Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

O Anel dos Vetores de Witt e o Problema de Waring

por

Abílio Lemos Cardoso Júnior

Brasília
2006

Dedico este trabalho ao meu pai, Abílio Lemos Cardoso, que sempre foi um grande companheiro. Ele partiu, mas seu exemplo de vida nunca será esquecido, pois está gravado em meu coração.

Agradecimentos

Primeiramente, agradeço a Deus pela benção da concretização deste trabalho.

Aos meus pais, Abílio Lemos Cardoso (em memória) e Maria Aparecida Teixeira pelos bons conselhos e apoio em todos os momentos.

Aos meus irmãos, Jovane, Abiliana, Abiney, Abilaine e Abilene.

À minha amada namorada, Mariana, pelo amor, paciência, cuidado, enfim pelo apoio nos momentos difícies.

Ao meu orientador, Prof. Hemar Godinho, pela atenção, pelas críticas construtivas, pelo incetivo para concretização deste trabalho.

À Profª. Marinês Guerreiro pelo incentivo durante a graduação.

À Profª. Aline Pinto pelo paciência e atenção ao longo deste trabalho.

À todos os amigos do departamento de matemática da UnB, pelos conselhos e apoio.

Por fim, agradeço a todos que, direta ou indiretamente, me ajudaram durante esse período do curso.

Resumo

Neste trabalho, fazemos um estudo geral do anel de valorização discreta completo. Construímos o anel dos vetores de Witt, denotado por $W(A)$, com coeficientes em um anel comutativo com unidade A. Definimos $W(k)$, onde k é um corpo perfeito de característica p, e mostramos que $W(k)$ é um anel de valorização discreta completo não ramificado. Em seguida tomamos k algébrico sobre $\mathbb{F}_p$ e concluímos que $W(k)$ é, a menos de isomorfismo, a única extensão completa não ramificada de $\mathbb{Z}_p$. Por fim, aplicamos o problema de Waring para $W(k)$.

Abstract

In this work we study complete discrete valuation rings. We construct the ring of Witt vectors, denoted by $W(A)$, with components in a commutative ring with unity A. We define $W(k)$, where k is a perfect field of characteristc p, and prove that $W(k)$, defined in this way, is a complete discrete unramified valuation ring. Afterwards, we take k algebraic over $\mathbb{F}_p$ and we conclude that $W(k)$ is, up to isomorphism, the unique complete unramified extension of Z_p. Finally, we apply the Waring's problem to $W(k)$.

Sumário

Introdução

Denotamos por $\mathfrak{R}$ um anel comutativo com unidade. Para um inteiro $n > 1$, definimos $g_{\mathfrak{R}}(n)$ como o menor inteiro s para o qual todo elemento de $\mathfrak{R}$ é uma soma de s n-ésimas potências de elementos de $\mathfrak{R}$, se tal inteiro existir, ou ∞ caso contrário. O *problema de Waring* para $\mathfrak{R}$ consiste em decidir se $g_{\mathfrak{R}}(n)$ é finito e estimá-lo, para todo n. Note que o usualmente chamado problema de Waring não é o que chamamos problema de Waring para $\mathbb{Z}$. Para n ímpar, o que chamamos problema de Waring para $\mathbb{Z}$ é freqüentemente conhecido como o problema "mais fácil" de Waring, ou seja, o problema de Waring referente apenas a inteiros positivos.

Em 1770, Waring publicou um trabalho onde afirmou que todo inteiro positivo N pode ser escrito como uma soma de:

(a) no máximo, 4 quadrados;
(b) no máximo, 9 cubos;
(c) no máximo, 19 quartas potências.

Embora ele não tenha apresentado nenhuma demonstração para estas afirmações, talvez, baseado na observação de muitos exemplos, ele suspeitava que, para cada inteiro positivo n, deveria existir um inteiro positivo $g(n)$ tal que todo inteiro positivo N pudesse ser expresso como a soma de, no máximo, $g(n)$ n-ésimas potências positivas.

No mesmo ano, Lagrange demonstrou que todo inteiro é a soma de, no máximo, 4 quadrados.

Em 1909, Hilbert provou, para todo n, a existência de um inteiro positivo $g(n)$, independente de N, com a seguinte propriedade: todo inteiro N pode ser expresso como a soma de, no máximo, $g(n)$ n-ésimas potências. A demonstração de Hilbert prova apenas a existência de $g(n)$, mas não fornece informações sobre o valor de $g(n)$.

Entre 1909 e 1912 Wieferich e Kempner mostraram que, todo inteiro é a soma de, no máximo, 9 cubos. Em 1940 Pillai mostrou que $g(6) = 73$. Em 1964 Chen Jingrun mostrou que $g(5) = 37$. Em 1986 Balusabramanian, Dress e Deshouillers mostraram que $g(4) = 19$.

Alguns resultados foram obtidos mais tarde para o seguinte problema: para p um número primo e n um inteiro positivo, queremos encontrar $\Gamma_p(n)$ de forma que ele seja

o menor inteiro positivo s para o qual pode-se resolver não trivialmente a seguinte congruência

$$x_1^n + \cdots + x_s^n \equiv N \,(\mathrm{mod}\, p^l), \tag{1}$$

para todo inteiro N e todo inteiro positivo l.

Hardy e Littlewood, usando métodos analíticos, mostraram em ([8], p.186, Teorema 12) que para todo p e n,

$$\Gamma_p(n) \leq 4n.$$

Em 1943, I. Chowla [5] mostrou que se $\frac{1}{2}(p-1)$ não divide n, então para todo $\epsilon > 0$,

$$\Gamma_p(n) \ll n^{1-c+\epsilon},$$

onde $c = (103 - 3\sqrt{641})/200$ e $\ll$ denota a desigualdade com uma constante fixa positiva. Posteriormente, Dodson [6] melhorou o expoente para 7/8.

Se p não divide n, então a solubilidade da congruência (1) é equivalente a solubilidade da congruência

$$x_1^n + \cdots + x_s^n \equiv N \,(\mathrm{mod}\, p). \tag{2}$$

Agora, se $\Gamma(n,p)$ é definido como o menor s tal que (2) é solúvel não trivialmente para todo N, então Dodson e Tietäväinen [7] mostraram que se $\frac{1}{2}(p-1)$ não divide n, para todo $\epsilon > 0$ vale:

$$\Gamma(n,p) \ll n^{\frac{1}{2}+\epsilon}.$$

Bovey [2] em 1976, generalizou os resultados de Dodson e Tietäväinen para o caso geral p-ádico e provou nas hipóteses da congruência (1) que:

$$\Gamma_p(n) \ll n^{\frac{1}{2}+\epsilon}.$$

Para o problema de Waring sobre corpos finitos consulte [4].

Em 1999, Voloch [3] em trabalho intitulado "On the p-adic Waring's problem", provou alguns resultados para extensões não ramificadas de $\mathbb{Z}_p$. Em particular, Voloch demonstrou que todo inteiro p-ádico é uma soma de 9 pd-ésimas potências, se p for suficientemente grande comparado a d.

Neste trabalho fazemos uma abordagem geral de anel de valorização discreta completo. Depois a partir de um anel comutativo com unidade A, construímos o anel dos vetores de Witt, denotado por $W(A)$, com coeficientes em A, seguindo o método adotado por Fontaine em sua nota sobre a construção dos vetores de Witt [9]. Definimos $W(k)$, onde k é um corpo perfeito de característica p, e mostramos que $W(k)$ é um anel de valorização discreta completo não ramificado. A construção original, realizada por Ernst Witt (1936), pode ser encontrada em [1]. Em seguida tomamos k algébrico sobre $\mathbb{F}_p$ e concluímos que $W(k)$ é, a menos de isomorfismo, a única extensão completa não ramificada de $\mathbb{Z}_p$. Por fim, fazemos uma aplicação do problema de Waring para $W(k)$. De uma forma mais precisa, podemos separar este trabalho da seguinte forma:

No Capítulo 1, apresentamos uma abordagem geral de um anel de valorização discreta completo $\widehat{\mathfrak{A}}$ qualquer, com corpo residual perfeito de característica p, obtendo vários resultados, tais como o conjunto dos representantes de Teichmüller e as operações soma e produto em $\widehat{\mathfrak{A}}$.

No Capítulo 2, construímos o anel dos vetores de Witt de acordo com o Método de Fontaine. Depois definimos $W(k)$ e obtivemos alguns resultados, tais como: a expansão p-ádica de um vetor de Witt e o isomorfismo $W(\mathbb{F}_p) \cong \mathbb{Z}_p$, onde $\mathbb{Z}_p$ é o anel dos inteiros p-ádicos, cujo corpo residual é $\mathbb{F}_p$. Na parte final do capítulo, aplicamos o problema de Waring para $W(k)$, quando k é algébrico sobre $\mathbb{F}_p$. Nestas circunstâncias, concluímos que $W(k)$ é, a menos de isomorfismo, a única extensão completa não ramificada de $\mathbb{Z}_p$. A parte final do capítulo foi baseada no trabalho de Voloch [3] denominado "On the p-adic Waring's problem". Não exibimos todos os resultados deste artigo, devido a sua conexão com a Geometria Algébrica, o que demandaria mais tempo para ser tratado.

Capítulo 1

Anel de Valorização Discreta Completo

Neste capítulo, será definido o Anel de Valorização Discreta Completo. Primeiramente, definiremos o Anel de Valorização Discreta, depois faremos uma abordagem usando seqüências de Cauchy, para obter um completamento para este anel e, equivalentemente, obteremos um completamento via limite projetivo. Na parte final do capítulo, apresentaremos o resultado de Teichümller para um anel de valorização discreta completo $\widehat{\mathfrak{A}}$, quando este tem característica zero e seu corpo residual tem característica p ou zero. Além disso, estudaremos a sua estrutura.

1.1 Anel de Valorização Discreta

Para nossos estudos, $\mathfrak{A}$ sempre será um anel comutativo com unidade.

Definição 1.1. Um anel $\mathfrak{A}$ é chamado **anel de valorização discreta** se ele for um domínio de ideais principais que tem um único ideal maximal não nulo M. Lembramos que um ideal M é maximal em $\mathfrak{A}$ se o anel quociente $\mathfrak{A}/M$ é um corpo.

O corpo $k = \mathfrak{A}/M$ é chamado corpo residual de $\mathfrak{A}$. Os elementos invertíveis de $\mathfrak{A}$ são aqueles que não pertencem a M, estes formam um grupo multiplicativo e são chamados as unidades de $\mathfrak{A}$, que representaremos por $U(\mathfrak{A})$. Pelo fato de $\mathfrak{A}$ ter um único ideal maximal, dizemos que ele é um anel local.

Os ideais não nulos de $\mathfrak{A}$ são da forma $\pi^n\mathfrak{A}$, onde π é um elemento irredutível em $\mathfrak{A}$, e mais $M = \pi\mathfrak{A}$.

Se a é um elemento irredutível de $\mathfrak{A}$ então $\langle a\rangle = \langle \pi^m\rangle$, ou seja, $a = \pi^m u$, onde $u \in U(\mathfrak{A})$, o que implica em $m = 1$. Assim, realmente vemos que π é o único irredutível a menos de associados, tal elemento é chamado **parâmetro uniformizador** de $\mathfrak{A}$.

Corolário 1.2. *O anel de valorização discreta $\mathfrak{A}$ é um domínio de fatoração única, ou seja, todo $a \in \mathfrak{A}$ é produto de irredutíveis.*

Observação 1.3. Podemos ver que os únicos ideais próprios de $\mathfrak{A}$ são $\langle\pi\rangle, \langle\pi^2\rangle, \ldots, \langle\pi^n\rangle, \ldots$ e que $\mathfrak{A}$ é um conjunto de polinômios em π com coeficientes em $U(\mathfrak{A})$.

Definiremos a função v por

$$v(a) = \begin{cases} n, & se\ \ a = \pi^n u\ \ ,\ \ u \in U(\mathfrak{A}) \\ \infty, & se\ \ a = 0 \end{cases}$$

onde $n \in \mathbb{N} \cup \{0\}$.

Lema 1.4. *A função v tem as seguintes propriedades:*
(i) $v(a \cdot b) = v(a) + v(b)$;
(ii) Se $v(a) \neq v(b)$, então $v(a+b) = min\{v(a), v(b)\}$, e se $v(a) = v(b)$, então $v(a+b) \geq min\{v(a), v(b)\}$;
(iii) $v(a) = 0$ se, e só se, a é uma unidade em $\mathfrak{A}$, isto é, a tem um inverso a^{-1} em $\mathfrak{A}$.

Demonstração: As duas primeiras propriedades são óbvias, pela própria definição de v. A terceira, demonstraremos.

Por (i) temos $v(1) = v(1 \cdot 1) = v(1) + v(1)$, logo $v(1) = 0$.
Suponhamos que a seja uma unidade em $\mathfrak{A}$, logo, existe $a^{-1} \in \mathfrak{A}$ tal que $a \cdot a^{-1} = 1$ e, assim,

$$0 = v(a \cdot a^{-1}) = v(a) + v(a^{-1}) \Rightarrow v(a^{-1}) = -v(a).$$

Como $v(a) \geq 0, \forall a \in \mathfrak{A}$ temos que $v(a) = 0$.

Reciprocamente, se $v(a) = 0$, usamos o fato que $a = \pi^n u$, $u \in U(\mathfrak{A})$ e assim devemos ter $n = 0$, o que mostra que a é uma unidade em $U(\mathfrak{A})$, ou seja, $a^{-1} \in \mathfrak{A}$. ∎

Assim, temos um par $(\mathfrak{A}, v)$ constituído do anel $\mathfrak{A}$ e uma função v aplicando elementos não-nulos de $\mathfrak{A}$ em um conjunto de inteiros não-negativos com as condições (i), (ii) e (iii) do lema acima satisfeitas. Assim, podemos dizer que um anel comutativo com unidade satisfazendo as condições (i), (ii) e (iii) é um **anel de valorização discreta**, ou seja,

temos uma nova caracterização para o anel de valorização discreta $\mathfrak{A}$. Note também que $v(\pi) = 1$.

Observação 1.5. Seja K o corpo de frações de $\mathfrak{A}$. Se deixarmos v assumir valores negativos, então haverá uma única extensão de v para K que ainda satisfaz as propriedades (i) e (ii) de 1.4. (Especificamente, se um elemento não-nulo de K é representado como uma fração a/b, então $v(a/b) = v(a) - v(b)$). Uma vez que esta extensão tenha sido feita, o conjunto de todos os $z \in K$ tal que $v(z) \geq 0$ é justamente o anel $\mathfrak{A}$ e o conjunto de todos os $z \in K$ tal que $v(z) > 0$ é o ideal maximal M de $\mathfrak{A}$.

Observação 1.6. O anel $\mathfrak{A}$ é um anel Noetheriano local e seu ideal M é principal. Lembramos que um anel é Noetheriano se cada seqüência crescente de ideais é estacionária (ou, equivalentemente, se cada ideal de $\mathfrak{A}$ é finitamente gerado).

Para simplificar a notação na proposição abaixo usaremos π^n para representar o ideal $\langle \pi^n \rangle$.

Proposição 1.7. *Seja $\mathfrak{A}$ um anel Noetheriano local cujo ideal maximal M é gerado por um elemento não-nilpotente, então $\bigcap \pi^n = 0$ e $\mathfrak{A}$ é um anel de valorização discreta.*

Demonstração: Seja π o gerador do ideal maximal M de $\mathfrak{A}$. Seja I um ideal do anel $\mathfrak{A}$ formado pelos elementos x tais que $x\pi^m = 0$, para m suficientemente grande. Como $\mathfrak{A}$ é Notheriano, I é finitamente gerado e, conseqüentemente existe um N fixo tal que $x\pi^N = 0$ para todo $x \in I$. Agora seja $y \in \bigcap \pi^n$, podemos então escrever $y = \pi^n x_n$, para todo n, e assim

$$\pi^n(x_n - \pi x_{n+1}) = 0 \quad \text{e} \quad x_n - \pi x_{n+1} \in I,$$

ou seja,

$$x_n \in I + \mathfrak{A}x_{n+1} \Rightarrow I + \mathfrak{A}x_n \subseteq I + \mathfrak{A}x_{n+1}, \text{ para todo } n \in \mathbb{N}$$

Como a seqüência de ideais $I + \mathfrak{A}x_n$ está crescendo, segue que $x_{n+1} \in I + \mathfrak{A}x_n$ para n grande, assim $x_{n+1} = z + tx_n$, para $z \in I$ e $t \in \mathfrak{A}$, e como $x_n = \pi x_{n+1} + z'$, com $z' \in I$, obtemos $(1 - \pi t)x_{n+1} \in I$. Mas $1 - \pi t$ não pertence a M, portanto é invertível ($\mathfrak{A}$ é local), conseqüentemente x_{n+1} pertence a I para n suficientemente grande e, tomando $n+1 \geq N$, vemos que $y = \pi^{n+1}x_{n+1}$ é zero, o que prova que

$$\bigcap \pi^n = 0.$$

Como por hipótese, nenhum dos π^n é zero, se y é um elemento não-nulo de $\mathfrak{A}$, então

y pode ser escrito na forma $\pi^n u$, com $u \notin M$, isto é, u é invertível.

