Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Corpos locais e equações diagonais sobre corpos p-ádicos

por

Luciana Lima Ventura

Brasília
Fevereiro de 2009

Agradecimentos

Agradeço, primeiramente, a Deus por esta oportunidade;

Aos meus pais, Antônio Fernando e Lusineida, e familiares por me apoiarem durante todo o processo;

Ao meu orientador, professor Hemar Godinho, pela orientação, dedicação e paciência durante o desenvolvimento deste trabalho;

Aos professores, Paulo Henrique e Nigel Pitt, pelas correções, sugestões e por terem aceitado participar da banca;

Aos professores Marcus Vinícius, Celius, João Carlos, Hemar, Nigel, Jairo, Elves, Carlos Alberto, Cátia e Carrión por contribuirem para a minha formação acadêmica;

Aos meus colegas e amigos de graduação, em especial Juliana, Igor, Simone e Jeferson que estiveram presentes também no mestrado, trocando idéias, esclarecendo dúvidas e me dando suporte;

Aos amigos que conheci durante esse período pelas palavras de incentivo, pelas horas (e horas...) de estudo, pelos momentos de descontração e, obviamente, pelos (tantos) almoços;

Ao Vagner por estar ao meu lado e me apoiar nos momentos de dificuldades;

Aos amigos da dança pelas palavras de incentivo e carinho e por compreenderem a minha ausência durante alguns períodos;

Aos funcionários do Departamento de Matemática da UnB;

E ao CNPq pelo apoio financeiro.

Resumo

Faremos um breve estudo sobre corpos locais para obter alguns resultados para corpos p-ádicos. Aproveitando esse estudo, juntamos neste trabalho algumas versões do Lema de Hensel. E baseado nos artigos de Alemu [1] e de Brink, Godinho e Rodrigues [3] veremos algumas condições suficientes sobre o número de variáveis para a solubilidade de sistemas de equações diagonais sobre corpos p-ádicos.

Palavras-chaves: corpos locais; corpos p-ádicos; lema de Hensel; sistema de equações diagonais.

Abstract

We will make a brief study of local fields to obtain some results for p-adic fields. Enjoying this study, we join in this work some versions of the Hensel's Lemma. Based on the articles of Alemu [1] and Brink, Godinho and Rodrigues [3], we see some sufficient conditions on the number of variables for the solubility of diagonal systems of equations on p-adic fields.

Key words: local fields; p-adic fields; Hensel's lemma; diagonal system of equations.

ÍNDICE

Introdução

A existência, ou não, de soluções para equações é um tema frequente na matemática. O tema da nossa dissertação é a busca de condições suficientes para que um sistema de polinômios homogêneos de grau k tenha zero não-trivial dentro do corpo dos números p-ádicos, teoria proposta por Kurt Hensel em 1897.

Em 1920, Emil Artin fez a seguinte conjectura

> *Um sistema com R formas de grau k com N variáveis sobre um corpo p-ádico K tem zero não-trivial em K se $N \geqslant Rk^2 + 1$.*

Para formas diagonais e $K = \mathbb{Q}_p$, a conjectura foi provada por Davenport e Lewis para uma equação [8] e para duas equações quando k é ímpar [9]. Eles ainda mostraram que, em ambos os casos, a condição $N = Rk^2 + 1$ quando $k = p - 1$, para um primo p, é suficiente para que o sistema tenha solução não-trivial.

No entanto, para o caso geral, essa afirmação é falsa como foi mostrado por Guy Terjanian [25] em 1966. Ele construiu um polinômio homogêneo de grau 4 sobre $\mathbb{Q}_2$ com 18 variáveis que não admite zero não-trivial. No caso de sistemas de formas simultaneamente diagonais, ainda acredita-se na conjectura. Assim, muitos matemáticos tem voltado seus estudos para obter a melhor condição sobre o número de variáveis que garanta solução de um sistema mas os resultados obtidos até agora são distantes do sugerido por Artin. Davenport e Lewis [10] mostraram que basta termos

$$N \geqslant \begin{cases} [9R^2k\ \log(3Rk)], \text{ se } k \text{ é ímpar} \\ [48R^2k^3\ \log(3Rk^2)], \text{ se } k \text{ é par diferente de 2} \end{cases}$$

para que o sistema tenha solução não-trivial em $\mathbb{Q}_p$, para todo primo p. Já Low, Pitman e Wolf [17] provaram que o sistema tem zero não-trivial em $\mathbb{Q}_p$ se o número de variáveis satisfaz

$$N \geqslant \begin{cases} [48Rk^3\ \log(3Rk^2)], \text{ se k}>2 \\ 2R^2k\ \log k, \text{ se } k \text{ é ímpar e suficientemente grande} \end{cases}$$

E Brüdern e Godinho [5] mostraram que

$$N \geqslant \begin{cases} R^3k^2, \text{ se } R \geqslant 3 \text{ e } k \geqslant 3 \\ 36k^2, \text{ se } R = 3 \text{ e } k = 2^n \text{ com } n \in \mathbb{N} \end{cases}$$

é suficiente para que exista solução não-trivial em $\mathbb{Q}_p$. Ainda para $K = \mathbb{Q}_p$, o resultado mais recente, provado por Michael Knapp [15], é que $N \geqslant 4R^2k^2$ é condição suficiente para que o sistema tenha zero não-trivial.

Agora, se K for uma extensão de $\mathbb{Q}_p$ de grau n então, para $R = 1$, temos zero não-trivial em K se

$$N > (2\tau + 3)^k(d^2k)^{k-1}, \text{ onde } d = (m, p^f - 1),$$

segundo Birch [2] ou se

$$N \geqslant 16n^2(\log k)^2k^2,$$

como demonstrado por Dodson [11].

Também para $R = 1$, Alemu [1] mostrou que

Teorema 1. *Se o polinômio tiver N variáveis satisfazendo*

$$N \geqslant \begin{cases} 4nk^2 - nk + 1, \ p = 2 \\ \max\{3nk^2 - nk + 1, 2k^3 - k^2\}, \ p \geqslant 3 \end{cases}$$

então existe zero não-trivial em K

E o trabalho mais recente é o do Skinner [23] onde ele prova que $N > k^{6\tau+4}$ é suficiente para que uma forma diagonal tenha solução não-trivial em K.

Agora, para R arbitrário, temos três importantes resultados:

Teorema 2. *O sistema homogêneo de R polinômios de grau k tem solução não-trivial se o número de variáveis N for maior ou igual a $R^2k^{2+2n\tau}$, onde $k = p^\tau m$ com $(p, m) = 1$.*

Teorema 3. *O sistema com R equações de grau k tem solução não-trivial se o número de variáveis N é maior que $4nR^2k^2$.*

Teorema 4. *Um sistema com R equações de grau k tem solução não-trivial se o número de variáveis N é maior que $(Rk)^{2\tau+5}$, onde $k = p^\tau m$ com $(p, m) = 1$.*

O Teorema 2 foi obtido por Knapp [15] e os Teoremas 3 e 4 por Brink, Godinho e Rodrigues [3]. Note que o Teorema 3 é uma generalização do resultado apresentado por Knapp para $K = \mathbb{Q}_p$ e o Teorema 4, ao contrário do Teorema 2, não depende do grau da extensão n. Além disso, podemos comparar esse último resultado com o obtido por Skinner quando $R = 1$.

Neste trabalho, começamos com o estudo dos corpos locais e suas propriedades pois os corpos p-ádicos são exemplos destes. Veremos as subestruturas dos corpos locais como o anel dos inteiros, os ideais desse anel e a estrutura dos anéis quocientes. Além disso,

introduziremos as funções logaritmo e exponencial p-ádicos para estabelecermos um homomorfismo entre duas subestruturas dos corpos p-ádicos. Os resultados dos dois primeiros capítulos servirão de base para o nosso estudo sobre a existência de soluções para os sistemas de polinômios homogêneos. Finalmente, no capítulo 3, estudaremos os trabalhos desenvolvidos por Alemu [1] e Brink, Godinho e Rodrigues [3] a fim de demonstrarmos os teoremas 1, 3 e 4.

CAPÍTULO 1

Corpos Locais

Neste capítulo veremos muitas definições e resultados básicos, necessários para a leitura dos capítulos seguintes.

1.1 Propriedades Gerais

Definição 1. Seja K um corpo. A aplicação $v : K \to \mathbb{Z} \cup \{\infty\}$ é uma *valorização* sobre K se, $\forall\, a, b \in K$:

(i) $v(a) = \infty \Leftrightarrow a = 0$;

(ii) $v(a\,b) = v(a) + v(b)$;

(iii) $v(a + b) \geqslant \min\{v(a), v(b)\}$.

Exemplo 1. Considere $K = \mathbb{Q}$ e p um primo. Podemos escrever

$$x = p^n \frac{a}{b}, \quad \text{com } (ab, p) = 1,$$

para todo x racional não nulo. Defina $v_p(x) = n$ se $x \in \mathbb{Q}\backslash\{0\}$ e $v_p(0) = \infty$. Então v_p é uma valorização que chamamos de *valorização p-ádica*.

Definição 2. Seja K um corpo. A aplicação $|\cdot| : K \to \mathbb{R}$ é um *valor absoluto* sobre K se existir $\alpha \in \mathbb{R}$ fixo tal que:

(i) $|a| \geqslant 0$, $\forall\, a \in K$, e $|a| = 0 \Leftrightarrow a = 0$;

(ii) $|a\,b| = |a||b|$, $\forall\, a, b \in K$;

(iii) $|a| \leqslant 1 \Rightarrow |1 + a| \leqslant \alpha$.

Um exemplo clássico é o *valor absoluto trivial* $|\cdot|_0$ dado por

$$|a|_0 = \begin{cases} 0 & \text{se } \ a = 0, \\ 1 & \text{caso contrário.} \end{cases}$$

Outro exemplo importante é o *valor absoluto p-ádico* definido sobre $K = \mathbb{Q}$ por

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{se } \ x \in \mathbb{Q}\backslash\{0\} \\ 0 & \text{se } \ x = 0 \end{cases}$$

onde v_p é a valorização p-ádica sobre $\mathbb{Q}$.

Escolhemos (iii) como o terceiro axioma ao invés da desigualdade triangular pois em alguns contextos é consideravelmente mais simples mostrar (iii).

Segue da definição as seguintes propriedades:

Propriedades 1. Seja $|\cdot|$ um valor absoluto sobre K. Temos

a) $|1| = 1$;

b) se $|a^n| = 1$, então $|a| = 1$;

c) $|-1| = |1|$, logo $|-a| = |a|$;

d) $|a^{-n}| = |a|^{-n}$

e) se K é um corpo finito, então $|\cdot|$ é trivial.

Demonstração:

a) Temos que $1 = 1^2$ daí $|1| = |1^2| = |1|^2$, por (ii). Como $|1| \neq 0$, concluímos que $|1| = 1$.

b) Por (ii), $1 = |a^n| = |a|^n$. Como valor absoluto é uma aplicação que assume valores reais, segue que $|a| = 1$.

c) Temos $(-1)^2 = 1$ então $|1| = |-1|^2$ e essa propriedade segue por b).

d) Por (ii) e (a), $|a^{-n}||a|^n = |a^{-n}a^n| = |1| = 1$. Portanto, $|a^{-n}| = |a|^{-n}$.

e) Se K é finito então existe $n \in \mathbb{N}$ tal que $a^n = 1, \forall\, a \in K\backslash\{0\}$. Pelos itens a) e b), temos $|a| = 1, \forall\, a \neq 0$. ■

Lema 1.1. *Se $|\cdot|$ é um valor absoluto sobre K e λ é um real positivo, então $||\cdot|| = |\cdot|^\lambda$ é um valor absoluto sobre K.*

Demonstração: (i) e (ii) são óbvios. Para mostrar (iii), tome $\alpha_1 = \alpha^\lambda$. Para todo $a \in K$ com $||a|| \leqslant 1$ temos $|a| \leqslant 1$ (pois, como λ é positivo e $|a|^\lambda \leqslant 1$ segue que $|a| \leqslant 1$), daí $|1+a| \leqslant \alpha$. Assim, $||1+a|| = |1+a|^\lambda \leqslant \alpha^\lambda = \alpha_1$. ■

É fácil verificar que $|\cdot|^\lambda = ||\cdot||$ para λ real positivo define uma relação de equivalência no conjunto dos valores absolutos. Neste caso, dizemos que esses valores absolutos são equivalentes e temos a seguinte notação $|\cdot| \sim ||\cdot||$.

Lema 1.2. *Uma condição necessária e suficiente para que o valor absoluto $|\cdot|$ satisfaça a desigualdade triangular é que podemos tomar $\alpha = 2$ na definição 2.*

Note que se tivermos $\alpha \leqslant 2$ na definição 2 então (iii) vale, em particular, para $\alpha_1 = 2$ e portanto o valor absoluto satisfaz a desigualdade triangular pelo lema acima.

Em geral, vamos nos preocupar apenas com as propriedades de classes de equivalência de valores absolutos. Assim, o Lema 1.2 nos permitirá usar a desigualdade triangular e suas propriedades conhecidas, pois como corolário deste lema segue que todo valor absoluto é equivalente a um que satisfaz a desigualdade triangular (basta tomar $\lambda = \log_\alpha 2$ se $\alpha > 2$ e definir $||\cdot|| = |\cdot|^\lambda$).

Demonstração do Lema 1.2: Suponha que a desigualdade triangular seja satisfeita. Então, $\forall\, a \in K$ tal que $|a| \leqslant 1$,

$$|1+a| \leqslant |1| + |a| \leqslant 2.$$

Para mostrar a suficiência, suponha $\alpha = 2$. Tome $a_1, a_2 \in K$ com $|a_1| \geqslant |a_2|$, então $|a| \leqslant 1$, onde $a_2 = aa_1$. Daí,

$$|a_1 + a_2| = |1+a||a_1| \leqslant 2|a_1|,$$

isto é,

$$|a_1 + a_2| \leqslant 2\max\{|a_1|, |a_2|\}$$

Por indução sobre n, encontramos

$$|a_1 + \cdots + a_{2^n}| \leqslant 2^n \max\{|a_j|, j = 1, \ldots 2^n\}.$$

Agora, sejam $a_1, \ldots, a_N \in K$. Tome n de forma que $2^{n-1} \leqslant N < 2^n$ e defina $a_{N+1} = \cdots = a_{2^n} = 0$. Então

$$|a_1 + \cdots + a_N| \leqslant 2^n \max\{|a_j|, j = 1, \ldots N\} \leqslant 2N \max_j\{|a_j|\}$$

Em particular, tomando $a_j = 1$, $j = 1, \ldots, N$, temos $|N| \leqslant 2N$, ou seja, temos um limite para o valor absoluto de todo inteiro positivo.

Sejam $b, c \in K$ e n um inteiro positivo. Então

$$\begin{aligned} |b+c|^n &= \left|\sum_{i=0}^{n} \binom{n}{i} b^i c^{n-i}\right| \leqslant 2(n+1)\max_i\left\{\left|\binom{n}{i} b^i c^{n-i}\right|\right\} \\ &= 2(n+1)\max_i\left\{\left|\binom{n}{i}\right| |b^i||c^{n-i}|\right\} \end{aligned}$$

$$\begin{aligned} &\leqslant 4(n+1)\max_i \left\{ \binom{n}{i} |b^i||c^{n-i}| \right\} \\ &\leqslant 4(n+1)\sum_{i=0}^{n} \binom{n}{i} |b^i||c^{n-i}| \\ &\leqslant 4(n+1)(|b|+|c|)^n. \end{aligned}$$

Tomando a raiz n-ésima e fazendo $n \to \infty$ sobre os reais, obtemos

$$|b+c| \leqslant |b| + |c|,$$

pois o limite de $\sqrt[n]{4(n+1)}$ quando n tende a infinito é 1. ■

Uma consequência da desigualdade triangular é

$$||a| - |b||_\infty \leqslant |a-b|,$$

onde $|\cdot|_\infty$ é o valor absoluto dos reais. A prova dessa desigualdade é a mesma que fazemos para o valor absoluto dos reais.

Definição 3. O valor absoluto $|\cdot|$ sobre um corpo K é não-arquimediano quando podemos tomar $\alpha = 1$ na definição 2. E é arquimediano caso contrário.

O valor absoluto trivial é um exemplo de valor absoluto não-arquimediano e o valor absoluto $|\cdot|_\infty$ sobre $\mathbb{R}$ é arquimediano.

Lema 1.3. *O valor absoluto $|\cdot|$ sobre K é não-arquimediano se, e somente se, satifaz a desigualdade ultramétrica*

$$|a+b| \leqslant \max\{|a|, |b|\}, \forall\, a, b \in K.$$

Além disso, todo valor absoluto equivalente a um valor absoluto não-arquimediano é não-arquimediano.

Demonstração: Seja $|\cdot|$ um valor absoluto não-arquimediano. Suponha que $|a+b| > \max\{|a|, |b|\}$ para algum a e algum b. Podemos supor $|a| \geqslant |b|$, daí $|c| \leqslant 1$ onde $b = ac$. Portanto,

$$|a| < |a+b| = |a||1+c| \leqslant |a|.$$

Absurdo! Isso mostra a necessidade de termos a desigualdade ultramétrica.

Agora, suponha que $|\cdot|$ satisfaça a desigualdade ultramétrica. Seja $a \in K$ tal que $|a| \leqslant 1$, então

$$|a+1| \leqslant \max\{|a|, |1|\} = 1.$$

O que completa a demonstração.

Sejam $|\cdot|$ e $||\cdot||$ dois valores absolutos não-arquimedianos e equivalentes. Ou seja, $\alpha = 1$ e existe λ real positivo tal que $||\cdot|| = |\cdot|^\lambda$. Pela demonstração do Lema 1.1, temos que $\alpha_1 = \alpha^\lambda = 1$. ■

Se o valor absoluto é não-arquimediano, então pelo lema acima temos que $|b| \leqslant \max\{|a+b|, |a|\}, \forall\, a, b \in K$. Supondo $|a| < |b|$, essa desigualdade se torna $|b| \leqslant |a+b|$. Mas, pela desigualdade ultramétrica, $|a+b| \leqslant |b|$, logo $|a+b| = |b|$. Assim provamos o seguinte resultado:

Lema 1.4. *Seja $|\cdot|$ um valor absoluto não-arquimediano. Se $|a| < |b|$, então $|a+b| = |b|$.*

Lema 1.5. *Um valor absoluto $|\cdot|$ sobre o corpo K é não-arquimediano se, e somente se, $|a| \leqslant 1$, para todo a no anel gerado por 1 ($\mathbb{Z}$ se car(K) = 0 e $\mathbb{F}_p$ se car(K) = p) em K.*

Demonstração: Primeiro vamos mostrar que a condição é necessária. Se $|\cdot|$ é não-arquimediano então

$$|2| = |1+1| \leqslant 1,$$

pela desigualdade ultramétrica. Segue por indução e pela Propriedade 1 (c) que $|n| \leqslant 1$, para todo n no anel gerado por 1.

Vamos argumentar de forma análoga a demonstração do Lema 1.2 para mostrar a suficiência. Pela observação feita após o enunciado do Lema 1.2, podemos supor que $|\cdot|$ satisfaz a desigualdade triangular. Então, para $a, b \in K$ e n inteiro positivo, temos

$$\begin{aligned} |a+b|^n &= \left|\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}\right| \leqslant \sum_{i=0}^{n} \left|\binom{n}{i}\right| |a^i||b^{n-i}| \\ &\leqslant \sum_{i=0}^{n} |a^i||b^{n-i}| \leqslant (n+1)\left(\max\{|a|, |b|\}\right)^n \end{aligned}$$

onde a segunda desigualdade segue da hipótese que $|m| \leqslant 1$ para todo m no anel gerado por 1. Agora, tome a raiz n-ésima e faça $n \to \infty$. O resultado segue pelo Lema 1.3. ■

O valor absoluto p-ádico sobre $\mathbb{Q}$ é não-arquimediano. De fato, $v(a)_p \geqslant 0$, para todo $a \in \mathbb{Z}$ (o anel gerado por um). Assim, $|a|_p \leqslant 1$, para todo $a \in \mathbb{Z}$. A conclusão segue pelo lema acima.

Corolário 1.1. *Sejam $K \subset F$ corpos e seja $|\cdot|$ um valor absoluto em F. Então $|\cdot|$ é não-arquimediano em F se, e somente se, sua restrição a K é não-arquimediana.*

Demonstração: Basta observar que $\langle 1\rangle \subset K \subset F$, onde $\langle 1\rangle$ = anel gerado por 1. ■

Corolário 1.2. *Se K tem característica prima, então toda valorização em K é não-arquimediana.*

Demonstração: Lembre que se K tem característica prima então contém um corpo finito. Pela Propriedade 1 (d) toda restrição de um valor absoluto a tal corpo é o valor absoluto trivial que é não-arquimediano. ■

Vamos introduzir algumas noções de análise no contexto de corpos com valores absolutos para falar de completude de um corpo.

Sejam K um corpo com valor absoluto $|\cdot|$ e $\{a_n\}_{n\geqslant 1}$ uma sequência em K. Dizemos que b é o limite dessa sequência com relação a $|\cdot|$ se, para todo ϵ real positivo, existir $n_0 = n_0(\epsilon)$ tal que $|a_n - b| < \epsilon$, para todo $n \geqslant n_0$. É fácil verificar que, quando o limite de uma sequência existe, ele é único. Se, para todo ϵ real positivo dado, existir $n_1 = n_1(\epsilon)$ tal que

$$m, n > n_1 \Rightarrow |a_m - a_n| < \epsilon$$

então dizemos que $\{a_n\}$ é uma sequência de Cauchy (ou fundamental). Toda sequência que tem limite é de Cauchy, mas a recíproca não é verdadeira, como veremos no exemplo abaixo.

Exemplo 2. Considere $\{a_n\}_{n\geqslant 1}$, contida no corpo $\mathbb{Q}$, tal que $a_1 = 2$ e

$$a_n^2 + 1 \equiv 0 \mod 5^n \tag{1.1}$$
$$a_{n+1} \equiv a_n \mod 5^n, \tag{1.2}$$

e o valor absoluto 5-ádico.

