ denota a parte inteira de x. Tomando valores absolutos, obtemos

$$|n| = |a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k| \leq |a_0| + |a_1| n_0^\alpha + |a_2| n_0^{2\alpha} + \cdots + |a_k| n_0^{k\alpha}.$$

Como n_0 é o *menor* inteiro tal que $|n_0| > 1$, temos $|a_i| \leq 1$, donde

$$\begin{aligned} |n| &\leq 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{k\alpha} \\ &= n_0^{k\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-k\alpha}) \\ &\leq n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} = n_0^{k\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1}. \end{aligned}$$

Assim, tomando $C = n_0^\alpha/(n_0^\alpha - 1)$, segue que

$$|n| \leq C n_0^{k\alpha} \leq C n^\alpha.$$

Aplicando este resultado ao inteiro n^N, obtemos

$$|n^N| \leq C n^{N\alpha}$$

(o ponto crucial é que C não depende de n). Logo, para qualquer $N > 0$,

$$|n| \leq \sqrt[N]{C}\, n^\alpha.$$

Fazendo $N \to \infty$, obtemos metade do que queremos: $|n| \leq n^\alpha$.

Resta mostrar a desigualdade na direção oposta. Para isso, voltamos à expressão

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k.$$

Como $n_0^{k+1} > n \geq n_0^k$, temos

$$n_0^{(k+1)\alpha} = |n_0^{k+1}| = |n + n_0^{k+1} - n| \leq |n| + |n_0^{k+1} - n|,$$

donde

$$|n| \geq n_0^{(k+1)\alpha} - |n_0^{k+1} - n| \geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha,$$

pela desigualdade que nós já provamos. Como $n \geq n_0^k$, segue que

$$\begin{aligned} |n| &\geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n_0^k)^\alpha \\ &= n_0^{(k+1)\alpha}\left(1 - (1 - \frac{1}{n_0})^\alpha\right) \\ &= C' n_0^{(k+1)\alpha} > C' n^\alpha, \end{aligned}$$

onde outra vez $C' = 1 - (1 - 1/n_0)^\alpha$ é independente de n. Como antes, segue que $|n| \geq n^\alpha$, donde $|n| = n^\alpha$, o que prova que $|\ |$ é de fato equivalente ao valor absoluto real $|\ |_\infty$.

b) Se $|\ |$ for *não-arquimediano*, então $|n| \leq 1$ para todo inteiro n. Como $|\ |$ não é trivial, existe um menor inteiro n_0 tal que $|n_0| < 1$.

Note, em primeiro lugar, que n_0 tem que ser um número primo, porque senão teríamos $n_0 = a \cdot b$ com $|a| = |b| = 1$ pela minimalidade de n_0, contradizendo $|n_0| < 1$. Seja, então, $p = n_0$.

Tomemos agora $n \in \mathbf{Z}$ não divisível por p; vamos provar que $|n| = 1$. De fato, dividindo n por p temos

$$n = rp + s$$

com $0 < s < p$, donde $|s| = 1$ pela minimalidade e $|rp| < 1$ porque $|r| \leq 1$ e $|p| < 1$. Como $|\ |$ é não-arquimediano, segue que $|n| = 1$.

Finalmente, dado $n \in \mathbf{Z}$ qualquer, escrevemos $n = p^v n'$ com $p \nmid n'$, e então

$$|n| = |p|^v |n'| = |p|^v = c^{-v},$$

para $c = |p|^{-1} > 1$, o que mostra que $|\ |$ é equivalente ao valor absoluto p-ádico. □

Este teorema reforça a idéia de que faz sentido pensar na inclusão $\mathbf{Q} \hookrightarrow \mathbf{R}$ como "o primo infinito" de $\mathbf{Q}$, já que, nestes termos, ele diz que todo valor absoluto em $\mathbf{Q}$ provém de um primo (finito ou infinito). Em muitos contextos aritméticos é importante trabalhar

com "todos os primos", isto é, considerar informações obtidas a partir de todos os valores absolutos. Um exemplo é o seguinte resultado:

Proposição 3.1.3 (Fórmula do Produto) *Dado $x \in \mathbf{Q}^\times$, temos*

$$\prod_{p \leq \infty} |x|_p = 1,$$

onde $p \leq \infty$ indica que tomamos o produto sobre todos os primos de $\mathbf{Q}$, inclusive o primo infinito.

DEMONSTRAÇÃO: É claro que basta provar a fórmula para o caso em que x é um inteiro positivo. Neste caso, escreva $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. Então

$$\begin{cases} |x|_q = 1 & \text{se } q \neq p_i \\ |x|_{p_i} = p_i^{-a_i} & \text{para } i = 1, 2, \ldots, k \\ |x|_\infty = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \end{cases}$$

e o resultado segue. □

Um resultado parecido vale para extensões finitas de $\mathbf{Q}$ (se tomarmos o cuidado de notar que nesse caso há *vários* "primos infinitos", um para cada inclusão em $\mathbf{R}$ ou $\mathbf{C}$). É claro que isto sugere que um análogo do Teorema de Ostrowski também vale nesses casos, o que é verdade (e é até mais fácil de provar, porque basta estudar o problema de estender um valor absoluto de um subcorpo para o corpo todo). A maior parte das referências trata o caso geral.

3.2 Completamentos

Entre os valores absolutos em $\mathbf{Q}$, o valor absoluto arquimediano se destaca porque existe uma inclusão $\mathbf{Q} \hookrightarrow \mathbf{R}$ em um corpo satisfazendo as seguintes codições:

- o valor absoluto $|\ |_\infty$ se estende a $\mathbf{R}$
- $\mathbf{R}$ é completo em relação à métrica induzida por esse valor absoluto

- $\mathbf{Q}$ é denso em $\mathbf{R}$ (em relação à métrica induzida por $|\ |_\infty$).

Resumimos essa lista de propriedades dizendo que $\mathbf{R}$ é o completamento de $\mathbf{Q}$ em relação ao valor absoluto $|\ |_\infty$. O propósito desta seção é reestabelecer a igualdade entre os valores absolutos, construindo um completamento para cada um dos valores absolutos p-ádicos. Os corpos completos que obteremos são os corpos de números p-ádicos.

A existência de completamentos é um fato geral da teoria dos espaços métricos; o leitor que assim preferir pode invocar esse teorema geral, obtendo de imediato o teorema final desta seção. Desta forma, esta seção se dirige aos que desejam ver a construção.

Seja $|\ | = |\ |_p$ um valor absoluto não-arquimediano em $\mathbf{Q}$. Uma seqüência $(x_n)_{n\in\mathbf{N}}$ se diz uma seqüência de Cauchy em $\mathbf{Q}$ (em relação ao valor absoluto fixado) se dado $\varepsilon > 0$ existe N tal que

$$n,\, m \geq N \Longrightarrow |x_n - x_m| < \varepsilon.$$

A não-arquimedianidade do nosso valor absoluto permite obter desde logo uma versão mais simples desta condição (que *não* funciona no caso arquimediano).

Lema 3.2.1 *Uma seqüência (x_n) de números racionais é uma seqüência de Cauchy em relação a um valor absoluto não-arquimediano $|\ |$ se e só se*

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

DEMONSTRAÇÃO: Pela não-arquimedianidade, se $m = n + r > n$, temos

$$|x_m - x_n| \leq \max\{|x_{n+1} - x_n|, |x_{n+2} - x_{n+1}|, \ldots, |x_{n+r} - x_{n+r-1}|\}.$$

O resultado segue imediatamente. □

Exercício 32 *Dê um exemplo que mostre que este lema é falso para o valor absoluto arquimediano.*

Uma seqüência de Cauchy pode ou não ter um limite; um corpo se diz completo em relação a um valor absoluto $|\ |$ se toda seqüência de Cauchy (em relação a $|\ |$) tem um limite em k.

Lema 3.2.2 *O corpo* $\mathbf{Q}$ *dos números racionais não é completo em relação a nenhum dos valores absolutos p-ádicos.*

DEMONSTRAÇÃO: Isto foi essencialmente deixado como exercício no Capítulo 1. Para construir uma seqüência de Cauchy que não tem limite em $\mathbf{Q}$, procuramos uma seqüência coerente de soluções módulo p^n de uma equação que não tenha soluções em $\mathbf{Q}$. Vamos fazer o caso $p \neq 2$ e deixar o caso $p = 2$ ao leitor.

Seja então $p \neq 2$ um primo, e escolha um inteiro $a \in \mathbf{Z}$ tal que:

- a não é um quadrado em $\mathbf{Q}$
- a é um resíduo quadrático módulo p.

Definimos uma seqüência de Cauchy (em relação a $|\ |_p$) tomando:

- x_0 é qualquer solução de $x_0^2 \equiv a \pmod{p}$;
- x_1 satisfaz $x_1 \equiv x_0 \pmod{p}$ e $x_1^2 \equiv a \pmod{p^2}$;
- em geral, $x_n \equiv x_{n-1} \pmod{p^n}$ e $x_n^2 \equiv a \pmod{p^{n+1}}$.

É um exercício fácil mostrar que uma tal seqüência sempre existe (a questão crucial é garantir a existência de x_0, e o resto segue porque $p \neq 2$).

Agora,

$$|x_{n+1} - x_n| = |\lambda p^{n+1}| \leq p^{-(n+1)} \to 0,$$

de modo que a seqüência é de Cauchy, e por outro lado

$$|x_n - a^2| = |\mu p^{n+1}| \leq p^{-(n+1)} \to 0,$$

de modo que o limite, se existisse, seria uma raiz quadrada de a. Como a não é quadrado em $\mathbf{Q}$, o limite não existe, e portanto $\mathbf{Q}$ não é completo. □

Exercício 33 *Complete a demonstração do Lema provando que* $\mathbf{Q}$ *não é completo em relação ao valor absoluto 2-ádico.*

Já que $\mathbf{Q}$ não é completo, queremos construir seu completamento. A idéia é usar o próprio conjunto das seqüências de Cauchy para construir o completamento.

Definição 11 *Seja* $|\ | = |\ |_p$ *um valor absoluto não-arquimediano em* $\mathbf{Q}$. *Definimos*

$$C = C_p(\mathbf{Q}) = \{(x_n) : (x_n) \text{ é seqüência de Cauchy em relação a } |\ |_p.$$

Notamos, em primeiro lugar, que C tem uma estrutura natural de anel:

Proposição 3.2.3 *As definições*

$$(x_n) + (y_n) = (x_n + y_n)$$

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

dão a C *uma estrutura de anel comutativo com unidade.*

DEMONSTRAÇÃO: Claro. □

Como duas seqüências podem "ter o mesmo limite", precisamos passar ao quociente por uma relação de equivalência que capture essa idéia. Para isso, começamos introduzindo o ideal das seqüências que tendem a zero.

Definição 12 $\mathcal{N} \subset C$ *é o ideal*

$$\mathcal{N} = \{(x_n) : x_n \to 0\}$$

das seqüências que tendem a zero na topologia induzida por $|\ |_p$.

Exercício 34 *Verifique que* $\mathcal{N}$ *é de fato um ideal de* C.

Lema 3.2.4 $\mathcal{N}$ *é um ideal maximal de* C.

DEMONSTRAÇÃO: Seja (x_n) uma seqüência de Cauchy que não tende a zero, e seja I o ideal gerado por (x_n) e $\mathcal{N}$. Queremos provar que $I = C$.

Como (x_n) não tende a zero e é de Cauchy, é possível achar um $c > 0$ e um inteiro N tais que $|x_n| \geq c > 0$ sempre que $n \geq \mathrm{N}$. Considere, então, a seqüência (y_n) definida por $y_n = 0$ se $n < \mathrm{N}$ e $y_n = 1/x_n$ se $n \geq \mathrm{N}$. Em primeiro lugar, para $n \geq \mathrm{N}$, temos

$$|y_{n+1} - y_n| = |\frac{1}{x_{n+1}} - \frac{1}{x_n}| = \frac{|x_{n+1} - x_n|}{|x_n x_{n+1}|} \leq \frac{|x_{n+1} - x_n|}{c^2} \longrightarrow 0,$$

de modo que $(y_n) \in \mathcal{C}$. Depois,

$$x_n y_n = \begin{cases} 0 & \text{se } n < \mathrm{N} \\ \\ 1 & \text{se } n \geq \mathrm{N} \end{cases}$$

donde se vê que

$$(x_n)(y_n) - (1) \in \mathcal{N},$$

de modo que $(1) \in I$, como queríamos demonstrar. □

Como $\mathcal{N}$ é maximal, o quociente é um corpo.