Esta representação é claramente única e isto mostra que $\mathfrak{A}$ é um domínio de integridade. Além disso, se escrevemos $v(y) = n$, vemos que a função v se estende à valorização discreta do corpo de frações de $\mathfrak{A}$ com $\mathfrak{A}$ como seu anel de valorização (veja Observação 1.5). ∎

Observação 1.8. Poderíamos usar o fato que $\mathfrak{A}$ é um domíno de integridade e assim $I = \{0\}$, $\pi x_n = x_{n+1}$, e a demonstração acima seria muito mais simples.

Podemos olhar para o anel de valorização discreta $\mathfrak{A}$ como um anel topológico. Lembramos que um anel topológico A é um espaço topológico, munido de uma estrutura de anel tal que as aplicações $s : A \times A \longrightarrow A$ e $p : A \times A \longrightarrow A$, definidas por $s(x, y) = x - y$ e $p(x, y) = xy$, são contínuas e que A é um espaço topológico de Hausdorff se para cada par de elementos distintos $x, y \in A$, existem vizinhanças abertas U, V tais que $x \in U$, $y \in V$ e $U \cap V = \emptyset$.Como $\mathfrak{A}$ satisfaz estas condições podemos enunciar o seguinte corolário.

Corolário 1.9. *O anel de valorização discreta $\mathfrak{A}$ é um espaço de Hausdorff se, e somente se, $\bigcap \pi^n = 0$.*

Apresentaremos, agora, uma série de resultados que nos ajudará a definir o completamento de $\mathfrak{A}$.

Lema 1.10. *Se $u_i \in \mathfrak{A}$ é uma unidade, para $0 \leq i \leq m$, então $\sum_{i=0}^{m} u_i \pi^i$ é uma unidade em $\mathfrak{A}$.*

Demonstração: Se u_i é uma unidade em $\mathfrak{A}$, então $\bar{u}_i \in \mathfrak{A}/M$ é não nulo, logo $\sum_{i=0}^{m} \bar{u}_i \pi^i$ é não nulo, e assim $\sum_{i=0}^{m} u_i \pi^i$ é uma unidade em $\mathfrak{A}$. ∎

Observação 1.11. Os elementos 1 e $1 + \pi$ são unidades em $\mathfrak{A}$, pois pertencem à mesma classe de equivalência em $\mathfrak{A}/M$, mas são diferentes em $\mathfrak{A}$.

Definição 1.12. Para $m \in \mathbb{N}$ definimos $B_m = \{u_i \in U(A) \cup \{0\} \,;\, u_i - u_j \notin \langle \pi \rangle \,, \forall\, i \neq j\}$.

A partir deste momento fixando m, o conjunto B_m está fixado. Assim podemos definir a seguinte aplicação bijetora $f : \mathfrak{A}/M \longrightarrow B_m$ dada por $\bar{a} \mapsto u$, onde u pertence à classe

residual $\bar{a}$. Esse conjunto B_m é chamado um **Sistema de Representantes** de $\mathfrak{A}/M$. Este não é o conjunto de representantes ideal, queremos um conjunto de modo que a aplicação f, definida acima, seja multiplicativa. Para tanto, precisamos que $\mathfrak{A}$ seja completo e isso mostraremos mais à frente.

Proposição 1.13. *Seja $\gamma \in \mathfrak{A}$. Então, para todo $n \in \mathbb{N}$, existem $a_0, \ldots, a_n \in B_m$ tais que $\gamma \equiv \sum_{j=0}^{n} a_j \pi^j \ (mod\ \pi^{n+1})$.*

Demonstração: Tome $a_0 \in B_m$ tal que γ pertence à classe lateral de a_0 módulo π, ou seja, $\gamma \equiv a_0 \,(\mathrm{mod}\,\pi)$, daí $\gamma = a_0 + \pi\gamma_1$, $\gamma_1 \in \mathfrak{A}$. Agora seja $a_1 \in B_m$ tal que $\gamma_1 \equiv a_1 \,(\mathrm{mod}\,\pi)$, ou seja, $\gamma_1 = a_1 + \pi\gamma_2$, para $\gamma_2 \in \mathfrak{A}$, portanto

$$\gamma - a_0 - a_1\pi - \gamma_2\pi^2 = 0 \Rightarrow \gamma \equiv a_0 + a_1\pi \ (\mathrm{mod}\,\pi^2), \text{ etc.}$$

∎

Proposição 1.14. *Se $\gamma \equiv \sum_{j=0}^{n} a_j \pi^j \ (mod\ \pi^{n+1})$ e $\gamma \equiv \sum_{j=0}^{k} b_j \pi^j \ (mod\ \pi^{n+1})$, com $k < n$ e $a_0, \ldots, a_n, b_0, \ldots, b_k \in B_m$, então $a_0 = b_0, \ldots, a_k = b_k$.*

Demonstração: Observe que $\gamma \equiv a_0 \,(\mathrm{mod}\,\pi)$ e $\gamma \equiv b_0 \,(\mathrm{mod}\,\pi)$, mas $a_0, b_0 \in B_m$, ou seja, $a_0 = b_0$. Agora sejam

$$\gamma \equiv a_0 + a_1\pi \,(\mathrm{mod}\,\pi^2) \quad \text{e} \quad \gamma \equiv b_0 + b_1\pi \,(\mathrm{mod}\,\pi^2).$$

Assim temos

$$\begin{array}{rcccc} \gamma & = & a_0 + a_1\pi + L\pi^2 & = & a_0 + b_1\pi + H\pi^2 \\ a_1 & = & b_1 + (H - L)\pi & \Rightarrow & a_1 = b_1 \end{array}$$

a última implicação é verdadeira devido a $\mathfrak{A}$ ser domínio de fatoração única. E assim prosseguindo obtemos o resultado desejado. ∎

Usando as proposições anteriores, concluímos que os elementos de $\mathfrak{A}_n = \mathfrak{A}/\pi^{n+1}$ são representados unicamente, para cada $n > 0$, por

$$a_0 + a_1\pi + \cdots + a_n\pi^n, \text{ onde } a_0, \ldots, a_n \in B_m \tag{1.1}$$

1.2 Um Completamento de $\mathfrak{A}$ Via Seqüência de Cauchy

Definição 1.15. Definimos, para $0 < \xi < 1$, a função $|\cdot|_\pi : \mathfrak{A} \longrightarrow \mathbb{R}$ da seguinte forma

$$|a|_\pi = \begin{cases} \xi^{v(a)} & , \quad se \quad a \neq 0 \\ 0 & , \quad se \quad a = 0 \end{cases},$$

onde v é uma valorização de $\mathfrak{A}$.

Dessa maneira, temos que $|a|_\pi \leq 1$, para todo $a \in \mathfrak{A}$ e $M = \pi\mathfrak{A} = \{a \in \mathfrak{A}; |a|_\pi < 1\}$.

Para essa função, valem as seguintes propriedades:

$$\begin{array}{l} (i) \ \ |x \cdot y|_\pi = |x|_\pi \cdot |y|_\pi \\ (ii) \ \ |x + y|_\pi \leq max\{|x|_\pi, |y|_\pi\} \\ (iii) \ \ |x|_\pi \geq 0, \forall x \in \mathfrak{A} \text{ e } |x|_\pi = 0 \Leftrightarrow x = 0 \\ (iv) \ \ |x - y|_\pi \leq max\{|x - z|_\pi, |z - y|_\pi\}. \end{array} \tag{1.2}$$

A propriedade (iv) é chamada desigualdade forte do triângulo.

Observação 1.16. A função $|\cdot|_\pi$ só será uma métrica em $\mathfrak{A}$ se este for um espaço de Hausdorff, pois $|x - y|_\pi = 0$ se, e somente se, $x - y \in \bigcap \pi^n$.

Assim, podemos falar em **seqüências de Cauchy** $\{x_n\}$ **em** $\mathfrak{A}$. Elas são as seqüências tais que dado $\epsilon > 0$, existe $n_0(\epsilon) \in \mathbb{N}$ tal que $|x_n - x_{n+i}|_\pi < \epsilon$, sempre que $n > n_0$, para todo $i \geq 0$. Observe que a relação $\ln \xi < \dfrac{\ln \epsilon}{v(x_{n_0} - x_{n_0+i})}$ deve ser satisfeita. Equivalentemente, podemos ver que uma seqüência $\{x_n\}$ de Cauchy é tal que $x_n - x_{n+i} \in \pi^{n(n_0)}$, para todo $i \geq 0$, onde $n(n_0) \to +\infty$ quando $n_0 \to +\infty$. Chamaremos de $\widehat{\mathfrak{A}}$ o completamento de $\mathfrak{A}$ com respeito à métrica $|\cdot|_\pi$, ou seja, seqüências de Cauchy em $\widehat{\mathfrak{A}}$ convergem. Note que a valorização v de $\mathfrak{A}$ pode ser estendida por definição a $\widehat{\mathfrak{A}}$, e quando v for aplicada em $\widehat{\mathfrak{A}}$ denotaremos por v_π.

Observações 1.17.
(1) Se u é uma unidade qualquer em $\widehat{\mathfrak{A}}$, então $|u|_\pi = \xi^{v_\pi(u)} = \xi^0 = 1$. A equação $\xi^m = 1$ só admite a solução $m = 0$, de modo que se $u \in \widehat{\mathfrak{A}}^*$ e $|u|_\pi = 1$, então $v_\pi(u) = 0$ e daí u é uma unidade em $\widehat{\mathfrak{A}}$.

(2) Pelo item (1), $|-1|_\pi = 1$. Assim, pela propriedade (i), temos

$$|-a|_\pi = |-1 \cdot a|_\pi = |-1|_\pi \cdot |a|_\pi = |a|_\pi,$$

para qualquer $a \in \widehat{\mathfrak{A}}$.

Agora definiremos a noção de convergência em $\widehat{\mathfrak{A}}$.

Definição 1.18. Seja $\{x_n\} = \{x_0, x_1, \ldots, x_m, \ldots\}$ uma seqüência em $\widehat{\mathfrak{A}}$ (isto é, $x_n \in \widehat{\mathfrak{A}}$, para todo $n \in \mathbb{N} \cup \{0\}$). Dizemos que "$\{x_n\}$ converge para $x \in \widehat{\mathfrak{A}}$" (indicaremos este fato pelo símbolo "$\lim\limits_{\pi} x_n = x$") se, e somente se, $\lim\limits_{n\to\infty} |x_n - x|_\pi = 0$ (note que $|x_n - x|_\pi$ é um número real).

Proposição 1.19. *Se a seqüência $\{x_n\} = \{x_0, x_1, \ldots, x_m, \ldots\}$ em $\widehat{\mathfrak{A}}$ converge seu limite é único.*

Demonstração: Suponhamos que x e y sejam ambos limites da seqüência $\{x_n\}$. Assim, dado $\epsilon > 0$, existe $n_1 \in \mathbb{N}$ tal que $|x_n - x|_\pi < \epsilon$, sempre que $n > n_1$, e da mesma forma existe $n_2 \in \mathbb{N}$ tal que $|x_n - y|_\pi < \epsilon$, sempre que $n > n_2$. Tomando $N = max\{n_1, n_2\}$ e escolhendo $n > N$ teremos $|x_n - x|_\pi < \epsilon$ e $|x_n - y|_\pi < \epsilon$. Agora, usando a desigualdade forte do triângulo temos $|x - y|_\pi = |x - x_n + x_n - y|_\pi \leq max\{|x_n - y|_\pi, |x_n - x|_\pi\} < \epsilon$ e daí $|x - y|_\pi < \epsilon$, ou seja, $x = y$. ∎

Observação 1.20. Note que, agora, faz sentido dizermos que a função $|\cdot|_\pi$ só será uma métrica em $\mathfrak{A}$ se este for um espaço de Hausdorff, pois assim garantimos a unicidade do limite da seqüência $\{x_n\}$ no anel $\widehat{\mathfrak{A}}$.

Lema 1.21. *Seja $\{x_n\}$ uma seqüência em $\widehat{\mathfrak{A}}$. Esta seqüência é convergente se, e somente se, $\lim\limits_{n\to\infty} |x_n - x_{n+i}|_\pi = 0$, para todo $i \geq 0$.*

Corolário 1.22. *Seja $\{x_n\}$ uma seqüência em $\widehat{\mathfrak{A}}$. Esta seqüência é convergente se, e somente se, $\lim\limits_{n\to\infty} |x_n - x_{n+1}|_\pi = 0$.*

Definimos o conceito de convergência de uma série em $\widehat{\mathfrak{A}}$. Se $\{x_n\}$ é uma seqüência

em $\widehat{\mathfrak{A}}$, construimos uma outra seqüência

$$\begin{aligned}
s_0 &= x_0 \\
s_1 &= x_0 + x_1 \\
&\vdots \\
s_m &= x_0 + x_1 + \cdots + x_m = \sum_{j=0}^{m} x_j \\
&\vdots
\end{aligned}$$

e investigamos a convergência de $\{s_m\}_{m=0}^{\infty}$. Se esta seqüência converge, podemos escrever, fazendo um abuso de notação,

$$\lim_{\pi} s_m = \sum_{n=0}^{\infty} x_n.$$

Um critério muito eficiente para verificar a convergência de uma série desta forma é apresentado no seguinte teorema.

Teorema 1.23. *A série* $\sum_{n=0}^{\infty} x_n$ *converge se, e somente se,* $\lim_{\pi} x_n = 0$.

Demonstração: A seqüência $\{s_m\}$, onde

$$s_m = \sum_{n=0}^{m} x_n,$$

converge (Corolário 1.22) se, e somente se, $\lim_{n\to\infty} |s_n - s_{n+1}|_\pi = 0$, ou seja, se, e somente se, $\lim_{n\to\infty} |x_{n+1}|_\pi = 0$ (que é a mesma coisa que dizer que $\lim_{\pi} x_n = 0$). ∎

Continuaremos usando a mesma notação $\mathfrak{A}$ para representar um anel de valorização discreta. Apresentaremos na seção seguinte, o completamento para este anel via limite projetivo e concluiremos que esse novo completamento é o mesmo encontrado na seção anterior.

1.3 Um Completamento de $\mathfrak{A}$ Via Limite Projetivo

Primeiramente, observamos que o conjunto formado pelos ideais $\pi^n\mathfrak{A}$ forma uma base de vizinhanças do zero e com isso temos uma topologia em $\mathfrak{A}$.

Com a representação (1.1), o homomorfismo canônico de anéis $\phi_n : \mathfrak{A}_n \to \mathfrak{A}_{n-1}$(o qual leva a classe lateral de um elemento mod π^{n+1} para a classe lateral deste mesmo elemento mod π^n), pode ser descrito omitindo o maior termo $a_n\pi^n$ na expansão (1.1).

Agora considere o sistema de homomorfismos de anéis

$$k = \mathfrak{A}_0 \overset{\phi_1}{\leftarrow} \mathfrak{A}_1 \overset{\phi_2}{\leftarrow} \mathfrak{A}_2 \overset{\phi_3}{\leftarrow} \cdots \overset{\phi_n}{\leftarrow} \mathfrak{A}_n \overset{\phi_{n+1}}{\leftarrow} \ldots \tag{1.3}$$

O produto direto de todos estes anéis consiste de todas seqüências infinitas $(b_0, \ldots, b_n, \ldots)$, onde $b_n \in \mathfrak{A}_n$ para todo n. Este conjunto forma um anel quando somamos e multiplicamos duas seqüências componente a componente. Agora, considere o subconjunto $\widehat{\mathfrak{A}}$ do produto direto $\prod_{i=0}^{\infty} \mathfrak{A}_i$ constituído das seqüências tais que:

$$\phi_n(b_n) = b_{n-1}, \forall\ n > 0,$$

chamadas **seqüências compatíveis**.