Primeiro vamos mostrar que essa sequência é bem definida. Conhecendo a_n, temos por (1.2) que $a_{n+1} = a_n + b5^n$ para algum b inteiro. Vamos encontrar b para que essa última equação satisfaça (1.1), ou seja,

$$(a_n + b5^n)^2 + 1 \equiv 0 \mod 5^{n+1}.$$

Desenvolvendo esse quadrado, podemos reescrever essa congruência como

$$(a_n^2 + 1) + 2a_n b5^n \equiv 0 \mod 5^{n+1}.$$

Por (1.1), podemos tomar $c_n 5^n = a_n^2 + 1$, daí

$$c_n + 2a_n b \equiv 0 \mod 5$$

e, como 5 não divide a_n, essa congruência tem solução. Assim, existe a_{n+1} satisfazendo as hipóteses.

Agora vamos mostrar que essa sequência é de Cauchy. Para $m > n$, temos

$$|a_m - a_n|_5 \leqslant \max\{|a_{j+1} - a_j|_5, j = n, \ldots, m-1\}.$$

E, para todo j inteiro positivo, $|a_{j+1} - a_j|_5 = |b5^j|_5 \leqslant 5^{-j}$. Portanto,

$$|a_m - a_n|_5 \leqslant \max\{5^{-j}, j = n, \ldots, m-1\} = 5^{-n},$$

o que implica que $\{a_n\}$ é uma sequência de Cauchy.

Suponha que $a \in \mathbb{Q}$ seja o limite de $\{a_n\}$, ou seja, dado $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que

$$n \geqslant n_0 \Rightarrow |a_n - a|_5 < \epsilon.$$

Por (1.1), temos $|a_n^2 + 1|_5 \leqslant 5^{-n}$, logo, o limite de $|a_n^2 + 1|_5$ é zero. Por outro lado, se $n \geqslant n_0$, então

$$\begin{aligned} ||a_n^2 + 1|_5 - |a^2 + 1|_5|_\infty &\leqslant |(a_n^2 + 1) - (a^2 + 1)|_5 \\ &= |a_n - a|_5 |a_n - a + 2a|_5. \end{aligned}$$

Como esse valor absoluto é não-arquimediano, isto é, podemos tomar $\alpha = 1$ na definição 2, o Lema 1.2 implica que $|\cdot|_5$ satisfaz a desigualdade triangular. Daí,

$$\begin{aligned} ||a_n^2 + 1|_5 - |a^2 + 1|_5|_\infty &\leqslant |a_n - a|_5^2 + |a_n - a|_5|2a|_5 \\ &< \epsilon^2 + |a|_5\epsilon. \end{aligned}$$

Logo $|a^2 + 1|_5$ é o limite de $|a_n^2 + 1|_5$. Pela unicidade do limite, segue que $|a^2 + 1|_5 = 0$, daí, pela definição de valor absoluto, $a^2 + 1 = 0$. Mas não existe $a \in \mathbb{Q}$ que satisfaça essa igualdade. Logo $\{a_n\}$ não tem limite, apesar de ser de Cauchy.

Um corpo é dito completo com relação ao valor absoluto $|\cdot|$ se toda sequência de Cauchy tem limite. E um subconjunto S de K é dito denso em K se, para todo $a \in K$ e $\epsilon > 0$, $\{x \in K : |a - x| < \epsilon\} \cap S \neq \emptyset$. Ou, equivalentemente, S é denso em K se, para todo $a \in K$, existir uma sequência $\{x_n\}$ em S tal que a é o limite dela.

Por exemplo, $\mathbb{Q}$ não é completo com relação ao valor absoluto $|\cdot|_m$, onde $m = p$ primo ou $m = \infty$. E $\mathbb{Q}$ é denso em $\mathbb{R}$ com o valor absoluto dos reais.

Sejam K um corpo com valorização $|\cdot|$ e F um corpo contendo K. Um valor absoluto $||\cdot||$ sobre F é uma extensão de $|\cdot|$ se eles assumirem os mesmos valores em K.

Se $|\cdot|$ é um valor absoluto sobre o corpo K, então definimos que um corpo $F \supset K$ junto com a valor absoluto $||\cdot||$, extensão de $|\cdot|$, é um completamento de K com respeito a $|\cdot|$ se F é completo e K é denso em F.

Teorema 1.1. *Seja K um corpo com valor absoluto $|\cdot|$. Um completamento de K existe e é único a menos de isomorfismo.*

A idéia da demonstração é tomar um valor absoluto equivalente a $|\cdot|$ que satisfaça a desigualdade triangular, assim K tem a estrutura de um espaço métrico, logo tem um completamento com respeito a métrica. Mostra-se que tal completamento tem a estrutura de um corpo e $||\alpha|| = \mathrm{D}(\alpha, 0)$ é o valor absoluto sobre ele, onde D é a métrica do completamento. Para maiores detalhes, veja [6].

1.2 Valor Absoluto Não-Arquimediano

Seja K um corpo com valor absoluto não-trivial não-arquimediano $|\cdot|$. Tome $\mathcal{O} = \{a \in K : |a| \leqslant 1\}$ e $\mathfrak{p} = \{a \in K : |a| < 1\}$. Segue das propriedades de valor absoluto não-arquimediano que $\mathcal{O}$ é um domínio de integridade que chamamos de *anel dos inteiros de K* e que $\mathfrak{p}$ é seu ideal.

Os elementos de K que tem valor absoluto igual a 1 são chamados de unidades. Tais elementos formam um grupo multiplicativo, o *grupo das unidades*, que denotaremos por $\mathcal{O}^* = \{a \in K : |a| = 1\}$. Vamos mostrar que $\mathcal{O}^*$ é realmente um grupo. A associatividade e a existência do elemento neutro são óbvios, então falta apenas verificar a existência do elemento inverso. Seja $a \in \mathcal{O}^*$. Como K é um corpo e $a \neq 0$, existe $b \in K$ tal que $ab = 1$.

Temos que $|b| = |a||b| = 1$, ou seja, $b \in \mathcal{O}^*$. Mais do que isso, os únicos elementos de $\mathcal{O}$ que possuem inverso em $\mathcal{O}$ são as unidades. De fato, sejam $a, b \in \mathcal{O}$ (i.e., $|a| \leqslant 1$ e $|b| \leqslant 1$) tais que $ab = 1$ então $|a||b| = 1$ de onde concluímos que $|a| = |b| = 1$. Assim, $\mathfrak{p}$ é ideal maximal de $\mathcal{O}$ e o anel quociente $k = \mathcal{O}/\mathfrak{p}$ é um corpo chamado de *corpo residual*. Note que $\mathfrak{p}$ é o único ideal maximal pois se I é um ideal de $\mathcal{O}$ tal que $I \not\subset \mathfrak{p}$ então I contém uma unidade e, portanto, $1 \in I$.

Ainda definimos o *grupo de valores* como o subgrupo multiplicativo dos reais positivos $\mathcal{V} = \{|a| : a \in K^*\}$, onde $K^* = K\backslash\{0\}$.

Observação. A função $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ definida por $f(x) = x^\lambda$ com $\lambda > 0$ é estritamente crescente com $f(0) = 0$ e $f(1) = 1$. Assim, se $|\cdot|$ e $||\cdot||$ são equivalentes e $a \in K$ temos

$$|a| < 1 \Leftrightarrow ||a|| < 1 \quad \text{e} \quad |a| = 1 \Leftrightarrow ||a|| = 1.$$

Portanto, o grupo das unidades e o ideal maximal são invariantes dentro de uma mesma classe de equivalência de valores absolutos.

Seja $\overline{K}$ o completamento de K com respeito a $|\cdot|$ e sejam $\mathcal{O}_{\overline{K}}$, $\mathfrak{p}_{\overline{K}}$ seus respectivos anel dos inteiros e ideal maximal. Note que $\mathcal{O}_K = \mathcal{O}_{\overline{K}} \cap K$ e $\mathfrak{p}_K = \mathfrak{p}_{\overline{K}} \cap K$. Então existe um homomorfismo

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & k_{\overline{K}} = \mathcal{O}_{\overline{K}}/\mathfrak{p}_{\overline{K}} \\ x & \mapsto & x + \mathfrak{p}_{\overline{K}} \end{array}$$

induzido pela inclusão $\mathcal{O}_K \hookrightarrow \mathcal{O}_{\overline{K}}$. O núcleo dessa aplicação é $\mathfrak{p}_K$, logo temos uma aplicação natural

$$k_K \longrightarrow k_{\overline{K}}. \tag{1.3}$$

Tome $\alpha \in \mathcal{O}_{\overline{K}}$, pela definição de $\overline{K}$ existe um $a \in K$ tal que $|\alpha - a| < 1$. Assim, $\alpha - a$ é um elemento de $\mathfrak{p}_{\overline{K}}$ e temos

$$|a| \leqslant \max\{|a - \alpha|, |\alpha|\} \leqslant 1,$$

ou seja, $a \in \mathcal{O}_K = \mathcal{O}_{\overline{K}} \cap K$. Portanto, $\alpha + \mathfrak{p}_{\overline{K}} = a + \mathfrak{p}_{\overline{K}}$ é a imagem de $a + \mathcal{O}_K$, ou seja, a aplicação (1.3) é sobrejetiva. Assim, temos que (1.3) é um isomorfismo, provando o seguinte resultado

Lema 1.6. *A aplicação $\varphi : k_K \longrightarrow k_{\overline{K}}$ definida por $\varphi(a+\mathfrak{p}_K) = a+\mathfrak{p}_{\overline{K}}$ é um isomorfismo.*

Definição 4. Dizemos que um valor absoluto não-arquimediano $|\cdot|$ é discreto se $\mathcal{V}$ é um subgrupo discreto de $\mathbb{R}_+^*$. Isto é, se existe algum $\delta > 0$ fixo tal que

$$1 - \delta < |a| < 1 + \delta \Rightarrow |a| = 1.$$

De uma forma mais geral, podemos definir valor absoluto não-arquimediano discreto como o valor absoluto que, para todo $|a| \in \mathcal{V}$, existe δ tal que

$$b \in K^* \text{ e } 0 \leqslant ||a| - |b||_\infty < \delta \Rightarrow |a| = |b|.$$

Lema 1.7. *Uma condição necessária e suficiente para que um valor absoluto seja discreto é que o ideal maximal $\mathfrak{p}$ seja principal.*

Demonstração: Vamos mostrar primeiro a suficiência. Seja $\pi \in \mathfrak{p}$ tal que $\mathfrak{p} = \pi\mathcal{O}$. Se $a \in K$ é tal que $|a| < 1$ então $a \in \mathfrak{p}$ e, por hipótese, existe $b \in \mathcal{O}$ tal que $a = \pi b$. Logo $|a| \leqslant |\pi| < 1$. E se $|a| > 1$ então $a^{-1} \in \mathfrak{p}$ e daí $|a|^{-1} \leqslant |\pi|$, ou seja, $|a| \geqslant |\pi|^{-1} > 1$. Portanto, se $|a| \in (|\pi|, |\pi|^{-1})$ então $|a| = 1$. Tomando $\delta = \min\{1 - |\pi|, |\pi|^{-1} - 1\}$, segue pela definição que $|\cdot|$ é discreto.

Agora, provaremos a necessidade. Suponha que o valor absoluto $|\cdot|$ é discreto com δ como na definição 4. O conjunto $A = \{|a| : |a| < 1\}$ é limitado então existe $\sup A$ que denotaremos por L. Pela definição de supremo, para todo $n \geqslant 1$, existe $|a_n| \in A$ com $|a_n| > L - 1/n$. Tome n_0 tal que $\delta > 1/(Ln_0 - 1)$, então se $n, m \geqslant n_0$ temos

$$\frac{|a_n|}{|a_m|} - 1 < \frac{L}{L - \frac{1}{m}} - 1 = \frac{1}{Lm - 1} \leqslant \frac{1}{Ln_0 - 1} < \delta$$

e

$$\frac{|a_n|}{|a_m|} - 1 > \frac{L - \frac{1}{n}}{L} - 1 = -\frac{1}{Ln} > -\frac{1}{Ln_0 - 1} > -\delta$$

Portanto $|a_n| = |a_m|$, para todo $n, m \geqslant n_0$. Em particular, para todo $n \geqslant n_0$,

$$|a_{n_0}| = |a_n| > L - \frac{1}{n}$$

daí

$$L \geqslant |a_{n_0}| \geqslant \lim_{n\to\infty} L - \frac{1}{n} = L$$

e segue que

$$|a_{n_0}| = L.$$

Assim, temos $L = \max A$, e seja $\pi = a_{n_0}$, logo $|\pi| = L$. Então para $a \in \mathfrak{p}$ temos $|a| < 1$ (i.e., $|a| \in A$) logo $|a| \leqslant |\pi|$. Tome $b \in K$ tal que $a = b\pi$, daí $|b| = |a||\pi^{-1}| \leqslant 1$, ou seja, $b \in \mathcal{O}$. Portanto, π gera $\mathfrak{p}$. ■

Se $\mathfrak{p} = \pi\mathcal{O}$, dizemos que π é um elemento gerador de $\mathfrak{p}$. Temos que quaisquer dois elementos geradores têm o mesmo valor absoluto. De fato, sejam π e π_1 dois geradores. Então existem $a, b \in \mathcal{O}$ tais que $\pi = a\pi_1$ e $\pi_1 = b\pi$. Assim,

$$|\pi| = |a||\pi_1| \leqslant |\pi_1| = |b||\pi| \leqslant |\pi|,$$

ou seja, $|\pi| = |\pi_1|$.

Mais que isso, dois geradores são sempre associados (i.e., $\pi = \pi_1\epsilon$ e $|\epsilon| = 1$) pois se $\pi = \pi_1 a$ com $a \in \mathcal{O}$ temos, pelo que acabamos de ver, $|a| = |\pi||\pi_1|^{-1} = 1$, ou seja, $a \in \mathcal{O}^*$.

Sejam $|\cdot|$ discreto e π um gerador de $\mathfrak{p}$. Vamos mostrar que, para todo $a \in K^*$, existe n inteiro tal que $|a| = |\pi|^n$. Dado $a \in K^*$, tome n inteiro de forma que

$$|\pi|^n \leqslant |a| < |\pi|^{n-1}.$$

Daí,

$$1 \leqslant \left|\frac{a}{\pi^n}\right| < |\pi|^{-1},$$

isto é, $|a/\pi^n| \in [1, |\pi|^{-1}) \subset (|\pi|, |\pi|^{-1})$. Então, pela demonstração do Lema 1.7, $|a/\pi^n| = 1$, logo $|a| = |\pi|^n$. Desse fato segue que $\mathcal{V} = \langle|\pi|\rangle$. Note que podemos escrever $a = \pi^n b$, onde $b \in \mathcal{O}^*$. Daí segue que se π divide ab então π divide a ou divide b. Com esses fatos, vemos que o elemento gerador é um elemento primo do anel $\mathcal{O}$.

Definimos n como a *ordem* de a e escrevemos $n = \text{ord } a$. Precisamos mostrar duas propriedades da aplicação ord: $K^* \longrightarrow \mathbb{Z}$. A primeira é que ord a não depende da escolha do elemento primo. E a segunda propriedade é que ord a não depende da escolha do valor absoluto dentro de uma classe de equivalência. De fato,

(i) Suponha que $|a| = |\pi|^n$ e $|a| = |\pi_1|^m$, onde π e π_1 são geradores de $\mathfrak{p}$. Então $|\pi|^n = |\pi_1|^m$, e como $|\pi| = |\pi_1| \neq 1$, segue que $n = m$.

(ii) Temos que $|\cdot| \sim ||\cdot||$ se, e somente se, $|\cdot|^\lambda = ||\cdot||$, para algum $\lambda > 0$. Suponha $|a| = |\pi|^n$ e $||a|| = ||\pi||^m$. Então,

$$||\pi||^m = ||a|| = |a|^\lambda = |\pi|^{n\lambda} = ||\pi||^n$$

e, como $||\pi|| \neq 1$, concluímos que $n = m$.

Com essas propriedades podemos definir $v_\mathfrak{p} : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ dado por $v_\mathfrak{p}(a) = \text{ord } a$ se $a \neq 0$ e $v_\mathfrak{p}(0) = \infty$. Então essa aplicação é uma valorização, a *valorização* $\mathfrak{p}$*-ádica* de K.

Assim, um valor absoluto não-arquimediano discreto induz uma valorização. Note que os axiomas de valor absoluto não-arquimediano, isto é, (ii) da definição 2 e desigualdade ultramétrica, são equivalentes aos axiomas (ii) e (iii) da definição 1, respectivamente, quando o valor absoluto é discreto.

Vimos que todo ideal não trivial de $\mathcal{O}$ está contido em $\mathfrak{p}$. Assim, como $\mathfrak{p}$ é gerado por um elemento, os ideais não triviais de $\mathcal{O}$ são

$$\mathfrak{p}^n = \pi^n\mathcal{O} = \{x \in K \mid v_\mathfrak{p}(x) \geqslant n\},\ n \geqslant 1.$$

Portanto, $\mathcal{O}$ é um anel de ideais principais. Note que

$$\mathcal{O} \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots \supset \{0\}.$$

Agora, considere o endomorfismo $\mathfrak{p}^n \longrightarrow \mathcal{O}/\mathfrak{p}$ entre os grupos aditivos definido por $\pi^n a \mapsto a \mod \mathfrak{p}$, para algum π primo. O núcleo dessa aplicação é $\mathfrak{p}^{n+1}$ então, pelo Teorema dos homomorfismos, $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$.

Podemos resumir os resultados acima como as seguintes propriedades.

Propriedades 2. Seja π um gerador de $\mathfrak{p}$. Assim,

a) se π_1 é outro gerador de $\mathfrak{p}$ então π e π_1 são associados;

b) todo elemento de K^* é da forma $\pi^n b$ para algum $n \in \mathbb{Z}$ e algum $b \in \mathcal{O}^*$;

c) π é primo;

d) se I é um ideal de $\mathcal{O}$ então $I = \langle \pi^n \rangle = \mathfrak{p}^n$ para algum $n \in \mathbb{N}$.

Vamos estender as noções da análise real aos corpos com valor absoluto, em especial aos corpos completos. Como veremos no primeiro lema abaixo, em algumas situações nos deparamos com algo mais simples que no caso real.

Dada uma sequência $\{a_n\}$ em K, a soma infinita $a_1 + a_2 + a_3 + \cdots$ é dita uma série. Tomamos

$$s_N = \sum_{n=0}^{N} a_n.$$

Assim, a série converge para s se $s = \lim_{N\to\infty} s_N$.

Lema 1.8. *Seja K um corpo completo com relação a $|\cdot|$. Então a série $\sum_{n=0}^{\infty} a_n$ converge se, e somente se, a sequência $\{a_n\}_{n\geqslant 0}$ converge para zero.*

Demonstração: Suponha que $\sum_{n=0}^{\infty} a_n$ é convergente com limite igual a s. Então

$$\lim_{N\to\infty} a_N = \lim_{N\to\infty} s_N - s_{N-1} = \lim_{N\to\infty} s_N - \lim_{N\to\infty} s_{N-1} = s - s = 0.$$

Agora, suponha que a_n converge para zero, ou seja, dado $\epsilon > 0$ existe $n_0 \in \mathbb{N}$ tal que se $n \geqslant n_0$, então $|a_n| < \epsilon$. Sejam $M > N \geqslant n_0$, então

$$|s_M - s_N| = |a_{N+1} + \cdots + a_M| \leqslant \max_{N+1\leqslant n\leqslant M} |a_n| < \epsilon.$$

Logo $\{s_N\}_{N\geqslant 0}$ é uma sequência de Cauchy e, como K é completo, é convergente. ■

Lema 1.9. *Seja K completo com relação ao valor absoluto discreto $|\cdot|$ e seja π um gerador de $\mathfrak{p}$. Tome $\mathcal{R} \subset \mathcal{O}$ o conjunto de representantes de $\mathcal{O}/\mathfrak{p}$. Então todo $a \in \mathcal{O}$ é unicamente determinado por*

$$a = \sum_{n=0}^{\infty} a_n \pi^n, \quad a_n \in \mathcal{R}.$$

Reciprocamente, toda série $\sum a_n \pi^n$ com $a_n \in \mathcal{R}$ converge para algum elemento $a \in \mathcal{O}$.

Demonstração: Dado $a \in \mathcal{O}$, existe um único $a_0 \in \mathcal{R}$ tal que $a - a_0 \in \mathfrak{p}$ (i.e., $a + \mathfrak{p} = a_0 + \mathfrak{p}$) e então $a = a_0 + \pi b_1$ para algum $b_1 \in \mathcal{O}$. Existe um único $a_1 \in \mathcal{R}$ tal que $b_1 - a_1 \in \mathfrak{p}$ e então $b_1 = a_1 + \pi b_2$ para algum $b_2 \in \mathcal{O}$. Continuando esse processo, temos para todo N

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots + a_N\pi^N + b_{N+1}\pi^{N+1},$$

onde $a_n \in \mathcal{R}$, $n = 0, 1, \ldots, N$, e $b_{N+1} \in \mathcal{O}$. Tome $s_N = a_0 + a_1\pi + \cdots + a_N\pi^N$, daí

$$|a - s_N| = |b_{N+1}\pi^{N+1}| \leqslant |\pi|^{N+1}.$$

Portanto, a série $\sum a_n\pi^n$ converge para a.

