Inteiros p-ádicos

XXI Semana Olímpica (Maceió, Alagoas)

(brought to you by ET)

Seja p um primo. Vamos introduzir a "incarnação aritmética" do anel de séries formais $\mathbb{F}_p[\![t]\!]$.

1 Anel dos inteiros p-ádicos

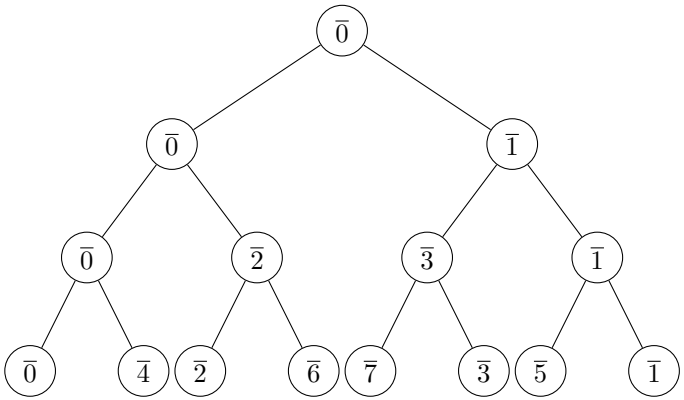
Definimos o *anel dos inteiros p-ádicos* $\mathbb{Z}_p$ como o subanel do anel produto

$$\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^3\mathbb{Z} \times \cdots$$

formado por "tuplas coerentes" $(\alpha_1, \alpha_2, \ldots)$: se $n \geq m$, exigimos que α_n tenha imagem α_m segundo o morfismo natural $\mathbb{Z}/p^n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^m\mathbb{Z}$. Em símbolos:

$$\mathbb{Z}_p \stackrel{\text{def}}{=} \left\{ (\overline{a}_n) \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} \;\middle|\; a_m \equiv a_n \pmod{p^m} \text{ se } n \geq m \right\}$$

Podemos visualizar inteiros p-ádicos através de uma árvore: os vértices desta árvore são os elementos de $\mathbb{Z}/p^n\mathbb{Z}$ para $n \geq 0$, arranjados em "níveis" segundo o valor de n; ligamos o vértice $\alpha \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ do nível $n+1$ ao vértice correspondente à sua imagem em $\mathbb{Z}/p^n\mathbb{Z}$ no nível n. Por exemplo, a figura a seguir ilustra os níveis iniciais $n = 0, 1, 2, 3$ desta árvore para o caso $p = 2$:



Assim, as "tuplas coerentes" de $\mathbb{Z}_p$ estão em correspondência biunívoca com os caminhos infinitos a partir da raiz desta árvore.

Embora ecologicamente correta, a represetação acima não é muito prática do ponto de vista algébrico. Uma maneira simples de representar um elemento em $\mathbb{Z}_p$ é através de sua "expansão infinita em base p". Para isto, escreva cada elemento de $\mathbb{Z}/p^n\mathbb{Z}$ como a classe de um inteiro $A_n \in \mathbb{Z}$ satisfazendo $0 \leq A_n < p^n$. Em base p:

$$A_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}, \qquad a_i \in \{0, 1, 2, \ldots, p-1\}$$

Se $m \leq n$ a condição $A_m \equiv A_n \pmod{p^m}$ é equivalente a $A_m = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$, ou seja, A_m é obtido "truncando-se" A_n. Portanto podemos simbolicamente representar o inteiro p-ádico

$$(a_0 \bmod p,\ a_0 + a_1 p \bmod p^2,\ a_0 + a_1 p + a_2 p^2 \bmod p^3, \ldots) \in \mathbb{Z}_p$$

através da "série de potências em p" a seguir, obtida "colando-se" os vários termos A_n:

$$a_0 + a_1 p + a_2 p^2 + \cdots \qquad (0 \leq a_i < p)$$

Exemplo 1 *Cálculos com esta representação são essencialmente feitos como no anel de séries formais $\mathbb{F}_p[\![t]\!]$, mas agora tomando-se o cuidado extra de considerar o "vai 1". Por exemplo, em $\mathbb{Z}_2$ tem-se*