Assim (1.3) será um sistema de homomorfismos sobrejetivos $\phi_i : \mathfrak{A}_i \longrightarrow \mathfrak{A}_{i-1}$. Isso nos leva a seguinte definição :

Definição 1.24. O **limite inverso** de $(\mathfrak{A}_i, \phi_i)$, denotado por

$$\varprojlim(\mathfrak{A}_i, \phi_i) \ \ ou \ \ \varprojlim \mathfrak{A}_i,$$

é o subconjunto de $\prod_{i=0}^{\infty} \mathfrak{A}_i$ formado pelos elementos $(b_0, b_1, b_2, \ldots)$, com $b_i \in \mathfrak{A}_i$, satisfazendo

$$\phi_i(b_i) = b_{i-1}.$$

Observação 1.25. O limite inverso $\widehat{\mathfrak{A}}$ de $(\mathfrak{A}_i, \phi_i)$ é um subanel do produto direto $\prod_{i=0}^{\infty} \mathfrak{A}_i$.

Note que existe um homomorfismo canônico

$$\theta : \mathfrak{A} \longrightarrow \widehat{\mathfrak{A}},$$

o qual associa cada $x \in \mathfrak{A}$ a uma seqüência cuja n-ésima componente é classe lateral de x mod π^{n+1}.

O homomorfismo θ é um mergulho, ou seja, um monomorfismo (imersão) de $\mathfrak{A}$ em $\widehat{\mathfrak{A}}$, pois $\bigcap \pi^n = 0$ e este é o núcleo do homomorfismo. Por meio deste mergulho, consideramos $\mathfrak{A}$ como um subanel de $\widehat{\mathfrak{A}}$ e $\widehat{\mathfrak{A}}$ é o completamento de $\mathfrak{A}$. Se acontecer $\mathfrak{A} \cong \widehat{\mathfrak{A}}$, dizemos que $\mathfrak{A}$ é ***completo***.

Segue de (1.1) que os elementos de $\widehat{\mathfrak{A}}$ estão em correspondência injetiva com as "séries infinitas" da forma

$$a_0 + a_1\pi + \cdots + a_n\pi^n + \cdots, \quad a_i \in B_m. \tag{1.4}$$

É fácil ver que $\widehat{\mathfrak{A}}$ é um domínio de integridade e mais, é um anel de valorização para a valorização v estendida. Agora considere o epimorfismo $\varphi_i : \widehat{\mathfrak{A}} \longrightarrow \mathfrak{A}/\pi^i\mathfrak{A}$ dado por $\sum_{j=0}^{\infty} a_j\pi^j \mapsto \sum_{j=0}^{i-1} a_j\pi^j + \pi^i\mathfrak{A}$. Temos, para cada $i \geq 0$,

$$\pi^i\left(\sum_{j=0}^{\infty} a_j\pi^j\right) = \sum_{j=i}^{\infty} a_{j-i}\pi^j,$$

assim $\pi^i\widehat{\mathfrak{A}} = Ker\varphi_i$ e daí

$$\widehat{\mathfrak{A}}/\pi^i\widehat{\mathfrak{A}} \cong \mathfrak{A}/\pi^i\mathfrak{A}.$$

Note ainda que $\pi^i\widehat{\mathfrak{A}}$ é único. Também poderíamos ter concluído o resultado acima a partir do seguinte teorema.

Teorema 1.26.
(a) Todo elemento $b \in \widehat{\mathfrak{A}}$ é congruente a um $b_{n-1} \in \mathfrak{A}$ módulo $\pi^m\widehat{\mathfrak{A}}$.
(b) Dois elementos de $\mathfrak{A}$ são congruentes módulo $\pi^m\widehat{\mathfrak{A}}$ em $\widehat{\mathfrak{A}}$ se, e somente se, são congruentes módulo $\pi^m\mathfrak{A}$ em $\mathfrak{A}$.

Demonstração:
(a) Seja $b = \{b_n\} \in \widehat{\mathfrak{A}}$. Então é fácil ver que a seqüência

$$\{b_0 - b_{n-1}, \ldots, b_t - b_{n-1}, \ldots\},$$

representa $b - b_{n-1}$.

Como $\{b_n\} \in \widehat{\mathfrak{A}}$, sabemos que $b_m \equiv b_{m-1} \pmod{\pi^m\widehat{\mathfrak{A}}}$, para todo $m \in \mathbb{N}$. Em particular, temos que, para $t \in \{0, 1, \ldots, n-1\}$, vale $b_{n-1} \equiv b_t \pmod{\pi^{t+1}\widehat{\mathfrak{A}}}$, ou ainda, $b_{n-1} - b_t \equiv 0 \pmod{\pi^{t+1}\widehat{\mathfrak{A}}}$ e assim $b - b_{n-1} \in \pi^n\widehat{\mathfrak{A}}$, ou seja, $b \equiv b_{n-1} \pmod{\pi^n\widehat{\mathfrak{A}}}$.

(b) Sejam $a, b \in \mathfrak{A}$ congruentes módulo $\pi^m\widehat{\mathfrak{A}}$ em $\widehat{\mathfrak{A}}$. Então existe $\alpha \in \widehat{\mathfrak{A}}$ tal que $a - b = \alpha\pi^m$. Se $\{\alpha_n\}$ representa α, temos, para todo $n \in \mathbb{N} \cup \{0\}$,

$$a - b \equiv \alpha_n \pi^m \,(\mathrm{mod}\, \pi^{n+1}\mathfrak{A}).$$

Em particular, tomando $n = m - 1$ na congruência acima obtemos

$$a - b \equiv \alpha_{m-1} \pi^m \,(\mathrm{mod}\, \pi^m\mathfrak{A}),$$

portanto

$$a \equiv b \,(\mathrm{mod}\, \pi^m\mathfrak{A}),$$

em $\mathfrak{A}$.

A afirmação recíproca é simples, pois temos $\mathfrak{A} \subset \widehat{\mathfrak{A}}$. Assim dois elementos de $\mathfrak{A}$ que são congruentes em $\mathfrak{A}$, obviamente, serão congruentes em $\widehat{\mathfrak{A}}$. ∎

Observação 1.27. Note que uma seqüência $\{b_n\}$ converge para b em $\widehat{\mathfrak{A}}$ se existe $n_0 \in \mathbb{N}$ tal que $b_n - b \in \pi^n\widehat{\mathfrak{A}}$, para todo $n > n_0$, e isso equivale à convergência usando a métrica $|\cdot|_\pi$, ou seja, esse completamento pela π-topologia é igual ao obtido usando a métrica.

Vejamos um exemplo para um melhor entendimento.

Exemplo 1.28. Seja $p \in \mathbb{N}$ um primo. Seja $\mathfrak{A}_0 = \{0\}$ e $\mathfrak{A}_i = \mathbb{Z}/p^i\mathbb{Z}$. Definimos o homomorfismo ϕ, com $i \geq 2$, por :

$$\begin{array}{rccc} \phi_i : & \mathbb{Z}/p^i\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^{i-1}\mathbb{Z} \\ & (x \bmod p^i) & \longmapsto & (x \bmod p^{i-1}) \end{array}$$

que são obviamente homomorfismos sobrejetivos. O limite inverso de $(\mathbb{Z}/p^i\mathbb{Z}, \phi_i)$ é chamado o anel dos inteiros p-ádicos e denotado por $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^i\mathbb{Z}$

Mais à frente determinaremos $\mathbb{Z}_p$ de modo mais detalhado, observando que cada $a \in \mathbb{Z}_p$ tem a representação (1.4).

1.4 Corpo Perfeito e Anel Perfeito

Definição 1.29. Seja L uma extensão de um corpo k. Um elemento $c \in L$, que é algébrico sobre k, é dito ser **separável** sobre k, se ele for uma raiz simples de $irr(k, c)$, onde $irr(k, c)$

é o polinômio irredutível sobre k de menor grau do qual c é raiz. A extensão L será uma **extensão separável** de k se ela for algébrica sobre k e se cada um de seus elementos for **separável** sobre k. Também dizemos que L é **separável** sobre k ou que L/k é **separável**. Se L/k é algébrica, mas não é separável, dizemos que L é uma **extensão inseparável** de k.

Definição 1.30. Um corpo **perfeito** é um corpo k tal que cada extensão algébrica L/k é separável.

Suponha que a característica de k seja p e considere a aplicação de k em k dada por

$$F(x) = x^p \ \ (x \in k).$$

Obviamente, devido a k ser de característica p, temos as seguinte relações, para todos $x, y \in k$, sendo que a primeira independe da característica.

$(i)(xy)^p = x^p y^p$,
$(ii)(x+y)^p = x^p + y^p$,

o que mostra que F é um homomorfismo de k em k. Como todo homomorfismo entre corpos é ou um monomorfismo ou nulo, e como $e^p = e$, esta aplicação deve ser um monomorfismo de k em k. O conjunto das imagens por esse monomorfismo é um subcorpo de k, que denotamos por

$$k^p = \{a^p / a \in k\}.$$

Observação 1.31. Note que se $x \in k$, então como F é injetora, segue que x tem, no máximo, uma p-ésima raiz em cada extensão de k. Temos $x \in k^p$ se, e somente se, x tem uma p-ésima raiz em k.

Teorema 1.32. *O corpo k é perfeito se, e somente se, ou a característica de k é zero ou a característica de k é p e $k^p = k$.*

Demonstração: Suponha que a característica de k seja 0. Seja K uma extensão algébrica de k, $a \in K$, e $p(x) = irr(k, a)$. Então $p'(x) \neq 0$ e $p'(x)$ é de grau menor que $p(x)$. Conseqüentemente $p(x)$ não pode dividir $p'(x)$, logo $p'(a) \neq 0$. Assim a é separável sobre k e concluímos que K/k é separável, ou seja, k é perfeito.

Agora, suponha que característica de k é p e sejam K, a, e $p(x)$ como acima. Assuma que $k^p = k$ e que a não é separável sobre k. Como $p'(a) = 0$, $\partial p'(x) < \partial p(x)$ e $p(x)$ é irredutível, temos que $p'(x) = 0$. Seja bx^m um termo de $p(x)$. Então $mbx^{m-1} = 0$ e devemos ter ou $b = 0$ ou m divisível por p. Assim

$$p(x) = \sum_{r=0}^{n} a_r x^{pr}.$$

Como $k^p = k$, cada a_r tem uma única p-ésima raiz em k. Seja $b_r^p = a_r$ para $r = 0, 1, \ldots, n$, então

$$p(x) = \sum_{r=0}^{n} b_r^p x^{pr} = \left(\sum_{r=0}^{n} b_r x^r \right)^p,$$

que contradiz o fato que $p(x)$ é irredutível em $k[x]$. Assim K/k deve ser separável e segue que k é perfeito.

Reciprocamente, suponha que a característica de k é p e que k é perfeito. Seja $a \in k$ e considere o polinômio $x^p - a \in k[x]$. Se este polinômio tem uma raiz b em k então $a = b^p \in k^p$. Suponha que ele não tenha uma raiz em k e seja $p(x)$ um de seus fatores mônico, irredutível e não constante em $k[x]$. Considere a extensão $k(b)$, onde $p(b) = 0$. Em $k(b)(x)$ temos $x^p - a = x^p - b^p = (x - b)^p$ e como $p(x)$ divide este polinômio temos $p(x) = (x - b)^m$ para algum m. Se $m = 1$ então $x - b \in k[x]$ e assim $b \in k$, o que não é verdade. Conseqüentemente $m > 1$. Mas então b não é raiz simples de $p(x)$ e como $p(x) = irr(k, b)$, $k(b)$ não é separável sobre k. Isto contradiz o fato que k é perfeito. Portanto, devemos ter $a \in k^p$, para todo $a \in k$, e assim $k^p = k$. ∎

Corolário 1.33. *Todo corpo finito é perfeito.*

Observação 1.34. Similarmente, um anel comutativo A de característica p, é perfeito se, e somente se, $A^p = A$.

1.5 Um Resultado Devido a Teichmüller

Inicialmente, demonstraremos um Lema que será utilizado tanto no resultado de Teichmüller, quanto na construção do Anel dos Vetores de Witt.

Lema 1.35. *Sejam $s \in \mathbb{N}$ e $a, b \in A$, onde A é um anel comutativo. Se $a \equiv b\,(mod\, p^s A)$, então $a^{p^j} \equiv b^{p^j}\,(mod\, p^{s+j} A)$, $j = 0, 1, 2, \ldots, n$.*

Demonstração: O processo será feito por indução, sobre j. Se $j = 0$, a implicação é óbvia. Para $j = 1$, temos que :

$$a \equiv b\,(\mathrm{mod}\, p^s A) \Rightarrow a - b = p^s \bar{a} \Rightarrow a = p^s \bar{a} + b \text{ com } \bar{a} \in A.$$

Assim,

$$a^p = (p^s \bar{a} + b)^p \Rightarrow a^p - b^p = (p^s \bar{a})^p + p(p^s \bar{a})^{p-1} b + \cdots + p(p^s \bar{a}) b^{p-1}.$$

Como $p \geq 2$ e $s \geq 1$ implicam em $ps \geq s + 1$,temos que $(p^s \bar{a})^p \in p^{s+1} A$.

Para os outros termos à direita da igualdade, observe que $s(p - l) + 1 \geq s + 1$, para todo $l \in \{1, 2, \ldots, p - 1\}$ e daí todos pertencem a $p^{s+1} A$. Logo, $a^p - b^p \in p^{s+1} A$.

Suponhamos que $a^{p^t} \equiv b^{p^t} (\mathrm{mod}\, p^{s+t} A)$, então

$$\begin{aligned} a^{p^{t+1}} - b^{p^{t+1}} &= p^{s+t} \bar{a} \\ a^{p^{t+1}} &= (p^{s+t} \bar{a} + b^{p^t})^p \\ a^{p^{t+1}} - b^{p^{t+1}} &= (p^{s+t} \bar{a})^p + p(p^{s+t} \bar{a})^{p-1} b^{p^t} + \cdots + p(p^{s+t} \bar{a})(b^{p^t})^{p-1}. \end{aligned}$$

Como $p \geq 2$ e $s \geq 1$, implicam em $p(s + t) \geq s + t + 1$, temos que $(p^{s+t} \bar{a})^p \in p^{s+t+1} A$.

Para os outros termos á direita da igualdade, observe que $(s+t)(p-l)+1 \geq s+t+1$, $\forall\ l \in \{1, 2, \ldots, p - 1\}$ e daí todos pertencem a $p^{s+t+1} A$. Assim, $a^{p^{t+1}} - b^{p^{t+1}} \in p^{s+t+1} A, \forall\ t \in \{0, 1, \ldots, n\}$. ∎

Nosso objetivo a partir daqui é obter um conjunto que denotaremos por $\bar{B}$ de modo que aplicação $f : k = \widehat{\mathfrak{A}}/\pi\widehat{\mathfrak{A}} \longrightarrow \bar{B}$ seja multiplicativa e $\bar{B}$ é o conjunto ideal que foi citado após a Definicão 1.12. Sabemos que existem os conjuntos

$$B_m = \{u_i \in U(A) \cup \{0\}\,; u_i - u_j \notin \langle \pi \rangle\,, \forall\, i \neq j\},\ m \in \mathbb{N},$$

contidos no anel de valorização discreta $\mathfrak{A}$, que são chamados sistema de representantes de $k = \mathfrak{A}/\pi\mathfrak{A}$ em $\mathfrak{A}$. Com um conjunto B_m fixo, definimos a aplicação bijetiva $f : k \longrightarrow B_m$

(veja Seção 1.1). O objetivo então é obter um conjunto $\bar{B} \in \widehat{\mathfrak{A}}$ tal que a aplicação $\{\cdot\} : k \longrightarrow \bar{B}$ além de bijetiva seja multiplicativa, lembre-se que $k = \mathfrak{A}/\pi\mathfrak{A} \cong \widehat{\mathfrak{A}}/\pi\widehat{\mathfrak{A}}$ e estaremos supondo k perfeito de característica p. Vejamos como obter $\bar{B}$. Devemos lembrar que sendo π um parâmetro uniformizador em $\widehat{\mathfrak{A}}$, então p deve ser divisível por π, quando característica de $\widehat{\mathfrak{A}}$ é zero.