Considere a soma

$$\sum_{n=0}^{\infty} a_n\pi^n, \text{ com } a_n \in \mathcal{R}.$$

Como $|a_n\pi^n| \leqslant |\pi|^n \to 0$ quando $n \to \infty$, pelo Lema 1.8, essa série converge para um $a \in K$. Isto é, dado $\epsilon > 0$, existe $N_0 = N_0(\epsilon)$ inteiro positivo tal que se $N \geqslant N_0$ então $|a - s_N| < \epsilon$. Além disso, para todo N temos

$$|s_N| = \left|\sum_{n=0}^{N} a_n\pi^n\right| \leqslant \max_{0\leqslant n\leqslant N} |a_n\pi^n| \leqslant 1.$$

Considere $\epsilon = 1$ e $N \geqslant N_0$, daí

$$|a| = |a - s_N + s_N| \leqslant \max\{|a - s_N|, |s_N|\} \leqslant 1$$

e, portanto, $a \in \mathcal{O}$. ■

Corolário 1.3. *Adicionando às hipóteses do Lema 1.9 que* $0 \in \mathcal{R}$*, temos que todo* $a \in K^*$ *é unicamente determinado por*

$$a = \sum_{n=N}^{\infty} a_n\pi^n,$$

para algum N *inteiro, com* $a_n \in \mathcal{R}$ *e* $a_N \neq 0$*.*

Demonstração: Basta observar que $\pi^{-N}a \in \mathcal{O}$ para algum $N \in \mathbb{Z}$. ■

Como exemplo temos o corpo dos números p-ádicos $\mathbb{Q}_p$ (o completamento de $\mathbb{Q}$ com relação ao valor absoluto p-ádico) cujo anel dos inteiros é $\mathbb{Z}_p$, o anel dos inteiros p-ádicos. Podemos tomar $\pi = p$ e $\mathcal{R} = \{0, 1, \ldots, p-1\}$ pois $\mathcal{O}_{\mathbb{Q}_p}/\mathfrak{p}_{\mathbb{Q}_p} = \mathbb{Z}_p/p\mathbb{Z}_p$ e $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. Uma introdução aos números p-ádicos pode ser encontrada no capítulo 5 de [22].

1.3 Lema de Hensel

Um corpo K completo com relação ao valor absoluto (não-trivial) discreto não-arquimediano $|\cdot|$ tal que o corpo residual $k = \mathcal{O}/\mathfrak{p}$ é finito é chamado de *corpo local*

A expressão *Lema de Hensel*, hoje, significa qualquer resultado que apresente condições suficientes para que um polinômio tenha raiz no anel dos inteiros de um corpo local. Neste trabalho veremos algumas versões desse lema.

Lema 1.10 (Lema de Hensel I). *Seja* K *completo com respeito a* $|\cdot|$ *e seja* $f(x) \in \mathcal{O}[x]$*. Se* $a_0 \in \mathcal{O}$ *satisfaz*

$$|f(a_0)| < |f'(a_0)|^2,$$

onde $f'(x)$ é a derivada formal, então existe $a \in \mathcal{O}$ tal que $f(a) = 0$. Além disso, a é a única solução de $f(x) = 0$ que satisfaz

$$|a - a_0| \leqslant \frac{|f(a_0)|}{|f'(a_0)|}.$$

Demonstração: Sejam $f_j(x) \in \mathcal{O}[x]$, $j = 1, 2$, definidas pela identidade

$$f(x + y) = f(x) + f_1(x)y + f_2(x, y)y^2 \tag{1.4}$$

com x e y indeterminadas independentes. Então

$$f'(x) = \lim_{y \to 0} \frac{f(x + y) - f(x)}{y} = f_1(x).$$

Tome $b_0 = -f(a_0)/f_1(a_0)$ então $b_0 \in \mathcal{O}$. De fato,

$$|b_0| = \left| \frac{f(a_0)}{f_1(a_0)} \right| < |f_1(a_0)| \leqslant 1$$

onde a primeira desigualdade vem da hipótese e a segunda de $f_1(x) \in \mathcal{O}[x]$ e $a_0 \in \mathcal{O}$. Assim, $f(a_0) + b_0 f_1(a_0) = 0$ com $b_0 \in \mathcal{O}$. Como $f_2(x, y) \in \mathcal{O}[x, y]$ e $a_0, b_0 \in \mathcal{O}$, por (1.4), temos

$$|f(a_0 + b_0)| = |f_2(a_0, b_0)\ b_0^2| \leqslant |b_0^2| = \frac{|f(a_0)|^2}{|f_1(a_0)|^2} < |f(a_0)|.$$

Novamente usando (1.4), temos

$$f(a_0 + b_0) = f(a_0) + f_1(a_0)b_0 + f_2(a_0, b_0)b_0^2$$

e

$$f(a_0) = f(a_0 + b_0) + f_1(a_0 + b_0)(-b_0) + f_2(a_0 + b_0, -b_0)b_0^2.$$

Somando as duas equações acima e simplificando temos

$$f_1(a_0 + b_0) - f_1(a_0) = b_0(f_2(a_0, b_0) + f_2(a_0 + b_0, -b_0))$$

daí

$$|f_1(a_0 + b_0) - f_1(a_0)| \leqslant |b_0| < |f_1(a_0)|$$

e, assim, $|f_1(a_0 + b_0)| = |f_1(a_0)|$ pelo Lema 1.4.

Tome $a_1 = a_0 + b_0$, então $|f(a_1)| < |f(a_0)|$ e $|f'(a_1)| = |f'(a_0)|$. Logo $|f(a_1)| < |f'(a_1)|^2$ e temos a hipótese do lema para $a_1 \in \mathcal{O}$. Repetindo o processo, construimos uma sequência $a_{n+1} = a_n + b_n$ com $b_n = -f(a_n)/f'(a_n)$ tal que

$$|f(a_{n+1})| < |f(a_n)| \quad \text{e} \quad |f'(a_n)| = |f'(a_0)|.$$

Seja $m = v_{\mathfrak{p}}(f'(a_0))$. Queremos mostrar que $|f(a_n)| \leqslant |\pi|^{2m+n+1}$. Para $n = 0$ e $n = 1$,

$$|f(a_0)| < |f'(a_0)|^2 = |\pi|^{2m} \Rightarrow |f(a_0)| \leqslant |\pi|^{2m+0+1}$$

$$|f(a_1)| < |f(a_0)| \leqslant |\pi|^{2m+1} \Rightarrow |f(a_1)| \leqslant |\pi|^{2m+1+1}.$$

Suponha que a desigualdade seja válida para $n-1$, Então

$$|f(a_n)| < |f(a_{n-1})| \leqslant |\pi|^{2m+n} \Rightarrow |f(a_n)| \leqslant |\pi|^{2m+n+1}.$$

Portanto com $n \to \infty$ temos $|f(a_n)| \to 0$ o que implica $f(a_n) \to 0$.

Além disso,

$$|a_{n+1} - a_n| = |b_n| = \frac{|f(a_n)|}{|f_1(a_n)|} = \frac{|f(a_n)|}{|f_1(a_0)|} \leqslant |\pi|^{m+n+1}.$$

Portanto $\{a_n\}$ é uma sequência de Cauchy e, pela completude, converge para algum a.

Vamos mostrar que $f(a_n)$ converge para $f(a)$. Daí, pela unicidade do limite, teremos $f(a) = 0$. Se $f(x) = c_0 + c_1 x + \cdots + c_d x^d$ então

$$\begin{aligned} |f(a_n) - f(a)| &= |c_1(a_n - a) + \cdots + c_r(a_n^d - a^d)| \\ &\leqslant \max_{1 \leqslant k \leqslant d} \{|c_k||a_n^k - a^k|\} \\ &\leqslant \max_k \{|a_n^k - a^k|\} \\ &= |a_n - a| \max_k \{1, |a_n^{k-1} + a_n^{k-2}a + \cdots a_n a^{k-2} + a^{k-1}|\} \\ &\leqslant |a_n - a|. \end{aligned}$$

Assim, temos a convergência.

Falta mostrar a última parte do lema. Temos

$$a - a_0 = \sum_{n=0}^{\infty} b_n$$

assim, para todo $\epsilon > 0$, existe N_0 tal que se $N > N_0$ então $|a - a_0 - \sum_{n=0}^{N_0} b_n| < \epsilon$. E, lembrando que $|b_n| = |f(a_n)|/|f'(a_n)| < |f(a_0)|/|f'(a_0)|$ segue

$$\left| \sum_{n=0}^{N_0} b_n \right| \leqslant \max_{0 \leqslant n \leqslant N_0} |b_n| < \frac{|f(a_0)|}{|f'(a_0)|}.$$

Tome $\epsilon < |f(a_0)|/|f'(a_0)|$, então

$$|a - a_0| \leqslant \max \left\{ \left| a - a_0 - \sum_{n=0}^{N_0} b_n \right|, \left| \sum_{n=0}^{N_0} b_n \right| \right\} < \frac{|f(a_0)|}{|f'(a_0)|}.$$

Suponha agora que exista $\alpha \neq a$ tal que $f(\alpha) = 0$ e $|\alpha - a_0| \leqslant |f(a_0)|/|f'(a_0)|$. Seja $\alpha = a + \beta$, então

$$0 = f(a + \beta) - f(a) = f_1(a)\beta + f_2(a, \beta)\beta^2$$

daí,

$$|f_1(a)| = |f_2(a,\beta)||\beta| \leqslant |\beta|.$$

Por outro lado,

$$|\beta| = |\alpha - a| \leqslant \max\{|\alpha - a_0|, |a - a_0|\} \leqslant \frac{|f(a_0)|}{|f_1(a_0)|} < |f_1(a_0)| = |f_1(a)|$$

o que nos dá uma contradição. ■

Uma versão mais simples do Lema de Hensel que, na verdade, é um caso particular da versão I é a seguinte:

Lema 1.11 (Lema de Hensel II). *Seja K completo com respeito a $|\cdot|$ e seja $f(x) \in \mathcal{O}[x]$. Se $a_0 \in \mathcal{O}$ satisfaz*

$$f(a_0) \equiv 0 \mod \pi \quad e \quad f'(a_0) \not\equiv 0 \mod \pi,$$

onde $f'(x)$ é a derivada formal, então existe $a \in \mathcal{O}$ tal que $f(a) = 0$ e $a \equiv a_0 \mod \pi$.

Exemplo 3. Veremos agora algumas aplicações do Lema de Hensel I.

(i) Seja $p \neq 2$. Seja $b \in \mathbb{Z}_p$ com $|b|_p = 1$ e suponha que exista $a_0 \in \mathbb{Z}_p$ tal que $|a_0^2 - b|_p < 1$. Definimos $f(x) = x^2 - b$, daí $|f'(a_0)|_p = |2a_0|_p = 1$ pois $|a_0| = 1$ pelas hipóteses. Segue pelo Lema 1.10 que $b = a^2$ para algum $a \in \mathbb{Z}_p$.

(ii) Seja $b \in \mathbb{Z}_2$ com $b \equiv 1 \mod 8$. Tomando $f(x) = x^2 - b$ temos $|f(1)|_2 \leqslant 2^{-3}$ e $|f'(1)|_2 = 2^{-1}$. Então, pelo Lema 1.10, $b = a^2$ para algum $a \in \mathbb{Z}_2$.

(iii) Seja $p \neq 3$. Seja $b \in \mathbb{Z}_p$ com $|b|_p = 1$. Suponha que $b \equiv a_0^3 \mod p$, para algum $a_0 \in \mathbb{Z}_p$. Aplicando o Lema 1.10 a função $f(x) = x^3 - b$, concluimos que $b = a^3$ para algum $a \in \mathbb{Z}_p$.

(iv) Se $b \in \mathbb{Z}_3$ com $|b|_3 = 1$, então uma condição necessária e suficiente para que b seja um cubo é que $b \equiv \pm 1 \mod 9$. Basta aplicar o Lema 1.10 a $f(x) = x^3 - b$ com $a_0 = \pm(1 + 3t)$, onde $t \in \{-1, 0, 1\}$, pois $b \equiv \pm(1 + 3t)^3 \mod 27$ para algum t.

A quinta aplicação será colocada como um lema devido a sua importância.

Lema 1.12. *Seja K um corpo completo com relação ao valor absoluto não-arquimediano $|\cdot|$ e com corpo residual k com $q = p^m$ elementos, onde car(k) = p. Então K contém todas as $(q-1)$-ésimas raízes da unidade.*

Demonstração: Como k é finito com $q = p^m$ elementos, o grupo multiplicativo k^* é cíclico de ordem $q - 1$. Assim, $\alpha^q = \alpha$ e $p\alpha = 0$ para todo elemento α de k. Em particular, $p \cdot \bar{1} = 0$ onde a barra denota redução módulo $\mathfrak{p}$, logo $p \cdot 1 \in \mathfrak{p}$. Daí, $(q-1) \cdot 1 \in \mathcal{O}^*$ pois, caso contrário, teríamos

$$1 = |-1| = |((q-1) - p^m) \cdot 1| \leqslant \max\{|(q-1) \cdot 1|, |p \cdot 1|^m\} < 1.$$

Considere a função $f(x) = x^{q-1} - 1$. Para cada $\alpha \in k^*$, tome $a_0 \in \mathcal{O}^*$ tal que $a_0 \equiv \alpha \mod \mathfrak{p}$. Então $|f(a_0)| < 1$, pois $f(a_0) \equiv \alpha^{q-1} - 1 \equiv 0 \mod \mathfrak{p}$, e $|f'(a_0)| = |(q-1)\cdot 1||a_0|^{q-2} = 1$. Pelo Lema 1.10, existe um único $a \in \mathcal{O}^*$ tal que $f(a) = 0$ e $a \equiv a_0 \mod \mathfrak{p}$, ou seja, a é uma raiz $(q-1)$-ésima da unidade em K e $a \equiv \alpha \mod \mathfrak{p}$. Portanto, K contém todas as $(q-1)$-ésimas raízes da unidade. ■

Observe que, pelo Lema 1.12, um corpo local possui todas as $(q-1)$-ésimas raízes da unidade, onde q é o número de elementos do seu corpo residual.

1.4 Ramificação

Sejam E uma extensão finita do corpo local F com grau $n = [E : F]$ e $||\cdot||$ o valor absoluto em E. $\mathcal{O}_E$ e $\mathcal{O}_F$ os anéis dos inteiros em E e F, respectivamente, $\mathfrak{p}_E, \mathfrak{p}_F$ seus respectivos ideais maximais e k_E, k_F os corpos residuais.

Lema 1.13. *Existe uma injetividade natural*

$$k_F \hookrightarrow k_E,$$

então k_E é uma extensão de k_F. Além disso, $f = [k_E : k_F] \leqslant [E : F] = n$.

Notação: $f = f(E/F)$ é chamado o grau da classe residual de E/F.

Demonstração: Note que $\mathcal{O}_F = F \cap \mathcal{O}_E$ e $\mathfrak{p}_F = F \cap \mathfrak{p}_E$. Assim, a inclusão $\mathcal{O}_F \subset \mathcal{O}_E$ nos dá uma aplicação natural

$$\begin{array}{rccc} \varphi: & \mathcal{O}_F & \longrightarrow & k_E \\ & a & \mapsto & \overline{a} = a + \mathfrak{p}_E \end{array}$$

onde $\mathrm{Ker}(\varphi) = \mathfrak{p}_F$. Então, $k_F \longrightarrow k_E$ é uma aplicação injetiva.

Vamos mostrar que quaisquer $n+1$ elementos de k_E são linearmente dependentes sobre k_F, daí teremos $[k_E : k_F] \leqslant n$. Sejam $\alpha_1, \ldots, \alpha_{n+1} \in k_E$ quaisquer. Tome $\hat{\alpha}_1, \ldots, \hat{\alpha}_{n+1} \in \mathcal{O}_E$ tais que $\alpha_i = \hat{\alpha}_i + \mathfrak{p}_E$, $i = 1, \ldots, n$. Esses elementos são linearmente dependentes sobre F pois $\dim_F E = n$, logo existem $a_i \in F$, não todos nulos com

$$\sum_{i=1}^{n+1} a_i \hat{\alpha}_i = 0.$$

Podemos supor $a_1 \neq 0$ então multiplicando a soma por a_1^{-1} e denotando $a_i a_1^{-1}$ por b_i temos

$$\hat{\alpha}_1 + \sum_{i=2}^{n+1} b_i \hat{\alpha}_i = 0.$$

Daí, denotando a redução módulo $\mathfrak{p}_E$ com a barra,

$$\alpha_1 + \sum_{i=2}^{n+1} \overline{b}_i \alpha_i = 0,$$

o que nos dá uma dependência linear não-trivial. ■

Definição 5. Com a notação acima, dizemos que:

(i) E/F é uma extensão não ramificada se $f = f(E/F) = n$;

(ii) E/F é uma extensão totalmente ramificada se $f = f(E/F) = 1$.

Lema 1.14. *Sejam $F \subseteq E \subseteq K$ extensões finitas. Então o grau das classes residuais satisfazem*

$$f(K/F) = f(K/E)f(E/F).$$

A igualdade segue do fato que $k_F \hookrightarrow k_E \hookrightarrow k_K$, daí se $\alpha_1, \ldots, \alpha_{f(K/E)}$ e $\beta_1, \ldots, \beta_{f(E/F)}$ são bases para k_K sobre k_E e k_E sobre k_F, respectivamente, então $\alpha_i\beta_j$, $i = 1, \ldots, f(K/E)$ e $j = 1, \ldots, f(E/F)$, é uma base para k_K sobre k_F e temos $[k_K : k_F] = [k_K : k_E][k_E : k_F]$. Essa demonstração é simples e pode ser encontrada em [14] p 203.

Um elemento a numa extensão E de F é dito separável sobre F se satisfizer um polinômio em $F[x]$ que não possui raízes múltiplas, i.e., se a derivada formal é diferente de zero em a . Uma extensão E de F é dita separável sobre F se todos os seus elementos são separáveis sobre F. Um corpo F é dito perfeito se todas as suas extensões finitas são separáveis. Como estamos em corpos locais, cujos corpos residuais são finitos, temos que se $\alpha \in k_E\backslash\{0\}$ e $q = \#k_E$, então $\alpha^{q-1} = 1$. Assim, o polinômio minimal de α sobre k_F é fator do polinômio $x^{q-1} - 1$. Mas esse polinômio não tem raízes repetidas pois os $q - 1$ elementos não nulos de k_E são raízes dele, então o polinômio minimal de α também não raízes repetidas. Portanto, k_F é um corpo perfeito.

Teorema 1.2. *Seja $\alpha \in k_E$. Então existe $\hat{\alpha} \in \mathcal{O}_E$ tal que $\alpha = \hat{\alpha} + \mathfrak{p}_E$ e*

$$[F(\hat{\alpha}) : F] = [k_F(\alpha) : k_F].$$

Além disso, o corpo $F(\hat{\alpha})$ depende apenas de α.

Demonstração: Seja $\phi(x) \in k_F[x]$ o polinômio minimal de α que, pelo que vimos acima, não tem raiz repetida. E seja $\Phi(x) \in \mathcal{O}_F[x]$ um levantamento de $\phi(x)$, isto é,

(i) $\phi(x)$ e $\Phi(x)$ têm o mesmo grau;

(ii) $\phi(x) = \overline{\Phi}(x)$, onde a barra representa a redução dos coeficientes módulo $\mathfrak{p}_E$.

Dessa forma, Φ e ϕ têm o mesmo número de raízes e toda raiz de $\Phi(x)$ módulo $\mathfrak{p}_E$ é uma raiz de $\phi(x)$ o que implica que as raízes estão em classes de resíduos módulo $\mathfrak{p}_E$ distintas. Em particular, existe apenas uma raiz de $\Phi(x)$ que é reduzida a α.

Tome $\hat{\alpha}_1$ um elemento de $\mathcal{O}_E$ que está na classe α. Daí,

$$\Phi(\hat{\alpha}_1) \equiv \phi(\alpha) \equiv 0 \mod \mathfrak{p}_E \quad \text{e} \quad \Phi'(\hat{\alpha}_1) \equiv \phi'(\alpha) \not\equiv 0 \mod \mathfrak{p}_E,$$

ou seja, $|\Phi(\hat{\alpha}_1)| < 1$ e $|\Phi'(\hat{\alpha}_1)| = 1$. Considerando $F(\hat{\alpha}_1)$ o nosso corpo base, pelo Lema 1.10, temos que existe $\hat{\alpha} \in F(\hat{\alpha}_1)$ tal que

$$\Phi(\hat{\alpha}) = 0 \quad \text{e} \quad |\hat{\alpha} - \hat{\alpha}_1| < 1.$$

Portanto, $\hat{\alpha}$ é a única raiz de $\Phi(x)$ na classe de resíduos α. Além disso, o polinômio $\Phi(x)$ é irredutível pois, caso contrário, ϕ seria redutível contradizendo sua minimalidade. Então

$$[F(\hat{\alpha}) : F] = \text{grau } \Phi = \text{grau } \phi = [k_F(\alpha) : k_F].$$

Suponha que $\hat{\alpha}_1$, um elemento na classe α, também satisfaça essa última igualdade. Assim, $[F(\hat{\alpha}) : F] = [F(\hat{\alpha}_1) : F]$. Vimos que $\hat{\alpha} \in F(\hat{\alpha}_1)$ então $F(\hat{\alpha}) \subseteq F(\hat{\alpha}_1)$ e daí temos $F(\hat{\alpha}) = F(\hat{\alpha}_1)$. ■

Corolário 1.4. *Existe uma bijeção entre os corpos intermediários K ($F \subseteq K \subseteq E$) que são não ramificados sobre F e os corpos k com $k_F \subseteq k \subseteq k_E$. O corpo correspondente a K é $k = k_K = \mathcal{O}_K/\mathfrak{p}_K$.*

Demonstração: Seja k um corpo intermediário $k_F \subseteq k \subseteq k_E$ e seja $q = \#k$. Como k é uma extensão finita e separável de k_F, k é uma extensão simples de k_F. Ou seja, existe um elemento não nulo α de k tal que $k = k_F(\alpha)$. Pelo Teorema 1.2, existe $\hat{\alpha} \in \mathcal{O}_E$ tal que $\alpha = \hat{\alpha} + \mathfrak{p}_E$ e $[F(\hat{\alpha}) : F] = [k_F(\alpha) : k_F]$. Seja $K = F(\hat{\alpha})$. Como $\hat{\alpha} \in \mathcal{O}_K = K \cap \mathcal{O}_E$, $\alpha \in k_K = k_{F(\hat{\alpha})}$. Daí $k_F(\alpha) \subset k_{F(\hat{\alpha})}$ e temos

$$[k_F(\alpha) : k_F] \leqslant [k_{F(\hat{\alpha})} : k_F] \leqslant [F(\hat{\alpha}) : F].$$

Assim, $[k_F(\alpha) : k_F] = [k_{F(\hat{\alpha})} : k_F]$ o que nos dá $k_F(\alpha) = k_{F(\hat{\alpha})}$. Portanto, K é um corpo intermediário não ramificado. ■

Corolário 1.5. *Existe um corpo intermediário L com a seguinte propriedade: L/F é não ramificada e toda extensão $K \subseteq E$ que é não ramificada sobre F está contida em L. Além disso, E/L é totalmente ramificada.*

Pelo Corolário 1.4, existe um corpo intermediário $F \subseteq L \subseteq E$, não ramificado, tal que $k_L = k_E$. Pela definição, E/L é totalmente ramificada. A outra propriedade segue da correspondência descrita no Corolário 1.4.