Definição 13 *O corpo dos números p-ádicos é o corpo quociente*

$$\mathbf{Q}_p = \mathcal{C}/\mathcal{N}\,.$$

Note que as seqüências constantes dão uma inclusão $\mathbf{Q} \hookrightarrow \mathbf{Q}_p$. Queremos estender o valor absoluto p-ádico a $\mathbf{Q}_p$. O próximo lema mostra que isto pode ser feito sem dificuldade.

Lema 3.2.5 *Seja $(x_n) \in \mathcal{C}$, $(x_n) \notin \mathcal{N}$. A seqüência de números reais $|x_n|_p$ se estabiliza, isto é, existe* N *tal que*

$$n, m \geq \mathrm{N} \Longrightarrow |x_n|_p = |x_m|_p.$$

DEMONSTRAÇÃO: Como (x_n) não tende a zero (e é de Cauchy), existem c e N_1 tais que

$$n \geq \mathrm{N}_1 \Longrightarrow |x_n| \geq c > 0.$$

Por outro lado, existe N_2 tal que

$$n, m \geq \mathrm{N}_2 \Longrightarrow |x_n - x_m| < c.$$

Logo, se $N = \max\{N_1, N_2\}$, temos

$$n, m \geq N \Longrightarrow |x_n - x_m| < \max\{|x_n|, |x_m|\},$$

o que implica $|x_n| = |x_m|$ pela não-arquimedianidade ("todo triângulo é isósceles"). □

Como $(x_n) \in \mathcal{N}$ se e só se $|x_n| \to 0$, segue que faz sentido definir

Definição 14 *Se $\lambda \in \mathbf{Q}_p$ e (x_n) é qualquer representante da classe λ, definimos*

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

Note que se $\lambda \in \mathbf{Q} \subset \mathbf{Q}_p$, isto dá o valor absoluto p-ádico original (tome a seqüência constante). Note também que, exceto no caso de $\lambda = 0$, o limite é de fato estacionário, de modo que a função

$$|\ |_p : \mathbf{Q}_p \longrightarrow \mathbf{R}_+$$

tem a mesma imagem (o mesmo "conjunto de valores") que o valor absoluto p-ádico em $\mathbf{Q}$.

Vamos verificar que de fato obtivemos o que desejávamos, e também que o resultado tem propriedades de unicidade suficientemente fortes para podermos de imediato esquecer como foi feita a construção.

Teorema 3.2.6 *Para cada primo $p \in \mathbf{Z}$, existe um corpo $\mathbf{Q}_p$ munido de um valor absoluto $|\ |_p$, satisfazendo:*

i) existe uma inclusão $\mathbf{Q} \hookrightarrow \mathbf{Q}_p$ de modo que a restrição de $|\ |_p$ a $\mathbf{Q}$ seja o valor absoluto p-ádico;

ii) a imagem de $\mathbf{Q}$ é densa em $\mathbf{Q}_p$;

iii) $\mathbf{Q}_p$ é completo em relação à métrica induzida por $|\ |_p$.

O corpo $\mathbf{Q}_p$ satisfazendo (i), (ii) e (iii) é único a menos de isomorfismo único (isométrico em relação aos valores absolutos).

DEMONSTRAÇÃO: Quase tudo já está feito. A construção dá um corpo $\mathbf{Q}_p$, e já verificamos que ele satisfaz *(i)* e *(ii)*. A condição *(iii)* segue sem dificuldade. Para provar a unicidade, basta notar que se um outro corpo K satisfaz *(i)*, *(ii)* e *(iii)*, temos uma inclusão de $\mathbf{Q} \subset \mathbf{Q}_p$ em K que é uma isometria, e portanto é contínua, em relação aos valores absolutos em $\mathbf{Q}_p$ e em K. Estendendo por continuidade dá o isomorfismo desejado, que é claramente único. □

Exercício 35 *Prove que $\mathbf{Q}_p$ satisfaz a condição (iii) do teorema.*

O fato de termos um resultado forte de unicidade mostra que podemos agora esquecer a construção de $\mathbf{Q}_p$ e trabalhar com suas propriedades. É o que faremos a seguir.

Exercício 36 *Por que é importante que $\mathbf{Q}_p$ seja único a menos de isomorfismo único? Dê um exemplo de um objeto algébrico que é único a menos de isomorfismo, mas não a menos de isomorfismo único.*

3.3 Propriedades básicas de $\mathbf{Q}_p$

O objetivo desta seção é entender melhor o corpo $\mathbf{Q}_p$. Começamos lembrando a caracterização de $\mathbf{Q}_p$ que concluiu a seção anterior:

- há um valor absoluto $|\ | = |\ |_p$ em $\mathbf{Q}_p$, e $\mathbf{Q}_p$ é completo em relação à métrica induzida por ele;
- há uma inclusão $\mathbf{Q} \hookrightarrow \mathbf{Q}_p$ com imagem densa, e $|\ |_p$ restrito a $\mathbf{Q}$ via essa inclusão coincide com o valor absoluto p-ádico.

Lembramos, também, que mostramos que a imagem de $\mathbf{Q}_p$ sob $|\ |_p$ é a mesma de $\mathbf{Q}$, isto é:

Lema 3.3.1 *Dado $x \in \mathbf{Q}_p$, $\neq 0$, existe $n \in \mathbf{Z}$ tal que $|x|_p = p^{-n}$.*

Outra forma de dizer isso é dizer que a valorização p-ádica v_p se estende a $\mathbf{Q}_p$.

Definição 15 *O anel dos inteiros p-ádicos é*

$$\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x|_p \leq 1\}.$$

Na linguagem do final do Capítulo 2, $\mathbf{Z}_p$ é o anel de valorização de $\mathbf{Q}_p$. Lembre também que $\mathbf{Z}_p$ é um conjunto fechaberto na toplogia p-ádica (porque toda bola fechada é).

Proposição 3.3.2 *O anel dos inteiros p-ádicos é um anel local cujo ideal maximal é* $p\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x|_p < 1\}$. *Além disso,*

i) $\mathbf{Q} \cap \mathbf{Z}_p = \mathbf{Z}_{(p)} = \{\frac{a}{b} \in \mathbf{Q} : p \not| b\}$.

ii) A inclusão $\mathbf{Z} \hookrightarrow \mathbf{Z}_p$ *tem imagem densa. Mais precisamente, dados* $x \in \mathbf{Z}_p$ *e* $n \geq 1$, *existe* $\alpha \in \mathbf{Z}$, $0 \leq \alpha \leq p^n - 1$, *tal que* $|x - \alpha| \leq p^{-n}$. *O inteiro* α *assim escolhido é único.*

iii) Dado $x \in \mathbf{Z}_p$, *existe uma seqüência de Cauchy* $\alpha_n \to x$, *do seguinte tipo:*

- $\alpha_n \in \mathbf{Z}$ *com* $0 \leq \alpha_n \leq p^n - 1$
- *para todo* n, $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

A seqüência (α_n) *nestas condições é única.*

DEMONSTRAÇÃO: Como $\mathbf{Z}_p$ é o anel de valorização de $\mathbf{Q}_p$, a primeira afirmação é clara. Para ver que o ideal de valorização é de fato gerado por p, basta ver que

$$|x| < 1 \Longrightarrow |x| \leq \frac{1}{p} \Longrightarrow |\frac{x}{p}| \leq 1 \Longrightarrow x \in p\mathbf{Z}_p,$$

já que a recíproca é imediata. Quanto às outras afirmações, *(i)* é imediato. Para ver *(ii)*, tome $x \in \mathbf{Z}_p$ e $n \geq 1$. Como $\mathbf{Q}$ é denso em $\mathbf{Q}_p$, existe $a/b \in \mathbf{Q}$ tal que

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

Como então

$$\left|\frac{a}{b}\right| \leq \max\{|x|, |x - \frac{a}{b}|\} \leq 1,$$

temos $a/b \in \mathbf{Z}_{(p)}$, isto é, $p \not| b$. Agora, como $p \not| b$, existe $b' \in \mathbf{Z}$ tal que $bb' \equiv 1 \pmod{p^n}$, donde

$$\left|\frac{a}{b} - ab'\right| \leq p^{-n}.$$

Finalmente, existe um único $\alpha \in \mathbf{Z}$, $0 \leq \alpha \leq p^n - 1$, tal que

$$|ab' - \alpha| \leq p^{-n}.$$

Juntando tudo, obtemos $|x - \alpha| \leq p^{-n}$. A unicidade é imediata.

Para concluir, *(iii)* segue imediatamente de *(ii)*. □

Corolário 3.3.3 $\mathbf{Q}_p = \mathbf{Z}_p[1/p]$, *isto é, dado* $x \in \mathbf{Q}_p$, *existe* $n \geq 0$ *tal que* $p^n x \in \mathbf{Z}_p$. *A multiplicação por* p *é um homeomorfismo* $\mathbf{Q}_p \longrightarrow \mathbf{Q}_p$. *Os conjuntos* $p^n\mathbf{Z}_p$ *com* $n \in \mathbf{Z}$ *formam um sistema fundamental de vizinhanças de* $0 \in \mathbf{Q}_p$, *e cobrem* $\mathbf{Q}_p$.

DEMONSTRAÇÃO: Tudo claro. □

Uma das coisas que este último resultado diz é que a topologia de $\mathbf{Q}_p$ está ligada de perto à sua estrutura algébrica. Por exemplo, $|x - y| \leq p^{-n}$ se e só se $x - y \in p^n\mathbf{Z}_p$. Os próximos resultados continuam explorando esta interrelação.

Corolário 3.3.4 *Para qualquer* $n \geq 1$, *a seqüência*

$$0 \longrightarrow p^n\mathbf{Z}_p \longrightarrow \mathbf{Z}_p \longrightarrow \mathbf{Z}/p^n\mathbf{Z} \longrightarrow 0$$

é exata com morfismos contínuos (com a topolgia discreta em $\mathbf{Z}/p^n\mathbf{Z}$*). Em particular,*

$$\mathbf{Z}_p/p^n\mathbf{Z}_p \cong \mathbf{Z}/p^n\mathbf{Z}.$$

DEMONSTRAÇÃO: Imediato do item *(iv)* da Proposição. □

Os conjuntos $a + p^n\mathbf{Z}_p$, com $a \in \mathbf{Q}$ e $n \in \mathbf{Z}$, são bolas em $\mathbf{Q}_p$, e portanto sào fechabertos. Como antes, segue que

Corolário 3.3.5 $\mathbf{Q}_p$ *é um espaço topológico Hausdorff e totalmente desconexo.*

Mais interessante é o seguinte resultado:

Corolário 3.3.6 *$\mathbf{Z}_p$ é compacto e $\mathbf{Q}_p$ é localmente compacto.*

DEMONSTRAÇÃO: É claro que basta provar que $\mathbf{Z}_p$ é compacto, já que $\mathbf{Z}_p$ é uma vizinhança de 0. Como já sabemos que $\mathbf{Z}_p$ é completo (é a bola fechada unitária em $\mathbf{Q}_p$, que é completo por construção), resta provar que $\mathbf{Z}_p$ é totalmente limitado, isto é, que dado $\varepsilon > 0$ existe uma cobertura finita de $\mathbf{Z}_p$ por bolas de raio ε. É claro que basta considerar $\varepsilon = p^{-n}$, $n \geq 0$, e então o fato segue imediatamente do fato que

$$\mathbf{Z}_p/p^n\mathbf{Z}_p \cong \mathbf{Z}/p^n\mathbf{Z}$$

é um conjunto finito (e da continuidade da projeção). □

Note que a finitude de $\mathbf{Z}_p/p^n\mathbf{Z}_p$ segue sem dificuldade da finitude de $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbf{F}_p$. Isto é um fato geral:

Exercício 37 *Sejam K um corpo, $|\ |$ um valor absoluto não-arquimediano em K, $\mathcal{O} \subset K$ o anel de valorização e $\wp \subset \mathcal{O}$ o ideal de valorização. Suponha que K é completo e que $\wp$ é principal. Mostre que $\mathcal{O}$ é compacto se e só se o corpo residual $\mathcal{O}/\wp$ é finito. Decida se as hipóteses de completude de K e principalidade de $\wp$ são necessárias.*

Seria desejável tornar mais concretos os elementos de $\mathbf{Q}_p$. Para isso, vamos descrever duas representações canônicas de um inteiro p-ádico. A primeira tem um papel teórico importante; a segunda, que é análoga à expansão decimal em $\mathbf{R}$, será a mais útil para "enxergar" os números p-ádicos.