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

o que, é claro, coincide com a fórmula usual da soma da PG:

$$1 + 2 + 2^2 + 2^3 + \cdots = \frac{1}{1-2} = -1$$

Se isto parece confuso, vamos retornar à definição original de $\mathbb{Z}_2$:

$$1 = (1 \bmod 2, 1 \bmod 2^2, 1 \bmod 2^3, \ldots)$$

$$1 + 2 + 2^2 + \cdots = (1 \bmod 2, 1 + 2 \bmod 2^2, 1 + 2 + 2^2 \bmod 2^3, \ldots)$$

Portanto a soma destas duas tuplas é de fato

$$0 = (0 \bmod 2, 0 \bmod 2^2, 0 \bmod 2^3, \ldots)$$

Podemos ver $\mathbb{Z}$ como um subanel de $\mathbb{Z}_p$. Para isto, note que o "mapa diagonal"

$$\begin{aligned} \mathbb{Z} &\hookrightarrow \mathbb{Z}_p \\ a &\mapsto (a \bmod p^n)_{n\in\mathbb{N}} \end{aligned}$$

é injetor (o único inteiro divisível por potências arbitrariamente grandes de p é 0). Pense em $\mathbb{Z}$ como subanel de $\mathbb{Z}_p$ formado pelas "séries finitas" na expansão em base p acima.

Analogamente ao caso de séries formais, temos

Lema 2 *O grupo de unidades do anel $\mathbb{Z}_p$ consiste nos inteiros p-ádicos que não são divisíveis por p, i.e., cujos "termos constantes" a_0 não são nulos:*

$$\mathbb{Z}_p^\times = \big\{a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p \;\big|\; a_0 \neq 0, \quad 0 \leq a_i < p\big\},$$

Prova Segue diretamente do fato de que $a \bmod p^n$ é uma unidade em $\mathbb{Z}/p^n\mathbb{Z}$ se, e somente se, a não é múltiplo de p. □

Definição 3 *Seja p um número primo. A* valorização p-ádica *é a função*

$$\begin{aligned} v_p \colon \mathbb{Z}_p \smallsetminus \{0\} &\to \mathbb{N} \\ \sum_{n\geq 0} a_n p^n &\mapsto \textit{menor } d \textit{ tal que } a_d \neq 0 \qquad (a_i \in \{0, 1, \ldots, p-1\}) \end{aligned}$$

Ou seja, dado um inteiro p-ádico não nulo $f \in \mathbb{Z}_p$, $p^{v_p(f)}$ é a maior potência de p que divide f. Estendemos a valorização p-ádica para uma função $v_p \colon \mathbb{Z}_p \to \mathbb{N} \cup \{\infty\}$ definindo $v_p(0) = \infty$, em que ∞ denota um símbolo tal que $\infty \geq n$ e $n + \infty = \infty$ para todo $n \in \mathbb{N} \cup \{\infty\}$.

Dado um elemento não nulo $f = \sum_{n\geq 0} a_n p^n \in \mathbb{Z}_p$ com valorização p-ádica $v_p(f) = d$, após "descascarmos" a maior potência de p que divide f obtemos uma fatoração

$$f = p^d \cdot \underbrace{(a_d + a_{d+1} p + a_{d+2} p^2 + \cdots)}_{\in \mathbb{Z}_p^\times} \qquad (0 \leq a_i < p,\ a_d \neq 0)$$

de modo que qualquer elemento não nulo de $\mathbb{Z}_p$ difere multiplicativamente de uma potência de p.

2 Análise p-ádica

Utilizando a valorização p-ádica, podemos estabelecer uma ponte com a análise da seguinte forma: defina a *norma p-ádica* como sendo a função $\|-\|_p \colon \mathbb{Z}_p \to \mathbb{R}_{\geq 0}$ dada por

$$\|a\|_p = p^{-v_p(a)} \qquad (a \in \mathbb{Z}_p)$$

Aqui interpretamos $\|0\|_p = p^{-\infty} = 0$. Diretamente das definições acima temos as seguintes propriedades: para quaisquer $a, b \in \mathbb{Z}_p$,