Corolário 1.6. *Seja F um corpo local. Para cada n inteiro positivo existe uma única (a menos de isomorfismo) extensão não ramificada E de F com grau n que é o corpo de decomposição sobre F de $x^q - x$, onde $q = q_F^n$ e $q_F = \#k_F$.*

Demonstração: O corpo k_F é finito então $\#k_F = q_F = p^m$, onde p é a característica de k e $m \in \mathbb{N}$. Para todo n natural, existe (a menos de isomorfismo) um corpo com p^t elementos. Em particular, existe um corpo com $p^{mn} = q_F^n$, para todo n. Pelo Corolário 1.4, existe uma extensão E/F não ramificada com $\#k_E = q_F^n$, daí $[E : F] = [k_E : k_F] = n$. E, pelo Lema 1.12, E contém todas as $(q-1)$-ésimas raízes da unidade, onde $q = \#k_E = q_F^n$.

Em particular, $f(x) = x^q - x$ se decompõe em fatores lineares sobre E, assim E contém o corpo de decomposição K desse polinômio. K não pode ser menor do que E pois seu corpo residual deve ter pelo menos q elementos. Então $E = K$. ■

Definimos o índice de ramificação de E/F como $e = e(E/F) = [\mathcal{V}_E : \mathcal{V}_F]$, onde $\mathcal{V}_E$ e V_F são os grupos de valores de E e F, respectivamente.

Lema 1.15. *Sejam $F \subseteq E \subseteq K$ extensões finitas. Então os índices de ramificação satisfazem*

$$e(K/F) = e(K/E)e(E/F).$$

Basta observar que temos a seguinte relação entre os grupos de valores: $\mathcal{V}_F \leqslant \mathcal{V}_E \leqslant \mathcal{V}_K$. portanto, segue da teoria de grupos que $[\mathcal{V}_K : \mathcal{V}_F] = [\mathcal{V}_K : \mathcal{V}_E][\mathcal{V}_E : \mathcal{V}_F]$.

Sejam π_F e π_E elementos primos de F e E, respectivamente, com relação ao valor absoluto $|\cdot|$. Como $\mathcal{V}_F \leqslant \mathcal{V}_E$, temos $|\pi_F| \in \mathcal{V}_E$. Daí $|\pi_F| = |\pi_E|^m$, para algum m inteiro, o que implica que $\mathcal{V}_F$ é gerado por $|\pi_E|^m$. Assim, $[\mathcal{V}_E : \mathcal{V}_F] = m$, mas $[\mathcal{V}_E : \mathcal{V}_F] = e$, logo $m = e$ e temos

$$|\pi_F| = |\pi_E|^e.$$

A seguir, temos o principal resultado ligando índice de ramificação, grau da classe residual e grau da extensão.

Teorema 1.3. *Seja E/F uma extensão finita (de um corpo local) de grau n. Então $n = ef$, onde $e = e(E/F)$ e $f = f(E/F)$.*

Demonstração: Seja π_E um elemento primo de E e sejam $\hat{\alpha}_1, \ldots, \hat{\alpha}_f$ algum levantamento para $\mathcal{O}_E$ da base de k_E/k_F (i.e., os elementos $\hat{\alpha}_1, \ldots, \hat{\alpha}_f$ reduzidos módulo $\mathfrak{p}_E$ formam uma base de k_E sobre k_F). Vamos mostrar que

$$B = \{\hat{\alpha}_i \pi_E^j : 1 \leqslant i \leqslant f,\ 0 \leqslant j \leqslant e-1\}$$

é uma base de E sobre F. Assim, precisamos mostrar que: (i) os elementos de B são linearmente independentes e (ii) todo elemento de E pode ser escrito como uma combinação linear dos elementos de B com coeficientes em F.

(i) Suponha que B não seja linearmente independente sobre F. Então existem $a_{ij} \in F$ com $1 \leqslant i \leqslant f$ e $0 \leqslant j \leqslant e-1$, não todos nulos, tais que

$$\sum_{\substack{1 \leqslant i \leqslant f \\ 0 \leqslant j \leqslant e-1}} a_{ij} \hat{\alpha}_i \pi_E^j = 0. \tag{1.5}$$

Dividindo a igualdade acima pelo coeficiente a_{ij} com maior valor absoluto, podemos assumir que todos os coeficientes a_{ij} estão em $\mathcal{O}_F$ e que existem I, J tais que $|a_{IJ}| = 1$ e

$$|a_{ij}| \leqslant |\pi_F|, \text{ para } \ 1 \leqslant i \leqslant f,\ j < J,$$

Reduzimos $\sum_i a_{iJ}\hat{\alpha}_i$ módulo $\mathfrak{p}_E$, obtendo um coeficiente não nulo $\overline{a}_{IJ}$. Como $\hat{\alpha}_i \mod \mathfrak{p}_E$, $i = 1, \ldots, f$, são linearmente independentes sobre k_F, essa redução é diferente de zero, ou seja, essa soma não está em $\mathfrak{p}_E$, e temos

$$\left| \sum_i a_{iJ} \hat{\alpha}_i \right| = 1.$$

Daí,

$$\begin{aligned} j = J \Rightarrow \left|\sum_i a_{iJ}\hat{\alpha}_i\pi_E^J\right| &= \left|\pi_E^J\right|\left|\sum_i a_{iJ}\hat{\alpha}_i\right| = |\pi_E|^J \\ j < J \Rightarrow \left|\sum_i a_{ij}\hat{\alpha}_i\pi_E^j\right| &= \left|\pi_E^j\right|\left|\sum_i a_{ij}\hat{\alpha}_i\right| \leqslant \max_i\{|a_{ij}||\hat{\alpha}_i|\} \\ &\leqslant \max_i |a_{ij}| \leqslant |\pi_F| \\ j > J \Rightarrow \left|\sum_i a_{ij}\hat{\alpha}_i\pi_E^j\right| &\leqslant \left|\pi_E^j\right| \max_i\{|a_{ij}||\hat{\alpha}_i|\} \leqslant |\pi_E|^j \leqslant |\pi_E|^{J+1} \end{aligned}$$

que pode ser resumido como

$$b_j = \left|\sum_i a_{ij}\hat{\alpha}_i\pi_E^j\right| \begin{cases} \leqslant |\pi_E|^e & \text{se } j < J \\ = |\pi_E|^J & \text{se } j = J \\ \leqslant |\pi_E|^{J+1} & \text{se } j > J \end{cases}$$

Por (1.5) temos que $\sum_j b_j = 0$, então

$$|\pi_E|^J = |b_J| = \left|\sum_{j\neq J} b_j\right| \leqslant \max_{j\neq J}|b_j| \leqslant |\pi_E|^{J+1}.$$

Absurdo! Isso termina a prova que B é linearmente independente.

(ii) Tome $x \in E$. Multiplicando por uma potência adequada de π_F, reduzimos ao caso $x \in \mathcal{O}_E$ (i.e., se $\pi_F^m x = \sum_{i,j} a_{ij}\hat{\alpha}_i\pi_E^j$ com $a_{ij} \in \mathcal{O}_F$ então $x = \sum_{i,j} A_{ij}\hat{\alpha}_i\pi_E^j$ com $A_{ij} = \pi_F^{-m}a_{ij} \in F$). Como $\alpha_i = \hat{\alpha}_i \mod \mathfrak{p}_E$, $i = 1, \ldots, f$, é uma base de k_E sobre k_F, existem $c_{i0} \in k_F$ tais que

$$\overline{x} = \sum_i c_{i0}\alpha_i$$

onde a barra significa redução módulo $\mathfrak{p}_E$. Para quaisquer levantamentos $\hat{c}_{i0} \in \mathcal{O}_F$, existe algum $x_1 \in \mathcal{O}_E$ tal que

$$x - \sum_i \hat{c}_{i0}\hat{\alpha}_i = \pi_E x_1 \in \mathfrak{p}_E = \pi_E\mathcal{O}_E.$$

Analogamente, temos

$$x_1 - \sum_i \hat{c}_{i1}\hat{\alpha}_i = \pi_E x_2 \in \mathfrak{p}_E,$$

para algum $x_2 \in O_E$. Logo,

$$x - \sum_i \hat{c}_{i0}\hat{\alpha}_i - \pi_E\sum_i \hat{c}_{i1}\hat{\alpha}_i = \pi_E^2 x_2 \in \mathfrak{p}_E^2.$$

Repetindo esse processo e vezes, encontramos $\hat{c}_{ij} \in \mathcal{O}_F$ tais que

$$x - \sum_{j=0}^{e-1}\sum_{i=1}^{f} \hat{c}_{ij}\hat{\alpha}_i\pi_E^j = \pi_E^e x_e \in \mathfrak{p}_E$$

para algum $x_e \in O_E$. Mas $|\pi_E|^e = |\pi_F|$, daí $\pi_E^e x_e = \pi_F x^{(1)}$ com $x^{(1)} \in \mathcal{O}_E$. Repetimos todo o processo com $x^{(1)}$ no lugar de x e assim por diante. Encontraremos uma sucessão de combinações lineares $c_r = \sum_{j=0}^{e-1} \sum_{i=1}^{f} \hat{c}_{ij}^{(r)} \hat{\alpha}_i \pi_E^j$ de elementos de B com coeficientes em $\mathcal{O}_F$ tais que

$$x - c_0 - \pi_F c_1 - \cdots - \pi_F^t c_t \quad \in \quad \pi_F^{t+1} \mathcal{O}_E,$$

para todo t inteiro não nulo. Fazemos t tender a infinito e rearranjando a série, obtemos $x = \sum_{i,j} a_{ij} \hat{\alpha}_i \pi_E^j$ onde $a_{ij} = \sum_{r=0}^{\infty} \hat{c}_{ij}^{(r)} \pi_F^r$ converge por completude e $a_{ij} \in \mathcal{O}_F$. ■

Corolário 1.7. *Uma extensão E/F finita de grau n é*

(i) não ramificada se, e somente se, $e(E/F) = 1$;

(ii) totalmente ramificada se, e somente se, $e(E/F) = n$.

1.5 Corpos p-ádicos

Nessa seção vamos estudar um tipo especial de corpo local.

Definição 6. Seja K um corpo completo com relação ao valor absoluto não-arquimediano $|\cdot|$. Dizemos que K é um corpo p-ádico se

(i) K tem característica zero;

(ii) $|\cdot|$ é discreto;

(iii) o corpo residual k é finito.

Note que (ii) e (iii) implicam que K é não-arquimediano local.

O lema a seguir é uma equivalência a definição de corpo p-ádico que demos acima.

Lema 1.16. *Uma condição necessária e suficiente para que um corpo K com valor absoluto $|\cdot|$ seja um corpo p-ádico é que K seja uma extensão finita de $\mathbb{Q}_p$, para algum p.*

Demonstração: Vamos começar pela necessidade. Seja K um corpo p-ádico. Então $K \supset \mathbb{Q}$ por (i) da definição. Por (iii), o corpo residual de K é finito logo tem característica p, ou seja, $p\,a \in \mathfrak{p}$, $\forall\ a \in \mathcal{O}^*$. Em particular, $p = p\,1 \in \mathfrak{p}$ e então $p = \pi^m a$ com $a \in \mathcal{O}^*$. Assim, se a é uma unidade de K com o valor absoluto $|\cdot|$ então $\pi \not| a$ e isso implica que $p \not| a$, logo a é uma unidade de K com o valor absoluto p-ádico. Tome $\lambda = \log_{|p|} p^{-1} > 0$ então

$$|\pi|^\lambda = |\pi^m|^{\lambda/m} = \left(|p|^\lambda\right)^{1/m} = |p|_p^{1/m} = |\pi^m a|_p^{1/m} = |\pi^m|_p^{1/m} |a|_p^{1/m} = |\pi|_p$$

daí, para todo $b \in K$, temos que $b = \pi^n c$ com $|c| = 1$ e

$$|b|^\lambda = |\pi^n|^\lambda = |\pi|_p^n = |\pi^n c|_p = |b|_p.$$

Portanto, o valor absoluto em K é equivalente ao valor absoluto p-ádico, o que implica que $\mathbb{Q}_p \subset K$, uma vez que K é completo. Se $\hat{\alpha}_1, \ldots, \hat{\alpha}_f$ é um levantamento para $\mathcal{O}$ da base de $k/\mathbb{F}_p$ então mostra-se, de maneira análoga à prova do Lema 1.3, que $\{\hat{\alpha}_i \pi^j \mid 1 \leqslant i \leqslant f,\ 0 \leqslant j \leqslant e-1\}$ é uma base para a extensão $K/\mathbb{Q}_p$. Daí, $[K : \mathbb{Q}_p] < \infty$.

Agora, suponha que K é uma extensão finita de $\mathbb{Q}_p$. Então (i) é satisfeito pois $\mathbb{Q} \in \mathbb{Q}_p$. Como $|k_{\mathbb{Q}_p}| = |\mathbb{F}_p| = p$ e, pelo Lema 1.13, $[k_K : k_{\mathbb{Q}_p}] \leqslant [K : \mathbb{Q}_p] < \infty$, temos a condição (iii) satisfeita. E (ii) segue do resultado abaixo

> Se $|\cdot|$ é discreta em F então é discreta em E, onde $F \subset E$.

que pode ser encontrado em [6] p. 123. ■

Definição 7. Seja q a cardinalidade do corpo residual do corpo p-ádico K. Definimos o valor absoluto renormalizado $|\cdot|_K$ em K por

$$|\pi|_K = q^{-1},$$

onde π é um elemento primo de K.

Esse valor absoluto é chamado de renormalizado porque a normalização natural do valor absoluto em um corpo p-ádico K é a extensão de $|\cdot|_p$ em $\mathbb{Q}_p \subset K$. Note que se $K = \mathbb{Q}_p$ então $|\cdot|_K \equiv |\cdot|_p$.

Lema 1.17. *Seja K um corpo p-ádico, com $[K : \mathbb{Q}_p] = n$, e com valor absoluto não-arquimediano discreto $|\cdot|$ tal que quando restrito a $\mathbb{Q}_p$ coincida com $|\cdot|_p$ (o valor absoluto p-ádico). Então para todo $a \in K$ tem-se que*

$$|a|_K = |a|^n.$$

Demonstração: Como $|\cdot|$ é discreto, $\mathfrak{p}_K$ é ideal principal. Então todo elemento a de K^* pode ser escrito como $a = \pi^m b$, onde π é primo e b uma unidade de K. Assim, se tivermos $|a|_K = |a|^n$ para algum a não nulo e não unitário então

$$|\pi|_K^m = |\pi^m b|_K = |a|_K = |a|^n = |\pi^m b|^n = |\pi|^{mn}$$

e, portanto,

$$|\pi|_K = |\pi|^n.$$

E, para qualquer $c = \pi^l d \in K^*$ com $d \in O_K^*$, teremos

$$|c|_K = |\pi^l d|_K = |\pi|_K^l = |\pi|^{ln} = |\pi^l d|^n = |c|^n.$$

Logo, basta mostrarmos que vale a igualdade do Teorema para um $a \in K$ não nulo e não unitário. Tome $a = p$, então

$$|p|_K = |\pi|_K^e,$$

onde e é o índice de ramificação de K sobre $\mathcal{O}_p$. Além disso, $q = p^f$, onde f é o grau da classe residual k_K. Portanto,

$$|p|_K = q^{-e} = p^{-ef} = p^{-n} = |p|_p^n = |p|^n.$$ ■

O resultado abaixo é um caso particular do Corolário 1.6.

Lema 1.18. *Para cada inteiro não negativo n, existe uma única extensão não ramificada K de $\mathbb{Q}_p$, com $[K : \mathbb{Q}_p] = n$, que é o corpo de decomposição de $x^q - x$ sobre $\mathbb{Q}_p$, onde $q = p^n$.*

Corolário 1.8. *Seja K um corpo p-ádico e seja $q = \#k_K$. Para todo inteiro não negativo n, existe uma única extensão não ramificada F de K com grau n que é o corpo de decomposição sobre K de $x^{q_F} - x$, $q_F = q^n$.*

Lema 1.19. *Seja K um corpo p-ádico. Se k_K é o corpo residual de K com $[k_K : \mathbb{F}_p] = n$ então, para todo $\alpha \in k_K$, podemos escolher um $\hat{\alpha} \in K$ tal que $\hat{\alpha}^q = \hat{\alpha}$ e $\hat{\alpha} \equiv \alpha \mod \mathfrak{p}_K$, onde $q = \#k_K = p^n$.*

Demonstração: Pelo Corolário 1.4 existe um corpo intermediário L tal que $L/\mathbb{Q}_p$ é uma extensão não ramificada e $k_L = k_K$. Pela demonstração do Lema 1.12, para cada $\alpha \in k_K^*$, existe um único $\hat{\alpha} \in \mathcal{O}_L \subset K$ tal que $\hat{\alpha}^{q-1} = 1$ e $\hat{\alpha} \equiv \alpha \mod \mathfrak{p}_L$. Daí segue o resultado. ■

Ao elemento $\hat{\alpha} \in K$ tal que $\hat{\alpha}^q = \hat{\alpha}$ e $\hat{\alpha} \equiv \alpha \mod \mathfrak{p}_K$, onde $\alpha \in k_K$, damos o nome de *representante de Teichmüller de α*. E definimos $\mathbb{T} = \{a \in \mathcal{O}_K \mid a^q = a,\ q = \#k_K\}$ como o conjunto dos representantes de Teichmüller.

CAPÍTULO 2

Números p-ádicos

Seja K um corpo p-ádico. Sejam $\mathcal{O}$ o anel dos inteiros de K, $\mathfrak{p}$ seu ideal maximal, π o gerador desse ideal e $k_K = \mathcal{O}/\mathfrak{p}$. Se e e f são o índice de ramificação e o grau da classe residual, respectivamente, da extensão $K/\mathbb{Q}_p$ então, como vimos, $[K : \mathbb{Q}_p] = n = ef$.

Esse capítulo também tem resultados importantes para a leitura do próximo capítulo. Começamos com a estrutura dos grupos $\mathcal{O}/\mathfrak{p}^t$, $t \geqslant 1$. E veremos mais uma versão do Lema de Hensel, cuja demonstração nos leva a um estudo da estrutura do grupo K^* e de uma relação entre os grupos $\mathfrak{p}^t$ e $\mathcal{U}^{(t)}$ quando $t > e/(p-1)$.

Na seção 2.2, representaremos algumas funções por séries de potências. Uma introdução a esse assunto, incluindo definições e resultados que serão utilizados aqui, pode ser encontrada no capítulo 4 do livro do Fernando Gouvêa [12]. Ele abordou o tema sobre o corpo dos racionais p-ádicos, mas as definições e os resultados necessários são válidos para um corpo p-ádico K qualquer.

2.1 A Estrutura Aditiva de $\mathcal{O}/\mathfrak{p}^t$

Seja G um grupo finito abeliano, escrito aditivamente. Definimos $s = s(G)$ como o menor inteiro positivo para o qual toda sequência em G com pelo menos s elementos tem uma subsequência não vazia cuja soma é zero, a identidade do grupo. Em geral, não temos o valor de $s(G)$ expresso formalmente, mas para p-grupos temos o seguinte resultado, devido a Olson [19].