Nosso ponto de partida é o item *(iv)* da Proposição acima: dado $x \in \mathbf{Z}_p$, existe uma seqüência $\alpha_n \to x$ com

- $\alpha_n \in \mathbf{Z}$, $0 \leq \alpha_n \leq p^n - 1$
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$,

e esta seqüência é única. Reciprocamente, toda seqüência deste tipo determina um elemento de $\mathbf{Z}_p$, porque é uma seqüência de Cauchy. Vamos resumir isto numa proposição; para

facilitar, vamos denotar por φ_n a projeção

$$\varphi_n : \mathbf{Z}_p \longrightarrow \mathbf{Z}/p^n\mathbf{Z}.$$

Note que $\varphi_n(x) = \alpha_n \pmod{p^n}$. Escrevemos, também,

$$A_n = \mathbf{Z}/p^n\mathbf{Z}$$

como anel topológico com a topologia discreta, e denotamos por $\psi_n : A_n \longrightarrow A_{n-1}$ a projeção canônica (redução mod p^{n-1}). O produto de todos os A_n, com a topologia produto, é um anel topológico compacto.

Proposição 3.3.7 *As projeções φ_n determinam uma inclusão*

$$\varphi \hookrightarrow \prod_{n\geq 1} A_n$$

que identifica $\mathbf{Z}_p$, como anel topológico, com o subanel fechado de $\prod A_n$ que consiste das seqüências (α_n) satisfazendo $\psi_n(\alpha_n) = \alpha_{n-1}$ para todo $n > 1$.

DEMONSTRAÇÃO: Basta juntar os fatos que já demonstramos; deixamos os detalhes como exercício para o leitor. □

Exercício 38 *Prove a Proposição. Note que a Proposição dá outra construção, mais algébrica, do anel $\mathbf{Z}_p$, e outra demonstração de que $\mathbf{Z}_p$ é compacto.*

Exercício 39 *Mostre que $\mathbf{Z}_p$ tem a seguinte propriedade universal: se um anel A possui homomorfismos $A \longrightarrow A_n$ para todo $n \geq 1$ tais que todos os triângulos*

$$\begin{array}{ccc} & & A_n \\ & \nearrow & \\ A & & \downarrow \ \psi_n \\ & \searrow & \\ & & A_{n-1} \end{array}$$

são comutativos, então existe um único homomorfismo $A \longrightarrow \mathbf{Z}_p$ fazendo todos os triângulos evidentes comutarem. Isto diz que $\mathbf{Z}_p$ é o limite inverso *dos A_n.*

Vamos agora obter uma representação canônica de todo inteiro p-ádico como soma de uma série de potências em p (a "expansão p-ádica"do Capítulo 1). Tomemos $x \in \mathbf{Z}_p$. Já sabemos que existem $\alpha_n \in \mathbf{Z}$ com as seguintes propriedades:

- $\alpha_n \equiv x \pmod{p^n}$
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$
- $0 \leq \alpha_n \leq p^n - 1$.

Vamos escrever cada um dos inteiros α_n "na base p"; como $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$, os n primeiros dígitos coincidirão. Assim, teremos

$$\begin{aligned} \alpha_0 &= b_0 & 0 \leq b_0 \leq p-1 \\ \alpha_1 &= b_0 + b_1 p & 0 \leq b_1 \leq p-1 \\ \alpha_2 &= b_0 + b_1 p + b_2 p^2 & 0 \leq b_2 \leq p-1 \end{aligned}$$

e assim por diante. Concatenando tudo, obtemos uma expressão

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$$

Para ver que isso funciona, verificamos primeiro a convergência.

Lema 3.3.8 *Dados quaisquer $b_i \in \mathbf{Z}$, a série*

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$$

converge em $\mathbf{Z}_p$.

DEMONSTRAÇÃO: Basta verificar que a seqüência das somas parciais é de Cauchy. Mas as somas parciais são $\alpha_n = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n$, de modo que

$$|\alpha_n - \alpha_{n-1}| = |b_n p^n| \leq p^{-n} \to 0,$$

e o resultado segue pelo Lema 3.2.1. □

Corolário 3.3.9 *Todo $x \in \mathbf{Z}_p$ se escreve de forma única como*

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$$

com $0 \leq b_i \leq p-1$.

DEMONSTRAÇÃO: Claro a partir da existência e da unicidade dos α_n acima. □

Para obter um $x \in \mathbf{Q}_p$ qualquer, basta dividir um elemento de $\mathbf{Z}_p$ por uma potência de p. Assim:

Corolário 3.3.10 *Todo $x \in \mathbf{Q}_p$ se escreve de forma única como*

$$\begin{aligned} x &= b_{-n_0} p^{-n_0} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots \\ &= \sum_{n \geq -n_0} b_n p^n \end{aligned}$$

com $0 \leq b_n \leq p-1$ e $-n_0 = v_p(x)$.

DEMONSTRAÇÃO: Se $x \in \mathbf{Q}_p$ e $v_p(x) = -n_0$, então $p^{n_0} x \in \mathbf{Z}_p$ e $p^{n_0} x \notin p\mathbf{Z}_p$. □

Assim, como no Capítulo 1, os números p-ádicos podem ser pensados como o conjunto das expansões p-ádicas. Como observamos de passagem antes, os b_n devem ser tomados em um conjunto de representantes das classes módulo p. Como $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbf{F}_p$, a escolha de $0 \leq b_n \leq p-1$ é bastante natural; há situações, entretanto, que requerem uma outra escolha, os "representantes de Teichmüller" (veja adiante).

Exercício 40 *Mostre que a condição $0 \leq b_n \leq p-1$ pode ser substituída por $b_n \in X$, onde X é um conjunto qualquer de representantes de $\mathbf{Z}_p/p\mathbf{Z}_p$ em $\mathbf{Z}_p$. (O importante é que os b_n não precisam ser inteiros!)*

As *unidades p-ádicas* são os elementos inversíveis de $\mathbf{Z}_p$; denotaremos esse conjunto por $\mathbf{Z}_p^\times$. É imediato que

$$\mathbf{Z}_p^\times = \{x \in \mathbf{Q}_p : |x| = 1\}$$

e que

$$\mathbf{Z}_p^{\times} \cap \mathbf{Q} = \{\frac{a}{b} \in \mathbf{Q} : p \not| ab\}.$$

As unidades p-ádicas formam um grupo, que, como veremos em breve, é bastante grande.

3.4 O Lema de Hensel

Talvez o resultado chave da teoria algégrica dos corpos completos não-arquimedianos seja o teorema conhecido como "Lema de Hensel", que (no nosso caso) dá uma condição para um polinômio ter uma raiz em $\mathbf{Z}_p$.

Teorema 3.4.1 (Lema de Hensel) *Seja* $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ *um polinômio com coeficientes em* $\mathbf{Z}_p$. *Suponhamos que exista um inteiro p-ádico* $\alpha_0 \in \mathbf{Z}_p$ *satisfazendo*

$$F(\alpha_0) \equiv 0 \pmod{p\mathbf{Z}_p}$$

e

$$F'(\alpha_0) \not\equiv 0 \pmod{p\mathbf{Z}_p},$$

onde $F'(X)$ *é a derivada formal de* $F(X)$. *Então existe* $\alpha \in \mathbf{Z}_p$ *tal que* $\alpha \equiv \alpha_0 \pmod{p\mathbf{Z}_p}$ *e* $F(\alpha) = 0$.

DEMONSTRAÇÃO: Para mostrar que α existe, construiremos uma seqüência de Cauchy, usando essencialmente o "método de Newton" para achar raízes de polinômios. O leitor atento reconhecerá uma idéia que vimos usando repetidamente desde o Capítulo 1.

Queremos construir uma seqüência $\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots$ satisfazendo, para todo $n \geq 1$,

i) $F(\alpha_n) \equiv 0 \pmod{p^{n+1}}$,

ii) $\alpha_n \equiv \alpha_{n-1} \pmod{p^n}$.

É imediato que tal seqüência será de Cauchy, e que se α for seu limite, teremos $F(\alpha) = 0$ e $\alpha \equiv \alpha_0 \pmod{p}$. Assim, a existência dos α_n já prova o teorema.

A existência de α_0 é a hipótese do teorema. Para obter α_1, notamos que a condição (ii) acima diz que

$$\alpha_1 = \alpha_0 + b_1 p$$

para algum $b_1 \in \mathbf{Z}_p$. Agora, pela fórmula de Taylor formal, temos

$$\begin{aligned} F(\alpha_1) &= F(\alpha_0 + b_1 p) \\ &= F(\alpha_0) + F'(\alpha_0) b_1 p + \text{termos em } p^n,\ n \geq 2 \\ &\equiv F(\alpha_0) + F'(\alpha_0) b_1 p \pmod{p^2} \end{aligned}$$

Assim, queremos determinar b_1 tal que

$$F(\alpha_0) + F'(\alpha_0) b_1 p \equiv 0 \pmod{p^2};$$

como $F(\alpha_0) \equiv 0 \pmod{p}$, podemos escrever $F(\alpha_0) = px$. Então a equação fica

$$px + F'(\alpha_0) b_1 p \equiv 0 \pmod{p^2},$$

que dá (dividindo por p)

$$x + F'(\alpha_0) b_1 \equiv 0 \pmod{p},$$

donde

$$b_1 \equiv -x(F'(\alpha_0))^{-1} \pmod{p},$$

que faz sentido, já que por hipótese $F'(\alpha_0)$ não é divisível por p (e portanto é inversível em $\mathbf{Z}_p$!). Escolhendo um tal b_1, e pondo $\alpha_1 = \alpha_0 + b_1 p$, temos as propriedades desejadas.

Um cálculo idêntico mostra que dado α_n é possível obter α_{n+1}, o que prova o teorema. □

É bom enfatizar que existem muitas versões deste resultado, todas conhecidas como "Lema de Hensel". Um exemplo de uma versão um pouco mais geral é dado no próximo exercício.

Exercício 41 *Mostre que o Lema de Hensel continua verdade se substituirmos a condição* $F'(\alpha_0) \not\equiv 0$ *por* $|F(\alpha_0)| < |F'(\alpha_0)|$. *Explique por que isto é mais geral que o enunciado acima. Dê um exemplo em que esta forma do Lema de Hensel é aplicável, mas a primeira não é.*

Exercício 42 *Tome p um primo, m um inteiro não divisível por p. Use o Lema de Hensel para determinar todas as raízes m-ésimas da unidade em $\mathbf{Q}_p$. É possível usar este método para decidir se existem raízes p-ésimas em $\mathbf{Q}_p$?*

Uma aplicação interessante do Lema de Hensel é a determinação dos quadrados em $\mathbf{Q}_p$, que confirma a argumentação intuitiva que fizemos no Capítulo 1.

Lema 3.4.2 *Seja $p \neq 2$ um primo, e seja $b \in \mathbf{Z}_p^\times$ uma unidade p-ádica. Se existe α_0 tal que $\alpha_0^2 \equiv b \pmod{p\mathbf{Z}_p}$, então b é um quadrado em $\mathbf{Z}_p^\times$.*

DEMONSTRAÇÃO: Aplique o Lema de Hensel ao polinômio $X^2 - b$, notando que $p \neq 2$ e $b \in \mathbf{Z}_p^\times$ garantem que $2\alpha_0 \not\equiv 0 \pmod{p}$. □

Corolário 3.4.3 *Seja $p \neq 2$ um primo. O grupo $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ tem ordem quatro. Se $c \in \mathbf{Z}_p^\times$ é qualquer elemento que não é um resíduo quadrático módulo $p\mathbf{Z}_p$, então $\{1, p, c, cp\}$ é um conjunto de representantes.*

DEMONSTRAÇÃO: Se $x \in \mathbf{Q}_p^\times$ é um quadrado, temos necessariamente que $v_p(x) = 2n$ é par; pondo $x = p^{2n}c$, teremos $c \in \mathbf{Z}_p^\times$, e basta aplicar o lema para concluir. □

Exercício 43 *Mostre que se $b \in \mathbf{Z}_2$, $b \equiv 1 \pmod{8\mathbf{Z}_2}$, então b é um quadrado em $\mathbf{Z}_2$. Conclua que o grupo $\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2$ é de ordem 8, e é gerado por $\{-1, 5, 2\}$. (Sugestão: use a versão mais geral do Lema de Hensel que apareceu no exercício 41.)*

3.5 O princípio local-global

Uma das implicações do Lema de Hensel é o fato de que, dado um polinômio com coeficientes em $\mathbf{Z}$, é (em geral) bastante fácil decidir se ele tem raízes em $\mathbf{Z}_p$. Basta, para isso, procurar raízes módulo p. O "mesmo" é verdade para raízes em $\mathbf{R}$, exceto que a redução módulo p fica substituída por considerações de sinal. Finalmente, é claro que se um polinômio tem

raízes em $\mathbf{Q}$, então ele certamente tem raízes em $\mathbf{Q}_p$ para todo $p \leq \infty$; assim, se houver um p para o qual não há raízes em $\mathbf{Q}_p$, saberemos que não há raízes em $\mathbf{Q}$. Foram este tipo de considerações, e em particular a busca de algum tipo de recíproca desta última afirmação, que motivaram o círculo de idéias conhecido por "princípio local-global".