(i)	$v_p(a) = \infty \iff a = 0$	$\|a\|_p = 0 \iff a = 0$
(ii)	$v_p(ab) = v_p(a) + v_p(b)$	$\|ab\|_p = \|a\|_p \cdot \|b\|_p$
(iii)	$v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$	$\|a+b\|_p \leq \max\{\|a\|_p, \|b\|_p\}$

com igualdade em (iii) se $v_p(a) \neq v_p(b) \iff \|a\|_p \neq \|b\|_p$. As propriedades acima justificam o nome *norma p-ádica* para $\|-\|_p$, sendo (iii) uma versão "super vitaminada" da desigualdade triangular, chamada *desigualdade ultramétrica*. Destas três propriedades, temos que

$$d_p(a, b) \stackrel{\text{def}}{=} \|a - b\|_p$$

define uma métrica em $\mathbb{Z}_p$, a chamada *métrica p-ádica*. Daí, podemos definir noções como limites da maneira usual: dada uma sequência (a_n) em $\mathbb{Z}_p$ e $L \in \mathbb{Z}_p$, $\lim a_n = L$ significa

$$\forall \epsilon > 0\ \exists n_0 \in \mathbb{N} \text{ tal que } n \geq n_0 \implies \|a_n - L\|_p < \epsilon$$

Observe que "p-adicamente pequeno" significa divisível por uma potência grande de p; mais precisamente, na métrica p-ádica temos

$$\boxed{\lim_{n\to\infty} p^n = 0}$$

Por exemplo, é assim que um aluno matriculado em Cálculo p-ádico I calcula derivadas ($x \in \mathbb{Z}_p$):

$$\lim_{n\to\infty} \frac{(x+p^n)^8 - x^8}{p^n} = \lim_{n\to\infty} 8x^7 + \binom{8}{2} x^6 p^n + \cdots + \binom{8}{7} x p^{6n} + p^{7n} = 8x^7$$

Análise p-ádica é bem mais agradável do que análise real, como mostra o seguinte

Lema 4 *Seja p um primo.*

(i) $\mathbb{Z}_p$ é um espaço métrico completo com relação à métrica p-ádica (i.e., toda sequência de Cauchy em $\mathbb{Z}_p$ converge).

(ii) (Sonho de todo estudante de cálculo) Dada uma sequência (a_n) em $\mathbb{Z}_p$,

$$\sum_{n\geq 0} a_n \textit{ converge} \iff \lim a_n = 0$$

Prova

(i) Dada uma sequência de Cauchy (a_n) em $\mathbb{Z}_p$ e $r \in \mathbb{N}$ fixado, a sequência $a_n \bmod p^r$ eventualmente estabiliza pois existe n_0 tal que $\|a_n - a_m\|_p \leq p^{-r}$ para todo $n, m \geq n_0$, ou seja, $n, m \geq n_0 \implies a_n \equiv a_m \pmod{p^r}$. Denotando por $a_\infty \bmod p^r$ este valor estável, como $a_n \equiv a_m \pmod{p^r} \Rightarrow a_n \equiv a_m \pmod{p^{r-1}}$, quando r varia obtemos uma tupla coerente $(a_\infty \bmod p^r)_{r\in\mathbb{N}}$, ou seja, um inteiro p-ádico L, que é claramente o limite de (a_n) visto que, para qualquer $r \in \mathbb{N}$ fixado, $L \equiv a_n \pmod{p^r} \iff \|L - a_n\| < p^{-r}$ para todo $n \gg 0$ por construção.

(ii) A implicação $\Rightarrow$ vale em qualquer espaço métrico; para mostrar $\Leftarrow$, por (i) devemos mostrar que as somas parciais $s_r = a_0 + a_1 + \cdots + a_r$ formam uma sequência de Cauchy. Mas isto segue diretamente da desigualdade ultramétrica: como por hipótese $\lim a_n = 0$, dado $\epsilon > 0$, existe n_0 tal que $n \geq n_0 \implies \|a_n\|_p < \epsilon$, logo

$$n \geq m \geq n_0 \implies \|s_n - s_m\|_p \leq \max_{m<i\leq n} \{\|a_i\|_p\} < \epsilon$$

□

3 Lema de Hensel

Uma das vantagens de se trabalhar com o anel $\mathbb{Z}_p$ é que ele possui "propriedades híbridas", exibindo características analíticas como $\mathbb{R}$ e uma aritmética que está entre a de um corpo finito $\mathbb{F}_p$ e a do anel $\mathbb{Z}$. Isto torna $\mathbb{Z}_p$ uma das ferramentas mais importantes em Teoria dos Números. Para ilustrar esta conexão, provaremos o famoso