Lema 2.1. *Seja G um p-grupo finito abeliano com invariantes $p^{e_1}, \ldots, p^{e_r}$, ou seja, $G =$*

$C_{p^{e_1}} \oplus \cdots \oplus C_{p^{e_r}}$. *Então*

$$s(G) = 1 + \sum_{i=1}^{r} (p^{e_i} - 1).$$

Identificamos o grupo aditivo $\mathcal{O}/\mathfrak{p}^t$ por G_t. Temos $|\mathcal{O}/\mathfrak{p}^t| = p^{ft}$ então G_t é um p-grupo finito e abeliano. Logo, pode ser escrito como uma soma direta dos subgrupos gerados pelos elementos de sua base, veja [20] (p. 126-129). Se $\hat{\alpha}_1, \ldots, \hat{\alpha}_f$ é um levantamento para $\mathcal{O}$ de uma base de $k_K/\mathbb{F}_p$, i.e., é uma base inteira do subcorpo não ramificado maximal de K, então

$$B = \{\hat{\alpha}_i \pi^j : 1 \leqslant i \leqslant f, 0 \leqslant j \leqslant e-1\}$$

é uma base inteira de K sobre $\mathbb{Q}_p$. Daí uma base para G_t está contida em

$$\{\hat{\alpha}_i \pi^j + \mathfrak{p}^t : 1 \leqslant i \leqslant f, 0 \leqslant j \leqslant e-1\}.$$

Seja $\{\hat{\alpha}_{i_1}\pi^{j_1} + \mathfrak{p}^t, \ldots, \hat{\alpha}_{i_s}\pi^{j_s} + \mathfrak{p}^t\}$ tal base. Assim,

$$G_t = \left\langle \hat{\alpha}_{i_1}\pi^{j_1} + \mathfrak{p}^t \right\rangle \oplus \cdots \oplus \left\langle \hat{\alpha}_{i_s}\pi^{j_s} + \mathfrak{p}^t \right\rangle. \tag{2.1}$$

Tome q e r tais que $t = qe + r$ com $0 \leqslant r < e$. Temos dois casos:

caso 1: $r = 0$

Nesse caso, $\pi^t = p^q$ e então

$$p^q \cdot (\alpha_i \pi^j) = \alpha_i \pi^{j+t} \in \mathfrak{p}^t,$$

para todo $1 \leqslant i \leqslant f$ e $0 \leqslant j \leqslant e-1$. Logo $o(\alpha_i\pi^j + \mathfrak{p}^t)$, a ordem de $\alpha_i\pi^j + \mathfrak{p}^t$, divide p^q. Seja $p^m = o(\alpha_i\pi^j + \mathfrak{p}^t)$, então $m \leqslant q$ e

$$\alpha_i \pi^j \pi^{em} = p^m \cdot (\alpha_i \pi^j) \in \mathfrak{p}^t$$

daí

$$j + em \geqslant t = eq \;\Rightarrow\; (q-m)e \leqslant j < e \;\Rightarrow\; q - m < 1$$

e como $q, m \in \mathbb{Z}$ segue que $q - m \leqslant 0$, ou seja, $q \leqslant m$. Portanto, $m = q$ e temos que cada elemento de B módulo $\mathfrak{p}^t$ tem ordem p^q. De (2.1), segue que $|G_t| = p^{qs}$. Mas $|G_t| = p^{ft}$, daí $s = n$ e isso quer dizer que todos os elementos de B módulo $\mathfrak{p}^t$ formam uma base para G_t. Então temos

$$G_t = \sum_{\substack{1 \leqslant i \leqslant f \\ 0 \leqslant j \leqslant e-1}} \left\langle \hat{\alpha}_i \pi^j + \mathfrak{p}^t \right\rangle = \sum_{l=1}^{n} C_{p^q}.$$

caso 2: $r > 0$

Nesse caso, $t = qe + r$ e temos

$$j < r \Rightarrow (\alpha_i \pi^j) \cdot p^{q+1} = \alpha_i \pi^{j+eq+e} \in \mathfrak{p}^t$$

$$r \leqslant j \leqslant e-1 \Rightarrow (\alpha_i \pi^j) \cdot p^q = \alpha_i \pi^{j+eq} \in \mathfrak{p}^t$$

Logo $o(\alpha_i\pi^j + \mathfrak{p}^t)$ divide p^{q+1} se $j < r$ e $o(\alpha_i\pi^j + \mathfrak{p}^t)$ divide p^q se $r \leqslant j \leqslant e-1$. Seja $p^m = o(\alpha_i\pi^j + \mathfrak{p}^t)$, então

$$\alpha_i\pi^j\pi^{em} = (\alpha_i\pi^j)\cdot p^m \in \mathfrak{p}^t$$

daí

$$j + em \geqslant t = eq + r \;\Rightarrow\; j - r \geqslant e(q-m). \tag{2.2}$$

Se $j < r$ então de (2.2) temos que $q - m < 0$, ou seja, $q < m \leqslant q+1$. Como $m \in \mathbb{Z}$, temos $m = q+1$. Se $r \leqslant j \leqslant e-1$ então de (2.2) temos que $e > e(q-m)$. Daí, analogamente ao caso 1, concluímos que $m = q$. Assim, cada elemento de $\{\hat{\alpha}_i\pi^j + \mathfrak{p}^t : 1 \leqslant i \leqslant f, 0 \leqslant j < r\}$ tem ordem p^{q+1} e cada elemento de $\{\hat{\alpha}_i\pi^j + \mathfrak{p}^t : 1 \leqslant i \leqslant f, r \leqslant j \leqslant e-1\}$ tem ordem p^q. Por um raciocínio análogo ao do caso 1, temos

$$G_t = \sum_{\substack{1\leqslant i\leqslant f\\ 0\leqslant j\leqslant e-1}} \left\langle \hat{\alpha}_i\pi^j + \mathfrak{p}^t \right\rangle = \sum_{l=1}^{rf} C_{p^{q+1}} + \sum_{l=1}^{f(e-r)} C_{p^q}.$$

Assim, segue dos resultados acima e do Lema 2.1, o seguinte lema.

Lema 2.2. *O grupo G_t é isomorfo a uma soma direta de rf grupos cíclicos de ordem p^{q+1} e $f(e-r)$ grupos cíclicos de ordem p^q. Além disso,*

$$s_t = s(G_t) = rfp^q(p-1) + ef(p^q - 1) + 1.$$

2.2 As funções log e exp

Defina

$$\mathcal{U}^{(n)} = 1 + \mathfrak{p}^n = \{x \in K \mid v_{\mathfrak{p}}(x-1) \geqslant n\},\ n \geqslant 1.$$

Note que se $a \in \mathcal{U}^{(n)}$ então $a^{-1} \in \mathcal{U}^{(n)}$ pois

$$v_{\mathfrak{p}}(a^{-1} - 1) = v_{\mathfrak{p}}(a^{-1}) + v_{\mathfrak{p}}(1-a) = v_{\mathfrak{p}}(a-1) \geqslant n.$$

Então $\mathcal{U}^{(n)}$ é um subgrupo de $\mathcal{O}^*$, para todo $n \geqslant 1$. Dizemos que $\mathcal{U}^{(n)}$ é o n-ésimo grupo da unidade se $n \geqslant 2$ e $\mathcal{U}^{(1)}$ é simplesmente o grupo da unidade.

Temos a seguinte cadeia decrescente

$$\mathcal{O}^* = \mathcal{U}^{(0)} \supset \mathcal{U}^{(1)} \supset \mathcal{U}^{(2)} \supset \cdots \supset \{1\}.$$

Além disso, $\mathcal{O}^*/\mathcal{U}^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^*$ e $(\mathcal{U}^{(n)}/\mathcal{U}^{(n+1)},\ \cdot\ ) \cong (\mathcal{O}/\mathfrak{p}, +)$, para $n \geqslant 1$. De fato, considere os homomorfismos sobrejetivos $\mathcal{O}^* \longrightarrow (\mathcal{O}/\mathfrak{p}^n)^*$ com $a \mapsto a \mod \mathfrak{p}^n$ e $\mathcal{U}^{(n)} \longrightarrow \mathcal{O}/\mathfrak{p}$ com $1 + a\pi^n \mapsto a \mod \mathfrak{p}$ então o núcleo dessas aplicações são $\mathcal{U}^{(n)}$ e $\mathcal{U}^{(n+1)}$, respectivamente. O resultado segue pelo Teorema dos homomorfismos.

Já sabemos que todo elemento $a \in K^*$ pode ser escrito da seguinte forma $a = \pi^t b$ com $t \in \mathbb{Z}$ e $b \in \mathcal{O}^*$. Como $\langle\pi\rangle = \{\pi^t \mid t \in \mathbb{Z}\} \cap \mathcal{O}^* = 1$, segue que $K^* = \langle\pi\rangle \times \mathcal{O}^*$. Além disso, o polinômio $X^{q-1} - 1$, onde $q = \#k_K$, se decompõe em fatores lineares em K, pelo Lema 1.12, logo $\mathcal{O}^*$ contém μ_{q-1} (o grupo das raízes $(q-1)$-ésimas da unidade).

Considere o endomorfismo

$$\begin{array}{rccc} \varphi: & \mathcal{O}^* & \longrightarrow & k_K^* \\ & b & \longmapsto & b+\mathfrak{p} \end{array}$$

Note que $\mathrm{Ker}(\varphi) = \mathcal{U}^{(1)}$ daí $\mathcal{O}^*/\mathcal{U}^{(1)} \cong k_K^*$. Além disso, $\mu_{q-1} \cong k_K^*$ pois ambos são cíclicos de ordem $q-1$, logo $\mathcal{O}^*/\mathcal{U}^{(1)} \cong \mu_{q-1}$. Como $\mu_{q-1} \cap \mathcal{U}^{(1)} = 1$ segue que $\mathcal{O}^* = \mu_{q-1} \times \mathcal{U}^{(1)}$. Portanto, o grupo multiplicativo de um corpo local K pode ser decomposto em

$$K^* = \langle \pi \rangle \times \mu_{q-1} \times \mathcal{U}^{(1)}$$

Lema 2.3. *Seja K um corpo p-ádico. Então existe um único homomorfismo contínuo*

$$\log : K^* \longrightarrow K$$

com $\log p = 0$ e para toda unidade $b \in \mathcal{U}^{(1)}$ tem-se que

$$\log(b) = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{(b-1)^j}{j} \tag{2.3}$$

Seja $v_{\mathfrak{p}} : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ a valorização $\mathfrak{p}$-ádica de K. Note que $v_{\mathfrak{p}} = e v_p$ onde v_p é a valorização p-ádica.

Demonstração: Primeiro temos que mostrar que a série logarítmica $\mathfrak{p}$-ádica (2.3) converge. Para todo $b \in \mathcal{U}^{(1)} = 1 + \mathfrak{p}$, temos $v_p(b-1) > 0$ daí $c = p^{v_p(b-1)} > 1$. E para todo $j \in \mathbb{N}$, $p^{v_p(j)} \leqslant j$ assim, com o logaritmo habitual, $v_p(j) \leqslant \log_p j$. Então, para cada membro da série, temos

$$\begin{aligned} v_p\left((-1)^{j+1}\frac{(b-1)^j}{j}\right) &= j v_p(b-1) - v_p(j) \geqslant j \log_p c - \log_p j \\ &= \log_p(c^j/j) \longrightarrow \infty, \end{aligned}$$

quando $j \to \infty$. Portanto, o termo geral da série converge para zero implicando na convergência da série, pelo Lema 1.8, pois K é completo.

Tome $b_1, b_2 \in \mathcal{U}^{(1)}$, então $b_1 b_2 \in \mathcal{U}^{(1)}$ e temos

$$\begin{aligned} \log(b_1 b_2) &= \sum_{j=1}^{\infty} (-1)^{j+1} \frac{(b_1 b_2 - 1)^j}{j} \\ &= \sum_{j=1}^{\infty} (-1)^{j+1} \frac{(b_1-1)^j}{j} \left(\frac{b_2-1}{b_1-1} + b_2\right)^j \\ &= \sum_{j=1}^{\infty} (-1)^{j+1} \frac{(b_1-1)^j}{j} \sum_{i=0}^{j} \binom{j}{i} \left(\frac{b_2-1}{b_1-1}\right)^{j-i} b_2^i \\ &= \sum_{j=1}^{\infty} (-1)^{j+1} \frac{(b_2-1)^j}{j} + \sum_{j=1}^{\infty} (-1)^{j+1} \frac{(b_1-1)^j}{j} \sum_{i=1}^{j} \binom{j}{i} \left(\frac{b_2-1}{b_1-1}\right)^{j-i} b_2^i \end{aligned}$$

$$\begin{aligned}
&= \log b_2 \ + \ \sum_{i=1}^{\infty} b_2^i \ \sum_{j=i}^{\infty} (-1)^{j+1} \ \frac{(b_1-1)^j}{j} \ \binom{j}{i} \left(\frac{b_2-1}{b_1-1}\right)^{j-i} \\
&= \log b_2 \ + \ \sum_{i=1}^{\infty} b_2^i \ \sum_{j=0}^{\infty} (-1)^{j+i+1} \ \frac{(j+i-1)!}{j!\ i!} \ \frac{(b_1-1)^i}{j} \ (b_2-1)^j \\
&= \log b_2 \ + \ \sum_{i=1}^{\infty} b_2^i (-1)^{i+1} \ \frac{(b_1-1)^i}{i} \ \sum_{j=0}^{\infty} (-1)^j \ \frac{(j+i-1)!}{(i-1)!j!} \ (b_2-1)^j
\end{aligned}$$

Considere $f(y) = y^{-i}$ então o segundo somatório é exatamente o desenvolvimento da série de Taylor de f em torno do ponto 1, daí

$$\begin{aligned}
\log(b_1 b_2) &= \log b_2 \ + \ \sum_{i=1}^{\infty} (-1)^{i+1} \frac{(b_1-1)^i}{i} \\
&= \log b_2 + \log b_1
\end{aligned}$$

e todas as séries convergem quando $b_1, b_2 \in \mathcal{U}^{(1)}$. Portanto, log definido como em (2.3), restrito a $\mathcal{U}^{(1)}$, é um homomorfismo.

Podemos representar cada elemento $a \in K^*$ da seguinte forma

$$a = \pi^{v_{\mathfrak{p}}(a)} \ \omega(a) \ u(a)$$

onde $\omega(a) \in \mu_{q-1}$ e $u(a) \in \mathcal{U}^{(1)}$. Em particular, $p = \pi^e \ \omega(p) \ u(p)$ o que nos dá

$$0 = \log p = e \log \pi + \log \omega(p) + \log u(p),$$

portanto

$$\log \pi = -e^{-1} \log u(p).$$

Assim, o homomorfismo $\log : K^* \longrightarrow K$ pode ser representado por

$$\log a = v_{\mathfrak{p}}(a) \log \pi + \log u(a) = -e^{-1} v_{\mathfrak{p}}(a) \log u(p) + \log u(a)$$

com $\log u(p)$ e $\log u(a)$ dados pela série (2.3). Esse homomorfismo é contínuo, aplicado em p dá zero e quando restrito a $\mathcal{U}^{(1)}$ é exatamente a série logarítmica $\mathfrak{p}$-ádica.

Vamos concluir provando a unicidade da função. Seja $\lambda : K^* \longrightarrow K$ uma extensão qualquer se $\log : \mathcal{U}^{(1)} \longrightarrow K$ com $\lambda(p) = 0$. Então, para todo $\omega \in \mu_{q-1}$, $\lambda(\omega) = (q-1)^{-1}\lambda(\omega^{q-1}) = 0$, e segue que

$$0 = \lambda(p) = e\lambda(\pi) + \lambda(u(p)) = e\lambda(\pi) + \log u(p),$$

portanto

$$\lambda(\pi) = -e^{-1} \log u(p) = \log \pi$$

Assim, usando a mesma representação acima, para todo $a \in K^*$ temos

$$\lambda(a) = v_{\mathfrak{p}}(a)\lambda(\pi) + \lambda(u(a)) = v_{\mathfrak{p}}(a) \log \pi + \log u(a) = \log a.$$

Portanto, log é unicamente definido e independe da escolha do primo π. ■

Teorema 2.1. *Seja K um corpo p-ádico com anel das valorizações $\mathcal{O}$ e ideal maximal $\mathfrak{p}$. Então, para $t > e/(p-1)$,*

$$\log : \mathcal{U}^{(t)} \longrightarrow \mathfrak{p}^t \quad e \quad \exp : \mathfrak{p}^t \longrightarrow \mathcal{U}^{(t)}$$

são isomorfismos inversos, onde

$$log(1+x) = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{x^j}{j} \quad e \quad \exp(y) = \sum_{j=0}^{\infty} \frac{y^j}{j!}.$$

Demonstração: (i) Já vimos que log é um homomorfismo de K^* sobre K. Vamos mostrar que a imagem de $\mathcal{U}^{(t)}$ está contida em $\mathfrak{p}^t$ quando $t > e/(p-1)$. Para todo inteiro $j > 1$, escrevemos $j = p^\alpha j_0$ com $(p, j_0) = 1$ e $\alpha \geqslant 0$, daí

$$\begin{aligned} \alpha = 0 \quad &\Rightarrow \quad \frac{v_p(j)}{j-1} = 0 \leqslant \frac{1}{p-1} \\ \alpha > 0 \quad &\Rightarrow \quad \frac{v_p(j)}{j-1} = \frac{\alpha}{p^\alpha j_0 - 1} \leqslant \frac{\alpha}{p^\alpha - 1} = \frac{\alpha}{(p-1)(p^{\alpha-1} + \cdots + p + 1)} \leqslant \frac{1}{p-1} \end{aligned}$$

Portanto,

$$\frac{v_p(j)}{j-1} \leqslant \frac{1}{p-1}$$

Seja $t > e/(p-1)$. Tome $(1+x) \in \mathcal{U}^{(t)} \backslash \{1\}$, então $v_p(x) \geqslant te^{-1} > (p-1)^{-1}$. E para todo $j > 1$ e $x \in \mathfrak{p}^t$ temos

$$v_p\left(\frac{x^{j-1}}{j}\right) = (j-1)v_p(x) - v_p(j) > (j-1)\frac{1}{p-1} - v_p(j) \geqslant 0,$$

ou seja, $x^{j-1}/j \in \mathfrak{p}$ se $x \in \mathfrak{p}^t$ e $j > 1$. Assim,

$$\begin{aligned} v_{\mathfrak{p}}(\log(1+x)) &= v_{\mathfrak{p}}\left(\sum_{j=1}^{\infty} (-1)^{j+1} \frac{x^j}{j}\right) \\ &= v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}\left(1 + \sum_{j=2}^{\infty} (-1)^{j+1} \frac{x^{j-1}}{j}\right) \\ &= v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(1+b) = v_{\mathfrak{p}}(x), \end{aligned}$$

pois $1 + b \in \mathcal{U}^{(1)}$. Portanto, para $t > e/(p-1)$, a função log leva $\mathcal{U}^{(t)}$ em $\mathfrak{p}^t$.

(ii) Agora vamos considerar a aplicação $\exp(y) = \sum_{j=0}^{\infty} y^j/j!$. Temos, pelo Lema A.1,

$$v_p\left(\frac{y^j}{j!}\right) = jv_p(y) - \frac{j - s(j)}{p-1} = j\left(v_p(y) - \frac{1}{p-1}\right) + \frac{s(j)}{p-1} \geqslant j\left(v_p(y) - \frac{1}{p-1}\right)$$

daí, se $v_p(y) > (p-1)^{-1}$, a série converge.

Se $y, z \in \mathfrak{p}^t$ com $t > e/(p-1)$, mostra-se de maneira análoga ao log que

$$\exp(y+z) = \exp(y)\exp(z)$$

onde todas as séries convergem. Logo exp é um homomorfismo quando seu domínio é $\mathfrak{p}^t$, $t > e/(p-1)$. Vamos mostrar que sua imagem está contida em $\mathcal{U}^{(t)}$.

Seja $t > e/(p-1)$. Tome $y \in \mathfrak{p}^t \backslash \{0\}$, então $v_p(y) > (p-1)^{-1}$ e se $j > 1$

$$v_p\left(\frac{y^{j-1}}{j!}\right) = (j-1)v_p(y) - v_p(j!) > (j-1)\frac{1}{p-1} - \frac{j-s(j)}{p-1} = \frac{s(j)-1}{p-1} \geqslant 0$$

Logo, $y^{j-1}/j! \in \mathfrak{p}$ se $j > 1$ e daí

$$v_{\mathfrak{p}}(\exp(y)-1) = v_{\mathfrak{p}}\left(\sum_{j=1}^{\infty}\frac{y^j}{j!}\right) = v_{\mathfrak{p}}(y) + v_{\mathfrak{p}}\left(1 + \sum_{j=2}^{\infty}\frac{y^{j-1}}{j!}\right) = v_{\mathfrak{p}}(y)$$

Assim, para $t > e/(p-1)$, exp leva $\mathfrak{p}^t$ em $\mathcal{U}^{(t)}$.

(iii) Vamos mostrar que as funções log e exp são inversas. Assim, poderemos concluir que $\log : \mathcal{U}^{(t)} \longrightarrow \mathfrak{p}^t$ e $\exp : \mathfrak{p}^t \longrightarrow \mathcal{U}^{(t)}$ são isomorfismos para $t > e/(p-1)$.

Defina $f(x) = \log(1+x)$ e $g(y) = \exp(y)$. Temos

$$f'(x) = \sum_{j=1}^{\infty}(-1)^{j+1}x^{j-1} = \sum_{j=0}^{\infty}(-1)^j x^j = \frac{1}{1+x}$$

$$g'(y) = \sum_{j=1}^{\infty}\frac{y^{j-1}}{(j-1)!} = \sum_{j=0}^{\infty}\frac{y^j}{j!} = g(y)$$

a) Queremos mostrar que

$$f(g(y)-1) = y, \ \forall\ y \in \mathfrak{p}^t.$$

Defina $\lambda_1(y) = f(g(y)-1) - y$, daí

$$\lambda_1'(y) = f'(g(y)-1)g'(y) - 1 = \frac{1}{1+(g(y)-1)}\ g(y) - 1 = 0.$$

Portanto, λ_1 é constante (veja [12], Corolário 4.4.5). Se $y = 0$ então $\lambda_1(0) = f(g(0)-1) - 0 = f(0) = 0$. Assim, $\lambda_1 \equiv 0$ e segue o resultado.

b) Queremos mostrar que

$$g(f(x)) = 1 + x, \ \forall\ x \in \mathfrak{p}^t. \tag{2.4}$$

Como vimos na demonstração do Teorema 2.1, $v_{\mathfrak{p}}(\exp(y)-1) = v_{\mathfrak{p}}(y)$, então $\exp(y) = 1$ se, e somente se, $y = 0$. Portanto o homomorfismo g é injetivo o que implica na existência de uma função inversa g^{-1}. Assim, (2.4) é equivalente a

$$f(x) = g^{-1}(1+x), \ \forall\ x \in \mathfrak{p}^t. \tag{2.5}$$

Defina $\lambda_2(x) = f(x) - g^{-1}(1+x)$, daí

$$\lambda_2'(x) = f'(x) - \frac{1}{g'(g^{-1}(1+x))} = \frac{1}{1+x} - \frac{1}{g(g^{-1}(1+x))} = 0.$$

Logo, λ_2 é constante. Como $\lambda_2(0) = f(0) - g^{-1}(1) = 0$, segue que $\lambda_2 \equiv 0$ e, portanto, temos (2.5). ■

Lema 2.4 (Lema de Hensel III). *Seja*

$$\begin{array}{ccccccc} a_{11}X_1^k & + & \cdots & + & a_{1N}X_N^k & = & 0 \\ \vdots & & & & \vdots & & \vdots \\ a_{R1}X_1^k & + & \cdots & + & a_{RN}X_N^k & = & 0 \end{array} \tag{2.6}$$

um sistema de R formas simultaneamente diagonais com coeficientes $a_{ij} \in \mathcal{O}$ e grau $k = p^\tau m$, $(p,m) = 1$. Defina

$$\gamma = \begin{cases} 1, \ \tau = 0 \\ e(\tau+1), \ \tau > 0 \ \ e \ \ p \neq 2 \\ e(\tau+2), \ \tau > 0 \ \ e \ \ p = 2 \end{cases}$$

Se o sistema acima tem solução $(x_1, \ldots, x_N) \in \mathcal{O}^N$ não singular módulo π^γ (i.e., as colunas da matriz dos coeficientes $A = (a_{ij})$ correspondentes aos índices j com $x_j \not\equiv 0 \mod \pi$ tem posto R módulo π) então tem solução não-trivial em K.