A idéia básica parece ser devida, outra vez, a Hensel, mas foi Hasse que a formulou claramente: cada $\mathbf{Q}_p$ dá informações "localmente em p", e $\mathbf{R}$ dá informações "localmente no ∞"; juntando todas essas informações, deve ser possível obter informações "globais", isto é, em $\mathbf{Q}$. Um exemplo simplório é:

Exercício 44 *Seja $x \in \mathbf{Q}$. Mostre que se, para todo p, tivermos $x \in \mathbf{Z}_p$, então $x \in \mathbf{Z}$.*

A coisa fica mais interessante para as equações diofantinas. Tomemos, por exemplo, a equação

$$X^2 - Y^2 + Z^2 = 0.$$

É claro que esta equação tem uma solução não-trivial em $\mathbf{Q}$, e portanto em $\mathbf{Q}_p$ para todo $p \leq \infty$. A pergunta natural é se algum tipo de recíproca é verdade.

O que uma recíproca significaria é que quando não houver solução em $\mathbf{Q}$ este fato poderia ser detetado examinando as soluções em algum $\mathbf{Q}_p$. Dado o Lema de Hensel isto significaria que a ausência de soluções deveria ser visível por argumentos de congruências (para os $\mathbf{Q}_p$ com $p < \infty$) ou por argumentos de sinal (para $\mathbf{R}$). Experimentalmente, isto é bastante plausível:

i) $X^2 + Y^2 + Z^2 = 0$ não tem soluções não-triviais em $\mathbf{R}$;

ii) $3X^2 + 2Y^2 - Z^2 = 0$ não tem soluções não-triviais em $\mathbf{Q}_3$ (verifique!);

iii) $X^2 - 3Y^2$ não tem soluções em $\mathbf{Q}_7$ (verifique!).

Isto sugere o seguinte:

Princípio Local-Global: *A existência ou não de soluções em $\mathbf{Q}$ de uma equação diofantina pode ser decidida a partir do estudo, para todo $p \leq \infty$, das soluções em $\mathbf{Q}_p$ da equação.*

É claro que este enunciado é vago demais para ser um "teorema", e o fato é que nesta generalidade ele é provavelmente falso. Apesar disso, o princípio local-global (interpretado de modo amplo) tem servido de guia para o estudo das equações diofantinas durante todo este século.

A versão mais simples de uma forma concreta do princípio seria a afirmação de que uma equação tem soluções em $\mathbf{Q}$ se e somente se tiver soluções em $\mathbf{Q}_p$ para todo p. Infelizmente, é perfeitamente possível que uma equação tenha soluções localmente para todo p (às vezes se diz "localmente em toda parte") sem que essas soluções locais possam ser "coladas" para produzir uma solução global. Por exemplo:

Exercício 45 *Mostre que a equação*

$$(X^2-2)(X^2-17)(X^2-34)=0$$

tem uma raiz em $\mathbf{Q}_p$ *para todo* $p \leq \infty$, *mas não tem nenhuma raiz em* $\mathbf{Q}$.

Exercício 46 *Decida se é verdade que um polinômio com coeficientes em* $\mathbf{Z}$ *é irredutível em* $\mathbf{Q}[X]$ *se e só se ele for irredutível em* $\mathbf{Q}_p[X]$ *para todo* $p \leq \infty$.

Exercício 47 *(Difícil) Mostre que* $X^4-17=2Y^2$ *soluções localmente em toda parte, mas não tem soluções em* $\mathbf{Q}$.

Apesar desses contra-exemplos, existem também exemplos bem-sucedidos:

Teorema 3.5.1 (Hasse-Minkowsky) *Seja*

$$F(X_1, X_2, \ldots X_n) \in \mathbf{Q}[X_1, X_2, \ldots X_n]$$

uma forma quadrática (isto é, um polinômio homogêneo de grau 2). A equação

$$F(X_1, X_2, \ldots X_n)=0$$

terá soluções não-triviais em $\mathbf{Q}$ *se e só se tiver soluções não-triviais em* $\mathbf{Q}_p$ *para todo* $p \leq \infty$.

Para uma demonstração, e mais detalhes, veja [11]. Deve-se notar que este teorema resolve completamente o problema de se determinar zeros não-triviais de formas quadráticas sobre $\mathbf{Q}$, porque é fácil mostrar que existe um algoritmo (simples) para decidir se existem soluções locais.

Mesmo em casos em que esta forma forte do princípio local-global é falsa, a idéia básica de que juntando dados locais "em toda parte" se obtêm dados globais continua muito útil. Um exemplo é a Conjetura de Birch e Swinnerton-Dyer sobre curvas elípticas, que diz, sob esta ótica, que a "quantidade" de soluções globais pode ser determinada a partir de informações locais. Assim, o princípio local-global permanece uma das motivações mais fortes para o estudo dos corpos p-ádicos.

Capítulo 4

Análise Elementar em $\mathbf{Q}_p$

O objetivo deste capítulo é examinar que forma tomam os princípios básicos da análise em $\mathbf{Q}_p$. Como $\mathbf{Q}_p$ é um corpo munido de um valor absoluto e é completo em relação à métrica induzida, a análise em $\mathbf{Q}_p$ deve ter uma forte analogia com a análise real. Mais precisamente, todos os resultados teóricos da análise real que não envolvam arquimedianidade, ordem, ou propriedades de conexão devem permanecer verdadeiros sobre $\mathbf{Q}_p$, já que a desigualdade ultramétrica implica a desigualdade triangular. Além disso, vale notar que tanto $\mathbf{Q}_p$ quanto $\mathbf{R}$ são localmente compactos, e nenhum dos dois é algebricamente fechado, o que reforça a analogia. Apesar disso, há diferenças importantes vindas da não-arquimedianidade.

4.1 Seqüências e séries

Nós já notamos, ao construir $\mathbf{Q}_p$, que o critério de Cauchy para a convergência de seqüências toma uma forma mais simples para valores absolutos não-arquimedianos. Vamos repetir o enunciado aqui:

Lema 4.1.1 *Seja (a_n) uma seqüência em $\mathbf{Q}_p$. A seqüência (a_n) é de Cauchy (e portanto convergente) se e só se*

$$\lim_{n\to\infty} |a_{n+1} - a_n| = 0.$$

DEMONSTRAÇÃO: É o Lema 3.2.1, cuja demonstração visivelmente só depende da não-arquimedianidade do valor absoluto. □

Segue um critério simples para a convergência de séries (que já vimos implicitamente acima):

Corolário 4.1.2 *Uma série* $\sum_{n=0}^{\infty} a_n$ *em* $\mathbf{Q}_p$ *converge se e só se* $a_n \to 0$, *e neste caso*

$$\left|\sum_{n=0}^{\infty} a_n\right| \leq \max_n |a_n|.$$

DEMONSTRAÇÃO: A convergência é clara, já que a_n é a diferença de duas somas parciais sucessivas. A estimativa para o valor absoluto segue imediatamente da não-arquimedianidade (ou usando o fato de que o valor absoluto de uma seqüência se estabiliza). □

Assim, é muito mais fácil decidir a convergência ou não de uma série em $\mathbf{Q}_p$ do que em $\mathbf{R}$. Isto é, até certo ponto, sempre assim: a teoria de séries sobre corpos completos não-arquimedianos é bastante simples. Um outro exemplo disto é o problema de reordenação de séries, que tratamos na próxima proposição.

Proposição 4.1.3 *Sejam* $b_{ij} \in \mathbf{Q}_p$, *e suponha que dado* $\varepsilon > 0$ *exista* $\mathrm{N} = \mathrm{N}(\varepsilon)$ *tal que*

$$\max(i, j) \geq \mathrm{N} \Longrightarrow |b_{ij}| < \varepsilon.$$

Então ambas as séries

$$\sum_i \left(\sum_j b_{ij}\right) \quad e \quad \sum_j \left(\sum_i b_{ij}\right)$$

convergem, e têm a mesma soma.

DEMONSTRAÇÃO: É imediato que as somas internas

$$\sum_j b_{ij} \quad \text{e} \quad \sum_i b_{ij}$$

convergem (no primeiro caso, para todo i, no segundo, para todo j). Além disso, se $i \geq \mathrm{N}$, temos

$$\left|\sum_j b_{ij}\right| \leq \max_j |b_{ij}| < \varepsilon;$$

analogamente, se $j \geq \mathrm{N}$, temos

$$\left|\sum_i b_{ij}\right| < \varepsilon,$$

Em particular, ambas as somas duplas convergem. Finalmente,

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{i=0}^{\mathrm{N}}\left(\sum_{j=0}^{\mathrm{N}} b_{ij}\right)\right| = \left|\sum_{i=0}^{\mathrm{N}}\left(\sum_{j=\mathrm{N}+1}^{\infty} b_{ij}\right) + \sum_{i=\mathrm{N}+1}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right| < \varepsilon,$$

donde as somas são iguais. □

Exercício 48 *Prove que se* $a = \sum a_n$, $b = \sum b_n$ *e*

$$c_n = \sum_{i=0}^{n} a_i b_{n-i},$$

então $\sum c_n$ *é convergente e tem soma* ab.

4.2 Séries de potências

Da mesma forma que em análise real, as séries de potências são uma maneira cômoda de se definir as funções elementares. Como se esperaria, a teoria p-ádica é análoga à teoria real, mas mais simples em vários pontos.

Consideremos uma série de potências

$$f(X) = \sum_{n=0}^{\infty} a_n X^n.$$

Para cada $x \in \mathbf{Q}_p$, já sabemos que $f(x)$ converge se e só se $|a_n x^n| \to 0$. Como no caso clássico, o domínio de convergência é um disco:

Proposição 4.2.1 *Seja* $f(X) = \sum_{n=0}^{\infty} a_n X^n$, *e definamos*

$$\rho = \frac{1}{\limsup \sqrt[n]{|a_n|}},$$

de modo que $0 \leq \rho \leq \infty$.

i) Se $\rho = 0$, $f(x)$ *converge apenas para* $x = 0$.

ii) *Se* $\rho = \infty$, $f(x)$ *converge para todo* $x \in \mathbf{Q}_p$.

iii) *Se* $0 < \rho < \infty$ *e* $|a_n|\rho^n \to 0$ *quando* $n \to \infty$, *então* $f(x)$ *converge se e só se* $|x| \leq \rho$.

iv) *Se* $0 < \rho < \infty$ *e* $|a_n|\rho^n$ *não tende a zero, então* $f(x)$ *converge se o só se* $|x| < \rho$.

DEMONSTRAÇÃO: A região de convergência é

$$\{x \in \mathbf{Q}_p : |a_n x^n| \to 0\}.$$

O resultado então segue imediatamente. □

Como no caso arquimediano, ρ é chamado o *raio de convergência* da série. Note que, ao contrário da situação clássica, os pontos do "bordo" da região de convergência têm todos o mesmo comportamento.

Lema 4.2.2 *Seja* $f(X) = \sum a_n X^n$ *uma série de potências com coeficientes em* $\mathbf{Q}_p$, *e seja* $\mathcal{D} \subset \mathbf{Q}_p$ *sua região de convergência. A função*

$$f : \mathcal{D} \to \mathbf{Q}_p$$

definida por $x \mapsto f(x)$ *é contínua em* $\mathcal{D}$.

DEMONSTRAÇÃO: Idêntico ao caso arquimediano. □

Como no caso clássico, é possível mudar o centro da expansão em série, isto é, considerar séries "em torno de α", onde α é um ponto qualquer da região de convergência. Surpreendentemente, no nosso caso isto não traz novidade:

Proposição 4.2.3 *Seja* $f(X) = \sum a_n X^n$ *uma série de potências com coeficientes em* $\mathbf{Q}_p$, *e seja* $\alpha \in \mathbf{Q}_p$ *um ponto tal que* $f(\alpha)$ *converge. Para cada* $m \geq 0$, *defina*

$$b_m = \sum_{n \geq m} \binom{n}{m} a_n \alpha^{n-m},$$

e considere a série de potências

$$g(X) = \sum_{m=0}^{\infty} b_m X^m.$$

i) A série que define b_m converge para todo m.

ii) As séries de potências $f(X)$ e $g(X)$ têm a mesma região de convergência, isto é, $f(\lambda)$ converge se e só se $g(\lambda)$ converge.

iii) Para todo λ na região de convergência, temos $g(\lambda) = f(\alpha + \lambda)$.