Definimos, agora, a seguinte aplicação projeção $\phi : \widehat{\mathfrak{A}} \longrightarrow k$. Agora, dado $\alpha \in k$ sabemos que $\alpha^{p^{-n}} \in k$, pois k é perfeito. Denotemos por L_n a imagem inversa pela ϕ de $\alpha^{p^{-n}} \in k$ e, por U_n o conjunto de todos x^{p^n} tais que $x \in L_n$. Observe que L_0 representa o conjunto de todos os representantes de α, ou seja, L_0 é a classe residual de α. Note, agora, que os U_n foram escolhidos de forma que cada elemento x^{p^n} representa α e daí cada U_n está contido na classe residual L_0, ou seja,

$$U_0 = L_0,\, U_1 = L_1^p \subset L_0,\, U_2 = L_2^{p^2} \subset L_1^p \subset L_0,\, \ldots$$

o que resulta em $U_0 \supset U_1 \supset U_2 \supset \cdots$, ou seja, os U_n's formam uma seqüência decrescente.

Tomando, agora, uma seqüência $(a_0, a_1^p, a_2^{p^2}, \ldots, a_n^{p^n}, \ldots)$, com $a_0 \in U_0 = L_0, a_1^p \in U_1$, etc, vemos que ela é de Cauchy, pois $\overline{a_n} = \alpha^{p^{-n}}$ e $\overline{a_{n+1}} = \alpha^{p^{-(n+1)}}$, onde $\overline{a_n}$ e $\overline{a_{n+1}}$ são as classes a que pertencem a_n e a_{n+1}, respectivamente. A última igualdade resulta em $\overline{a_{n+1}^p} = \alpha^{p^{-n}}$ e assim temos $\overline{a_n} = \overline{a_{n+1}^p}$, o que resulta em $a_n^{p^n} \equiv a_{n+1}^{p^{(n+1)}} \pmod{\pi^{n+1}\widehat{\mathfrak{A}}}$, pelo Lema 1.35. Observe, também, que qualquer seqüência tomada desta forma tem suas coordenadas como representantes de α, assim como $\widehat{\mathfrak{A}}$ é completo, podemos escrever $\{\alpha\} = \lim U_n$. Afirmamos que o limite só depende de α. De fato, se

$$b_n \equiv a_n (\mathrm{mod}\, \pi),$$

então pelo Lema 1.35,

$$b_n^{p^n} \equiv a_n^{p^n} (\mathrm{mod}\, \pi^{n+1}).$$

Daí tanto a seqüência $\left(b_n^{p^n}\right)$, quanto a seqüência $\left(a_n^{p^n}\right)$, convergem para $\{\alpha\}$.

Mostraremos que $\bigcap U_n = \{\alpha\}$. De fato, se a_0 tiver uma p^n-ésima raiz $a_n \in \widehat{\mathfrak{A}}$, para todo $n \geq 0$, então, fazendo essa escolha, obteremos a seqüência constante $(a_0, a_0, a_0, \ldots)$, e assim $a_0 = \{\alpha\}$. Em geral, usando o fato que $a_0 \equiv a_1^p \,(\mathrm{mod}\, \pi), a_0 \equiv a_2^{p^2} \,(\mathrm{mod}\, \pi), a_0 \equiv a_3^{p^3} \,(\mathrm{mod}\, \pi), \ldots$, isto é válido porque cada $a_n^{p^n}$ representa α, ou seja, todos pertencem a

mesma classe residual. Concluímos assim que $a_0 \equiv \{\alpha\} \pmod{\pi}$ e $\{\alpha\}$ é de fato um representante de α. Como em L_0 estão todos os representantes de α, concluímos que $\{\alpha\} \in L_0 = U_0$. E agora, considere a seqüência $(a_1^p, a_2^{p^2}, \dots)$, que obviamente também converge para $\{\alpha\}$, assim $a_1^p \equiv \{\alpha\} \pmod{\pi}$ e, olhando para o fato que a seqüência $(a_n^{p^n})_{n\geq 1} \in \prod_{n=1}^{\infty} U_n$, concluímos que $\{\alpha\} \in U_1$. Prosseguindo desta forma e observando que cada $a_n^{p^n}$ pertence a um U_n fixo, logo $a_n^{p^n} \equiv \{\alpha\} \pmod{\pi}$, para cada $n \geq 0$, ou seja, $\{\alpha\} \in U_n$, para todo $n \geq 0$. Assim, obtemos o resultado desejado que é $\bigcap U_n = \{\alpha\}$.

Desta maneira, $\bar{B} = \{\{\alpha\} \,|\alpha \in k\}$, onde $\{\alpha\}$ é encontrado da forma acima. O conjunto $\bar{B}$ é chamado ***conjunto dos representantes de Teichmüller***.

Lema 1.36. *O sistema de representantes $\alpha \mapsto \{\alpha\}$ de k em $\widehat{\mathfrak{A}}$ é único, ou seja, o conjunto $\bar{B}$ é único.*

Demonstração: Suponhamos que exista outro sistema de representantes $\alpha \mapsto [\alpha]$, então teremos $[\alpha] \in U_n$, para todo n. Como as seqüências em U_n são de Cauchy, concluímos que $[\alpha] = \lim U_n$ e daí, pela unicidade do limite, temos que $[\alpha] = \{\alpha\}$. ∎

Pela própria construção de $\bar{B}$, concluímos o seguinte resultado.

Corolário 1.37. *A aplicação $\{\cdot\} : k \longrightarrow \bar{B}$, dada por $\alpha \mapsto \{\alpha\}$, é bijetiva.*

Agora, provaremos que o sistema de representantes $\bar{B}$ é multiplicativo.

Lema 1.38. *O conjunto $\bar{B}$ é um sistema de representantes multiplicativo.*

Demonstração: Considere a aplicação $\{\cdot\} : k \longrightarrow \widehat{\mathfrak{A}}$ dada por $\alpha \mapsto \{\alpha\}$ assim dados $\alpha, \beta \in k$ sejam $(a_n^{p^n}), (b_n^{p^n})$ seqüências convergindo para $\{\alpha\}, \{\beta\}$, respectivamente. Como $(xy)^p = x^p y^p$ não importando a característica de $\widehat{\mathfrak{A}}$, está claro pela convergência de $(a_n^{p^n} b_n^{p^n})$ para $\{\alpha\}\{\beta\}$ que

$$\{\alpha\}\{\beta\} = \{\alpha\beta\}. \tag{1.5}$$

∎

Note que, se $\mathfrak{A}$ tem característica p, também temos

$$a_n^{p^n} + b_n^{p^n} = (a_n + b_n)^{p^n},$$

e daí,

$$\{\alpha\} + \{\beta\} = \{\alpha + \beta\}\,. \tag{1.6}$$

Assim, usando o Corolário 1.37, (1.5) e (1.6), concluímos que $\bar{B} \cong k$ se $\widehat{\mathfrak{A}}$ tiver característica p.

Decorre diretamente do Lema 1.38 que $\{\alpha^p\} = \{\alpha\}^p$. Agora provaremos o seguinte lema.

Lema 1.39. *Um elemento $y \in \widehat{\mathfrak{A}}$ é um representante multiplicativo da classe lateral α se, e somente se, ele for um p^n-ésima potência em $\widehat{\mathfrak{A}}$.*

Demonstração: Suponhamos que $y \in \widehat{\mathfrak{A}}$ seja um representante multiplicativo de $\alpha \in k$. Logo

$$\alpha \in k \Rightarrow \{\alpha\} = y \in \widehat{\mathfrak{A}},\ \text{mas}\ \alpha = b^{p^n} \in k\ (k\text{é perfeito}),\ \text{assim}$$
$$\{b\}^{p^n} = y,\ \text{ou seja,}\ y\ \text{é uma}\, p^n - \text{ésima potência em}\ \widehat{\mathfrak{A}}.$$

Reciprocamente, se y é uma p^n-ésima potência em $\widehat{\mathfrak{A}}$, então existe $a \in \widehat{\mathfrak{A}}$ tal que $y = a^{p^n}$. Assim construímos a seqüência $(a^{p^n}, a^{p^n}, \dots) = a^{p^n}$, onde cada componente é um representante de α. Esta seqüência é de Cauchy e converge para $\{\alpha\}$, ou seja, $\{\alpha\} = a^{p^n}$, para todo $n \geq 0$. ∎

O que foi visto, até agora nesta seção, pode ser resumido no seguinte teorema. Este é o resultado devido a Teichmüller.

Teorema 1.40. *Seja $\widehat{\mathfrak{A}}$ um anel de valorização discreta completo. Assuma que $k = \widehat{\mathfrak{A}}/\pi\widehat{\mathfrak{A}}$ é um corpo perfeito de característica p. Então:*
(i) Existe um e somente um sistema de representantes $\{\cdot\} : k \longrightarrow \widehat{\mathfrak{A}}$ tal que este é multiplicativo, isto é, $\{\alpha\beta\} = \{\alpha\}\{\beta\}$ para todos $\alpha, \beta \in k$.
(ii) Se $\widehat{\mathfrak{A}}$ tem característica p, este sistema de representantes é aditivo, isto é, $\{\alpha + \beta\} = \{\alpha\} + \{\beta\}$.
(iii) $\{\cdot\} : k \longrightarrow \widehat{\mathfrak{A}}$ comuta com p-ésimas potências: $\{\alpha^p\} = \{\alpha\}^p$.
(iv) Para que $a \in \widehat{\mathfrak{A}}$ pertença a $\bar{B} = \{k\}$, é necessário e suficiente que a seja uma p^n-ésima potência em $\widehat{\mathfrak{A}}$ para todo $n \geq 0$.

Agora faremos um exemplo de como obter o conjunto dos representantes multiplicativos para um anel de valorização discreta completo específico, a saber $\mathbb{Z}_p$. Para isso, precisaremos do seguinte lema.

Lema 1.41 (Lema de Hensel I). *Seja f um polinômio sobre $\widehat{\mathfrak{A}}$ e seja $a \in \widehat{\mathfrak{A}}$, $\widehat{\mathfrak{A}}$ um anel de valorização discreta completo, tal que $f^{'}(a) \neq 0$ e*

$$\left| \frac{f(a)}{f'(a)^2} \right|_\pi < 1.$$

Então a seqüência de Newton

$$a_{n+1} = a_n - \frac{f(a)}{f^{'}(a)}, n = 0, 1, \ldots$$

que começa com $a_0 = a$ converge para um zero ξ de f. Este zero satisfaz a desigualdade,

$$|\xi - a|_\pi < \left| f^{'}(a) \right|_\pi$$

e este é o único zero de f satisfazendo esta desigualdade.

Demonstração: Ver ([16], p. 47)

Exemplo 1.42. Seja p um primo e considere o polinômio $f(x) = x^{p-1} - 1$ sobre $\mathbb{Z}_p$. Para cada $a \in \mathbb{Z}_p$ tal que $a \not\equiv 0 \,(\mathrm{mod}\, p)$, temos também que

$$f^{'}(a) = (p-1)a^{p-2} \not\equiv 0 \,(\mathrm{mod}\, p) \Rightarrow \left| f^{'}(a)^2 \right|_p = 1.$$

Conseqüentemente existe, pelo Lema 1.41, uma única $(p-1)$-ésima raiz da unidade em $\mathbb{Z}_p$ que é congruente a a módulo p. Isto determina o seguinte isomorfismo :

$$\theta : H \longrightarrow U_{p-1}(\mathbb{Z}_p),$$

onde H é um grupo multiplicativo dos elementos não-nulos módulo p de $\mathbb{Z}_p$, ou seja, $H = \mathbb{F}_p^*$ e $U_{p-1}(\mathbb{Z}_p)$ é o grupo de todas $(p-1)$-ésimas raízes da unidade. Assim, o conjunto $U_{p-1}(\mathbb{Z}_p) \cup \{0\}$ é chamado o conjunto dos ***representantes multiplicativos*** do corpo residual $\mathbb{F}_p \cong \mathbb{Z}/p$.

1.6 A Estrutura de $\widehat{\mathfrak{A}}$

Continuaremos usando a notação $\{\alpha\}$, do Teorema 1.40. Assumiremos, daqui para frente, que $\widehat{\mathfrak{A}}$ tem característica zero. Assim como em (1.1), temos que cada elemento

$a \in \widehat{\mathfrak{A}}$ tem uma única representação

$$a = \{\alpha_0\} + \{\alpha_1\}\,\pi + \cdots + \{\alpha_n\}\,\pi^n + \cdots, \;\; \{\alpha_i\} \in \bar{B},$$

mas não sabemos como somar e multiplicar essas expressões até agora.

Sabemos que p é divisível por π,

$$p = u\pi^r,$$

onde u é uma unidade em $\widehat{\mathfrak{A}}$ e $r = v(p)$. Isso nos leva a seguinte definição :

Definição 1.43. Se r, dado como acima, for igual a 1, dizemos que $\widehat{\mathfrak{A}}$ é não ramificado.

Neste caso, já que a escolha do parâmetro uniformizador π é arbitrária, faremos a escolha canônica $\pi = p$, e daí um típico elemento $a \in \widehat{\mathfrak{A}}$ tem a representação

$$a = \{\alpha_0\} + \{\alpha_1\}\,p + \cdots + \{\alpha_n\}\,p^n + \cdots, \;\; \{\alpha_i\} \in \bar{B}. \tag{1.7}$$

Por exemplo, $\mathbb{Z}_p$ é não ramificado.

Agora veremos como somar e multiplicar dois elementos de $\widehat{\mathfrak{A}}$. Isto será abordado no seguinte teorema.