Demonstração: Seja $(x_1, \ldots, x_N)$ uma solução não singular de (2.6) módulo π^γ. Podemos supor que $x_1, \ldots, x_R \not\equiv 0 \mod \pi$ e que as R primeiras colunas de A tem posto R módulo π, i.e., formam uma matriz não singular módulo π. Se fizermos operações com as linhas de A, a solução não se altera, então vamos supor

$$A = \begin{pmatrix} a_{11} & & 0 & a_{1,R+1} & \ldots & a_{1N} \\ & \ddots & & \vdots & & \vdots \\ 0 & & a_{RR} & a_{R,R+1} & \ldots & a_{RN} \end{pmatrix}$$

com $a_{11}, \ldots, a_{RR} \not\equiv 0 \mod \pi$. Temos $x_i^k \equiv u_i \mod \pi^\gamma$ onde

$$u_i = -\frac{a_{i,R+1}x_{R+1}^k + \cdots + a_{iN}x_N^k}{a_{ii}}, \quad i = 1, \ldots, R.$$

Afirmação. Se $X^k - u \equiv 0 \mod \pi^\gamma$ tem solução então $X^k - u = 0$ tem solução em $\mathcal{O}^*$, i.e., uma unidade $u \in \mathcal{O}^*$ é uma k-ésima potência se existe $b \in \mathcal{O}^*$ tal que $u \equiv b^k \mod \pi^\gamma$.

Portanto, pela afirmação acima, a equação $X^k - u_i = 0$ tem solução $x_i' \in \mathcal{O}^*$ o que nos dá $(x_1', \ldots, x_R', x_{R+1}, \ldots, x_N)$ uma solução não-trivial de (2.6).

Falta mostrar a afirmação. Para $\tau = 0$, segue do Lema de Hensel II. Suponha $\tau > 0$ e considere as aplicações

$$\mathfrak{p}^e \longrightarrow k\mathfrak{p}^e = \mathfrak{p}^{e\tau+e} = \mathfrak{p}^\gamma \ \text{ se } \ p \neq 2$$

e

$$\mathfrak{p}^{2e} \longrightarrow k\mathfrak{p}^{2e} = \mathfrak{p}^{\gamma} \text{ se } p = 2$$

ambas definidas por $x \mapsto kx$. Se $t > e/(p-1)$ então as funções exponencial $\mathfrak{p}$-ádica e logaritmo $\mathfrak{p}$-ádico são isomorfismos inversos entre $(\mathfrak{p}^t, +)$ e $(\mathcal{U}^{(t)}, \cdot)$. Para $p \neq 2$ temos

$$\mathcal{U}^{(e)} \xrightarrow{\log} \mathfrak{p}^e \xrightarrow{x \mapsto kx} \mathfrak{p}^{\gamma} \xrightarrow{\exp} \mathcal{U}^{(\gamma)}$$

daí, compondo essas funções temos um endomorfismo $\mathcal{U}^{(e)} \longrightarrow \mathcal{U}^{(\gamma)}$ definido por $x \mapsto x^k$. Analogamente, temos $\mathcal{U}^{(2e)} \longrightarrow \mathcal{U}^{(\gamma)}$ com $x \mapsto x^k$ se $p = 2$. Portanto, os elementos do conjunto $b^k\,\mathcal{U}^{(\gamma)} = b^k + \mathfrak{p}^{\gamma}$, o qual contém u, são todos k-ésimas potências. ■

CAPÍTULO 3

Equações diagonais sobre corpos p-ádicos

Novamente temos K um corpo p-ádico com anel dos inteiros $\mathcal{O}$, ideal maximal $\mathfrak{p}$ e π o gerador desse ideal. Sejam e e f o índice de ramificação e o grau da classe residual, respectivamente, da extensão $K/\mathbb{Q}_p$ e $[K:\mathbb{Q}_p] = n = ef$.

Vamos considerar o sistema

$$\begin{array}{ccccccccc} F_1 & = & a_{11}X_1^k & + & \cdots & + & a_{1N}X_N^k & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ F_R & = & a_{R1}X_1^k & + & \cdots & + & a_{RN}X_N^k & = & 0 \end{array} \tag{3.1}$$

com R equações diagonais, cujos coeficientes a_{ij} estão em $\mathcal{O}$. Escrevemos $k = p^\tau m$ com $(p,m) = 1$. Procuramos condições suficientes para que esse sistema tenha solução $x = (x_1, \ldots, x_N) \in K^N$ não-trivial, ou seja, com pelo menos uma das coordenadas x_j diferente de zero.

3.1 π-normalização

Definimos

$$\vartheta(F_1, \ldots, F_R) = \prod_{j_1,\ldots,j_R} \det(a_{ij_i}), \quad i = 1, \ldots, R$$

onde o produtório se estende sobre todas as R-uplas de sufixos distintos $j_1, \ldots, j_R$ de $1, \ldots, N$.

Observação. Note que essa definição considera submatrizes com mesmas colunas só que em ordens distintas. Por exemplo, se tivermos a matriz de coeficientes

$$A = \begin{pmatrix} 8 & 2 & 1 \\ 9 & 8 & 5 \end{pmatrix}$$

então, para o cálculo de ϑ, consideramos ambas as submatrizes

$$\begin{pmatrix} 8 & 2 \\ 9 & 8 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 2 & 8 \\ 8 & 9 \end{pmatrix}$$

Dizemos que dois sistemas de equações aditivas com coeficientes em $\mathcal{O}$ são equivalentes se um pode ser obtido a partir do outro através da combinação das seguintes operações:

(i) trocando a variável X_i por $\pi^{\alpha}X_i$, para algum inteiro α, ou seja,

$$G_i(X_1,\dots,X_N) = F_i(\pi^{\alpha_1}X_1,\dots,\pi^{\alpha_N}X_N), \quad i=1,\dots,R; \tag{3.2}$$

(ii) tomando uma combinação $\mathcal{O}$-linear não singular das equações, ou seja,

$$H_i(X_1,\dots,X_N) = \sum_{j=1}^{R} d_{ij}F_j(X_1,\dots,X_N), \quad i=1,\dots,R \tag{3.3}$$

com $(d_{ij}) \in M_{R\times R}(\mathcal{O})$ e $\det(d_{ij}) \neq 0$.

Um sistema $F_1,\dots,F_R$ é dito π-normalizado se $\vartheta(F_1,\dots,F_R) \neq 0$ e a potência de π dividindo $\vartheta(F_1,\dots,F_R)$ é menor ou igual a potência de π dividindo $\vartheta(G_1,\dots,G_R)$ para todo sistema $G_1,\dots,G_R$ equivalente a $F_1,\dots,F_R$. Como todo sistema $F_1,\dots,F_R$ com $\vartheta(F_1,\dots,F_R) \neq 0$ é equivalente a um sistema π-normalizado, é suficiente encontrar solução não-trivial para sistemas π-normalizados.

Lema 3.1. *Um sistema π-normalizado de formas aditivas pode ser escrito, renumerando as variáveis, se necessário, como*

$$F_i = f_i(X_1,\dots,X_r) + \pi g_i(X_{r+1},\dots,X_N) \tag{3.4}$$

para $i=1,\dots,R$, onde $r \geqslant N/k$, e se $1 \leqslant i \leqslant r$ então o coeficiente de x_i não é divisível por π em pelo menos uma das R formas $f_1,\dots,f_R$.

Além disso, se tivermos quaisquer s combinações lineares de $f_1,\dots,f_R$ independentes módulo π, e denotarmos por q_s o número de variáveis que tem coeficiente não divisível por π em pelo menos uma dessas combinações, então para cada s com $1 \leqslant s \leqslant R-1$, temos

$$q_s \geqslant \frac{sN}{Rk}.$$

Antes de passarmos a prova desse lema, precisamos do seguinte resultado:

Lema 3.2. *Seja $M = N(N-1)\dots(N-R+1)$ o número de R-uplas distintas de sufixos em $\{1,\dots,N\}$. Se G_i é como em (3.2) então*

$$\vartheta(G_1,\dots,G_R) = \pi^{kRM\alpha/N}\vartheta(F_1,\dots,F_R)$$

onde $\alpha = \alpha_1 + \cdots + \alpha_N$. E se H_i é como em (3.3) então

$$\vartheta(H_1,\dots,H_R) = D^M\vartheta(F_1,\dots,F_R)$$

onde $D = \det(d_{ij}) \neq 0$.

Demonstração: (i) Se $G_i = b_{i1}X_1^k + \cdots + b_{iN}X_N^k$ então $b_{ij} = \pi^{k\alpha_j}a_{ij}$ e daí $\det(b_{ij_i}) = \pi^{k\mu}\det(a_{ij_i})$ com $\mu = \alpha_{j_1} + \cdots + \alpha_{j_R}$. Somando os M μ's referentes as R-uplas distintas temos $\alpha RM/N$, que nos dá o resultado.

(ii) Se $H_i = c_{i1}X_1^k + \cdots + c_{iN}X_N^k$ então

$$c_{ij} = \sum_{h=1}^{R} d_{ih}a_{hj}$$

e daí $\det(c_{ij_i}) = D\det(a_{ij_i})$, de onde segue o resultado. ■

Demonstração do Lema 3.1: Definimos f_i como a forma que possui todas as variáveis com coeficiente não divisível por π em pelo menos uma das F_i's e renumeramos tais variáveis por $X_1, \ldots, X_r$, assim, temos (3.4).

Para $i = 1, \ldots, R$, considere as formas

$$\pi^{-1}F_i(\pi X_1, \ldots, \pi X_r, X_{r+1}, \ldots, X_N) = \pi^{k-1}f_i(X_1, \ldots, X_r) + g_i(X_{r+1}, \ldots X_N)$$

obtidas das F_i's por uma combinação das operações (3.2), com $\alpha = r$, e (3.3), com $D = \pi^{-R}$. Então o valor de ϑ das novas formas é igual a $\pi^{kRMr/N-RM}\vartheta(F_1, \ldots, F_R)$. Como os coeficientes das novas formas são inteiros e $F_1, \ldots, F_R$ é π-normalizado, temos $kRMr/N - RM \geqslant 0$ o que implica em $r \geqslant N/k$.

Tome $h_1, \ldots, h_s$, s combinações lineares independentes módulo π de $f_1, \ldots, f_R$ e considere $H_1, \ldots, H_s$ as mesmas combinações de $F_1, \ldots, F_R$. Completamos esse novo sistema com $R - s$ formas dentre $F_1, \ldots, F_R$ para obter um sistema de R formas independentes módulo π. Então $H_1, \ldots, H_R$ são obtidas a partir de $F_1, \ldots, F_R$ através de (3.3) com D_0 não divisível por π. Seja q_s o número de variáveis que aparecem em pelo menos uma das $h_1, \ldots, h_s$ com coeficiente não divisível por π e donote essas variáveis por $X_1, \ldots X_{q_s}$. As formas

$$\pi^{-1}G_i(\pi X_1, \ldots, \pi X_{q_s}, X_{q_s+1}, \ldots, X_N), \quad \text{se } i = 1, \ldots, s$$

$$G_i(\pi X_1, \ldots, \pi X_{q_s}, X_{q_s+1}, \ldots, X_N), \quad \text{se } i = s+1, \ldots, R$$

obtidas a partir de $F_1, \ldots, F_R$ através de (3.2), com $\alpha = q_s$, e (3.3), com $D = \pi^{-s}D_0$, tem coeficientes inteiros. Assim, $kRMq_s/N - sM \geqslant 0$ o que nos dá $q_s \geqslant sN/kR$. ■

Dizemos que uma variável X_j está no nível l se π^l divide a_{ij}, $\forall\ i = 1, \ldots R$, mas π^{l+1} não divide algum a_{ij}. Num sistema π-normalizado todas a variáveis estão em níveis menores que k. De fato, se algum X_j estivesse no nível $l \geqslant k$, então as formas $F_i(X_1, \ldots, X_{j-1}, \pi^{-1}X_j, X_{j+1}, \ldots, X_N)$ teriam coeficientes inteiros e seu ϑ seria igual a

$$\pi^{-kRM/N}\vartheta(F_1, \ldots, F_R)$$

contradizendo a π-normalidade de $F_1, \ldots, F_R$.

3.2 Uma forma diagonal

Nesta seção, veremos condições suficientes sobre o número de variáveis, obtidas por Alemu [1], para que uma equação diagonal tenha solução não-trivial num corpo p-ádico. Demonstraremos três teoremas nesse sentido, incluindo o Teorema 1 citado na introdução.

Seja k um número natural. Defina $\Gamma(k)$ como o menor número s de variáveis para o qual a equação

$$F = a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k,$$

onde os a_i's são todos inteiros p-ádicos não-nulos, represente zero em K. Obviamente não consideramos a solução trivial.

E defina, para cada t natural, $\gamma^*(k,t)$ como o menor s tal que que a congruência

$$F = a_1x_1^k + \cdots + a_sx_s^k \equiv 0 \mod \pi^t,$$

onde os a_i's são unidades p-ádicas, tenha solução não-trivial.

Seja F uma forma diagonal sobre $\mathcal{O}$ de grau k. F pode ser normalizada como

$$F = F_0 + \pi F_1 + \cdots + \pi^{k-1}F_{k-1}$$

onde F_i é uma forma diagonal de grau k com coeficientes em $\mathcal{O}^*$ e r_i variáveis. Se $i \neq j$ então F_i e F_j não tem variáveis em comum e daí $s = r_0 + \cdots + r_{k-1}$. Além disso, podemos supor $r_0 \geqslant r_i$, $i = 1, \ldots, k-1$.

3.2.1 Lema de Hensel

A seguir temos mais uma versão do Lema de Hensel. Apesar de I e IV serem versões muito parecidas, inclusive na demonstração, essa é mais refinada que a primeira que vimos pois em I precisávamos que o quadrado do valor absoluto da primeira derivada num ponto a_0 excedesse o valor absoluto da equação no mesmo ponto, i.e., que o dobro da valorização de $f'(a_0)$ fosse menor que a valorização de $f(a_0)$.

Defina

$$\bar{e} = \left[\frac{e}{p-1}\right] + 1,$$

onde $[\,\cdot\,]$ significa parte inteira.

Lema 3.3 (Lema de Hensel IV). *Seja M um inteiro não negativo. Sejam $f(x) \in \mathcal{O}_K[x]$ de grau k e $\{a_n\}_{n=0}^{\infty}$ uma sequência dada por*

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

satisfazendo

$$f(a_0) \equiv 0 \mod \pi^{M+\bar{e}} \tag{3.5}$$

e para todo $n = 0, 1, 2, \ldots$:

$$f^{(i)}(a_n) \equiv 0 \mod \pi^M, \tag{3.6}$$

$$f^{(i)}(a_n) \not\equiv 0 \mod \pi^{M+1}. \tag{3.7}$$

Então existe $\xi \in \mathcal{O}_K$ *tal que*

$$\xi \equiv a_0 \mod \pi^{\bar{e}} \quad e \quad f(\xi) = 0.$$

Demonstração: Defina $t_n = M + \bar{e} + n$, $n = 0, 1, \ldots$ Vamos mostrar primeiro que, para cada inteiro n,

$$f(a_n) \equiv 0 \mod \pi^{t_n}, \tag{3.8}$$

e

$$a_{n+1} \equiv a_n \mod \pi^{\bar{e}+n}. \tag{3.9}$$

pois (3.8) e (3.9) implicam respectivamente que $f(a_n)$ converge para zero quando $n \to \infty$ e que $\{a_n\}_{n \geqslant 0}$ é uma sequência de Cauchy. Assim, como estamos num corpo completo, $\{a_n\}$ converge para algum $\xi \in \mathcal{O}_K$ e daí

$$0 = \lim_{n\to\infty} f(a_n) = f\left(\lim_{n\to\infty} a_n\right) = f(\xi),$$

provando parte do Lema.

Faremos a demonstração da primeira congruência por indução sobre n. Pela hipótese (3.5) do Lema, (3.8) é válida para $n = 0$. Suponha que seja válida para $n - 1$. Usando a expansão de Taylor de f e a definição da sequência $\{a_n\}$, temos

$$\begin{aligned} f(a_n) &= f(a_{n-1}) + f'(a_{n-1})(a_n - a_{n-1}) + \cdots + \frac{f^{(k)}(a_{n-1})}{k!}(a_n - a_{n-1})^k \\ &= f(a_{n-1}) + f'(a_{n-1})\left(-\frac{f(a_{n-1})}{f'(a_{n-1})}\right) + \cdots + \frac{f^{(k)}(a_{n-1})}{k!}\left(-\frac{f(a_{n-1})}{f'(a_{n-1})}\right)^k \\ &= \frac{f''(a_{n-1})}{2!}\left(-\frac{f(a_{n-1})}{f'(a_{n-1})}\right)^2 + \cdots + \frac{f^{(k)}(a_{n-1})}{k!}\left(-\frac{f(a_{n-1})}{f'(a_{n-1})}\right)^k. \end{aligned}$$

Por (3.6), (3.7), a hipótese de indução e o Lema A.1, para cada $i \in \{2, 3, \ldots, k\}$,

$$\begin{aligned} v_{\mathfrak{p}}\left(\frac{f^{(i)}(a_{n-1})}{i!}\left(-\frac{f(a_{n-1})}{f'(a_{n-1})}\right)^i\right) &= v_{\mathfrak{p}}(f^{(i)}(a_{n-1})) + i\ v_{\mathfrak{p}}\left(-\frac{f(a_{n-1})}{f'(a_{n-1})}\right) - v_{\mathfrak{p}}(i!) \\ &\geqslant M + i(t_{n-1} - M) - e\frac{i - s(i)}{p-1}. \end{aligned}$$

Note que para provar (3.8) para n, é suficiente mostrar que, para $i = 2, \ldots, k$,

$$M + i(t_{n-1} - M) - e\frac{i - s(i)}{p-1} > t_{n-1}, \tag{3.10}$$

pois essa desigualdade implica que cada parcela da expansão acima é zero módulo π^{t_n}, logo $f(a_n)$ o é. Mas (3.10) é equivalente a

$$t_{n-1} > M + e\frac{i - s(i)}{(p-1)(i-1)}\,.$$

Lembrando que $s(i) \geqslant 1$,

$$M + e\frac{i - s(i)}{(p-1)(i-1)} \leqslant M + \frac{e}{p-1} < M + \bar{e} = t_0 \leqslant t_{n-1}$$

e isso termina a prova de (3.8).

Das definições de $\{a_n\}_{n\geqslant 0}$ e t_n e de (3.8), temos

$$v_{\mathfrak{p}}(a_{n+1} - a_n) = v_{\mathfrak{p}}\left(-\frac{f(a_n)}{f'(a_n)}\right) = t_n - M = \bar{e} + n,$$

portanto $a_{n+1} \equiv a_n \mod \pi^{\bar{e}+n}$.

Agora falta apenas mostrar que $\xi \equiv a_0 \mod \pi^{\bar{e}}$, onde ξ é o limite da sequência $\{a_n\}$. De fato, utilizando recorrência na definição de $\{a_n\}$, temos

$$a_n = a_0 - \sum_{k=0}^{n-1} \frac{f(a_k)}{f'(a_k)}$$

fazendo n tender a infinito,

$$\xi = a_0 - \sum_{k=0}^{\infty} \frac{f(a_k)}{f'(a_k)}.$$

Para cada k inteiro não negativo,

$$v_{\mathfrak{p}}\left(\frac{f(a_k)}{f'(a_k)}\right) = t_k - M = \bar{e} + k \geqslant \bar{e},$$

logo $v_{\mathfrak{p}}(a_0 - \xi) \geqslant \bar{e}$ e temos $\xi \equiv a_0 \mod \pi^{\bar{e}}$. ■

Seja $f(x) = b_1x^k + b_2 \in \mathcal{O}[x]$ onde $b_1 \in \mathcal{O}^*$ e $k = p^\tau m, (p, m) = 1$. Suponha que exista $a_0 \in \mathcal{O}^*$ tal que $b_1a_0^k + b_2 \equiv 0 \mod \pi^{e\tau+\bar{e}}$. Como

$$f^{(i)}(x) = k\cdots(k-i+1)b_1x^{k-i}, \quad i = 1, \ldots, k$$

segue que $f^{(i)}(c) \equiv 0 \mod \pi^{e\tau}$, para todo $c \in \mathcal{O}$. Além disso, $f'(c) \not\equiv 0 \mod \pi^{e\tau+1}$, para todo $c \in \mathcal{O}^*$, em particular para os elementos da sequência $\{a_n\}_{n\geqslant 0}$ definida no Lema 3.3 com o a_0 acima. Então f tem zero não trivial por Hensel.

Sempre podemos obter um polinômio desse tipo a partir de uma forma diagonal sobre $\mathcal{O}$; por exemplo, se a forma tiver s variáveis, damos valores a $s-1$ deixando apenas uma variável livre. Assim, se tivermos um a_0 satisfazendo as hipóteses, podemos garantir a existência de um zero não-trivial para a forma.