DEMONSTRAÇÃO: A afirmação *(i)* é clara, já que α pertence à região de convergência de $f(x)$, de modo que

$$\left|\binom{n}{m} a_n \alpha^{n-m}\right| \leq |a_n \alpha^{n-m}| = |\alpha|^{-m} \cdot |a_n \alpha^n| \to 0.$$

Para ver *(ii)* e *(iii)*, note que se λ pertence à região de convergência de $f(X)$, então $\alpha + \lambda$ também pertence, donde

$$f(\alpha + \lambda) = \sum_n a_n (\alpha + \lambda)^n = \sum_n \sum_{m \leq n} \binom{n}{m} a_n \alpha^{n-m} \lambda^m,$$

e basta aplicar a Proposição 4.1.3 para ver que $g(\lambda)$ converge e é igual a $f(\alpha + \lambda)$. Trocando os papéis de g e f, segue que as regiões de convergência são de fato iguais, e conclui a demonstração. □

Note que uma das coisas de este resultado indica é que o método clássico de "continuação analítica" não funciona no nosso contexto, já que mudar o centro nunca altera a região de convergência. Apesar disso, é possível construir uma teoria de "funções analíticas" sobre corpos não-arquimedianos com propriedades análogas às clássicas: trata-se da "geometria analítica rígida" de Tate, cujo desenvolvimento é infelizmente muito técnico para ser discutido aqui (veja por exemplo [4]).

O próximo resultado tem um papel central na teoria das funções definidas por séries de potências.

Teorema 4.2.4 (Strassman) *Seja $f(X) = \sum_{n=0}^{\infty} a_n X^n$ uma série de potências não-nula com coeficientes em $\mathbf{Q}_p$, e suponha que tenhamos $a_n \to 0$ quando $n \to \infty$, de modo que $f(x)$ converge para todo $x \in \mathbf{Z}_p$. Defina um inteiro positivo* N *pondo*

$$|a_N| = \max_n |a_n|$$
$$|a_n| < |a_N| \quad \text{se } n > N$$

Então a função $f : \mathbf{Z}_p \longrightarrow \mathbf{Q}_p$ *definida por* $f(X)$ *tem no máximo* N *zeros.*

Note que o número N existe porque temos $|a_n| \to 0$ por hipótese. Este resultado costuma ser demonstrado através do "Teorema de Preparação de Weierstrass p-ádico"; em vez disso, damos uma demonstração direta (seguindo Cassels em [5]).

DEMONSTRAÇÃO: Usamos indução em N.

a) Se $\mathrm{N} = 0$, temos $|a_0| > |a_n|$ para todo $n \geq 1$, e queremos provar que $f(x) \neq 0$ para todo $x \in \mathbf{Z}_p$. De fato, se $f(x) = 0$, teríamos

$$0 = f(x) = a_0 + a_1 x + a_2 x^2 + \cdots,$$

donde

$$\begin{aligned} |a_0| &= |a_1 x + a_2 x^2 + \cdots| \\ &\leq \max_{n \geq 1} |a_n x^n| \\ &\leq \max_{n \geq 1} |a_n|, \end{aligned}$$

o que contradiz $|a_0| > |a_n|$.

b) Para o caso geral, usamos essencialmente uma expansão de Taylor. Suponha que

$$\begin{aligned} |a_{\mathrm{N}}| &= \max_n |a_n| \\ |a_n| &< |a_{\mathrm{N}}| \quad \text{se } n > \mathrm{N} \end{aligned}$$

e suponha ainda que $f(\alpha) = 0$ para algum $\alpha \in \mathbf{Z}_p$. Escolha $x \in \mathbf{Z}_p$ qualquer. Então

$$\begin{aligned} f(x) &= f(x) - f(\alpha) = \sum_{n \geq 1} a_n (x^n - \alpha^n) \\ &= (x - \alpha) \sum_{n \geq 1} \sum_{j < n} a_n x^j \alpha^{n-1-j}. \end{aligned}$$

Pela Proposição 4.1.3, podemos reordenar em potências de x, obtendo

$$f(x) = (x - \alpha) \sum_{n=0}^{\infty} b_j x^j,$$

onde

$$b_j = \sum_{k \geq 0} a_{j+1+k} \alpha^k.$$

Agora, note que

$$|b_j| \leq \max_{k\geq 0} |a_{j+1+k}| \leq |a_N|$$

$$|b_{N-1}| = |a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \cdots| = |a_N|$$

e, se $j \geq N$,

$$|b_j| \leq \max_{k\geq 0} |a_{j+k+1}| \leq \max_{j\geq N+1} |a_j| < |a_N|.$$

Assim, $g(X)$ satisfaz as condições do teorema para $N-1$. Por indução, $g(X)$ tem no máximo $N-1$ zeros em $\mathbf{Z}_p$, donde $f(X)$ tem no máximo N zeros, como queríamos. □

Este resultado tem vários corolários importantes. Começamos destacando um corolário da demonstração:

Corolário 4.2.5 *Seja $f(X) = \sum a_n X^n$ uma série de potências convergente em $\mathbf{Z}_p$, e sejam $\alpha_1, \ldots, \alpha_m$ os zeros de $f(X)$ em $\mathbf{Z}_p$. Então*

$$f(X) = (X - \alpha_1)\cdots(X - \alpha_m)g(X),$$

onde $g(X)$ é uma série de potências convergente em $\mathbf{Z}_p$ que não possui zeros em $\mathbf{Z}_p$.

DEMONSTRAÇÃO: Claro. □

É claro que, como $\mathbf{Z}_p$ é simplesmente o disco unitário em $\mathbf{Q}_p$, basta uma alteração de escala para estender o resultado a outros discos.

Corolário 4.2.6 *Seja $f(X) = \sum a_n X^n$ uma série de potências convergente em $p^m\mathbf{Z}_p$ para algum $m \in \mathbf{Z}$. Então $f(X)$ tem um número finito de zeros em $p^m\mathbf{Z}_p$.*

DEMONSTRAÇÃO: Considere $g(X) = f(p^m X) = \sum a_n p^{mn} X^n$. Por hipótese, $g(x)$ converge se $x \in \mathbf{Z}_p$, e basta aplicar o Teorema a $g(X)$ para concluir. □

Corolário 4.2.7 *Sejam $f(X) = \sum a_n X^n$ e $g(X) = \sum b_n X^n$ séries de potências convergentes em algum disco $p^m\mathbf{Z}_p$. Se existirem infinitos $\alpha \in p^m\mathbf{Z}_p$ tais que $f(\alpha) = g(\alpha)$, então $a_n = b_n$ para todo $n \geq 0$.*

DEMONSTRAÇÃO: Aplique o teorema a $f - g$.□

Corolário 4.2.8 *Seja $f(X) = \sum a_n X^n$ uma série de potências convergente em algum disco $p^m\mathbf{Z}_p$. Se a função definida por $f(X)$ for periódica, isto é, se existir $\pi \in p^m\mathbf{Z}_p$ tal que $f(x + \pi) = f(x)$ para todo $x \in p^m\mathbf{Z}_p$, então $f(X)$ é constante.*

DEMONSTRAÇÃO: A série $f(X) - f(0)$ se anula em $n\pi \in p^m\mathbf{Z}_p$ para todo $n \in \mathbf{Z}$. □

Corolário 4.2.9 *Seja $f(X) = \sum a_n X^n$, e suponha que $f(X)$ é inteira, isto é, que tenha raio de convergência infinito. Então $f(X)$ tem no máximo um conjunto enumeraável de zeros. Além disso, se o conjunto de zeros de $f(X)$ for infinito, então eles formam uma seqüência α_n com $|\alpha_n| \to \infty$.*

DEMONSTRAÇÃO: O múmero de zeros em cada $p^m\mathbf{Z}_p$ é finito. □

É natural (e tentador) conjeturar a partir destes resultados que deve existir uma representação de uma função inteira como um produto infinito; algo como

$$f(X) = h(X)\prod(1 - \alpha^{-1}X),$$

onde os α_n são os zeros de $f(X)$ e onde $h(X)$ não tem nenhum zero. É imediato que uma representação deste tipo de fato existe, mas o caso dos polinômios já mostra que ela só será interessante se passarmos ao *fecho algébrico* de $\mathbf{Q}_p$. Isto introduz uma dificuldade séria: ao contrário do que acontece no caso de $\mathbf{R}$, o fecho algébrico de $\mathbf{Q}_p$ *não é completo* em relação à topologia p-ádica, de modo que é preciso um novo completamento. Assim, o análogo p-ádico de $\mathbf{C}$ é o completamento de um fecho algébrico de $\mathbf{Q}_p$, que é normalmente denotado por

$\mathbf{C}_p$. O corpo $\mathbf{C}_p$ é o contexto "natural" para a análise p-ádica mais avançada; nestas notas, entretanto, vamos "insistir no erro" e trabalhar sempre só com $\mathbf{Q}_p$.

Exercício 49 *Ache o raio de convergência das seguintes séries de potências:*

i) $\sum n!X^n$

ii) $\sum p^n X^n$

iii) $\sum p^{-n} X^n$

Exercício 50 *O que pode ser dito quanto aos zeros das funções definidas pelas séries de potências do exercício anterior?*

4.3 Algumas Funções Elementares

Vamos agora usar séries de potências para definir funções p-ádicas. Começamos, é claro, pela exponencial e o logaritmo p-ádicos. Ao contrário do caso arquimediano, é o logaritmo que tem as propriedades mais simples.

Começamos com a série clássica:

$$f(X) = \log(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} + \cdots$$

(Usamos a notação log—e não log—para enfatizar que estamos considerando a série formal, e não a função.) Como os coeficientes são racionais, $f(X)$ faz sentido como série de potências sobre $\mathbf{Q}_p$. Vamos calcular o seu raio de convergência; note que no caso p-ádico ter inteiros no denominador não é tão bom quanto em $\mathbf{R}$, já que $1/n$ é *grande* p-adicamente quando n for muito divisível por p. Por outro lado, a "maioria" dos n não são muito divisíveis por p.

Se $f(X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}$, temos

$$|a_n| = \left|\frac{1}{n}\right| = p^{v_p(n)},$$

de modo que

$$\sqrt[n]{|a_n|} = p^{v_p(n)/n} \to 1$$

quando $n \to \infty$; logo, $\rho = 1$. Para o caso em que $|x| = 1$, é fácil ver que o termo geral não tende a zero. Logo, provamos:

Lema 4.3.1 *A série* $f(X) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n}$ *converge para* $|x| < 1$.

Assim, $f(X)$ define uma função na bola "aberta" $B(0,1)$ de raio 1 em trono do zero. É natural então definir:

Definição 16 *Seja* $B = B(1,1) = \{x \in \mathbf{Z}_p : |x-1| < 1\} = 1 + p\mathbf{Z}_p$. *O logaritmo p-ádico é a função* $\log_p : B \longrightarrow \mathbf{Q}_p$ *definida por*

$$\log_p(x) = \log(1 + (x-1)) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{(x-1)^n}{n}.$$

Vale notar que a propriedade fundamental do logaritmo,

$$\log(1+X) + \log(1+Y) = \log(1 + X + Y + XY),$$

é uma igualdade formal de séries de potências. Logo, se tomarmos $x, y \in 1 + p\mathbf{Z}_p$, teremos

$$\log_p x + \log_p y = \log_p(xy),$$

exatamente como na situação clássica.

OBSERVAÇÃO: Talvez seja melhor explicitar o argumento. A igualdade formal

$$\log(1+X) + \log(1+Y) = \log((1+X)(1+Y))$$

significa que se escrevermos

$$F(X,Y) = \sum(-1)^{n+1}\left[\frac{(X+Y+XY)^n}{n} - \frac{X^n}{n} - \frac{Y^n}{n}\right] = \sum_{n,m} c_{n,m}X^nY^m,$$

então teremos $c_{m,n} = 0$ para cada m, n. Se agora $\alpha, \beta \in p\mathbf{Z}_p$, temos, pela Proposição 4.1.3,

$$\log_p((1+\alpha)(1+\beta)) - \log_p(1+\alpha) - \log_p(1+\beta) = \sum c_{n,m}\alpha^n\beta^m = 0,$$

donde a conclusão. Note que é essencial algum reordenamento de séries.

Exercício 51 *Mostre que se* $p = 2$, *então* $-1 \in B$ *e* $\log_p(-1) = 0$. *Compare o exemplo da seção 3 do Capítulo 1. Obtenha uma estimativa para a maior potência de* 2 *que divide uma soma parcial.*

Exercício 52 *Use o Teorema de Strassman para mostrar que se* $p \neq 2$ *teremos* $\log_p(x) = 0$ *se e só se* $x = 1$, *e que se* $p = 2$ *teremos* $\log_p(x) = 0$ *se e só se* $x = \pm 1$.