Teorema 1.44. *Assuma que $\widehat{\mathfrak{A}}$ é não ramificado. As operações no anel $\widehat{\mathfrak{A}}$ são unicamente determinadas pelas operações em k.*

Demonstração: Para somarmos dois elementos de $\widehat{\mathfrak{A}}$ procedemos da seguinte forma. Sejam $a, b \in \widehat{\mathfrak{A}}$, assim podemos escrever

$$a + b = \{\alpha_0\} + \{\beta_0\} + (\{\alpha_1\} + \{\beta_1\})p + \cdots, \tag{1.8}$$

onde $a = \{\alpha_0\} + \{\alpha_1\}\,p + \cdots$ e $b = \{\beta_0\} + \{\beta_1\}\,p + \cdots$. Portanto saberemos quem é $a + b$ assim que determinarmos $\{\alpha_i\} + \{\beta_i\}$ para cada $i \in \{0, 1, \dots\}$. Veremos, também, que o produto depende desta soma. Assim, a estrutura completa de $\widehat{\mathfrak{A}}$ é determinada pela fórmula

$$\{\alpha\} + \{\beta\} = \sum_{n=0}^{\infty} \left\{\bar{S}_n(\alpha, \beta)\right\} p^n, \tag{1.9}$$

onde $\bar{S}_n(\alpha,\beta) \in k$ precisa ser determinada para todo n. Usando a representação (1.9), podemos escrever $a+b$ da seguinte forma

$$\begin{gathered} a+b = \left\{\bar{S}_0(\alpha_0,\beta_0)\right\} + \left\{\bar{S}_0(\alpha_1,\beta_1) + \bar{S}_1(\alpha_0,\beta_0)\right\} p + \\ + \left\{\bar{S}_0(\alpha_2,\beta_2) + \bar{S}_1(\alpha_1,\beta_1) + \bar{S}_2(\alpha_0,\beta_0)\right\} p^2 + \cdots \\ + \left\{\bar{S}_0(\alpha_n,\beta_n) + \bar{S}_1(\alpha_{n-1},\beta_{n-1}) + \cdots + \bar{S}_n(\alpha_0,\beta_0)\right\} p^n + \cdots , \end{gathered}$$

ou seja, saberemos quem é $a+b$ quando determinarmos $\bar{S}_i(\alpha_j,\beta_j)$, para todos $i,j \in \mathbb{N}$. Usaremos a seguinte notação $\bar{S}_n(a,b) = \sum_{i=0}^{n} \bar{S}_i(\alpha_{n-i},\beta_{n-i})$. Assim,

$$a+b = \left\{\bar{S}_0(a,b)\right\} + \left\{\bar{S}_1(a,b)\right\} p + \left\{\bar{S}_2(a,b)\right\} p^2 + \cdots + \left\{\bar{S}_n(a,b)\right\} p^n + \cdots . \tag{1.10}$$

Mostraremos primeiro que $\bar{S}_0(\alpha,\beta) = \alpha+\beta$. De fato, sejam $(a_n^{p^n})$ e $(b_n^{p^n})$ seqüências convergindo para $\{\alpha\}$ e $\{\beta\}$, respectivamente. Lembremos que $a_n^{p^n} \in U_n^1$ e $b_n^{p^n} \in U_n^2$, para todo $n \geq 0$ e que $\{\alpha\} = \lim U_n^1$ e $\{\beta\} = \lim U_n^2$. Construindo, agora, a seqüência $(a_0+b_0, c_1^p, c_2^{p^2}, \dots)$, onde $a_0+b_0 \in U_0^3$ e $c_n^{p^n} \in U_n^3$, para todo $n \geq 1$, vemos que a_0+b_0 é um representante de $\alpha+\beta$ e os $c_i^{p^i}$'s foram escolhidos de forma a representarem $\alpha+\beta$. Conseqüentemente, a seqüência $(a_0+b_0, c_1^p, c_2^{p^2}, \dots)$ converge para $\{\alpha+\beta\}$. Obviamente, a seqüência $(a_0+b_0, a_1^p+b_1^p, a_2^{p^2}+b_2^{p^2}, \dots)$ converge para $\{\alpha\}+\{\beta\}$ e temos a seguinte congruência $c_n^{p^n} \equiv a_n^{p^n} + b_n^{p^n} \pmod p$, para todo $n \geq 1$, ou seja, todos os termos estão na mesma classe residual e mais $a_0+b_0 \equiv \{\alpha\}+\{\beta\} \pmod p$ e $a_0+b_0 \equiv \{\alpha+\beta\} \pmod p$, ou seja, $\{\alpha+\beta\} \equiv \{\alpha\}+\{\beta\} \pmod p$ e daí $\bar{S}_0(\alpha,\beta) = \alpha+\beta$.

Agora mostraremos quem é $-a = -\{\alpha_0\} - \{\alpha_1\} p - \{\alpha_2\} p^2 - \cdots$, o inverso aditivo de a. Primeiramente, computamos $-\{\alpha\} \in \widehat{\mathfrak{A}}$. Se p é ímpar, então o representante multiplicativo de $-1 \in k$ é $-1 \in \widehat{\mathfrak{A}}$. A saber, se $a_n \in \widehat{\mathfrak{A}}$ é tal que

$$a_n^{p^n} = 1,$$

então

$$(-a_n)^{p^n} = -1.$$

Conseqüentemente, se p é ímpar,

$$-\{\alpha\} = \{-1\}\{\alpha\} = \{-\alpha\}.$$

Entretanto, se $p = 2$, -1 tem a expansão $2-$ádica,

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

Conseqüentemente,

$$-\{\alpha\} = (-1)\{\alpha\} = \{\alpha\} + \{\alpha\}2 + \cdots + \{\alpha\}2^n + \cdots$$

O processo para determinar $a+b$ será por indução. Assumiremos que a estrutura do anel residual $\widehat{\mathfrak{A}}/p^n$ tenha sido determinada (isto é, que sabemos todas as operações do anel $\widehat{\mathfrak{A}}$ módulo p^n). Determinaremos a estrutura de $\widehat{\mathfrak{A}}/p^{n+1}$. Primeiramente, determinaremos a estrutura de $\widehat{\mathfrak{A}}/p^2$.

Sejam

$$\begin{aligned} a &= \{\alpha_0\} + \{\alpha_1\}p \\ b &= \{\beta_0\} + \{\beta_1\}p. \end{aligned}$$

Multiplicando a e b, temos

$$ab \equiv \{\alpha_0\beta_0\} + (\{\alpha_0\beta_1\} + \{\alpha_1\beta_0\})p \pmod{p^2}. \tag{1.11}$$

Já que

$$\{\alpha_0\beta_1\} + \{\alpha_1\beta_0\} \equiv \{\alpha_0\beta_1 + \alpha_1\beta_0\} \pmod{p}, \tag{1.12}$$

substituindo (1.12) em (1.11), obtemos

$$ab \equiv \{\alpha_0\beta_0\} + (\{\alpha_0\beta_1 + \alpha_1\beta_0\})p \pmod{p^2}.$$

Assim, usando a mesma notação de (1.10), temos $\bar{P}_0(a,b) = \alpha_0\beta_0$ e $\bar{P}_1(a,b) = \alpha_0\beta_1 + \alpha_1\beta_0$, ou seja,

$$ab \equiv \left\{\bar{P}_0(a,b)\right\} + (\left\{\bar{P}_1(a,b)\right\})p \pmod{p^2}. \tag{1.13}$$

Mas somando a e b, temos

$$a + b = \{\alpha_0\} + \{\beta_0\} + (\{\alpha_1\} + \{\beta_1\})p. \tag{1.14}$$

Agora,

$$\{\alpha_0\} + \{\beta_0\} \equiv \{\alpha_0 + \beta_0\} + \left\{\bar{S}_1(\alpha_0, \beta_0)\right\}p \pmod{p^2}. \tag{1.15}$$

Conseqüentemente, substituindo (1.15) em (1.14), temos

$$a+b \equiv \{\alpha_0+\beta_0\} + \left\{\alpha_1+\beta_1+\bar{S}_1(\alpha_0,\beta_0)\right\} p \pmod{p^2}, \tag{1.16}$$

o que mostra que a fórmula para $a+b$ será conhecida, assim que determinarmos $\bar{S}_1(\alpha_0,\beta_0)$.

Uma vez que k é perfeito, podemos tomar p-ésimas raízes. Então $\left\{\alpha_0^{1/p}\right\} + \left\{\beta_0^{1/p}\right\}$ é um representante de $\alpha_0^{1/p}+\beta_0^{1/p}$, e daí

$$\left\{\alpha_0^{1/p}\right\} + \left\{\beta_0^{1/p}\right\} \equiv \left\{\alpha_0^{1/p}+\beta_0^{1/p}\right\} \pmod{p},$$

onde $\left\{\alpha_0^{1/p}+\beta_0^{1/p}\right\}^p = \{\alpha_0+\beta_0\}$, pois k tem característica p. Usando este fato e o Lema 1.35, elevamos ambos os lados a p-ésima potência e obtemos

$$\left(\left\{\alpha_0^{1/p}\right\} + \left\{\beta_0^{1/p}\right\}\right)^p \equiv \{\alpha_0+\beta_0\} \pmod{p^2}. \tag{1.17}$$

Expandindo o lado esquerdo pela fórmula binomial, temos

$$\{\alpha_0\} + \{\beta_0\} + \sum_{l=1}^{p-1} \binom{p}{l} \left\{\alpha_0^{(p-l)/p}\beta_0^{l/p}\right\}. \tag{1.18}$$

Colocando p em evidência no coeficiente binomial, escrevemos um polinômio em $\left\{\alpha_0^{1/p}\right\}$ e $\left\{\beta_0^{1/p}\right\}$ com coeficientes inteiros. Substituindo (1.18) em (1.17), obtemos

$$\{\alpha_0\} + \{\beta_0\} \equiv \{\alpha_0+\beta_0\} - \sum_{l=1}^{p-1} \frac{1}{p} \binom{p}{l} \left\{\alpha_0^{(p-l)/p}\beta_0^{l/p}\right\} p \pmod{p^2}. \tag{1.19}$$

Assim, substituindo (1.19) em (1.15), obtemos

$$\bar{S}_1(\alpha_0,\beta_0) = -\sum_{l=1}^{p-1} \frac{1}{p} \binom{p}{l} \alpha_0^{(p-l)/p}\beta_0^{l/p}.$$

Portanto, concluímos que

$$a+b = \{\alpha_0+\beta_0\} + \left\{\alpha_1+\beta_1 - \sum_{l=1}^{p-1} \frac{1}{p} \binom{p}{l} \alpha_0^{(p-l)/p}\beta_0^{l/p}\right\} p \pmod{p^2},$$

ou seja,

$$a+b=\left\{\bar{S}_0(a,b)\right\}+\left\{\bar{S}_1(a,b)\right\}p\,(\mathrm{mod}\,p^2).$$

Finalmente, assumimos que sabemos a estrutura de $\mathfrak{A}/p^n$. Sejam,

$$\begin{aligned} a &= \sum_{i=0}^{n}\{\alpha_i\}\,p^i \;\in\; \mathfrak{A}/p^{n+1} \\ b &= \sum_{i=0}^{n}\{\beta_i\}\,p^i \;\in\; \mathfrak{A}/p^{n+1}. \end{aligned}$$

Então

$$ab=\sum_{l=0}^{n}\sum_{i+j=l}\{\alpha_i\beta_j\}\,p^l.$$

Vimos, anteriormente, que $\sum_{i+j=l}\{\alpha_i\beta_j\}$ nos dará uma expansão p-ádica. Para $l\geq 1$, temos que esta expansão só precisa ser determinada até o coeficiente de p^{n-l}, pois no produto ab, devido ao p^l multiplicando $\sum_{i+j=l}\{\alpha_i\beta_j\}$, todos os outros termos da expansão se anularão, uma vez que estamos multiplicando a e b em $\widehat{\mathfrak{A}}/p^{n+1}$. Como a estrutura de $\widehat{\mathfrak{A}}/p^n$ é conhecida por hipótese, resulta que a expansão de $\sum_{i+j=l}\{\alpha_i\beta_j\}$ até o coeficiente de p^{n-l} é conhecida. Para $l=0$, temos $\{\alpha_0\beta_0\}$. Assim, a multiplicação em $\mathfrak{A}/p^{n+1}$ é determinada por adição. Para adição, temos

$$a+b=\sum_{i=0}^{n}(\{\alpha_i\}+\{\beta_i\})p^i\in\mathfrak{A}/p^{n+1}.$$

Para cada i, temos que $\{\alpha_i\}+\{\beta_i\}=\sum_{i=0}^{\infty}\left\{\bar{S}_i(\alpha_i,\beta_i)\right\}p^i$. Assim, para $i\geq 1$, a expansão p-ádica de $\{\alpha_i\}+\{\beta_i\}$ precisa somente ser determinada até o coeficiente de p^{n-1}, uma vez que todos os outros termos na soma $a+b$ serão congruentes a zero módulo p^{n+1}. Lembre-se que estamos somando a e b em $\mathfrak{A}/p^{n+1}$. Por hipótese, sabemos a estrutura de $\mathfrak{A}/p^n$, logo a expansão de $\{\alpha_i\}_{i\geq 1}+\{\beta_i\}_{\geq 1}$ até o coeficiente de p^{n-1} é conhecida. Note que, pela hipótese de indução, conhecemos todos os coeficientes da expansão de $\{\alpha_0\}+\{\beta_0\}$ até p^{n-1}, portanto, saberemos quem é $a+b$ uma vez que determinarmos o coeficiente de p^n na expansão de $\{\alpha_0\}+\{\beta_0\}$. Agora, como k é perfeito, podemos tomar p^n-ésimas raízes, assim $\left\{\alpha_0^{p^{-n}}\right\}+\left\{\beta_0^{p^{-n}}\right\}$ é um representante de $\alpha_0^{p^{-n}}+\beta_0^{p^{-n}}$. Omitindo o índice

zero, teremos pelo Lema 1.35,

$$\left(\left\{\alpha^{p^{-n}}\right\}+\left\{\beta^{p^{-n}}\right\}\right)^{p^n} \equiv \{\alpha+\beta\} \pmod{p^{n+1}}.$$

Novamente, estamos usando o fato que $\left\{\alpha^{p^{-n}}+\beta^{p^{-n}}\right\}^{p^n} = \{\alpha+\beta\}$, pois a característica de k é p. Expandindo o lado esquerdo da última congruência pela fórmula binomial, teremos

$$\{\alpha\}+\{\beta\}+\sum_{l=1}^{p^n-1}\binom{p^n}{l}\left\{\alpha^{1-lp^{-n}}\beta^{lp^{-n}}\right\}.$$

Como p divide todos os coeficientes binomiais, podemos colocá-lo em evidência, então teremos um polinômio em $\left\{\alpha^{p^{-n}}\right\}$ e $\left\{\beta^{p^{-n}}\right\}$ com coeficientes inteiros, ou seja,

$$\{\alpha\}+\{\beta\} \equiv \{\alpha+\beta\}-\sum_{l=1}^{p^n-1}\frac{1}{p}\binom{p^n}{l}\left\{\alpha^{1-lp^{-n}}\beta^{lp^{-n}}\right\}p \pmod{p^{n+1}}.$$

Pela hipótese de indução, determinamos a expansão p-ádica do polinômio

$$\sum_{l=1}^{p^n-1}\frac{1}{p}\binom{p^n}{l}\left\{\alpha^{1-lp^{-n}}\beta^{lp^{-n}}\right\},$$

até o coeficiente de p^{n-1}. E assim, finalmente, obtemos na última congruência acima a expansão p-ádica de $\{\alpha_0\}+\{\beta_0\}$ até o coeficiente de p^n e isto prova o que desejávamos.∎

Assim, temos o seguinte teorema.

Teorema 1.45. *Sejam $\widehat{\mathfrak{A}}_1$ e $\widehat{\mathfrak{A}}_2$ anéis de valorização discreta completos não ramificados de característica zero tendo o mesmo corpo residual k perfeito de característica $p>0$. Então existe um único isomorfismo de $\widehat{\mathfrak{A}}_1$ com $\widehat{\mathfrak{A}}_2$ induzindo a identidade sobre k.*

Demonstração: Do argumento usado no teorema anterior, a aplicação dada por

$$\sum_{n=0}^{\infty}\{\alpha\}_1 p^n \longrightarrow \sum_{n=0}^{\infty}\{\alpha\}_2 p^n,$$

onde $\{\alpha\}_i$ é o representante multiplicativo de $\alpha \in k$ no anel $\widehat{\mathfrak{A}}_i$, $i=1,2$, é o único isomorfismo. ∎

Na próxima seção, obteremos o sistema de representantes de k em $\widehat{\mathfrak{A}}$ quando ambos têm característica zero.

1.7 Resultados quando $\widehat{\mathfrak{A}}$ e k têm a mesma Característica

Proposição 1.46. *Se o corpo residual k do anel $\widehat{\mathfrak{A}}$ tem característica zero, então $\widehat{\mathfrak{A}}$ contém um subcorpo isomorfo a k.*

Demonstração: Necessitamos do seguinte lema para fazer a demonstração.

Lema 1.47 (Lema de Zorn). *Seja $\boldsymbol{S}$ um conjunto parcialmente ordenado. Suponhamos que cada subconjunto simplesmente ordenado de $\boldsymbol{S}$ tenha um limite superior (limite inferior) em $\boldsymbol{S}$. Então $\boldsymbol{S}$ tem um elemento máximo (mínimo).*

Seja $\phi : \widehat{\mathfrak{A}} \longrightarrow k$ um homomorfismo canônico. Para um inteiro $n \neq 0$, $\phi(n) \neq 0$ por hipótese (característica de k é zero) e assim os inteiros não-nulos são mergulhados nas unidades de $\widehat{\mathfrak{A}}$, o qual contém o corpo $\mathbb{Q}$ (conjunto dos números racionais). Considere o conjunto não-vazio de todos os subcorpos de $\widehat{\mathfrak{A}}$ ordenados pela inclusão. Aplicando o Lema 1.47 (Lema de Zorn), obtemos um subcorpo maximal k_0 de $\widehat{\mathfrak{A}}$ e $\phi(k_0)$ é então um subcorpo de k isomorfo a k_0. Temos então que considerar dois casos.

Caso 1 : k é uma extensão transcendente de $\phi(k_0)$, ou seja, existe um $\eta \in k$ que não satisfaz equação polinomial com coeficientes em $\phi(k_0)$.