Teorema 5 (Lema de Hensel) *Seja $f(x) \in \mathbb{Z}_p[x]$ e seja $f'(x) \in \mathbb{Z}_p[x]$ sua derivada (formal). Seja $a \in \mathbb{Z}_p$ e suponha que $r = v_p(f'(a)) \neq \infty$. Então se $f(a) \equiv 0 \pmod{p^{2r+1}}$ (i.e., a é uma aproximação p-ádica boa o suficiente de uma raiz de $f(x)$) então existe uma raiz $\theta \in \mathbb{Z}_p$ de $f(x)$ tal que $\theta \equiv a \pmod{p^r}$.*

Prova Construiremos indutivamente uma sequência (a_n) em $\mathbb{Z}_p$ tal que $a_0 = a$ e, para todo $n \in \mathbb{N}$,

(i) $a_{n+1} \equiv a_n \pmod{p^{r+1+n}}$;

(ii) $f(a_n) \equiv 0 \pmod{p^{2r+1+n}}$;

(iii) $v_p(f'(a_n)) = r$

A prova terminará uma vez que obtivermos esta sequência, pois por (i) (a_n) será de Cauchy e por (ii) $\theta = \lim a_n$ será uma raiz de $f(x)$ com $\theta \equiv a \pmod{p^r}$. Observe ainda que (i) implica (iii) automaticamente pois $f'(a_n) \equiv f'(a_0) \pmod{p^{r+1}}$ e $v_p(f'(a_0)) = r$.

Suponha que a_n já esteja definido. Por (i) e (ii), queremos encontrar $h \in \mathbb{Z}_p$ tal que $a_{n+1} = a_n + hp^{r+1+n}$ e

$$0 \equiv f(a_{n+1}) \equiv f(a_n) + hp^{r+1+n} \cdot f'(a_n) \pmod{p^{2r+2+n}}$$

pela "expansão de Taylor" de $f(x)$ e do fato de $(hp^{r+1+n})^i \equiv 0 \pmod{p^{2r+2+n}}$ para $i \geq 2$.

Por hipótese de indução, $f(a_n) = tp^{2r+1+n}$ e $f'(a_n) = up^r$ com $t \in \mathbb{Z}_p$ e $u \in \mathbb{Z}_p^\times$, logo a congruência acima é equivalente a

$$0 \equiv tp^{2r+1+n} + hup^{2r+1+n} \pmod{p^{2r+2+n}} \iff -t \equiv hu \pmod{p}$$

logo basta definir $h = -tu^{-1}$. □

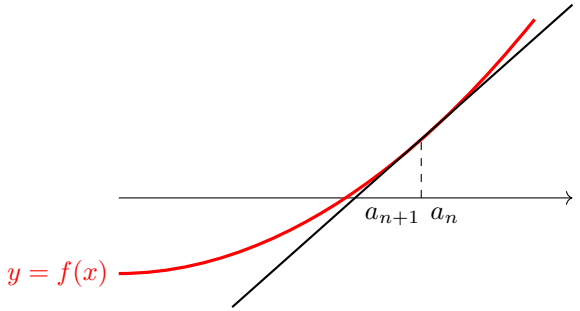
O caso em que $r = 0$ é o mais utilizado e em geral é apresentado na seguinte formulação de "levantamento de raízes simples":

Corolário 6 *Seja $f(x) \in \mathbb{Z}_p[x]$ e seja $\overline{f}(x) \in \mathbb{F}_p[x]$ o polinômio obtido a partir de $f(x)$ por redução módulo p de seus coeficientes. Seja $a \in \mathbb{Z}_p$ tal que sua imagem $\overline{a} \in \mathbb{F}_p$ seja uma raiz simples de $\overline{f}(x)$, ou seja, $\overline{f}(\overline{a}) = \overline{0}$ e $\overline{f}'(\overline{a}) \neq \overline{0}$ em $\mathbb{F}_p$. Então existe uma raiz $\theta \in \mathbb{Z}_p$ de $f(x)$ tal que $\theta \equiv a \pmod{p}$.*

Observe que neste caso, a sequência da prova no lema de Hensel se escreve

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

que é exatamente a obtida aplicando-se o método de Newton para aproximações de raízes de $f(x)$!