3.2.2 Alguns limites de $\Gamma(k)$

Seja $k = p^\tau m$, com $(p, m) = 1$ e $\tau \geqslant 1$. Tome $N = (\gamma^*(k, e\tau + \bar{e}) - 1)k + 1$. Então

$$r_0 \geqslant \frac{(\gamma^*(k, e\tau + \bar{e}) - 1)k + 1}{k} = (\gamma^*(k, e\tau + \bar{e}) - 1) + \frac{1}{k}$$

mas $r_0 \in \mathbb{N}$, daí

$$r_0 \geqslant (\gamma^*(k, e\tau + \bar{e}) - 1) + 1 = \gamma^*(k, e\tau + \bar{e}).$$

Pela definição de γ^*, temos que

$$F_0 \equiv 0 \mod \pi^{e\tau+\bar{e}}$$

tem solução não-trivial e, pela observação feita após o Lema 3.3, F_0 tem zero não-trivial. Portanto, F tem zero não-trivial e segue que

$$\Gamma(k) \leqslant (\gamma^*(k, e\tau + \bar{e}) - 1)k + 1. \tag{3.11}$$

Lema 3.4. *Seja s_t como definido no Lema 2.2 com $t = e\tau + \bar{e}$. Então $\gamma^*(k, e\tau + \bar{e}) \leqslant s_t$.*

Demonstração: Sejam $a_1, \ldots, a_{r_0}$ os coeficientes de F_0 com $r_0 \geqslant s_t$. Pelo definição de s_t, existe uma subsequência $a_{i_1}, \ldots, a_{i_n}$ tal que

$$\sum_{j=1}^{n} a_{i_j} \equiv 0 \mod \pi^{e\tau+\bar{e}}.$$

Tome x a r_0-upla cujas coordenadas são dadas por

$$x_l = \begin{cases} 1, \text{ se } l \in \{i_1, \ldots, i_n\} \\ 0, \text{ caso contrário} \end{cases}$$

Então

$$F_0(x) \equiv 0 \mod \pi^{e\tau+\bar{e}}.$$

Pelo Lema 3.3, F_0 tem zero não-trivial. Portanto, $\gamma^*(k, e\tau + \bar{e}) \leqslant s_t$. ■

Seja $k + e\tau + \bar{e} - 1 = t = qe + r, \ 0 \leqslant r < e$.

Lema 3.5. *Se F é uma forma diagonal de grau k em s variáveis e $s \geqslant rf(p^{q+1} - 1) + (e - r)f(p^q - 1) + 1$, então F representa zero em $\mathcal{O}$.*

Demonstração: Pelo Lema 2.2,

$$s(\mathcal{O}/\mathfrak{p}^{k+e\tau+\bar{e}-1}) = rf(p^{q+1} - 1) + (e - r)f(p^q - 1) + 1.$$

Do número de variáveis de F segue, pelo Lema 2.1, que existe um subconjunto do conjunto de coeficientes de F, digamos $\{a_{i_1}, \ldots, a_{i_u}\}$, tal que

$$\sum_{j=1}^{u} a_{i_j} \equiv 0 \mod \pi^{k+e\tau+\bar{e}-1}.$$

Tome x a s-upla cujas coordenadas são

$$x_l = \begin{cases} 1, \text{ se } \ l \in \{a_{i_1}, \ldots, a_{i_u}\} \\ 0, \text{ caso contrário} \end{cases}$$

Então $F(x) \equiv 0 \mod \pi^{k+e\tau+\bar{e}-1}$.

Temos $0 \leqslant v_{\mathfrak{p}}(a_{i_j}) \leqslant k-1$ para $j = 1, \ldots, u$. Daí, para todo $i_j \in \{i_1, \ldots, i_u\}$,

$$\frac{\partial F}{\partial x_{i_j}}(x) = k a_{i_j} \equiv 0 \mod \pi^{v_{\mathfrak{p}}(a_{i_j})+e\tau}$$

e

$$\frac{\partial F}{\partial x_{i_j}}(x) = k a_{i_j} \not\equiv 0 \mod \pi^{k+e\tau}$$

com $(k+e\tau+\bar{e}-1)-(v_{\mathfrak{p}}(a_{i_j})-e\tau) \geqslant \bar{e}$. Pelo Lema 3.3, F representa zero em $\mathcal{O}$. ■

Teorema 3.1. *Se $k+\bar{e} \leqslant e$, então*

$$\Gamma(k) \leqslant (k+\bar{e}-1)f(p^{\tau+1}-1) + (e-k-\bar{e}+1)f(p^{\tau}-1) + 1.$$

Demonstração: Como $k+e\tau+\bar{e}-1 = t = qe+r$ com $0 \leqslant r < e$, temos

$$q = \left[\frac{k+\bar{e}-1}{e} + \tau\right].$$

Se $k+\bar{e} \leqslant e$, então $\left[\frac{k+\bar{e}-1}{e} + \tau\right] = \tau$ e temos $r = k+\bar{e}-1$. Pelo Lema 3.5, se F tiver pelo menos

$$(k+\bar{e}-1)f(p^{\tau+1}-1) + (e-k-\bar{e}+1)f(p^{\tau}-1) + 1$$

variáveis, então F representa zero em $\mathcal{O}$. Portanto,

$$\Gamma(k) \leqslant (k+\bar{e}-1)f(p^{\tau+1}-1) + (e-k-\bar{e}+1)f(p^{\tau}-1) + 1.$$ ■

Teorema 3.2. *Se k é ímpar e $\tau \geqslant 1$, então*

$$\Gamma(k) \leqslant \left[\frac{f(k+e+\bar{e}-1)\log k}{\log 2}\right] + 1.$$

Demonstração: Seja F uma forma diagonal do tipo

$$a_1 x_1^k + \cdots + a_s x_s^k$$

com $0 \leqslant v_{\mathfrak{p}}(a_i) \leqslant k-1$, para $i = 1, \ldots, s$, e

$$s \geqslant \left[\frac{f(k+e+\bar{e}-1)\log k}{\log 2}\right] + 1.$$

Pela demonstração do Lema 3.5, é suficiente mostrar que $F \equiv 0 \mod \pi^{k+e\tau+\bar{e}-1}$ tem solução não-trivial. Para isso, considere todas as possíveis somas de subconjuntos não vazios de $A = \{a_1, \ldots, a_s\}$. Temos $2^s - 1$ tais subconjuntos. Note que

$$\begin{aligned} s &\geqslant \left[\frac{f(k+e+\bar{e}-1)\log k}{\log 2}\right] + 1 \\ &> \frac{f(k+e+\bar{e}-1)\tau \log p}{\log 2} \\ &\geqslant f(k+e\tau+\bar{e}-1)\log_2 p \\ &= \log_2 p^{f(k+e\tau+\bar{e}-1)} \end{aligned}$$

daí $2^s > p^{f(k+e\tau+\bar{e}-1)}$.

Se uma das somas for divisível por $\pi^{k+e\tau+\bar{e}-1}$, trabalharemos com ela. Caso contrário, como $2^s - 1 \geqslant p^{f(k+e\tau+\bar{e}-1)} = |\mathcal{O}/\mathfrak{p}^{k+e\tau+\bar{e}-1}|$, pelo princípio da casa de pombos, existem dois conjuntos diferentes B_1 e B_2 de A tais que

$$\sum_{b\in B_1} b \equiv \sum_{b\in B_2} b \mod \pi^{k+e\tau+\bar{e}-1}.$$

Eliminando os elementos de $B_1 \cap B_2$, se necessário, podemos assumir que B_1 e B_2 são disjuntos. Tome a s-upla x com as seguintes coordenadas

$$x_i = \begin{cases} 1, & \text{se } i \text{ é subíndice de um elemento de } B_1 \\ -1, & \text{se } i \text{ é subíndice de um elemento de } B_2 \\ 0, & \text{caso contrário} \end{cases}$$

Então

$$F(x) = \sum_{b\in B_1} b - \sum_{b\in B_2} b \equiv 0 \mod \pi^{k+e\tau+\bar{e}-1}.$$

Assim, F representa zero em $\mathcal{O}$ e daí

$$\Gamma(k) \leqslant \left[\frac{f(k+e+\bar{e}-1)\log k}{\log 2}\right] + 1.$$

■

A prova do Lema 3.7 utiliza o próximo resultado.

Lema 3.6. *Seja K uma extensão não ramificada de $\mathbb{Q}_p$. Se $F_1, \ldots, F_R \in \mathcal{O}[x_1, \ldots, x_s]$ são formas de graus $k_1, \ldots, k_R$, respectivamente, e $s > \sum_{i=1}^{R} k_i(1 + p + \cdots + p^{t_i-1})$, então existe solução não trivial para o sistema*

$$F_i(x_1, \ldots, x_s) \equiv 0 \mod p^{t_i}.$$

A prova desse resultado utiliza vetores de Witt, que foge um pouco do nosso estudo. Por esse motivo será omitida aqui, mas pode ser encontrada no artigo do Browkin [4] para $R = 1$, a prova para $R > 1$ é análoga.

Lema 3.7. *Seja $F \in \mathcal{O}[x_1, \ldots, x_s]$ uma forma de grau k e seja*

$$s > \begin{cases} kt & \text{se } t \leqslant e \\ ke(1 + p + \cdots + p^{\tau-1}) + k(e_1 + 1)p^\tau & \text{se } t > e \end{cases}$$

onde $t = \tau e + (e_1 + 1)$ e $0 \leqslant e_1 < e$. Então a congruência

$$F(x_1, \ldots, x_s) \equiv 0 \mod \pi^t$$

tem solução não trivial.

Demonstração: Seja L o subcorpo não ramificado maximal de K. Então $1, \pi, \ldots, \pi^{e-1}$ é uma base de K sobre L e podemos escrever $F = F_0 + \pi F_1 + \cdots + \pi^{e-1}F_{e-1}$, onde os coeficientes de F_i estão no anel $\mathcal{O}_L$ dos inteiros de L e grau$(F_i) = k$.

(i) Se $t \leqslant e$ então podemos considerar o sistema

$$F_i(x_1, \ldots, x_s) \equiv 0 \mod p,\ i = 0, 1, \ldots, t-1.$$

O Teorema de Chevalley-Warning afirma que todo sistema de polinômios homogêneos sobre um corpo finito tem zero não-trivial se o número de variáveis é maior que a soma dos graus dos polinômios (veja [7] p. 72 e [13] p. 11). Como $s > kt$, pelo Teorema de Chevalley-Warning, esse sistema tem solução não-trivial $a_1, \ldots, a_s \in \mathcal{O}_L$. Lembrando que $\pi^e = p$, segue que

$$F(a_1, \ldots, a_s) = F_0(a_1, \ldots, a_s) + \cdots + \pi^{e-1}F_{e-1}(a_1, \ldots, a_s) \equiv 0 \mod \pi^t$$

(ii) Agora vamos analisar o caso $n > e$. Considere o sistema

$$\begin{aligned} F_i(x_1, \ldots, x_s) &\equiv 0 \mod p^{\tau+1},\ i = 0, 1, \ldots, e_1 \\ F_j(x_1, \ldots, x_s) &\equiv 0 \mod p^\tau,\ j = e_1 + 1, \ldots, e-1. \end{aligned} \tag{3.12}$$

Temos que

$$\begin{aligned} \sum_{i=0}^{e-1} k(1 + p + \cdots + p^{t_i - 1}) &= (e_1 + 1)k(1 + \cdots + p^\tau) + (e - (1 + e_1))k(1 + \cdots + p^{\tau-1}) \\ &= ek(1 + p + \cdots + p^{\tau-1}) + (e_1 + 1)kp^\tau < s \end{aligned}$$

então, pelo Lema 3.6, (3.12) tem solução não-trivial $a_1, \ldots, a_s \in \mathcal{O}_L$. Como π^t divide $p^{\tau+1}$ e $\pi^{t-(e_1+1)} = p^\tau$, temos

$$F_i(a_1, \ldots, a_s) \equiv 0 \mod \pi^{t-i},$$

$i = 0, 1, \ldots, e-1$. Portanto,

$$F(a_1, \ldots, a_s) \equiv 0 \mod \pi^t. \qquad \blacksquare$$

Sejam F uma forma diagonal de grau k cujos coeficientes são unidades de K e $t = e\tau + \bar{e}$, com $e\tau = v_{\mathfrak{p}}(k)$. O Lema 3.7 garante solução não-trivial para a congruência

$$F \equiv 0 \mod \pi^{e\tau + \bar{e}}$$

se $p \neq 2$ e

$$s > ke\frac{p^\tau - 1}{p-1} + k\bar{e}p^\tau,$$

ou, se $p = 2$ e

$$s > ke(p^{\tau+1} - 1) + kp^{\tau+1}.$$

Assim, se $p \neq 2$, temos

$$\gamma^*(k, e\tau + \bar{e}) \leqslant ke\frac{p^\tau - 1}{p-1} + k\bar{e}p^\tau + 1$$

que substituindo em (3.11) nos dá

$$\Gamma(k) \leqslant k^2\left(e\frac{p^\tau - 1}{p-1} + \bar{e}p^\tau\right) + 1 \tag{3.13}$$

E se $p = 2$ então

$$\Gamma(k) \leqslant k^2(e(p^{\tau+1} - 1) + p^{\tau+1}) + 1$$

Agora, para encerrar a seção, veremos o resultado principal do trabalho do Alemu [1].

Teorema 3.3. *Se $p \geqslant 3$ então*

$$\Gamma(k) \leqslant \max\{3nk^2 - nk + 1, 2k^3 - k^2\}.$$

Se $p = 2$ então

$$\Gamma(k) \leqslant 4nk^2 - nk + 1.$$

Demonstração: Considere o caso $p \geqslant 3$. A relação (3.11), o Lema 3.4 e o Lema 2.2 nos dão

$$\begin{aligned}
\Gamma(k) &\leqslant (\bar{e}fp^\tau(p-1) + ef(p^\tau - 1))k + 1 \\
&\leqslant \left(\left(1 + \frac{e}{p-1}\right)fp^\tau(p-1) + ef(p^\tau - 1)\right)k + 1 \\
&= ((p - 1 + e)fp^\tau + ef(p^\tau - 1))k + 1.
\end{aligned}$$

Se $e \geqslant p - 1$ então

$$\Gamma(k) \leqslant (3efp^\tau - ef)k + 1 \leqslant 3nk^2 - nk + 1.$$

E se $e < p - 1$ então, pela relação (3.13),

$$\begin{aligned}
\Gamma(k) &\leqslant k^2\left(e\frac{p^\tau - 1}{p-1} + \bar{e}p^\tau\right) + 1 \\
&\leqslant k^2(p^\tau - 1 + p^\tau) \\
&\leqslant 2k^3 - k^2
\end{aligned}$$

o que encerra o caso $p \geqslant 3$.

Para $p = 2$, temos

$$s_t = f(2^{\tau+1}(1+e) - e) + 1$$

pelo Lema 2.2. Substituindo na equação (3.11),

$$\Gamma(k) \leqslant f(2^{\tau+1}(1+e) - e)k + 1.$$

Como $e \geqslant 1$ e $m \geqslant 1$, temos $e + 1 \leqslant 2me$ daí

$$(e+1)2^{\tau+1} - e \leqslant 2^{\tau+2}me - e = 4ke - e$$

Assim,

$$\Gamma(k) \leqslant f4k^2e - fek + 1 = 4nk^2 - kn + 1. \qquad \blacksquare$$

3.3 R formas diagonais

Agora vamos estudar o caso geral, um sistema com R formas simultaneamente diagonais, com o objetivo de demonstrar os Teoremas 3 e 4. Precisamos definir algumas funções auxiliares. Primeiro temos $\Gamma(R,k)$ o menor inteiro tal que todo sistema como (3.1) com $N > \Gamma(R,k)$ variáveis tem solução não-trivial sobre K.

Uma solução $x \in \mathcal{O}^N$ é dita *primitiva* se pelo menos uma coordenada x_j é uma unidade em $\mathcal{O}$. Definimos nossa segunda função $\Phi(R,k,\nu)$ como o menor inteiro tal que todo sistema (3.1) com $N > \Phi(R,k,\nu)$ variáveis tem solução primitiva módulo π^ν. O Teorema de Chevalley-Warning implica que $\Phi(R,k,1) \leqslant Rk$.

Uma relação importante dessa função Φ e que será utilizada posteriormente é que

$$\Phi(R,k,a+b) + 1 \leqslant (\Phi(R,k,a)+1)(\Phi(R,k,b)+1), \ \forall\ a,b \geqslant 1.$$

Mostraremos essa desigualdade a seguir utilizando contração e expansão de variáveis. Precisamos encontrar uma solução primitiva módulo π^{a+b} para um sistema com

$$N = (\Phi(R,k,a)+1)(\Phi(R,k,b)+1)$$

variáveis. Primeiro dividimos o sistema (3.1) em $\Phi(R,k,a)+1$ subsistemas de formas diagonais,

$$\begin{array}{ccccccc}
a_{1,j(\Phi(R,k,b)+1)+1}X^k_{j(\Phi(R,k,b)+1)+1} & + & \cdots & + & a_{1,(j+1)(\Phi(R,k,b)+1)}X^k_{(j+1)(\Phi(R,k,b)+1)} & = & 0 \\
\vdots & & & & \vdots & & \vdots \\
a_{R,j(\Phi(R,k,b)+1)+1}X^k_{j(\Phi(R,k,b)+1)+1} & + & \cdots & + & a_{R,(j+1)(\Phi(R,k,b)+1)}X^k_{(j+1)(\Phi(R,k,b)+1)} & = & 0
\end{array}$$

$j = 0, \ldots, \Phi(R,k,a)$, cada um com $\Phi(R,k,b)+1$ variáveis. Cada subsistema tem uma solução $(x_{j(\Phi(R,k,b)+1)+1}, \ldots, x_{(j+1)(\Phi(R,k,b)+1)})$ primitiva módulo π^b. Multiplicamos cada

uma dessas soluções por uma nova variável formando um novo sistema de formas diagonais com $\Phi(R,k,a)+1$ variáveis

$$\begin{array}{ccccccc}
\left(\displaystyle\sum_{l=1}^{\Phi(R,k,b)+1} a_{1l}\ x_l^k\right) Y_1^k & + & \cdots & + & \left(\displaystyle\sum_{l=(\Phi(R,k,b)+1)\Phi(R,k,a)}^{N} a_{1l}\ x_l^k\right) Y_{\Phi(R,k,a)+1}^k & = & 0 \\
\vdots & & & & \vdots & & \vdots \\
\left(\displaystyle\sum_{l=1}^{\Phi(R,k,b)+1} a_{Rl}\ x_l^k\right) Y_1^k & + & \cdots & + & \left(\displaystyle\sum_{l=(\Phi(R,k,b)+1)\Phi(R,k,a)}^{N} a_{Rl}\ x_l^k\right) Y_{\Phi(R,k,a)+1}^k & = & 0
\end{array}$$

Esse novo sistema possui solução $(y_1,\ldots,y_{\Phi(R,k,a)+1})$ primitiva módulo π^a. Assim,

$$(x_1\ y_1,\ \ldots\ ,x_{\Phi(R,k,b)+1}\ y_1,\ \ldots\ ,x_{\Phi(R,k,a)(\Phi(R,k,b)+1)+1}\ y_{\Phi(R,k,a)+1},\ \ldots\ ,x_N\ y_{\Phi(R,k,a)+1})$$

é uma solução primitiva módulo π^{a+b} para o sistema original.

Suponha que o sistema (3.1) é π-normalizado. Podemos admitir que $X_1,\ldots,X_{n_0}$ são as variáveis do nível zero. Denote por A_0 a matriz dos coeficientes dessas variáveis. Seja q_s como definido no Lema 3.1.

Definimos $\mu(d)$ como o maior número de colunas de A_0 que estão num subespaço d-dimensional de k_K^R, $d=0,\ldots,R-1$. Então é simples observar que

$$q_s+\mu(R-s)=n_0,\quad s=1,\ldots,R.$$

Como $q_s \geqslant sN/(Rk)$ e $n_0 \leqslant N$, temos

$$\frac{sN}{Rk}+\mu(R-s)\leqslant N.$$

Portanto

$$\mu(d)\leqslant N-(R-d)\frac{N}{Rk},\quad d=0,\ldots,R-1 \tag{3.14}$$

Lema 3.8. *Suponha que o sistema (3.1) é π-normalizado e tem mais que $k(tR-1)$ variáveis onde t é arbitrário. Então a matriz de coeficientes A contém t submatrizes $R\times R$ disjuntas que são não singulares módulo π.*

O resultado abaixo será necessário para a demonstração do Lema 3.8. Sua demonstração pode ser encontrada em [17], p. 33-34, 55-59.

Lema 3.9. *Seja A uma matriz $R\times N$ sobre o corpo F e t um inteiro positivo. A matriz A possui t submatrizes $R\times R$ disjuntas que são não singulares sobre F se, e somente se,*

$$N-|J|\geqslant t(R-r(A_J)),\quad \forall\ J\subseteq\{1,\ldots,N\},$$

onde A_J é a submatriz de A que consiste das colunas $\mathbf{a}_j$ com $j\in J$ e $r(A_J)=$ posto de A_J.

Demonstração do Lema 3.8: Para todo $d = 0, 1, \ldots, R-1$, substituindo $N > k(tR-1)$ em (3.14), temos

$$\begin{aligned} \mu(d) &\leqslant N - (R-d)\frac{N}{Rk} < N - (R-d)\frac{tR-1}{R} \\ &= N - (R-d)t + \frac{R-d}{R} \end{aligned}$$

Como $\mu(d) \in \mathbb{Z}$, temos $N - \mu(d) \geqslant t(R-d)$. Pelo lema anterior, A contém t submatrizes $R \times R$ disjuntas não singulares módulo π. ■

Lema 3.10. *Suponha que o sistema (3.1) é π-normalizado e tem mais que $Rk\Phi(R,k,\nu) - k(R-1)^2$ variáveis onde ν é arbitrário. Então (3.1) tem solução não singular módulo π^ν.*

Demonstração: Suponha que (3.1) tem $N = k(tR-1)+1$ variáveis para algum t definido adiante. Pelo Lema 3.8, A tem t submatrizes $R \times R$ disjuntas que são não singulares módulo π. Descartamos todas as variáveis que não estão em nenhuma dessas t submatrizes, restando tR variáveis. Tome $t-1$ dessas submatrizes e, em cada uma delas, troque as R variáveis $X_{i_1}, \ldots, X_{i_R}$ por uma nova variável Y_i. Obtemos um novo sistema com $R + t - 1$ variáveis. Se $t = \Phi(R,k,\nu) - R + 2$ então esse sistema tem solução $(x_1, \ldots, x_R, y_1, \ldots, y_{t-1})$ primitiva módulo π^ν. Note que não podemos ter as $t-1$ novas variáveis dessa solução iguais a zero módulo π pois as colunas correspondentes as R variáveis antigas remanescentes formam uma submatriz não singular módulo π, logo essa submatriz possui inversa módulo π. Assim, "inflando" as novas variáveis, temos uma solução não singular módulo π

$$(x_1, \ldots, x_R, \underbrace{y_1, \ldots, y_1}_{R \text{ vezes}}, \ldots, \underbrace{y_{t-1}, \ldots, y_{t-1}}_{R \text{ vezes}})$$

para o sistema inicial com $N = Rk\Phi(R,k,\nu) - k(R-1)^2 + 1$ variáveis. ■

Lema 3.11. *Sejam $f_1, \ldots, f_R \in \mathbb{Z}_p[X_1, \ldots, X_N]$ polinômios com coeficientes inteiros p-ádicos, sem termos constantes, e seja d_i o grau de f_i. Se $N > \sum_{i=1}^{R} d_i(p-1)^{-1}(p^{\nu_i}-1)$, então*

$$f_i(X_1, \ldots, X_N) \equiv 0 \mod p^{\nu_i},\ i = 1, \ldots, R$$

tem solução não-trivial $x_1, \ldots, x_N \in \mathbb{T}$, onde $\mathbb{T} = \{x \in \mathbb{Z}_p \mid x^p = x\}$ é o conjunto dos representantes de Teichmüller.