Exercício 53 *Seja* $p \neq 2$, *e considere* $x \in \mathbf{Q}_p$ *tal que* $x^p = 1$. *Use o logaritmo p-ádico para mostrar que se* $x \in 1 + p\mathbf{Z}_p$, *então* $x = 1$. *Conclua que* $\mathbf{Q}_p$ *não contém nenhuma raiz p-ésima primitiva da unidade.*

Exercício 54 *Faça o análogo do exercício anterior para* $p = 2$ *e raízes quartas da unidade.*

Já vimos que o logaritmo p-ádico tem propriedades análogas às do logaritmo clássico. Passemos agora à exponencial. Classicamente, a série

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \cdots$$

converge para todo $x \in \mathbf{R}$, porque os coeficientes $1/n!$ tendem a zero muito rapidamente. É claro que no nosso contexto a coisa se complica, porque $n!$ vai ficando cada vez mais divisível por p quando n cresce, de modo que em $\mathbf{Q}_p$ $1/n! \to \infty$ quando $n \to \infty$. O primeiro passo é determinar a rapidez do crescimento desta seqüência, isto é, determinar exatamente o quanto $n!$ é divisível por p.

Lema 4.3.2 *Para um primo p qualquer, temos*

$$v_p(n!) = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor < \frac{n}{p-1},$$

onde $\lfloor \cdot \rfloor$ *é a função parte inteira.*

DEMONSTRAÇÃO: A fórmula

$$v_p(n!) = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

é clássica e elementar; deixâmo-la como exercício para o leitor interessado. A desigualdade segue imediatamente de $\lfloor x \rfloor \leq x$. □

Exercício 55 *Prove a fórmula*

$$v_p(n!) = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Exercício 56 *Seja n um inteiro positivo e $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$ sua expansão em base p. Seja $s = a_0 + a_1 + \cdots + a_k$ a soma dos dígitos da expansão. Mostre que*

$$v_p(n!) = \frac{n-s}{p-1}.$$

Agora podemos provar

Lema 4.3.3 *Seja $g(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$. Então $g(x)$ converge se e só se*

$$|x| < p^{-1/(p-1)}.$$

DEMONSTRAÇÃO: Como

$$|a_n| = |1/n!| = p^{v_p(n!)} < p^{n/(p-1)},$$

temos de imediato que

$$\rho \geq p^{-1/(p-1)}.$$

Logo, a série converge para $|x| < p^{-1/(p-1)}$.

Por outro lado, se $|x| = p^{-1/(p-1)}$ e $n = p^m$, temos

$$v_p(n!) = v_p(p^m!) = 1 + p + \cdots + p^{m-1} = \frac{p^m - 1}{p-1},$$

donde (lembre que $v_p(x) = 1/(p-1)$)

$$v_p(\frac{x^n}{n!}) = v_p(\frac{x^{p^m}}{p^m!}) = \frac{p^m}{p-1} - \frac{p^m-1}{p-1} = \frac{1}{p-1},$$

donde $x^n/n!$ não tende a zero, e o lema segue. □

OBSERVAÇÃO: O leitor atento terá notado que para $p \neq 2$ e $x \in \mathbf{Z}_p$ temos

$$|x| < p^{-1/(p-1)} \Longleftrightarrow |x| \leq p^{-1} \Longleftrightarrow x \in p\mathbf{Z}_p \Longleftrightarrow |x| < 1,$$

de modo que para $p \neq 2$ a exponencial converge no disco aberto de raio 1 em $\mathbf{Z}_p$. Parece, então, que todo o cuidado acima para achar o raio correto de convergência é inútil e pedante.

Na realidade, vale a pena enfatizar o raio correto de convergência, porque os resultados que estamos obtendo valem em geral, inclusive sobre o fecho algébrico de $\mathbf{Q}_p$, onde de fato existem elementos com

$$p^{-1/(p-1)} \leq |x| < 1.$$

De qualquer forma vale notar que, em $\mathbf{Z}_p$, temos:

- para $p \neq 2$, $g(x) = \exp(x)$ converge para $x \in p\mathbf{Z}_p$,
- para $p = 2$, $g(x) = \exp(x)$ converge para $x \in 4\mathbf{Z}_2$,

já que $-1/(2-1) = -1$.

Definição 17 *Seja* $D = B(0, p^{-1/(p-1)}) = \{x \in \mathbf{Z}_p : |x| < p^{-1/(p-1)}\}$. *A exponencial p-ádica é a função* $\exp_p : D \longrightarrow \mathbf{Q}_p$ *definida por*

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Como no caso do logaritmo, a propriedade formal da exponencial se preserva: se $x, y \in D$ temos $x + y \in D$ e

$$\exp_p(x + y) = \exp_p(x) \exp_p(y).$$

Outra propriedade formal de séries de potências que nós gostaríamos fosse preservada no caso p-ádico é a relação

$$\exp(\log(1 + X)) = 1 + X.$$

A versão p-ádica requer apenas um pouco de cuidado com as regiões de convergência.

Proposição 4.3.4 *Seja* $x \in \mathbf{Z}_p$, *com* $|x| < p^{-1/(p-1)}$. *Então temos*

$$|\exp_p(x) - 1| < 1$$

e

$$\log_p(\exp_p(x)) = x.$$

Além disso, ainda sob a condição $|x| < p^{-1/(p-1)}$, *temos ainda*

$$|\log_p(1 + x)| < p^{-1/(p-1)}$$

e também

$$\exp_p(\log_p(1+x)) = 1+x.$$

DEMONSTRAÇÃO: Vamos verificar as estimativas; as igualdades seguem, dadas as estimativas, de relações formais entre séries e da Proposição 4.1.3, como acima.

A primeira estimativa é fácil: se $|x| < p^{-1/(p-1)}$, temos

$$\exp_p(x) = 1 + \sum_{n=1}^{\infty} \frac{X^n}{n!}$$

e

$$\left|\frac{x^n}{n!}\right| < p^{-n/(p-1)} \cdot p^{v_p(n!)} < 1,$$

donde

$$|\exp_p(x) - 1| < 1,$$

como queríamos.

Para a segunda estimativa, seja $|x| < p^{-1/(p-1)}$. Temos

$$\left|\frac{x^n}{n}\right| < p^{-n/(p-1)} \cdot p^{v_p(n)},$$

de modo que queremos provar que

$$v_p(n) - \frac{n}{p-1} \leq \frac{-1}{p-1};$$

isto é um exercício fácil que deixamos ao leitor. □

Exercício 57 *Prove que para qualquer $n \geq 1$, temos*

$$v_p(n) - \frac{n}{p-1} \leq \frac{-1}{p-1}.$$

(Sugestão: mostre que o maior valor possível ocorre quando $n = 1$ ou quando $n = p$.)

Vale enfatizar que:

- se $|x| < 1$ mas $|x| \geq p^{-1/(p-1)}$, pode bem ser que $\log_p(1+x)$ não pertença ao domínio da exponencial (ache um exemplo para $p = 2$);

- ainda pior, se $|x| < 1$ mas $|x| \geq p^{-1/(p-1)}$, pode acontecer que

$$|\log_p(1+x)| < p^{-1/(p-1)}$$

mas

$$\exp_p(\log_p(1+x)) \neq 1+x.$$

O exemplo mais imediato desta dificuldade é $p = 2$, $x = -2$, quando $\log_p(1+x) = \log_p(-1) = 0$, donde

$$\exp_p(\log_p(-1)) = 1 \neq -1.$$

Exercício 58 *Explique por que este último exemplo não contradiz o argumento feito acima acerca de identidades formais de séries de potências. O que é que não dá certo neste caso?*

Exercício 59 *Siga o modelo acima para definir funções p-ádicas análogas ao seno e ao cosseno, e determine suas regiões de convergência. Mostre que se* $p \equiv 1 \pmod 4$ *e* $i^2 = -1$ *em* $\mathbf{Q}_p$, *então*

$$\exp_p(ix) = \cos_p(x) + i\,\mathrm{sen}_p(x)$$

para x *na região comum de convergência das funções em questão.*

Vamos usar estes resultados sobre o logaritmo e a exponencial p-ádicos para entender melhor a estrutura do grupo $\mathbf{Z}_p^\times$ das unidades p-ádicas. Para simplificar, vamos introduzir um parâmetro q definido da seguinte forma:

- se p é um primo ímpar, pomos $q = p$;
- se $p = 2$, pomos $q = 4$.

Dessa forma, $\exp_p(x)$ está definido se $x \in q\mathbf{Z}_p$ e $\log_p(x)$ está definido se $x \in 1 + p\mathbf{Z}_p$. Sejam

$$\mathrm{U} = \{x \in \mathbf{Z}_p^\times : |x-1| < 1\} = 1 + p\mathbf{Z}_p$$

$$\mathrm{U}_1 = \{x \in \mathbf{Z}_p^\times : |x-1| < p^{-1/(p-1)}\} = 1 + q\mathbf{Z}_p.$$

Note que temos $\mathrm{U}_1 \subset \mathrm{U} \subset \mathbf{Z}_p^\times$, que $\mathrm{U} = \mathrm{U}_1$ se $p \neq 2$, e que U e U_1 são *subgrupos* de $\mathbf{Z}_p^\times$.

Proposição 4.3.5 *Sejam* U *e* U_1 *como acima, e seja*

$$W = \{x \in \mathbf{Z}_p : |x| < p^{-1/(p-1)}\} = q\mathbf{Z}_p,$$

pensado como grupo aditivo.

i) A função $\log_p$ *define um homomorfismo de grupos*

$$\log_p : \mathrm{U} \longrightarrow \mathbf{Z}_p^+,$$

com imagem contida no ideal de valorização $\wp = p\mathbf{Z}_p$.

ii) A função $\log_p$ *define um isomorfismo de grupos*

$$\log_p : \mathrm{U}_1 \xrightarrow{\sim} W,$$

com inversa $\exp_p$. *Em particular,* $\mathrm{U}_1 \cong W \cong \mathbf{Z}_p^+$ *é livre de torsão.*

DEMONSTRAÇÃO: Basta traduzir os resultados acima. □

Agora é fácil descrever a estrutura de $\mathbf{Z}_p^\times$:

Corolário 4.3.6 *Para todo p, temos que* $\mathbf{Z}_p^\times \cong V \times \mathrm{U}_1$, *onde*

i) V é o subgrupo de torsão de $\mathbf{Z}_p^\times$, *e* $V = (\mathbf{Z}/q\mathbf{Z})^\times$, *e portanto é cíclico de ordem* $\varphi(q)$;

ii) $\mathrm{U}_1 \cong \mathbf{Z}_p^+$ *é um pró-p-grupo livre de torsão.*

DEMONSTRAÇÃO: Os resultados que já obtivemos mostram que existe um seqüência exata

$$1 \longrightarrow \mathrm{U}_1 \longrightarrow \mathbf{Z}_p^\times \longrightarrow (\mathbf{Z}/q\mathbf{Z})^\times \longrightarrow 0.$$

É imediato que a seqüência cinde se $p = 2$, já que nesse caso $(\mathbf{Z}/q\mathbf{Z})^\times = \{\pm 1\}$. Para provar que a seqüência cinde quando $p \neq 2$, basta invocar o Lema de Hensel aplicado à equação $X^{p-1} - 1$. O resto segue imediatamente. □

Em particular, este corolário mostra que existe uma inclusão

$$\omega : \mathbf{F}_p^\times \cong V \hookrightarrow \mathbf{Z}_p^\times,$$

que estendemos a $\mathbf{F}_p$ pondo $\omega(0) = 0$. A função ω se chama *caráter de Teichmüller*; ela define um caráter de Dirichlet via

$$\mathbf{Z} \twoheadrightarrow \mathbf{F}_p \xrightarrow{\omega} \mathbf{Z}_p,$$

que é também denotado por ω. Completamos a confusão denotando também por ω a projeção $\omega : \mathbf{Z}_p^\times \longrightarrow V$. O conjunto $V \cup \{0\}$ é um conjunto de representantes para as classes módulo $p\mathbf{Z}_p$ (os "representantes de Teichmüller"), e portanto os elementos de V podem ser usados como coeficientes na expansão p-ádica; esta escolha é às vezes bastante conveniente.