Exemplo 7 *Seja p um primo. Como $x^{p-1} - \overline{1} \in \mathbb{F}_p[x]$ se fatora completamente em $p-1$ fatores distintos (pequeno teorema de Fermat)*

$$x^{p-1} - \overline{1} = (x - \overline{1})(x - \overline{2}) \ldots (x - \overline{p-1})$$

pelo lema de Hensel $x^{p-1} - 1$ também se fatora completamente em $\mathbb{Z}_p[x]$. Ou seja, todas as raízes $(p-1)$-ésimas da unidade pertencem a $\mathbb{Z}_p$. Por exemplo, para $p = 5$

estas raízes são

$$\begin{aligned} 1 \\ i &\stackrel{\text{def}}{=} 2 + 5 + 2\cdot 5^2 + 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + \cdots \\ -i &= 3 + 3\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3 + 5^4 + 2\cdot 5^6 + \cdots \\ -1 &= 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + 4\cdot 5^4 + 4\cdot 5^5 + 4\cdot 5^6 + \cdots \end{aligned}$$

4 Para aprender mais

Existem diversos livros excelentes sobre o assunto, por exemplo

- J.W.S. Cassels, *Local Fields*, LMSST 3, London Mathematical Society.
- J. Neukirch, *Algebraic Number Theory*, Grundlehren der Matematischen Wissenschaft 332, Springer-Verlag.
- J.-P. Serre, *A Course in Arithmetic*, GTM, Springer-Verlag.
- ET, *An Invitation to Local Fields*, notas do mini-curso oferecido no congresso Groups, Rings and Group Rings (Ubatuba-São Paulo, 2008)

Em particular, o livro do Serre traz uma prova completamente elementar (que só depende da reciprocidade quadrática e do lema de Hensel) do famoso

Teorema 8 (Haße-Minkowski) *Seja*

$$f(x_1, \ldots, x_n) = a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2$$

uma forma quadrática com coeficientes em $\mathbb{Q}$. Então $f(x_1, \ldots, x_n) = 0$ tem solução não trivial em $\mathbb{Q}$ se, e só se, possui solução não trivial sobre $\mathbb{R}$ e $\mathbb{Q}_p$ para todo p.

Este é um exemplo do famoso *princípio local-global*, que é o cerne de vários resultados profundos em Teoria dos Números. Por exemplo, conjectura-se que uma versão modificada deste princípio (a finitude do grupo de Tate-Shafarevich) também vale para curvas elípticas sobre $\mathbb{Q}$, o que nos daria um algoritmo para encontrar todos os seus pontos racionais!

5 Exercícios

1 *Mostre que*

(a) os ideais de $\mathbb{Z}_p$ são todos principais, da forma (0) ou (p^n) para algum $n \in \mathbb{N}$.

(b) o corpo de frações de $\mathbb{Z}_p$ consiste nas "séries de Laurent" em p, i.e.,

$$\begin{aligned} \mathbb{Q}_p &\stackrel{\text{def}}{=} \operatorname{Frac} \mathbb{Z}_p = \left\{ \sum_{n \geq n_0} a_n p^n \;\middle|\; n_0 \in \mathbb{Z},\ 0 \leq a_i < p \right\} \\ &= \{u \cdot p^n \mid n \in \mathbb{Z},\ u \in \mathbb{Z}_p^\times\} \cup \{0\} \end{aligned}$$

2 *Mostre que um p-ádico $\sum_{n \geq n_0} a_n p^n \in \mathbb{Q}_p$ $(0 \leq a_i < p)$ pertence a $\mathbb{Q}$ se, e só se, seus dígitos formam uma sequência periódica a partir de um certo ponto.*

3 *(a) Mostre que $x^2 = 2$ tem solução em $\mathbb{Z}_7$ e calcule seus primeiros dígitos em base 7.*

(b) Escreva $\pm 2/3 \in \mathbb{Z}_5$ em base 5.

(c) Mostre que a sequência 10^{-n}, $n \in \mathbb{N}$, não converge em $\mathbb{Q}_p$ para nenhum primo p.

4 *Considere o inteiro p-ádico $f = \sum_{i \geq 0} a_i p^i \in \mathbb{Z}_p$ escrito em base p. Seja $a \in \mathbb{Z}_p$ um outro p-ádico. Mostre que*

$$\lim_{n \to \infty} (1 + ap)^{\sum_{0 \leq i \leq n} a_i p^i}$$

converge. Isto permite definir a exponenciação $(1 + ap)^f$.