Neste caso temos $\phi(\xi) = \eta$, para algum $\xi \in \widehat{\mathfrak{A}}$. Por hipótese, todo elemento não-nulo da álgebra $k_0[\xi]$ gerada por ξ sobre k_0 são unidades em $\widehat{\mathfrak{A}}$, assim o corpo $k_0(\xi)$ está contido em $\widehat{\mathfrak{A}}$. Isto é impossível, pois k_0 é maximal em $\widehat{\mathfrak{A}}$

Caso 2 : k é uma extensão algébrica de $\phi(k_0)$.

Suponhamos que exista um $\omega \in k$, com $\omega \notin \phi(k_0)$. Seja

$$\bar{f}(x) = x^m + \phi(b_{m-1})x^{m-1} + \cdots + \phi(b_0),$$

o polinômio minimal de ω sobre $\phi(k_0)$. Já que k tem característica zero, teremos

$$0 \neq \bar{f}'(\omega) = m\omega^{m-1} + (m-1)\phi(b_{m-1})\omega^{m-1} + \cdots + \phi(b_1).$$

Considere o polinômio

$$f(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0,$$

com coeficientes em k_0. Pelo Lema 1.41 (Lema de Hensel I), este polinômio tem uma raiz $a \in \widehat{\mathfrak{A}}$ tal que $\phi(a) = \omega$. Como $\bar{f}$ é irredutível, f também é, assim $k_0(a)$ é um subcorpo de $\widehat{\mathfrak{A}}$. Isto nos leva a uma contradição, devido a k_0 ser maximal em $\widehat{\mathfrak{A}}$.

Assim, mostramos que $\phi(k_0) \cong k$. ∎

Observação 1.48. A conclusão da Proposição 1.46 é válida para cada Anel de Valorização Discreta Completo $\widehat{\mathfrak{A}}$ cujo corpo residual tem a mesma característica de $\widehat{\mathfrak{A}}$, mas a prova para característica p exige grande técnica (ver Teorema 27, p. 304 de [19]).

Corolário 1.49. *Se o corpo residual k do anel $\widehat{\mathfrak{A}}$ tem a mesma característica de $\widehat{\mathfrak{A}}$, então $\widehat{\mathfrak{A}}$ é isomorfo ao anel das séries de potências formais $k[[x]]$.*

Demonstração: Pela observação acima e pela Proposição 1.46, tomamos $k \subset \widehat{\mathfrak{A}}$. Seja π um parâmetro uniformizador. Então $\widehat{\mathfrak{A}}$ contém o anel $k[\pi]$, gerado por π sobre $\widehat{\mathfrak{A}}$. Se

$$f(\pi) = a_n\pi^n + \cdots + a_1\pi + a_0,$$

é um polinômio em π com coeficientes em k e $a_n \neq 0$, então $v(f(\pi)) \leq n$, mais ainda, $f(\pi) \neq 0$. Assim, $k[\pi]$ é isomorfo ao anel dos polinômios $k[x]$ por um isomorfismo deixando k fixo e mandando π em x. Como $\widehat{\mathfrak{A}}$ é completo, este isomorfismo pode ser estendido a um isomorfismo de $\widehat{\mathfrak{A}}$ em $k[[x]]$. ∎

Observação 1.50. Como cada elemento de $k[[x]]$ é associado a uma série infinita, está claro que $k[[x]]$ é completo. De fato, a representação (1.7) pode sugerir que, a menos de isomorfismo, o único Anel de Valorização Discreta Completo com corpo residual k seja o anel $k[[x]]$, o que é um fato verdadeiro quando k tem característica zero (ver Corolário 1.49), mas se a característica de k não for zero isto não acontece. Como veremos na próxima seção.

1.8 Uma Construção de Z_p

Um fato interessante é que embora a série (1.7) pareça ser uma série de potências, ela não necessariamente soma e multiplica simplesmente como séries de potências, o exemplo seguinte ilustra bem isso.

Exemplo 1.51. Seja p um número primo. Defina a valorização v sobre o anel $\mathbb{Z}$ dos inteiros por $v(a) = n$, se p^n é a maior potência de p dividindo a. Se $v(a) = n, v(b) = m$, então claramente p^{n+m} é maior potência de p dividindo $a \cdot b$, portanto, vale (i) do Lema 1.4. Se $n < m$, então obviamente a maior potência de p dividindo $a + b$ é p^n, ao passo que se $n = m$, então p^n é possivelmente a maior potência de p que divide $a + b$, assim a propriedade (ii) do Lema 1.4 se verifica.

Já a propriedade (iii) do lema 1.4 não se verifica, assim devemos trabalhar em um anel de certa forma maior que $\mathbb{Z}$, ou seja, um anel que contenha $\mathbb{Z}$ e que seja Anel de Valorização. Vejamos então como será esse anel. Primeiramente, tomamos inteiros b tal que $v(b) = 0$ (ou seja, inteiros b tais que p não os divide) e assim o anel $\mathfrak{R}$ será constituído de todos os números racionais da forma a/b, onde p não divide b, definimos a valorização de tais números como sendo a valorização do numerador. E assim é obvio que se $v(a/b) = 0$ então a/b é uma unidade em $\mathfrak{R}$, isto é, a/b tem inverso em $\mathfrak{R}$, ou seja, a propriedade (iii) do Lema 1.4 é verificada. E concluímos então que $\mathfrak{R}$ é um Anel de Valorização Discreta, este será chamado de "anel dos racionais p-inteiros". Este anel tem um parâmetro uniformizador canônico, o primo p.

Fazendo alguns cálculos, podemos ver que

$$\mathfrak{R}_n = \mathbb{Z}/p^{n+1},$$

o anel dos inteiros módulo p^{n+1}. Como representantes de

$$k = \mathbb{Z}/p,$$

podemos, portanto, tomar os inteiros $0, 1, \ldots, p-1$. Assim, os elementos do completamento são representados pelas séries infinitas

$$a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots,$$

onde $0 \leq a_n < p, \forall n \in \mathbb{N}$. Este completamento denotaremos por $\mathbb{Z}_p$ e chamaremos de **anel dos inteiros p-ádicos**. Ele foi descoberto por K. Hensel no final do século dezenove. Como $\mathbb{Z} \subset \mathbb{Z}_p, \mathbb{Z}_p$ tem característica zero, enquanto que seu corpo residual $\mathbb{Z}/p = k$ tem característica p. Conseqüentemente, $\mathbb{Z}_p \ncong k[[x]]$. De fato, se tomarmos dois inteiros positivos ordenados e expressá-los por suas expansões(finitas) p-ádicas, está claro que não se somam e multiplicam as expansões como séries de potências formais.

Os resultados deste capítulo serão destacados no próximo Capítulo quando construírmos o anel dos vetores de Witt, denotado por $W(A)$, onde A é um anel comutativo com unidade. Posteriormente, definiremos $W(k)$, onde k é um corpo perfeito de característica $p > 0$ e, mostraremos que ele é um anel de valorização discreta completo.

Capítulo 2

O Anel dos Vetores de Witt e o Problema de Waring

Neste capítulo faremos uma construção do **Anel dos Vetores de Witt**, que é devida a Ernst Witt (1936). Este é um exemplo de anel de valorização discreta completo não ramificado. Faremos duas abordagens, na primeira exigiremos apenas que k seja um anel comutativo com unidade, depois trabalharemos com k como corpo perfeito de característica p. No final do capítulo, aplicaremos o problema de Waring para $W(k)$.

2.1 O Anel dos Vetores de Witt com Coeficientes em um Anel Comutativo com Unidade

Fixando um número primo p, para cada inteiro positivo n, escrevemos

$$\phi_n(\bar{x}) = \sum_{d|p^n} d x_{l(d)}^{p^n/d}, \text{ onde } l(d) = log_p d \text{ e } \bar{x} = (x_1, x_2, \dots).$$

Para simplificar a notação, usaremos $\phi_n = \phi_n(\bar{x})$.

Estes polinômios serão chamados as **componentes secundárias** de $\bar{x} = (x_1, x_2, \dots)$. A seqüência de componentes secundárias determina $\bar{x}$ unicamente, uma vez que podemos mostrar por indução que x_n é um polinômio com coeficientes racionais nas componentes secundárias. Escrevendo de uma forma melhor, temos

$$\phi_n(x_0, x_1, \ldots, x_n) = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n, \ \forall\ n \geq 0. \tag{2.1}$$

Note que $\phi_n(x_0, x_1, \ldots, x_n) = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n \in \mathbb{Z}[x_0, \ldots, x_n]$.

Observação 2.1. Temos as seguintes propriedades para ϕ_i :
(i) $\phi_0 = x_0$
(ii) Valem as seguintes fórmulas de recorrência:

$$\phi_{n+1}(x_0, \ldots, x_{n+1}) = x_0^{p^{n+1}} + px_1^{p^n} + \cdots + p^{n+1}x_{n+1} = x_0^{p^{n+1}} + p\phi_n(x_1, \ldots, x_{n+1}) \tag{2.2}$$

$$\phi_{n+1}(x_0, \ldots, x_{n+1}) = x_0^{p^{n+1}} + px_1^{p^n} + \cdots + p^{n+1}x_{n+1} = \phi_n(x_0^p, \ldots, x_n^p) + p^{n+1}x_{n+1} \tag{2.3}$$

No que segue, considere A um anel comutativo com unidade e $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$.

Proposição 2.2. *Sejam $s \in \mathbb{N}$, $n \in \mathbb{N}_0$ e $a_0, \ldots, a_n, b_0, \ldots, b_n \in A$. Se $a_i \equiv b_i\ (mod\, p^s A)$, para $i = 0, 1, 2, \ldots, n$, então*

$$\phi_i(a_0, \ldots, a_i) \equiv \phi_i(b_0, \ldots, b_i)\ (mod\, p^{s+i}A),\ i = 0, 1, \ldots, n.$$

Demonstração: Pelo Lema 1.35, para $t \in \{0, 1, \ldots, n\}$, temos que :

$$\begin{aligned}
a_0^{p^t} &\equiv b_0^{p^t}\ (\mathrm{mod}\, p^{s+t}A)\\
pa_1^{p^{t-1}} &\equiv pb_1^{p^{t-1}}\ (\mathrm{mod}\, p^{s+t}A)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
p^{t-1}a_{t-1}^p &\equiv p^{t-1}b_{t-1}^p\ (\mathrm{mod}\, p^{s+t}A)\\
p^t a_t &\equiv p^t b_t\ (\mathrm{mod}\, p^{s+t}A).
\end{aligned}$$

Somando ambos os lados, temos

$$\phi_t(a_0, \ldots, a_t) \equiv \phi_t(b_o, \ldots, b_t)\ (\mathrm{mod}\, p^{s+t}A).$$

■

Seja $A^{\mathbb{N}_0}$ o conjunto de todas as seqüências $\bar{x} = (x_n)_{n\in\mathbb{N}_0}$ com $x_n \in A$, para todo $n \in \mathbb{N}_0$. Usando a interpretação óbvia de $\phi_j(\bar{x})$, defina a aplicação,

$$\phi = \phi_A : A^{\mathbb{N}_0} \longrightarrow A^{\mathbb{N}_0},$$

por $\phi(\bar{x}) = (\phi_n(\bar{x}))_{n\in\mathbb{N}_0}$, ou seja,

$$\phi(x_0,\dots,x_n) = (\phi_0,\phi_1,\phi_2,\dots) = (x_0, x_0^p + px_1, x_0^{p^2} + px_1^p + p^2x_2,\dots).$$

E assim, podemos enunciar e provar a seguinte proposição.

Proposição 2.3. *Suponha que p não seja um divisor do zero em A e suponha que A tenha um endomorfismo σ, com $\sigma(a) \equiv a^p \ (mod\, pA)$, para todo $a \in A$. Então $\phi : A^{\mathbb{N}_0} \longrightarrow A^{\mathbb{N}_0}$ é injetiva, com imagem constituída pelas seqüências (b_n) para as quais :*

$$\sigma(b_n) \equiv b_{n+1} \ (mod\, p^{n+1}A), \ \textit{para todo } n \in \mathbb{N}_0. \tag{2.4}$$

Demonstração: A recorrência para ϕ_j mostra que $\bar{b} = \phi(\bar{a})$ se, e somente se, $b_0 = a_0$, e $b_n = \phi_{n-1}(a_0^p,\dots,a_{n-1}^p) + p^n a_n, \ \forall\ n \geq 1$, ou seja, $b_n = \phi_n(a_0,\dots,a_n)$.

Assim, se p não é divisor do zero em A, tomemos duas seqüências (x_n),(y_n) e suponhamos $\phi(x_n) = \phi(y_n)$. Assim, temos

$$\begin{array}{rcl} x_0 = y_0 & \Rightarrow & x_0^p = y_0^p \\ x_0^p + px_1 = y_0^p + py_1 & \Rightarrow & x_1 = y_1 \\ \vdots & & \vdots \\ \phi_n(x_0,\dots,x_n) = \phi_n(y_0,\dots,y_n) & \Rightarrow & x_n = y_n. \end{array}$$

Para provar a relação (2.4), sejam $\bar{a} \in A^{\mathbb{N}_0}$ e $\bar{b} = \phi(\bar{a})$. Como $\sigma(a_j) \equiv a_j^p \ (\mathrm{mod}\, pA)$, a Proposição 2.2 mostra que

$$\begin{aligned} &\sigma(b_{n-1}) = \sigma(\phi_{n-1}(a_0,\dots,a_{n-1})) = \phi_{n-1}(\sigma(a_0),\dots,\sigma(a_{n-1})) \\ &\sigma(b_{n-1}) \equiv \phi_{n-1}(a_0^p,\dots,a_{n-1}^p) \ (\mathrm{mod}\, p^nA). \end{aligned}$$

Como $p^n a \equiv 0 \ (\mathrm{mod}\, p^nA)$, a fórmula de recorrência (2.3) para ϕ_i mostra que

$$\sigma(b_{n-1}) \equiv \phi_n(a_0,\dots,a_n) \ (\mathrm{mod}\, p^nA),$$

ou seja,

$$\sigma(b_{n-1}) \equiv b_n \ (\mathrm{mod}\, p^nA).$$

■

De posse de todos estes resultados, podemos enunciar o teorema que é sem dúvida o

mais importante deste capítulo, pois ele nos dará a ferramenta para somarmos e multiplicarmos elementos do **Anel dos Vetores de Witt** que será definido mais a frente.

Teorema 2.4. *Considere o anel* $D = \mathbb{Z}[x_0, \ldots, x_n, \ldots, y_0, \ldots, y_n, \ldots]$ *de polinômios em várias variáveis enumeráveis, e escreva* $\bar{x} = (x_n), \bar{y} = (y_n)$ *elementos de* $D^{\mathbb{N}_0}$. *Suponha que* $f \in \mathbb{Z}[X, Y]$ *seja um polinômio em duas variáveis. Então existe uma única seqüência* $\bar{\psi}_f = ((\psi_f)_n)_{n\in\mathbb{N}_0} \in D^{\mathbb{N}_0}$, *tal que* $\phi_n(\bar{\psi}_f) \in D$ *e*

$$\phi_D(\bar{\psi}_f) = f(\phi_D(\bar{x}), \phi_D(\bar{y})),$$

isto é,

$$\phi_n((\psi_f)_0, \ldots, (\psi_f)_n) = f(\phi_n(\bar{x}), \phi_n(\bar{y})), \ \forall\ n \in \mathbb{N}_0.$$

Demonstração: Note primeiramente que p não é divisor de zero em D. Considere o endomorfismo $\sigma : D \longrightarrow D$ dado por:

$$\sigma(g(x_0, \ldots, x_n, \ldots, y_0, \ldots, y_n, \ldots)) = g(x_0^p, \ldots, x_n^p, \ldots, y_0^p, \ldots, y_n^p, \ldots),$$

ou seja, $\sigma(z) = z$, para $z \in \mathbb{Z}$ e $\sigma(x_j) = x_j^p$, $\sigma(y_j) = y_j^p$, para $j \in \mathbb{N}_0$. Assim $\sigma(a) \equiv a^p \pmod{pD}$ para todo $a \in D$, ou seja, estamos com as hipóteses da Proposição 2.3 satisfeitas para o anel D. Usando a fórmula de recorrência (2.3) de ϕ_n, obtemos

$$\sigma(f(\phi_n(\bar{x}), \phi_n(\bar{y})) = f(\phi_n(\bar{x}^p), \phi_n(\bar{y}^p)) \equiv f(\phi_{n+1}(\bar{x}), \phi_{n+1}(\bar{y})) \pmod{p^{n+1}D}.$$

Pela Proposição 2.3 temos $\sigma(b_n) \equiv b_{n+1} \pmod{p^{n+1}D}$, onde $b_n = \phi_n(\bar{a})$ ou $\bar{b} = \phi(\bar{a})$. Logo, para o caso acima, $b_n = f(\phi_n(\bar{x}), \phi_n(\bar{y}))$ e para ela existe uma única seqüência $\bar{\psi}_f = ((\psi_f)_n)_{n\in\mathbb{N}_0}$ tal que $\phi_n((\psi_f)_0, \ldots, (\psi_f)_n) = b_n$. ∎

Exemplo 2.5. Seja $f(X, Y) = X + Y$. Determine $(\psi_f)_0$ e $(\psi_f)_1$ tais que $\phi_1((\psi_f)_0, (\psi_f)_1) = f(\phi_1(x_0, x_1), \phi_1(y_0, y_1))$.