Exercício 60 *Prove que se $p \neq 2$ e $x \in \mathbf{Z}_p^\times$, então*

$$\omega(x) = \lim_{n\to\infty} x^{p^n}.$$

É comum denotar o quociente $x/\omega(x) \in \mathrm{U}_1$ por $\langle x \rangle$, de modo que a decomposição em produto de $\mathbf{Z}_p^\times$ se reflete, a nível dos elementos, na equação

$$x = \omega(x)\langle x \rangle.$$

Para concluir nossa aventura pelas funções elementares p-ádicas, consideremos a série binomial; classicamente,

$$(1+X)^\alpha = \mathbf{B}(\alpha, X) = \sum_{n=0}^{\infty} \binom{\alpha}{n} X^n,$$

onde, é claro,

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\ldots(\alpha-n+1)}{n!}.$$

O comportamento da série no caso p-ádico depende de α. Vamos estudar o caso $\alpha \in \mathbf{Z}_p$, e deixar o outro caso (que é mais fácil!) ao leitor. Começamos notando que os coeficientes são inteiros p-ádicos.

Lema 4.3.7 *Se $\alpha \in \mathbf{Z}_p$ e $n \geq 0$, então $\binom{\alpha}{n} \in \mathbf{Z}_p$.*

DEMONSTRAÇÃO: Para cada n, considere o polinômio

$$P_n(X) = \frac{X(X-1)\dots(X-n+1)}{n!} \in \mathbf{Q}[X].$$

Ele define uma função contínua $P_n : \mathbf{Q}_p \longrightarrow \mathbf{Q}_p$, e já sabemos que se $\alpha \in \mathbf{Z}$,

$$P_n(\alpha) = \binom{\alpha}{n} \in \mathbf{Z}.$$

Como $\mathbf{Z}$ é denso em $\mathbf{Z}_p$, a conclusão segue. □

Corolário 4.3.8 *Se $\alpha \in \mathbf{Z}_p$ e $|x| < 1$, a série*

$$\mathbf{B}(\alpha, x) = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n$$

converge.

DEMONSTRAÇÃO: Claro. □

Como nos casos anteriores, segue de uma igualdade formal de séries de potências que se $\alpha = a/b \in \mathbf{Z}_{(p)}$ e $|x| < 1$ temos

$$(\mathbf{B}(\frac{a}{b}, x))^b = (1+x)^a.$$

Logo, faz sentido escrever

$$\mathbf{B}(\frac{a}{b}, x) = (1+x)^{a/b},$$

ou até *definir* para $\alpha \in \mathbf{Z}_p$ qualquer,

$$(1+x)^\alpha := \mathbf{B}(\alpha, x).$$

Deve-se tomar o cuidado, entretanto, de distinguir a função p-ádica $\mathbf{B}(a/b, x)$ da sua análoga real, mesmo quando $x \in \mathbf{Q}$.

EXEMPLO: (Seguindo Koblitz) Tome $p = 7$, $\alpha = 1/2$ e $x = 7/9$, de modo que $x \in 7\mathbf{Z}_7$ e $1 + x = 16/9$. Em $\mathbf{R}$, temos

$$(1+x)^{1/2} = \frac{4}{3}.$$

Em $\mathbf{Q}_7$, por outro lado, temos que $|x| = 1/7$, donde, se $n \geq 1$,

$$\left|\binom{1/2}{n} x^n\right| \leq |x|^n = \frac{1}{7^n} < 1,$$

de modo que

$$(1+x)^{1/2} = 1 + \sum_{n\geq 1} \binom{1/2}{n} x^n \in 1 + 7\mathbf{Z}_7.$$

Mas

$$\left|\frac{4}{3} - 1\right| = \left|\frac{1}{3}\right| = 1,$$

de modo que temos que ter (em $\mathbf{Q}_7$)

$$(1+7/9)^{1/2} = \mathbf{B}(\frac{1}{2}, \frac{7}{9}) = \frac{-4}{3} = 1 - \frac{7}{3}.$$

A questão é que uma mesma série $\sum a_n$ com $a_n \in \mathbf{Q}$ pode convergir tanto em $\mathbf{R}$ quanto em $\mathbf{Q}_p$, mas ter limites diferentes.

Apesar desta dificuldade, vamos escrever $(1+x)^\alpha$ em vez de $\mathbf{B}(\alpha, x)$, deixando que o contexto decida em que corpo estamos trabalhando.

Exercício 61 *Mostre que o valor de* $\mathbf{B}(\alpha, x)$ *não depende da métrica quando* $x \in \mathbf{Q}$ *e* $\alpha \in \mathbf{Z}$.

Exercício 62 (Koblitz) *Seja* $\alpha \in \mathbf{Q}$ *tal que* $1+\alpha$ *é um quadrado em* $\mathbf{Q}$*; digamos* $\sqrt{1+\alpha} = a/b$ *com* a *e* b *positivos e primos entre si. Seja* S *o conjunto de primos (inclusive o primo infinito, se for o caso) tais que a série binomial* $\mathbf{B}(1/2, \alpha)$ *converge em* $\mathbf{Q}_p$ *(para* a/b *ou para* $-a/b$*, é claro). Prove que:*

i) Se p *é um primo ímpar, então* $p \in S$ *se e só se* $p|(a+b)$ *ou* $p|(a-b)$*, e que teremos* $\mathbf{B}(1/2, \alpha) = -a/b$ *no primeiro caso,* $\mathbf{B}(1/2, \alpha) = a/b$ *no segundo.*

ii) Temos $2 \in S$ *se e só se* a *e* b *são ambos ímpares; o limite é* a/b *se* $a \equiv b \pmod 4$*,* $-a/b$ *se* $a \equiv -b \pmod 4$.

iii) Temos $\infty \in S$ *se e só se* $0 < a/b < \sqrt{2}$*, e a soma é sempre* a/b.

iv) Não existe nenhum α *para o qual* S *é vazio, e* S *tem um só elemento se e só se* $\alpha \in \{8, \frac{16}{9}, 3, \frac{5}{4}\}$.

v) Exceto pelos α citados no item anterior, sempre existem p, $q \in S$ tais que a soma em $\mathbf{Q}_p$ é diferente da soma em $\mathbf{Q}_q$.

Uma maneira divertida de entender a situação é pensar em α como a variável. Para um $n \in \mathbf{Z}_p$ qualquer e α um inteiro, podemos considerar a função

$$f(\alpha) = n^\alpha.$$

O problema de estender esta função para valores p-ádicos (mais precisamente, para o maior número possível de valores p-ádicos) se chama o *problema de interpolação p-ádica* da função $\alpha \mapsto n^\alpha$. O que mostramos, então, é que

Corolário 4.3.9 *Dado $n \in 1 + p\mathbf{Z}_p$, existe uma função contínua $f_n : \mathbf{Z}_p \longrightarrow \mathbf{Q}_p$ tal que quando $\alpha \in \mathbf{Z}$ temos $f_n(\alpha) = n^\alpha$.*

DEMONSTRAÇÃO: Definimos $f_n(\alpha) = \mathbf{B}(\alpha, n-1)$; a única coisa que falta verificar é a continuidade, que deixamos ao leitor. □

Exercício 63 *Mostre que $\mathbf{B}(\alpha, x)$ é contínua como função de α.*

Exercício 64 *Suponha que tenhamos uma função contínua $g : \mathbf{Z}_p \longrightarrow \mathbf{Q}_p$ tal que $g(\alpha) = n^\alpha$ para todo inteiro* positivo *α. Mostre que $g = f_n$. Idem se a relação a interpolar valer para inteiros negativos.*

Exercício 65 *Outra opção para interpolar $\alpha \mapsto n^\alpha$ seria definir*

$$n^\alpha = \exp_p(\alpha \log_p(n)).$$

Decida se isto funciona, e se define a mesma função f_n.

A condição $n \in 1 + p\mathbf{Z}_p$ é um tanto incômoda; seria desejável removê-la. Infelizmente, isto é um tanto difícil. Por exemplo, se $p|n$ teremos que $|n^\alpha|$ fica arbitrariamente pequeno quando $\alpha \to \infty$, de modo que a única "extensão" possível seria identicamente nula. Mas

mesmo a extensão para todo o grupo de unidades p-ádicas é complicada, basicamente por causa do subgrupo de torsão. (Exceto para $p = 2$, já que nesse caso $\mathbf{Z}_p^\times = 1 + 2\mathbf{Z}_2$, e não há extensão a fazer.)

Seja $p \neq 2$; vamos tentar interpolar a função $\alpha \mapsto n^\alpha$ para $n \in \mathbf{Z}_p^\times$ qualquer. Lembre, em primeiro lugar, que obtivemos uma decomposição

$$\mathbf{Z}_p^\times = V \times \mathrm{U}_1 \cong \mathbf{F}_p^\times \times (1 + p\mathbf{Z}_p),$$

e que para $x \in \mathbf{Z}_p^\times$ escrevemos $x = \omega(x)\langle x \rangle$ conforme essa decomposição. Para um inteiro qualquer α, temos

$$n^\alpha = \omega(n)^\alpha \langle n \rangle^\alpha.$$

Como $\omega(n)$ é uma raiz $(p-1)$-ésima da unidade, se $\alpha \equiv \alpha_0 \pmod{p-1}$ isto fica

$$n^\alpha = \omega(n)^{\alpha_0} \langle n \rangle^\alpha.$$

Agora, como $\langle n \rangle \in 1 + p\mathbf{Z}_p$, já sabemos interpolar a parte $\alpha \mapsto \langle n \rangle^\alpha$. Assim, a função p-ádica

$$f_{\alpha_0}(\alpha) = \omega(n)^{\alpha_0} \langle n \rangle^\alpha$$

coincide com (i.é interpola) a função $\alpha \mapsto n^\alpha$ restrita aos inteiros $\alpha \equiv \alpha_0 \pmod{p-1}$. Formalmente:

Proposição 4.3.10 *Sejam $n \in \mathbf{Z}_p^\times$ e $\alpha_0 \in \{0, 1, \ldots, p-1\}$, e seja*

$$A_{\alpha_0} = \{\alpha \in \mathbf{Z} : \alpha \equiv \alpha_0 \pmod{p-1}\} \subset \mathbf{Z}.$$

Então

$$f_{\alpha_0}(\alpha) = \omega(n)^{\alpha_0} \langle n \rangle^\alpha$$

define uma função $f_{\alpha_0} : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ tal que

$$f_{\alpha_0}(\alpha) = n^\alpha \qquad \text{se } \alpha \in A_{\alpha_0}.$$

Note que todas as funções f_{α_0} coincidem se $n \in 1 + p\mathbf{Z}_p$.

Os leitores que acharem esta situação um tanto insatisfatória talvez prefiram interpretá-la da seguinte forma: as funções f_{α_0} definem uma função

$$\mathcal{F} : \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z} \longrightarrow \mathbf{Z}_p$$

dada por $\mathcal{F}(\alpha, \alpha_0) = f_{\alpha_0}(\alpha)$. Considere, então, a inclusão diagonal

$$\mathbf{Z} \hookrightarrow \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}.$$

Se $\alpha \in \mathbf{Z}$, sua imagem pela inclusão é (α, α_0) onde $\alpha_0 \equiv \alpha \pmod{p-1}$, de modo que a restrição de $\mathcal{F}$ à imagem de $\mathbf{Z}$ é

$$\alpha \mapsto \mathcal{F}(\alpha, \alpha_0) = f_{\alpha_0}(\alpha) = \omega(n)^{\alpha_0}\langle n\rangle^{\alpha} = n^{\alpha}.$$

Assim, $\mathcal{F}$ dá uma interpolação da função $\alpha \mapsto n^{\alpha}$, desde que pensemos em $\mathbf{Z}$ como contido num conjunto maior que $\mathbf{Z}_p$.

Problemas de interpolação deste tipo são extremamente importantes nas aplicações da análise p-ádica à aritmética. Alguns exemplos serão esboçados no próximo capítulo.

Exercício 66 *Prove que* $2^{p-1} \equiv 1 \pmod{p^2}$ *se e só se* p *divide o numerador de*

$$\sum_{j=1}^{p-1} \frac{(-1)^j}{j}.$$

Exercício 67 *Prove que para todo inteiro positivo* k,

$$\sum_{n=0}^{\infty} n^k p^n \in \mathbf{Q}.$$

Exercício 68 *Mostre que a região de convergência da série* $g(X) = \sum n a_n X^{n-1}$ *está contida na região de convergência da série* $f(X) = \sum a_n X^n$. *Mostre que se definirmos a derivada de uma função em* $\mathbf{Q}_p$ *de modo análogo à definição sobre* $\mathbf{R}$, *então* $g(x) = f'(x)$ *para todo* x *na região de convergência de* f.

Exercício 69 *Dê um exemplo de uma função* $f : \mathbf{Q}_p \longrightarrow \mathbf{Q}_p$ *tal que, para todo* $a \in \mathbf{Q}_p$,

$$\lim_{x \to a} \frac{f(x) - f(a)}{x - a} = 0,$$

mas que não é localmente constante.