5 *Mostre: para todo $a \in \mathbb{Z}$ primo com p, a^{p^n} converge em $\mathbb{Q}_p$.*

6 (Levantamento de fatorações separáveis) *Prove o seguinte resultado, uma generalização do lema de Hensel: se $f \in \mathbb{Z}_p[x]$ é um polinômio mônico cuja redução módulo p se fatora como $\overline{f} = \overline{g}\overline{h}$ com $\overline{g}, \overline{h} \in \mathbb{F}_p[x]$ mônicos e primos entre si, então existem levantamentos mônicos $g, h \in \mathbb{Z}_p[x]$ de $\overline{g}$ e $\overline{h}$ tais que $f = gh$.*

7 *Seja $p \neq 2$ um número primo. Seja ainda $u \in \mathbb{Z}$ um resíduo não quadrático módulo p.*

(a) Prove que $\{1, u, p, up\}$ forma um conjunto de representantes de classe do grupo quociente $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$.

(b) Mostre que $\mathbb{Q}_p$ possui exatamente 3 extensões quadráticas.

(c) Mostre que a forma quadrática $x^2 + uy^2 + pz^2 + upw^2$ é anisotrópica (i.e., $x^2 + uy^2 + pz^2 + upw^2 = 0$ só tem solução trivial).

(d) Mostre que qualquer forma quadrática sobre $\mathbb{Q}_p$ com 5 ou mais variáveis é isotrópica (i.e., representa 0 não trivialmente).

8 *Mostre*

(a) $u \in \mathbb{Z}_2^\times$ *é um quadrado perfeito se, e só se,* $u \equiv 1 \pmod 8$.

(b) $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\pm\overline{1}, \pm\overline{5}, \pm\overline{2}, \pm\overline{10}\}$ *é um grupo isomorfo a* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

(c) há exatamente 7 extensões quadráticas de $\mathbb{Q}_2$ *dentro de seu fecho algébrico.*

(d) toda forma quadrática sobre $\mathbb{Q}_2$ *com 5 ou mais variáveis é necessariamente isotrópica.*

9 (Unidades em $\mathbb{Z}_p$) *Considere as séries*

$$\exp(z) \stackrel{\text{def}}{=} \sum_{n\geq 0} \frac{z^n}{n!} \qquad e \qquad \log(1+z) \stackrel{\text{def}}{=} \sum_{n\geq 1} (-1)^{n+1} \frac{z^n}{n}$$

e o subgrupo multiplicativo de $\mathbb{Z}_p^\times$

$$U^{(n)} = \{a \in \mathbb{Z}_p^\times \mid a \equiv 1 \pmod{p^n}\}$$

Mostre que

(a) $\log(1+z)$ *converge para todo* $z \in \mathbb{Z}_p$.

(b) $\exp(z)$ *converge para todo* $z \in \mathbb{Z}_p$ *com* $v_p(z) \geq 1$ *se* $p \neq 2$ *e com* $v_2(z) \geq 2$ *se* $p = 2$.

(c) $\log(1+z)$ *e* $\exp(z)$ *definem isomorfismos de grupos entre* $U^{(1)}$ *e* (p) *se* $p \neq 2$ *e entre* $U^{(2)}$ *e* (2^2) *se* $p = 2$.

(d) $\mathbb{Q}_p$ *contém todo o subgrupo* μ_{p-1} *das raízes* $(p-1)$*-ésimas da unidade.*

(e) temos isomorfismos de grupos

$$\mathbb{Q}_p^\times \cong \begin{cases} \mathbb{Z} \oplus \mu_{p-1} \oplus \mathbb{Z}_p & \text{se } p \neq 2 \\ \mathbb{Z} \oplus \{\pm 1\} \oplus \mathbb{Z}_p & \text{se } p = 2 \end{cases}$$

10 *Seja* $f(x) \in \mathbb{Z}_p[\![x]\!]$ *tal que nem todos os seus coeficientes sejam divisíveis por* p. *Então existe um único polinômio da forma*

$$g(x) = x^r + b_{r-1}x^{r-1} + \cdots + b_0 \qquad (p \mid b_i)$$

tal que $f(x) = g(x) \cdot u(x)$ *com* $u(x)$ *uma unidade em* $\mathbb{Z}_p[\![x]\!]$.

11 *Mostre que o único automorfismo de* $\mathbb{Q}_p$ *é a identidade. Dica: considere as raízes* $(p-1)$*-ésimas da unidade.*