Solução: Sabemos que

$$\phi_0((\psi_f)_0) = (\psi_f)_0 = f(\phi_0(x_0), \phi_0(y_0)) = f(x_0, y_0) \Rightarrow (\psi_f)_0 = x_0 + y_0.$$

Procedendo da mesma forma e usando o resultado obtido acima, temos

$$\begin{aligned}
\phi_1((\psi_f)_0,(\psi_f)_1) &= ((\psi_f)_0)^p + p(\psi_f)_1 = f(\phi_1(x_0,x_1),\phi_1(y_0,y_1)) \\
p(\psi_f)_1 &= f(x_0^p + px_1, y_0^p + py_1) - (x_0+y_0)^p \\
(\psi_f)_1 &= x_1 + y_1 + \frac{x_0^p + y_0^p - (x_0+y_0)^p}{p} \\
(\psi_f)_1 &= x_1 + y_1 - \frac{1}{p}\sum_{i=1}^{p-1} \left(\begin{array}{c} p \\ i \end{array} \right) x_0^i y_0^{p-i}.
\end{aligned}$$

Analogamente, obtemos

$$(\psi_f)_2 = x_2 + y_2 + \frac{x_1^p + y_1^p - \left(x_1 + y_1 + \frac{x_0^p + y_0^p - (x_0+y_0)^p}{p}\right)^p}{p} + \frac{x_0^{p^2} + y_0^{p^2} - (x_0+y_0)^{p^2}}{p^2}.$$

Exemplo 2.6. Seja $f(X,Y) = XY$. Determine $(\psi_f)_0$ e $(\psi_f)_1$, tal que $\phi_1((\psi_f)_0,(\psi_f)_1) = f(\phi_1(x_0,x_1),\phi_1(y_0,y_1))$.

Solução: Sabemos que

$$\phi_0((\psi_f)_0) = (\psi_f)_0 = f(\phi_0(x_0,\phi_0(y_0)) = f(x_0,y_0) \Rightarrow (\psi_f)_0 = x_0y_0.$$

Procedendo da mesma forma e usando o resultado obtido acima, temos

$$\begin{aligned}
\phi_1((\psi_f)_0,(\psi_f)_1) &= ((\psi_f)_0)^p + p(\psi_f)_1 = f(\phi_1(x_0,x_1),\phi_1(y_0,y_1)) \\
p(\psi_f)_1 &= f(x_0^p + px_1, y_0^p + py_1) - (x_0y_0)^p \\
p(\psi_f)_1 &= (x_0y_0)^p + p(x_0^p y_1 + y_0^p x_1 + p(x_1y_1)) - (x_0y_0)^p \\
(\psi_f)_1 &= x_0^p y_1 + y_0^p x_1 + p(x_1y_1).
\end{aligned}$$

Analogamente, obtemos

$$\begin{aligned}
(\psi_f)_2 = x_0^{p^2} y_2 + y_0^{p^2} x_2 + (x_1y_1)^p + p(x_1^p y_2 + y_1^p x_2 + p(x_2y_2)) + \\
+ \frac{x_0^{p^2} y_1^p + y_0^{p^2} x_1^p - (x_0^p y_1 + y_0^p x_1 + p(x_1y_1))^p}{p}.
\end{aligned}$$

Observação 2.7. Note que todas as $(\psi_f)_i$'s encontradas, nos dois exemplos, possuem coeficientes inteiros, para todo $i \in \mathbb{N}_0$. Elas também nos dão as três primeiras coordenadas do vetor resultante da soma e multiplicação, respectivamente, de dois vetores no anel que definiremos abaixo.

Sejam $(S_0, \dots, S_n, \dots)$, $(P_0, \dots, P_n, \dots)$ e $(I_0, \dots, I_n, \dots)$ as seqüências de polinômios em $D = \mathbb{Z}[x_0, \dots, x_n, \dots, y_0, \dots, y_n, \dots]$ do Teorema 2.4, correspondentes a $f(X,Y) = X + Y$, $f(X,Y) = XY$ e $f(X,Y) = -X$, respectivamente. Definiremos o **Anel dos Vetores de Witt** abaixo, cuja soma, produto e inverso aditivo são dados pelas aplicações S_i's, P_i's e I_i's, respectivamente.

Definição 2.8. Para um anel comutativo com unidade A, os vetores de Witt com coeficientes em A, denotado por $W(A)$, é o conjunto $A^{\mathbb{N}_0}$ com as operações soma de Witt e multiplicação de Witt, ou seja, $W(A) = (A^{\mathbb{N}_0}, +, \cdot)$, dadas por

$$\begin{aligned} \bar{a} + \bar{b} &= (S_0(\bar{a}, \bar{b}), \dots, S_n(\bar{a}, \bar{b}), \dots) \\ \bar{a} \cdot \bar{b} &= (P_0(\bar{a}, \bar{b}), \dots, P_n(\bar{a}, \bar{b}), \dots). \end{aligned}$$

Obviamente, temos uma relação destes S_i's com os $\bar{S}_i$'s encontrados no Teorema 1.44 quando A for um corpo perfeito de característica p. Isso será provado, quando obtivermos a expansão p-ádica de um vetor de Witt nestas circunstâncias.

Pelo Teorema 2.4 valem as seguintes relações :

$$\begin{aligned} \phi_n(S_0(\bar{a}, \bar{b}), S_1(\bar{a}, \bar{b}), \dots, S_n(\bar{a}, \bar{b})) &= \phi_n(\bar{a}) + \phi_n(\bar{b}) \\ \phi_n(P_0(\bar{a}, \bar{b}), P_1(\bar{a}, \bar{b}), \dots, P_n(\bar{a}, \bar{b})) &= \phi_n(\bar{a}) \cdot \phi_n(\bar{a}). \end{aligned} \tag{2.5}$$

Vejamos como obter o vetor de Witt $-\bar{x}$.

Exemplo 2.9. Claramente temos $(-x)_0 = -x_0$. Seja $\bar{y} = -\bar{x}$. Sabemos que $y_0 = -x_0$. Como $\phi_1(\bar{y}) = -\phi_1(\bar{x})$, temos, usando (2.1),

$$(-x_0)^p + py_1 = -x_0^p - px_1.$$

Se p é ímpar, podemos cancelar $-x_0^p$ na equação acima, obtendo $y_1 = -x_1$. Se $p = 2$, entretanto, escrevemos

$$x_0^2 + 2y_1 = -x_0^2 - 2x_1 \Rightarrow y_1 = -x_0^2 - x_1.$$

Usando o fato que $-1 \equiv 1 \pmod 2$, obtemos finalmente

$$(-x)_1 = \begin{cases} -x_1 & , \ se\ p \neq 2 \\ x_1 + x_0^2 & , \ se\ p = 2 \end{cases} \tag{2.6}$$

De forma análoga, obtemos

$$(-x)_2 = \begin{cases} -x_2 & , \ se\ p \neq 2 \\ x_1x_0 + x_2 + x_1^2 + x_0^4 & , \ se\ p = 2 \end{cases} \tag{2.7}$$

De fato, temos que

$$(-x)_n = -x_n, \text{ para todo } n \in \mathbb{N}_0,$$

quando p é ímpar, mas para $p = 2$ a fórmula para $(-x)_n$ é mais complicada.

Para um vetor particular $x = (x_0, 0, \dots)$, podemos ver, usando as fórmulas (2.6), (2.7) e as que seguem delas, que

$$-x = (x_0, x_0^2, x_0^4, \dots, x_0^{2^n}, \dots),$$

obviamente, quando $p = 2$.

Observação 2.10. $W(A)$ é um anel comutativo com unidade, a saber $1 = (1, 0, \dots)$, o elemento neutro da soma é $0 = (0, 0, \dots)$ e o inverso aditivo foi encontrado no exemplo acima.

2.2 O Anel dos Vetores de Witt com Coeficientes em um Corpo Perfeito de Característica p

Considere k um corpo perfeito de característica p.

Definição 2.11. O anel $W(k)$ dos vetores de Witt com coeficientes em k, consiste de todos os vetores infinitos

$$\bar{x} = (x_0, x_1, \dots), \ x_i \in k, \ \forall\ i \in \mathbb{N}_0.$$

com as soma e multiplicação de Witt da Definição 2.8.

Observação 2.12. No desenvolvimento desta definição, usamos o Teorema 2.4 e a Observação 2.7, pois os coeficientes dos polinômios, dando a soma e a multiplicação, são significativos módulo p, somente porque eles são inteiros.

Observação 2.13. Uma propriedade dos polinômios de Witt que é importante para certas aplicações, é expressa pelas seguintes fórmulas :

$$\begin{aligned}&(i)\ S_n(\bar{x},\bar{y}) = x_n + y_n + M_n(x_0,\dots,x_{n-1};y_0,\dots,y_{n-1})\\ &(ii)\ P_n(\bar{x},\bar{y}) = x_0^{p^n}y_n + y_0^{p^n}x_n + N_n(x_0,\dots,x_{n-1};y_0,\dots,y_{n-1}),\end{aligned}$$

onde M_n e N_n são polinômios não envolvendo x_n e y_n (lembre-se que estamos analisando os coeficientes de S_n e P_n módulo p). Obviamente as relações (2.5) continuam valendo para estes S_n's e P_n's.

Definiremos agora dois importantes operadores sobre os vetores de Witt.

Definição 2.14. Se $\bar{x} = (x_0,\dots,x_n,\dots)$ é um vetor de Witt, definimos a aplicação $V : W(k) \longrightarrow W(k)$ por

$$V(\bar{x}) = (0, x_0,\dots,x_{n-1},\dots).$$

Definição 2.15. Se $\bar{x} = (x_0,\dots,x_n,\dots)$ é um vetor de Witt, definimos a aplicação $F : W(k) \longrightarrow W(k)$ por

$$F(\bar{x}) = (x_0^p,\dots,x_n^p,\dots).$$

Claramente temos $VF = FV$.

Usando as fórmulas de recorrências (2.2) e (2.3), obtemos

$$\begin{aligned}&\phi_n(V(\bar{x})) = p\phi_{n-1}(\bar{x})\\ &\phi_n(\bar{x}) = \phi_{n-1}(F(\bar{x})) + p^n x_n,\end{aligned} \tag{2.8}$$

para todo $n \geq 1$.

Proposição 2.16. *Seja k um corpo perfeito de característica p. Então o operador V é um endomorfismo aditivo de $W(k)$ e o operador F (Frobenius) é um automorfismo do anel $W(k)$. Além do mais,*

$$\boldsymbol{p}\bar{x} = \boldsymbol{p}(x_0,\dots,x_n,\dots) = V(F(\bar{x})) = (0, x_0^p,\dots,x_n^p,\dots),\ \textit{para todo } \bar{x} \in W(k).$$

Demonstração: A aplicação V é aditiva. De fato, tome $\bar{x}, \bar{y} \in W(k)$, assim temos

$$\begin{aligned}
&V(\bar{x}+\bar{y}) = V(S_0, S_1, \dots, S_n, \dots) = (0, S_0, S_1, \dots, S_{n-1}, \dots)\\
&V(\bar{x}) = (0, x_0, \dots, x_{n-1}, \dots) = \bar{a}\\
&V(\bar{y}) = (0, y_0, \dots, y_{n-1}, \dots) = \bar{b}\\
&\bar{a}+\bar{b} = (0, x_0+y_0, x_1+y_1 - \frac{1}{p}\sum_{i=1}^{p-1}\begin{pmatrix} p \\ i \end{pmatrix} x_0^i y_0^{p-i}, \dots)\\
&\bar{a}+\bar{b} = (0, S_0, S_1, \dots)
\end{aligned}$$

Conseqüentemente,

$$V(\bar{x}+\bar{y}) = V(\bar{x}) + V(\bar{y}).$$

Que F é multiplicativa e aditiva, segue do fato que os polinômios de Witt P têm coeficientes no corpo primo módulo p, daí eles satisfazem

$$P(x_0^p, \dots, x_n^p; y_0^p, \dots, y_n^p) = P(x_0, \dots, x_n; y_0, \dots, y_n)^p$$

A aplicação F é certamente bijetiva, pois por hipótese k é perfeito o que resulta no automorfismo $x \mapsto x^p$, concluindo que $k = k^p$ (ver Teorema 1.32).

Agora provaremos a parte final da proposição. Seja $\bar{y}$ o vetor obtido pela soma de Witt de $\bar{x}$ a si mesmo, p vezes.

Queremos mostrar que

$$y_n \equiv (V(F(\bar{x})))_n \pmod{p}, \text{ para todo } n \in \mathbb{N}_0,$$

ou seja, mostrar que o vetor de Witt $\bar{y}$ tem zero na primeira coordenada e x_n^p, $n \geq 0$, módulo p nas outras coordenadas. Por (2.5), temos

$$\phi_n(\bar{y}) = p\phi_n(\bar{x}), \text{ para todo } n \in \mathbb{N}_0.$$

Para $n = 0$, temos

$$y_0 = px_0 \Rightarrow y_0 \equiv 0 \pmod{p}.$$

Para $n \geq 1$, usando as identidades (2.8), obtemos

$$\begin{aligned} \phi_{n-1}(F(\bar{y})) + p^n y_n &= \phi_n(\bar{y}) \\ &= p\phi_n(\bar{x}) \\ &= \phi_{n+1}(V(\bar{x})) \\ &= \phi_n(F(V(\bar{x}))) + p^{n+1}(V(\bar{x}))_{n+1} \\ &= \phi_{n-1}(F(F(V(\bar{x})))) + p^n(F(V(\bar{x})))_n + p^{n+1}(V(\bar{x}))_{n+1}. \end{aligned} \tag{2.9}$$

Por hipótese de indução, temos

$$y_i \equiv (F(V(\bar{x})))_i \pmod{p}, \text{ para todo } i < n,$$

e elevando à p-ésima potência, obtemos pelo lema 1.35

$$(F(\bar{y}))_i \equiv (F(F(V(\bar{x}))))_i \pmod{p^2}, \text{ para todo } i < n.$$

Usando a Proposição 2.2, esta congruência resulta em

$$\phi_{n-1}(F(\bar{y})) \equiv \phi_{n-1}(F(F(V(\bar{x})))) \pmod{p^{n+1}}.$$

Substituindo isso na igualdade (2.9), temos

$$p^n y_n \equiv p^n(F(V(\bar{x})))_n \pmod{p^{n+1}},$$

e daí, dividindo por p^n, obtemos

$$y_n \equiv (F(V(\bar{x})))_n \pmod{p},$$

que é a congruência desejada. ∎

Corolário 2.17. *O anel $W(k)$ tem característica zero e seu anel residual módulo p é canonicamente isomorfo a k.*

Demonstração: Para cada $n \in \mathbb{N}$, temos

$$p^n(1,0,0,\dots) = (VF)^n(1,0,0,\dots) = (0,0,\dots,1,0,\dots),$$

onde $(VF)^n$ representa a aplicação (VF) aplicada n vezes. Obviamente, temos $p^n(1,0,0,\dots) \neq 0$. A Proposição 2.16 implica que o ideal gerado por p, consiste dos vetores $\bar{x}$ com

$x_0 = 0$, ou seja, $pW(k) = \{(0, x_0^p, x_1^p, \dots); x_i \in k\} = \{(0, x_1, x_2, \dots); x_i \in k\}$. A segunda igualdade pode ser escrita devido a k ser perfeito, pois podemos fazer a seguinte mudança de variáveis $x_i^p \to x_j$ e, sem perda de generalidade, fazemos $j = i + 1$.