Demonstração: A idéia dessa demonstração é trocar cada congruência módulo p^{ν_i} por ν_i congruências módulo p para então aplicarmos o Teorema de Chevalley-Warning.

Vamos definir a aplicação $\Delta : \mathbb{Z}_p[X_1, \ldots, X_N] \longrightarrow \mathbb{Z}_p[X_1, \ldots, X_N]$ por

$$\begin{aligned} (\Delta f)(X_1, \ldots, X_N) = p^{-1} \quad & [f(X_1, \ldots, X_N)^p - f^{(p)}(X_1^p, \ldots, X_N^p) + \\ & f^{(p)}(X_1, \ldots, X_N) - f(X_1, \ldots, X_N)] \end{aligned}$$

onde $f^{(p)}(X_1, \ldots, X_N)$ é o polinômio obtido pelo levantamento de cada coeficiente de f a uma p-ésima potência (i.e., $f^{(p)}(X_1, \ldots, X_N) = a_1^p X_1^k + \cdots + a_N^p X_N^k$). Definimos também $\Delta^{(j)} f = \Delta(\Delta^{(j-1)} f)$ se $j > 1$ e, por conveniência, $\Delta^{(0)} f = f$.

Note que Δf é um polinômio em $X_1, \ldots, X_N$ de grau no máximo p (grau$f$). Além disso, Δf tem coeficientes em $\mathbb{Z}_p$. De fato, a aplicação que leva x em x^p é o automorfismo identidade de $\mathbb{F}_p$, daí quando aplicamos o homomorfismo que leva de $\mathbb{Z}_p[X_1, \ldots, X_N]$ para $\mathbb{F}_p[X_1, \ldots, X_N]$, os dois primeiros termos se cancelam e os dois últimos termos se cancelam. Logo, o que está entre colchetes é 0 módulo p.

Seja $f(X_1, \ldots, X_N) = c$ um polinômio constante, então $\Delta f = \Delta c = p^{-1}(c^p - c)$. Queremos mostrar que $c \equiv 0 \mod p^\nu$ se, e somente se, $\Delta^{(0)}c, \Delta^{(1)}c, \ldots, \Delta^{(\nu-1)}c$ são todos congruentes a zero módulo p.

Considere a valorização p-ádica v_p. Suponha que $v_p(\Delta^{(j)}c) \geqslant 1$. Indutivamente temos

$$v_p(\Delta^{(j+1)}c) = v_p(p^{-1}((\Delta^{(j)}c)^p - \Delta^{(j)}c)) = -1 + v_p(\Delta^{(j)}c) = -(j+1) + v_p(c).$$

Assim, se $c \equiv 0 \mod p^\nu$ então $v_p(c) \geqslant \nu$ o que implica em $v_p(\Delta^{(j)}c) \geqslant -j + \nu$ daí, $\Delta^{(j)}c \equiv 0 \mod p$, $j = 0, \ldots, \nu - 1$. Agora, suponha que $\Delta^{(0)}c, \ldots, \Delta^{(\nu-1)}c \equiv 0 \mod p$. Então $v_p(c) = v_p(\Delta^{(\nu-1)}c) + (\nu - 1) \geqslant \nu$, ou seja, $c \equiv 0 \mod p^\nu$.

Tome $a_1, \ldots, a_N \in \mathbb{T}$. Como $a_j^p = a_j$, temos $f^{(p)}(a_1^p, \ldots, a_N^p) = f^{(p)}(a_1, \ldots, a_N)$, daí

$$\begin{aligned}(\Delta f)(a_1, \ldots, a_N) &= p^{-1}[f(a_1, \ldots, a_N)^p - f(a_1, \ldots, a_N)] \\ &= \Delta(f(a_1, \ldots, a_N)).\end{aligned}$$

Portanto, para os elementos do conjunto de Teichmüller, temos $f(a_1, \ldots, a_N) \equiv 0 \mod p^\nu$ se, e somente se, $(\Delta^{(j)}f)(a_1, \ldots, a_N) \equiv 0 \mod p$, $j = 0, \ldots, \nu - 1$.

Assim, concluímos que resolver o sistema de equações

$$f_i(a_1, \ldots, a_N) \equiv 0 \mod p^{\nu_i},\ i = 1, \ldots, R$$

não-trivialmente com variáveis em $\mathbb{T}$ é equivalente a resolver não-trivialmente o sistema de congruências

$$(\Delta^{(j)}f_i)(a_1, \ldots, a_N) \equiv 0 \mod p,$$

$j = 0, \ldots, \nu_i - 1$ e $i = 1, \ldots R$, onde grau$(\Delta^{(j)}f_i) \leqslant p$ grau$(\Delta^{(j-1)}f_i) \leqslant p^j d_i$.

Pelo Teorema de Chevalley-Warning, esse novo sistema tem solução não trivial se o número de variáveis for maior que a soma dos graus, ou seja, se

$$N > \sum_{i=1}^{R}\sum_{j=0}^{\nu_i - 1} p^j d_i = \sum_{i=1}^{R} d_i \frac{p^{\nu_i} - 1}{p - 1}.$$

■

Lema 3.12. *Com γ definido como no Lema 2.4, temos*

$$\Phi(R, k, \gamma) \leqslant \begin{cases} p(p-1)^{-1}nRk, & p > 2 \\ 4nRk, & p = 2 \end{cases}$$

Demonstração: Procuramos uma solução primitiva módulo π^γ para o sistema (3.1). O grupo aditivo $\mathcal{O}/\mathfrak{p}^\gamma$ é isomorfo a soma direta de n grupos cíclicos de ordem $p^{\gamma/e}$,

$$\mathcal{O}/\mathfrak{p}^\gamma = \langle\lambda_1\rangle \oplus \cdots \oplus \langle\lambda_n\rangle,$$

onde $\langle\lambda_i\rangle = \{z\,\lambda_i |\, z \in \mathbb{Z}\}$. Escrevemos cada coeficiente a_{ij} de (3.1) módulo π^γ como

$$a_{ij} \equiv b_{ij}^{(1)}\lambda_1 + \cdots + b_{ij}^{(n)}\lambda_n \mod p^{\gamma/e}, \text{ com } b_{ij}^{(l)} \in \mathbb{Z}.$$

Dessa forma, é suficiente resolver as nR congruências

$$b_{i1}^{(l)}X_1^k + b_{i2}^{(l)}X_2^k + \cdots + b_{iN}^{(l)}X_N^k \equiv 0 \mod p^{\gamma/e}, \tag{3.15}$$

$1 \leqslant i \leqslant R$ e $1 \leqslant l \leqslant n$. Vamos nos restringir ao conjunto de representantes de Teichmüller para encontrar condição suficiente sobre N para que esse novo sistema tenha solução. Observe que $\{x^k \mid x \in \mathbb{T}\} = \{x^{(k,p-1)} \mid x \in \mathbb{T}\}$, então podemos trocar o expoente k por $(k, p-1)$. Pelo lema anterior, o sistema (3.15) tem solução não-trivial $x_1, \ldots, x_N \in \mathbb{T}$ se $N > nR(k,p-1)(p-1)^{-1}(p^{\gamma/e}-1)$. Como $k = p^\tau m$, $(k, p-1)$ divide m. Daí

$$p \neq 2 \Rightarrow \Phi(R,k,\gamma) \leqslant nR(k,p-1)p^{\tau+1}(p-1)^{-1} \leqslant nRkp(p-1)^{-1}$$

$$p = 2 \Rightarrow \Phi(R,k,\gamma) \leqslant nR(k,p-1)p^{\tau+2}(p-1)^{-1} \leqslant nRkp^2 = 4nRk \qquad \blacksquare$$

Uma combinação dos Lemas 2.4 e 3.10 nos diz que um sistema π-normalizado com $N = Rk\Phi(R,k,\gamma) - k(R-1)^2 + 1$ variáveis possui uma solução não-trivial em K. Assim,

$$\Gamma(R,k) \leqslant Rk\Phi(R,k,\gamma) - k(R-1)^2 \leqslant Rk\Phi(R,k,\gamma).$$

e, pelo Lema 3.12,

$$\Gamma(R,k) \leqslant \begin{cases} nR^2k^2p(p-1)^{-1} & \text{se } p > 2 \\ 4nR^2k^2 & \text{se } p = 2 \end{cases}$$

Em todo caso, temos $\Gamma(R,k) \leqslant 4nR^2k^2$. Assim, provamos o seguinte resultado devido a Brink, Godinho e Rodrigues [3].

Teorema 3.4. *Seja n o grau da extensão $K/\mathbb{Q}_p$. Então (3.1) tem solução não-trivial se o número de variáveis N é maior que $4nR^2k^2$.*

Lema 3.13. *Todo $a \in \mathcal{O}$ pode ser escrito como*

$$a \equiv c_0^{p^\tau} + \pi c_1^{p^\tau} + \pi^2 c_2^{p^\tau} + \cdots + \pi^{p^\tau-1}c_{p^\tau-1}^{p^\tau} \mod p$$

com $c_j \in \mathcal{O}$ e π o elemento primo de $\mathcal{O}$.

Demonstração: Seja $\mathcal{R} \subset \mathcal{O}$ um conjunto de representantes de $\mathcal{O}/\mathfrak{p}$. Seja $q = p^f = |\mathcal{O}/\mathfrak{p}|$. Utilizando o fato de que a aplicação de $\mathbb{F}_q$ em $\mathbb{F}_q$ dada por $x \mapsto x^q$ é bijeção (na verdade, é uma identidade), mostramos que a definida por $x \mapsto x^p$ também é bijeção. Então a aplicação $x \mapsto x^{p^\tau}$ é uma bijeção de $\mathbb{F}_q$ em $\mathbb{F}_q$ e, portanto, $\{r^{p^\tau} \mid r \in \mathcal{R}\}$ também é um

conjunto de representantes de $\mathcal{O}/\mathfrak{p}$. Assim, pelo Lema 1.9, podemos escrever todo $a \in \mathcal{O}$ como

$$\begin{aligned} a &= \sum_{n=0}^{\infty} r_n^{p^\tau} \pi^n \\ &= \pi^0 \sum_{i=1}^{\infty} r_{ip^\tau}^{p^\tau} \pi^{ip^\tau} + \pi^1 \sum_{i=1}^{\infty} r_{1+ip^\tau}^{p^\tau} \pi^{ip^\tau} + \cdots + \pi^{p^\tau-1} \sum_{i=1}^{\infty} r_{p^\tau-1+ip^\tau}^{p^\tau} \pi^{ip^\tau} \\ &\equiv \sum_{j=0}^{p^\tau-1} \pi^j \left(\sum_{i=1}^{\infty} r_{j+ip^\tau} \pi^i \right)^{p^\tau} \mod p \end{aligned}$$

Basta tomar $c_j = \sum_{i=1}^{\infty} r_{j+ip^\tau} \pi^i$ para termos o lema. ■

Lema 3.14. $\Phi(R,k,e) \leqslant \Phi(Rp^\tau, m, e)$.

Demonstração: Temos que mostrar que se $N > \Phi(Rp^\tau, m, e)$ então o sistema com R equações de grau k e N variáveis tem solução primitiva módulo π^e.

Considere as R congruências

$$a_{i1} X_1^k + \cdots + a_{iN} X_N^k \equiv 0 \mod p, \quad i = 1, \ldots, R. \tag{3.16}$$

com $N > \Phi(Rp^\tau, m, e)$. Escrevemos cada coeficiente a_{ij} como no Lema 3.13, então cada polinômio acima se torna a soma de p^τ polinômios. Assim, encontrar uma solução primitiva para (3.16) é equivalente a encontrar uma solução primitiva para as Rp^τ congruências

$$c_{i1}^{p^\tau} X_1^k + \cdots, + c_{iN}^{p^\tau} X_N^k \equiv 0 \mod p, \quad i = 1, \ldots, Rp^\tau.$$

Mais ainda, como

$$c_{i1}^{p^\tau} X_1^k + \cdots + c_{iN}^{p^\tau} X_N^k \equiv (c_{i1} X_1^m + \cdots + c_{iN} X_N^m)^{p^\tau} \mod p$$

basta encontrarmos uma solução primitiva para as Rp^τ congruências

$$c_{i1} X_1^m + \cdots + c_{iN} X_N^m \equiv 0 \mod p, \quad i = 1, \ldots, Rp^\tau \tag{3.17}$$

que existe pela definição de Φ pois $N > \Phi(Rp^\tau, m, e)$. ■

Por fim, temos o segundo resultado do trabalho de Brink, Godinho e Rodrigues [3].

Teorema 3.5. *O sistema (3.1) tem solução não-trivial se o número de variáveis N é maior que $(Rk)^{2\tau+5}$.*

Demonstração: Como vimos, os Lemas 2.4 e 3.10 nos dão

$$\Gamma(R,k) \leqslant Rk\Phi(R,k,\gamma) - k(R-1)^2.$$

Se k não é divisível por p, então $\gamma = 1$ e, pelo que vimos no início da seção,

$$\Gamma(R,k) \leqslant (Rk)^2 - k(R-1)^2.$$

Assim, $\Gamma(Rp^\tau, m) \leqslant (Rk)^2 - m(Rp^\tau - 1)^2$. Se $\tau = 0$ então $\Gamma(R,k) \leqslant (Rk)^2 - m(R-1)^2 \leqslant (Rk)^2$, que é menor que a cota do teorema.

Suponha $\tau > 0$. Se $N > \Gamma(Rp^\tau, m)$ então, por definição, (3.17) tem solução não-trivial o que implica que tem solução primitiva módulo π^e, logo $\Phi(Rp^\tau, m, e) \leqslant \Gamma(Rp^\tau, m)$. E, pelo lema anterior, $\Phi(R,k,e) < (Rk)^2$. Assim, temos

$$\begin{aligned}
\Gamma(R,k) &\leqslant Rk\Phi(R,k,\gamma) - k(R-1)^2 \leqslant Rk\Phi(R,k,\gamma) \\
&< Rk(\Phi(R,k,\gamma)+1) \leqslant Rk(\Phi(R,k,e)+1)^{\gamma/e} \\
&\leqslant Rk\left((Rk)^2\right)^{\gamma/e} \leqslant (Rk)^{1+2(\tau+2)} \\
&= (Rk)^{2\tau+5}
\end{aligned}$$

■

APÊNDICE A

Um resultado sobre valorização

Lema A.1. *Se m é um inteiro não negativo e p é primo, então*

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

onde $s(m)$ é a soma dos dígitos que representam m na base p.

Demonstração: Se $m = 0$ o lema é verdadeiro. Para provar o lema para $m > 0$, primeiro vamos mostrar que

$$v_p(m!) = \sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right],$$

em seguida que

$$\sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right] = \frac{m - s(m)}{p-1}$$

daí seguirá a igualdade desejada.

Observe que se $p^i > m$ então $[m/p^i] = 0$. Assim, a série acima tem finitos termos não nulos. Para $h \in \mathbb{N}$ é simples verificar que

$$\left[\frac{h}{p^i}\right] - \left[\frac{h-1}{p^i}\right] = \begin{cases} 1, & \text{se } p^i \text{ divide } h \\ 0, & \text{caso contrário} \end{cases}$$

Em particular, se $v_p(h) = l$ então

$$\left[\frac{h}{p^i}\right] - \left[\frac{h-1}{p^i}\right] = \begin{cases} 1, & \text{se } 1 \leqslant i \leqslant l \\ 0, & \text{caso contrário} \end{cases}$$

Assim,

$$\begin{aligned} v_p(m!) &= v_p(m\ldots 1) = \sum_{h=1}^{m} v_p(h) = \sum_{h=1}^{m}\sum_{i=1}^{\infty}\left(\left[\frac{h}{p^i}\right] - \left[\frac{h-1}{p^i}\right]\right) \\ &= \sum_{i=1}^{\infty}\sum_{h=1}^{m}\left(\left[\frac{h}{p^i}\right] - \left[\frac{h-1}{p^i}\right]\right) = \sum_{i=1}^{\infty}\left[\frac{m}{p^i}\right]. \end{aligned}$$

Seja

$$m = p^u a_u + \cdots + p\,a_1 + a_0, \text{ com } \quad 0 \leqslant a_i < p,$$

a representação de m na base p. Daí,

$$\begin{aligned} \left[\frac{m}{p}\right] &= p^{u-1}a_u + \cdots + p\,a_2 + a_1 \\ \left[\frac{m}{p^2}\right] &= p^{u-2}a_u + \cdots + a_2 \\ &\vdots \\ \left[\frac{m}{p^u}\right] &= a_u \end{aligned}$$

o que implica em

$$\begin{aligned} \sum_{i=1}^{\infty}\left[\frac{m}{p^i}\right] &= \sum_{i=1}^{u}\left[\frac{m}{p^i}\right] = (p^{u-1} + \cdots + p + 1)a_u + \cdots + (p+1)a_2 + a_1 \\ &= \frac{1}{p-1}((p^u - 1)a_u + \cdots + (p^2-1)a_2 + (p-1)a_1) \\ &= \frac{m - s(m)}{p-1}. \end{aligned}$$

E isso termina a demonstração do Lema. ■

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Y. Alemu, *On zeros of diagonal forms over* $\mathfrak{p}$*-adic fields*, Acta Arith. **48** (1987), no. 3, 261–273.

[2] B. J. Birch, *Diagonal equations over* $\mathfrak{p}$*-adic fields*, Acta Arith. **9** (1964), 291–300.

[3] D. Brink, H. Godinho & P. H. Rodrigues, *Simultaneous diagonal equations over* $\mathfrak{p}$*-adic fields*, Acta Arith. **132.4** (2008), 393–399.

[4] J. Browkin, *On zeros of forms*, Bull. Acad. Polon. Sci. Ser. Sci. Math., Astronom. et Phys. **17** (1969), 611–616.

[5] J. Brüdern & H. Godinho, *On Artin's Conjecture, I: Systems of diagonal forms*, Bull. London Math. Soc. **31** (1998), 305–313.

[6] J. W. S. Cassels, *Local fields*, London Math. Soc. Student Texts **3**, Cambridge: Cambridge University Press, 1986.

[7] H. Cohen, *Number theory, Volume I: Tools and diophantine equations*, Graduate texts in mathematics **239**, Springer, 2007.

[8] H. Davenport & D. J. Lewis, *Homogeneous additive equation*, Proc. Roy. Soc. London Ser. A **274** (1963), 443–460.

[9] H. Davenport & D. J. Lewis, *Two additive equations*, Number Theory (ed. W. J. LeVeque and E. G. Strauss), Proc. Sympos. Pure Math **12** (1969), 74–98.

[10] H. Davenport & D. J. Lewis, *Simultaneous equations of additive type*, Philos. Trans. Roy. Soc. London Ser. A **264** (1969), 557–595.

[11] M. Dodson, *Some estimates for diagonal equations over* $\mathfrak{p}$*-adic fields*, Acta Arith. **40** (1982), 117–124.

[12] F. Q. Gouvêa, *p-adic numbers: An introduction*, Springer, 2 ed., 1997.

[13] M. J. Greenberg, *Lectures on forms in many variables*, London mathematical society lecture note series; **0031**, New york: W. A. Benjamin, 1969.

[14] I. N. Herstein, *Tópicos de Álgebra*, Editora Polígono S.A., 1970.

[15] M. P. Knapp, *Systems of diagonal equations over* $\mathfrak{p}$*-adic fields*, J. London Math. Soc. (2) **63** (2001), no. 2, 257–267.

[16] R. Lidl & H. Niederreiter, *Finite Fields*, Cambridge: Cambridge University Press, 1997.

[17] L. Low, J. Pitman & A. Wolff, *Simultaneous diagonal congruences*, J. Number Theory **29** (1988), 31–59.

[18] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992.

[19] J. E. Olson, *A combinatorial problem on finite abelian groups, I and II*, J. Number Theory **1** (1969), 8–10 e 195–199.

[20] J. J. Rotman, *An introduction to the theory of groups*, Graduate texts in mathematics **148**, Springer, 1995.

[21] S. H. Schanuel, *An extension of Chevalley's theorem to congruences modulo prime powers*, J. Number Theory **6** (1974), 284–290.

[22] S. Shokranian, M. Soares & H. Godinho, *Teoria dos números*, Editora Universidade de Brasília, 2 ed., 1999.

[23] C. Skinner, *Local solvability of diagonal equations (again)*, Acta Arith. **124** (2006), no. 1, 73–77.

[24] S. Stevens, *Local fields*, Anais da Escola de Matemática da Universidade de East Anglia, http://www.mth.uea.ac.uk/∼h008/teaching/4A22/local.pdf, último acesso em novembro de 2008.

[25] G. Terjanian, *Une contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris Ser. A **262** (1966), 612.