Capítulo 5

Envoi

Os primeiros passos estão dados. Não é nossa intenção ir mais fundo na teoria nestas notas. Queremos, entretanto, indicar ao leitor as possibilidades que lhe estão agora abertas dando alguma indicação dos rumos para onde vai a teoria a partir deste ponto. Este capítulo, então, contém apenas descrições informais, com referências, de algumas questões importantes que envolvem os números p-ádicos.

5.1 Extensões de $\mathbf{Q}_p$

A principal parte da teoria que foi completamente ignorada nestas notas é a passagem de $\mathbf{Q}_p$ para suas extensões finitas, e, paralelamente, a passagem da consideração de valores absolutos em $\mathbf{Q}$ para valores absolutos em extensões finitas de $\mathbf{Q}$. Esta passagem não envolve nenhuma dificuldade essencial, exceto pelo fato de que os primos de $\mathbf{Q}$ têm que ser substituídos pelos primos de uma extensão finita, o que nos força a estudar os problemas de decomposição de primos em extensões finitas. Este estudo se chama "teoria dos números algébricos"; de fato, boa parte dessa teoria pode ser desenvolvida em termos de valores absolutos e suas extensões de um corpo para um corpo maior. Para mais detalhes, veja [8], [1] ou [5]. A exposição de Serre em [12] trata com cuidado especial a questão da ramificação.

Um dos problemas centrais nesta teoria é o seguinte: dado um corpo completo não-arquimediano (digamos $\mathbf{Q}_p$, ou uma extensão finita), determinar todas as suas extensões

galoisianas finitas. Se nos restringirmos às extensões *abelianas*, este problema está completamente resolvido. A solução se chama "teoria de corpos de classe local"; uma exposição pode ser encontrada em [12].

A passagem de uma teoria de corpos de classes local para uma teoria global, isto é , para uma teoria que descreva as extensões abelianas de um corpo de números algébricos e como os primos se decompõem nessas extensões, não é muito difícil. Dessa forma, o estudo dos corpos locais dá um caminho natural para se estudar um problema fundamental da teoria dos números algébricos.

O problema de estender a teoria de corpos de classe ao caso não-abeliano permanece decididamente em aberto, mesmo no caso local. As principais conjeturas nesse sentido são o conjunto de idéias conhecido como "a filosofia de Langlands", que relaciona (conjeturalmente) extensões de corpos de números a objetos análogos às formas modulares clássicas. Uma das características da filosofia de Langlands é que ela tem um caráter local, isto é, ela obteria resultados sobre corpos globais analisando primeiro a situação para corpos locais. O princípio local-global permanece, assim, um método fundamental na exploração deste tipo de problema.

Uma conseqüência menos profunda, mas importante, da teoria é que ela permite passar de $\mathbf{Q}_p$ para o seu fecho algébrico, e daí para o completamento $\mathbf{C}_p$, que é o contexto "natural" para a análise p-ádica. Veja, por exemplo, a discussão em [8].

5.2 L-funções p-ádicas

Uma outra forma de se usar métodos p-ádicos para estudar questões aritméticas é a teoria das L-funções p-ádicas. A idéia inicial é essencialmente a que consideramos acima em relação à função $\alpha \mapsto n^{\alpha}$: encontramos "valores especiais" de uma função aritmética, e procuramos uma função p-ádica que os interpole. O resultado é uma função p-ádica que possui propriedades aritméticas interessantes, e que pode ser usada para estudar problemas aritméticos.

Considere, por exemplo, a função zeta de Riemann, definida para $s \in \mathbf{C}$ com $\Re(s) > 1$

por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Classicamente, se obtém uma continuação analítica desta função ao plano todo, exceto por um polo simples em $s = 1$; esta continuação analítica obedece à equação funcional

$$(\pi)^{-s/2}\,\Gamma(s/2)\,\zeta(s) = (\pi)^{-(1-s)/2}\,\Gamma((1-s)/2)\,\zeta(1-s),$$

ou, equivalentemente,

$$\zeta(1-s) = \frac{2\cos(\pi s/2)\Gamma(s)}{(2\pi)^s}\zeta(s).$$

Um cálculo bastante conhecido dá que $s = 2k$ é um inteiro positivo par, temos

$$\zeta(2k) = -\frac{(-1)^k \pi^{2k} 2^{2k-1}}{(2k-1)!}\frac{\mathrm{B}_{2k}}{2k},$$

onde B_i denota o i-ésimo número de Bernouilli; substituindo na equação funcional, obtemos que

$$\zeta(1-2k) = -\frac{\mathrm{B}_{2k}}{2k}.$$

Se, por outro lado, $k > 1$ for ímpar, é trivial verificar que tanto $\zeta(1-k)$ quanto B_k são zero. Assim, obtemos, para qualquer inteiro $k > 1$

$$\zeta(1-k) = -\frac{\mathrm{B}_k}{k}.$$

Como estes "valores especiais" são números racionais, faz sentido pensá-los como elementos de $\mathbf{Q}_p$, e procurar interpolar a função

$$1 - k \mapsto -\frac{\mathrm{B}_k}{k}.$$

Note que como os inteiros negativos são densos em $\mathbf{Z}_p$, a extensão contínua desta função a $\mathbf{Z}_p$, se existir, será única.

Na realidade não é muito difícil perceber que o problema de interpolação não pode ser posto exatamente nesses termos. Em primeiro lugar, a função zeta possui uma expansão em produto de Euler

$$\zeta(s) = \prod_q \left(1 - \frac{1}{q^s}\right)^{-1},$$

onde q percorre todos os primos. Como estamos querendo uma função p-ádica, acaba sendo necessário "remover o fator de Euler em p", isto é, considerar a função

$$\zeta^*(s) = \left(1 - \frac{1}{p^s}\right)\zeta(s).$$

Isso altera a função a interpolar para

$$1 - k \mapsto -\left(1 - \frac{1}{p^{1-k}}\right)\frac{\mathrm{B}_k}{k}.$$

Mesmo esta modificação não basta: como no caso da função n^α, a interpolação inclui um "twist" que faz que ela só coincida com a função original quando k pertence a uma classe de congruência módulo $p-1$. Feitas todas essas ressalvas, a função que estamos procurando de fato existe, e é dada por uma série de potências com raio de convergência estritamente maior que 1. A notação que é normalmente usada é ζ_p.

Há várias maneiras de provar que a função ζ_p existe, e que de fato ela tem boas propriedades. A construção original é devida a Kubota e Leopoldt. O leitor encontrará exposições detalhadas em [8] e [7]. A exposição de Koblitz é especialmente interessante porque constrói ζ_p como a transformada de Mellin de uma medida p-ádica, um processo que tem forte analogia com o caso clássico (e ainda tem a vantagem de ensinar ao leitor os rudimentos de uma teoria de integração p-ádica).

Mais geralmente, estudam-se as L-funções

$$\mathrm{L}(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

onde χ é um caráter de Dirichlet. Este caso é essencialmente o mesmo que o da função zeta: não só não acontece nada de novo, como até fica mais fácil de entender a teoria se considerarmos todas as L-funções de uma só vez (porque o "twist" mencionado acima pode ser descrito explicitamente em termos de L-funções).

Um dos aspectos mais interessantes da teoria das L-funções p-ádicas são as "conjeturas principais" ("main conjectures"), que receberam esse nome porque generalizam a "conjetura principal" de Iwasawa sobre a relação entre torres de corpos ciclotômicos e a L-função p-ádica de Kubota e Leopoldt. Em vários contextos diferentes, o que essas conjeturas dizem é que duas "candidatas a L-função p-ádica" coincidem. Mais precisamente, em muitos contextos é

possível obter uma primeira L-funçãp p-ádica por interpolação, como acima, e uma segunda como série característica de um módulo de Iwasawa (veja [14] para uma definição). A conjetura principal para a situação em questão dirá que as duas funções assim obtidas diferem apenas por uma função cujos valores são sempre unidades p-ádicas. Em particular, seus zeros coincidirão. Como os zeros de uma L-função p-ádica carregam uma certa quantidade de informação aritmética, as conjeturas principais têm implicações profundas para a aritmética da situação em questão. O caso de corpos ciclotômicos é discutido em [14]; a demonstração da conjetura principal neste caso, devida a Mazur e Wiles, envolve técnicas extremamente sutis da teoria de curvas modulares—veja [9].

5.3 Mais análise, e geometria analítica rígida

Não é preciso dizer que há muitas idéias, problemas e métodos da análise p-ádica que não pudemos mencionar nesta introdução. Por exemplo, é possível fazer análise funcional p-ádica, em parte por analogia com a teoria clássica, e em parte motivada por problemas específicos vindos da teoria dos números ou da geometria algébrica. Assim, a versão p-ádica da teoria espectral para operadores compactos foi desenvolvida por Serre tendo como referência os trabalhos de B. Dwork sobre a racionalidade da função zeta de certas variedades algébricas. Dwork, por sinal, é autor de um grande número de trabalhos difíceis e profundos que aplicam métodos p-ádicos a vários tipos de problemas da geometria algébrica, especialmente geometria de variedades sobre corpos finitos (veja, por exemplo, a discussão da "cohomologia de Dwork" em [3]).

Uma outra área de trabalho em análise p-ádica é a teoria de funções analíticas (isto é, definidas por séries de potências). O alvo mais importante aqui é construir uma teoria em que valha algum tipo de princípio de continuação analítica. Os pioneiros deste tipo de trabalho foram M. Krasner, L. Schnirelman e K. Mahler, mas não há dúvida que o nome mais importante nesta área é o de J. T. Tate, que criou a "geometria analítica rígida". A idéia de Tate é que o princípio de continuação analítica falha porque há abertos demais; logo, sua teoria limita os abertos "permitidos" (usando uma idéia de Grothendieck que se tem tornado muito importante nas últimas décadas). Uma vez feita a construção básica de uma teoria de

continuação analítica, Tate consegue construir uma teoria de variedades analíticas p-ádicas que é paralela, em muitos aspectos, à teoria de variedades complexas, e que tem sido muito útil no estudo de vários problemas da geometria diofantina, especialmente nas mãos de R. Coleman.

Além das referências gerais, como [8] e [5], o leitor interessado especificamente nestes aspectos da teoria encontrará exposições de aspectos mais avançados da análise funcional p-ádica nos livros [1] de Y. Amice e [10] de A. F. Monna. Quanto à geomtria rígida, o paper original de Tate é [13], e há exposições e aplicações em [6] e especialmente [4]. Este último livro também trata um grande número de temas de análise funcional p-ádica que são relevantes à geometria rígida.

Os aspectos que citamos não esgotam as aplicações dos números p-ádicos nem da análise p-ádica. (Veja-se, por exemplo, o título da tese de doutorado do autor...) É tempo, entretanto, de deixarmos que o leitor procure novos exemplos por si mesmo, se assim o desejar.

Bibliografia

[1] Y. Amice. *Les Nombres p-adiques.* Presses Universitaires de France, 1975.

[2] G. Bachman. *Introduction to p-Adic Numbers and Valuation Theory.* Academic Press, 1964.

[3] D. Barsky and P. Robba, editors. *Cohomologies p-adiques.* Volume 23 of *Mémoires S.M.F.*, Société Mathématique de France, Paris, 1986.

[4] S. Bosch, U. Güntzer, and R. Remmert. *Non-Archimedian Analysis.* Springer-Verlag, 1984.

[5] J. W. S. Cassels. *Local Fields.* Cambridge University Press, 1986.

[6] L. Gerritzen and M. van der Put. *Mumford Groups and Schottky Curves.* Volume 817 of *Lecture Notes in Mathematics*, Springer-Verlag, 1980.

[7] K. Iwasawa. *Lectures on p-adic L-functions.* Volume 74 of *Annals of Mathematics Studies*, Princeton University Press, 1972.

[8] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-functions.* Springer-Verlag, Berlin, Heidelberg, New York, 1977, 1984[2].

[9] B. Mazur and A. Wiles. "Class Fields of Abelian Extensions of **Q**". *Inv. Math.*, 76:179–330, 1984.

[10] A. F. Monna. *Analise Non-Archimedienne.* Springer-Verlag, Berlin, Heidelberg, New York, 1970.

[11] J.-P. Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

[12] J.-P. Serre. *Local Fields.* Springer-Verlag, 1974.

[13] J. T. Tate. "Rigid Analytic Spaces". *Inv. Math.*, 12:257–289, 1971.

[14] Larry C. Washington. *Introduction to Cyclotomic Fields.* Springer-Verlag, 1982.

Impresso na Gráfica do
inpe