Conseqüentemente, o anel residual módulo p é isomorfo a k pelo isomorfismo induzido do homomorfismo $\bar{x} \to x_0$, ou seja, $W(k)/I = \{x_0 + I; x_0 \in k\} \cong k$, onde $I = pW(k)$. Segue que $W(k)$ deve ter característica zero. ∎

Observações 2.18.
(*i*) Agora definiremos a valorização v sobre $W(k)$, por $v(\bar{x}) = n$, com a condição que $x_n \neq 0$, e $x_i = 0$, para todo $i < n$. Equivalentemente, $v(\bar{x}) = n$ fornecido de modo que $\bar{x} = up^n$, onde $p^n = p^n(1, 0, \dots)$ e $u_0 \neq 0$. O produto up^n é dado pelo produto de Witt da Definição 2.8. Já que p gera um ideal maximal em $W(k)$ (Corolário 2.17), u é uma unidade em $W(k)$. Segue que $W(k)$ é um ***anel de valorização discreta*** com valorização v. Como $p = 1 \cdot p$, com $p = p(1, 0, \dots)$ temos que $v(p) = 1$, ou seja, $W(k)$ é não ramificado.

(*ii*) O anel residual de $W(k)$ módulo p^n é canonicamente isomorfo ao anel $W_n(k)$, obtido por truncamento de todos os vetores de Witt após a n-ésima coordenada, ou seja, um vetor $a = (a_0, a_1, \dots, a_{n-1})$ pertence a $W_n(k)$, ($W_n(k) \cong W(k)/p^n$). Vemos que $W_1(k) \cong k$ e usando o mesmo raciocínio da Seção 1.3 do Capítulo 1, temos um isomorfismo canônico

$$W(k) \cong \varprojlim W_n(k), \tag{2.10}$$

e daí $W(k)$ é completo.

Podemos resumir nossos resultados, enunciando o seguinte teorema.

Teorema 2.19. *Seja k um corpo perfeito de característica p. Então $W(k)$ é um anel de valorização discreta completo não ramificado de característica zero, com corpo residual k.*

No Capítulo 1 vimos que a partir de um anel de valorização discreta completo $\widehat{\mathfrak{A}}$, facilmente encontramos $k = \widehat{\mathfrak{A}}/\pi\widehat{\mathfrak{A}}$. A pergunta que surge naturalmente é: se temos um corpo k, como obteremos um $\widehat{\mathfrak{A}}$ de modo que k seja seu corpo residual ? A resposta foi dada por Witt com a construção de $W(k)$, como vimos.

Para concluir nossa discussão, exibiremos a expansão p-ádica de um vetor de Witt e faremos um exemplo. Primeiramente, note que o representante multiplicativo $\{\alpha\}$ de

$\alpha \in k$ em $W(k)$ é o vetor de Witt $(\alpha, 0, \dots)$. Assim, usando o produto de Witt, temos

$$\begin{aligned}
\{\alpha\}\, p(1,0,\dots) &= (0, \alpha^p, 0, \dots) \\
\{\alpha\}\, p^2(1,0,\dots) &= (0,0,\alpha^{p^2}, 0, \dots) \\
\dots\dots\dots\dots\dots & \quad \dots\dots\dots\dots\dots \\
\{\alpha\}\, p^n(1,0,\dots) &= (0,0,\dots,\alpha^{p^n}, 0, \dots),
\end{aligned}$$

pela Proposição 2.16, e isto pode ser feito para qualquer $n \in \mathbb{N}$. Pode-se, então mostrar, usando a definição de soma de Witt, que a expansão p-ádica de um vetor de Witt $\bar{x} = (x_0, x_1, \dots)$ é dada por

$$\bar{x} = \sum_{n=0}^{\infty} \left\{ x_n^{p^{-n}} \right\} p^n,$$

onde p^n representa $p^n(1,0,\dots)$ e $\left\{ x_n^{p^{-n}} \right\} = (x_n^{p^{-n}}, 0, \dots)$.

Como $\bar{x} = \sum_{n=0}^{\infty} \left\{ x_n^{p^{-n}} \right\} p^n$ e $\bar{y} = \sum_{n=0}^{\infty} \left\{ y_n^{p^{-n}} \right\} p^n$, usaremos o Teorema 1.44 para obtermos $\bar{x} + \bar{y}$. Assim,

$$\begin{aligned}
\bar{S}_0(\bar{x}, \bar{y}) &= x_0 + y_0 \\
\bar{S}_1(\bar{x}, \bar{y}) &= x_1^{p^{-1}} + y_1^{p^{-1}} - \frac{1}{p} \sum_{l=1}^{p-1} \binom{p}{l} (x_0^{p^{-1}})^{p-l} (y_0^{p^{-1}})^{l}.
\end{aligned}$$

Quando escrevemos $\bar{x} + \bar{y}$ na forma vetorial, obtemos

$$\bar{x} + \bar{y} = (\bar{S}_0(\bar{x}, \bar{y}), \bar{S}_1(\bar{x}, \bar{y})^p, \dots, \bar{S}_n(\bar{x}, \bar{y})^{p^n}, \dots).$$

Mas os polinômios $\bar{S}_i$'s têm coeficientes no corpo primo módulo p. Logo

$$\bar{x} + \bar{y} = (\bar{S}_0(\bar{x}, \bar{y}), \bar{S}_1(\bar{x}^p, \bar{y}^p), \dots, \bar{S}_n(\bar{x}^{p^n}, \bar{y}^{p^n}), \dots).$$

Assim,

$$\begin{aligned}
\bar{S}_0(\bar{x}, \bar{y}) &= x_0 + y_0 \\
\bar{S}_1(\bar{x}^p, \bar{y}^p) &= x_1 + y_1 - \frac{1}{p} \sum_{l=1}^{p-1} \binom{p}{l} x_0^{p-l} y_0^{l} \\
&\vdots \\
\bar{S}_n(\bar{x}^{p^n}, \bar{y}^{p^n}) &= S_n(\bar{x}, \bar{y}).
\end{aligned}$$

Note que esta é a relação dos S_i's da Definição 2.8 com os $\bar{S}_i$'s do Teorema 1.44. Existe

também uma relação para os P_i's da Definição 2.8 com os $\bar{P}_i$'s do Teorema 1.44, como veremos a seguir.

Se $\bar{x} = \sum_{n=0}^{\infty} \left\{ x_n^{p^{-n}} \right\} p^n$ e $\bar{y} = \sum_{n=0}^{\infty} \left\{ y_n^{p^{-n}} \right\} p^n$, então usando o Teorema 1.44, temos

$$\bar{P}_0(\bar{x}, \bar{y}) = x_0 y_0 \text{ e } \bar{P}_1(\bar{x}, \bar{y}) = x_0 y_1^{p^{-1}} + x_1^{p^{-1}} y_0.$$

Assim a expansão p-ádica de $\bar{x}\bar{y}$ é

$$\bar{x}\bar{y} = \left\{ \bar{P}_0(\bar{x}, \bar{y}) \right\} + \left\{ \bar{P}_1(\bar{x}, \bar{y}) \right\} p + \cdots$$

e na forma vetorial, temos

$$\bar{x}\bar{y} = (\bar{P}_0(\bar{x}, \bar{y}), \bar{P}_1(\bar{x}, \bar{y})^p, \dots).$$

Usando o fato que os polinômios $\bar{P}_i$'s têm coeficientes no corpo primo módulo p, temos

$$\begin{aligned} \bar{P}_0(\bar{x}, \bar{y}) &= x_0 y_0 = P_0(\bar{x}, \bar{y}) \\ \bar{P}_1(\bar{x}^p, \bar{y}^p) &= x_0^p y_1 + y_0^p x_1 = P_1(\bar{x}, \bar{y}). \end{aligned}$$

De uma forma geral, temos

$$\bar{P}_n(\bar{x}^{p^n}, \bar{y}^{p^n}) = P_n(\bar{x}, \bar{y}).$$

2.2.1 Um Exemplo Ilustrativo

Agora veremos um exemplo para ilustrar toda a teoria até aqui definida.

Exemplo 2.20. Seja $k = \mathbb{F}_p$. Então $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ e, conseqüentemente,

$$W(\mathbb{F}_p) \cong \mathbb{Z}_p$$

o anel dos inteiros p-ádicos.

Solução: Seja $\bar{a} = (a_0, a_1, \dots, a_{n-1}) \in W_n(\mathbb{F}_p)$, $a_i \in \mathbb{F}_p$. Sabemos que o representante multiplicativo $\left\{ a_i^{p^{-i}} \right\}$ de $a_i \in \mathbb{F}_p$ em $W_n(\mathbb{F}_p)$ é o vetor de Witt $(a_i^{p^{-i}}, 0, \dots, 0)$ (isto é

possível porque $\mathbb{F}_p$ é perfeito de característica p). Logo

$$\begin{aligned}\left\{a_1^{p^{-1}}\right\} p(1,0,\dots) &= (0,a_1,0,\dots,0)\\ \left\{a_2^{p^{-2}}\right\} p^2(1,0,\dots) &= (0,0,a_2,0,\dots,0),\end{aligned}$$

pela Proposição 2.16. Assim, usando a soma de Witt, temos que a expansão p-ádica de um vetor $\bar{a} \in W_n(\mathbb{F}_p)$, é dada por

$$\bar{a} = \sum_{i=0}^{n-1} \left\{a_i^{p^{-i}}\right\} p^i.$$

Agora, considere a aplicação $f : W_n(\mathbb{F}_p) \longrightarrow \mathbb{F}_p$ de classe residual. Existe um único subconjunto $\bar{B} \subset W_n(\mathbb{F}_p)$ tal que $f|_{\bar{B}}$ é bijetiva. Note que $\bar{B}^*$ é o grupo de todas $(p-1)$-ésimas raízes da unidade em $\mathbb{Z}_p$, obtidas no Exemplo 1.42. Podemos tomar $\bar{B} = \{0, 1, \dots, p-1\}$. Agora, se considerarmos $\{\cdot\} : \mathbb{F}_p \longrightarrow W_n(\mathbb{F}_p)$ um sistema de representantes multiplicativos, pelo Teorema 1.40, temos

$$\begin{aligned}f(\{x\}) &= x, \text{ para todo } x \in \mathbb{F}_p\\ \{xy\} &= \{x\}\{y\}, \text{ para todos } x, y \in \mathbb{F}_p\\ \{\mathbb{F}_p\} &= \bar{B}.\end{aligned}$$

Assim, cada elemento $\bar{a}$ de $W_n(\mathbb{F}_p)$ pode ser escrito unicamente como

$$\bar{a} = \sum_{i=0}^{n-1} b_i p^i,$$

onde $b_i = \left\{a_i^{p^{-i}}\right\} \in \bar{B}$. E esse é um típico elemento de $\mathbb{Z}/p^n\mathbb{Z}$. Assim, temos um isomorfismo $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$, onde a soma e o produto são dados pelos $\bar{S}_i$'s e $\bar{P}_i$'s do Teorema 1.44. Logo, do Exemplo 1.28 e do isomorfismo (2.10) concluímos que,

$$W(\mathbb{F}_p) \cong \mathbb{Z}_p.$$

Observação 2.21. Poderíamos ter aplicado o Teorema 1.45 e ter concluído diretamente que $W(\mathbb{F}_p) \cong \mathbb{Z}_p$.

Começaremos uma seção onde discutiremos o problema de Waring para $W(k)$. Para $\mathbb{Z}_p$, o problema tem sido muito estudado, veja [2] e as referências que seguem.

2.3 Alguns Resultados para $W(k)$

Suponhamos que k é algébrico sobre $\mathbb{F}_p$. Pelas Observações 2.18, sabemos que $W(k)$ é um anel de valorização discreta completo não ramificado e assim este pode ser visto, a menos de isomorfismo, como a única extensão completa não ramificada de $\mathbb{Z}_p$, pelo Teorema 1.45.

Considere K o corpo de frações de $W(k)$, ou seja, $W(k) = \{a \in K; |a|_p \leq 1\}$. Assim, temos $\mathbb{Q}_p \subset K$, onde $\mathbb{Q}_p$ é o corpo de frações de $\mathbb{Z}_p$, chamado corpo dos números p-ádicos. Como $W(k)$ é não ramificado, temos que $[k : \mathbb{F}_p] = [K : \mathbb{Q}_p]$. Nesta seção, provaremos alguns resultados para $W(k)$ que serão muito importantes na aplicação do problema de Waring para este conjunto.

No Capítulo 1, enunciamos o Lema 1.41 (Lema de Hensel I) para um anel de valorização discreta completo $\widehat{\mathfrak{A}}$ qualquer. Agora, enunciaremos e o provaremos para $\widehat{\mathfrak{A}} = W(k)$, a prova do caso geral é essencialmente a mesma. Para diferenciar do caso geral, chamaremos este de Lema de Hensel II.

Lema 2.22 (Lema de Hensel II). *Considere o polinômio $f(x) \in W(k)[x]$ e suponha que existe $a_0 \in W(k)$ satisfazendo*

$$|f(a_0)| < |f^{'}(a_0)^2|, \tag{2.11}$$

onde $|\cdot| = |\cdot|_p$. Então existe $a \in W(k)$ tal que $f(a) = 0$.

Demonstração: Sejam $f_j(x)$ $(j = 1, 2, \dots)$ definidos de acordo com a expansão finita do polinômio $f(x)$ em $x + y$:

$$f(x + y) = f(x) + f_1(x)y + f_2(x)y^2 + \cdots \tag{2.12}$$

onde x, y são variáveis independentes. Então de (2.12) temos,

$$\lim_{y \to 0} \frac{f(x + y) - f(x)}{y} = f_1(x) = f^{'}(x). \tag{2.13}$$

Seja $b_0 = -f(a_0)f_1(a_0)^{-1}$. Segue de (2.11) e (2.13) que

$$|b_0| = |f(a_0)||f_1(a_0)|^{-1} < |f_1(a_0)|^2|f_1(a_0)|^{-1} = |f_1(a_0)| \leq 1. \tag{2.14}$$

Portanto $b_0 \in W(k)$ e satisfaz a igualdade

$$f(a_0) + b_0 f_1(a_0) = 0.$$

Calculando $f(a_0 + b_0)$ em (2.12) obtemos

$$f(a_0 + b_0) = f(a_0) + f_1(a_0)b_0 + f_2(a_0)b_0^2 + \cdots = f_2(a_0)b_0^2 + f_3(a_0)b_0^3 + \cdots$$

Por (ii) de (1.2) temos,

$$|f(a_0 + b_0)| \leq max|f_j(a_0)b_0^j| \ \ (j \geq 2).$$

Agora $f_j(a_0) \in W(k)$, portanto, $|f_j(a_0)| \leq 1$ e assim,

$$|f(a_0 + b_0)| \leq max|b_0|^j \leq |b_0^2| = \frac{|f(a_0)|^2}{|f_1(a_0)|^2}.$$

Utilizando (2.11) obtemos

$$|f(a_0 + b_0)| < |f(a_0)| \leq |f_1(a_0)|.$$

Podemos supor, assim como antes, que

$$f_1(x + y) = f_1(x) + f_{11}(x)y + f_{12}(x)y^2 + \cdots$$

onde $f_1(x), f_{1j}(x) \in W(k)[x]$, $(j \geq 1)$. Utilizando (2.11) e (2.14) concluímos que

$$|f_1(a_0 + b_0) - f_1(a_0)| \leq max|f_{ij}(a_0)b_0^j| \leq |b_0| < |f_1(a_0)|.$$

Portanto, temos a seguinte desigualdade:

$$|f_1(a_0 + b_0) - f_1(a_0)| < |f_1(a_0)|.$$

Da desigualdade anterior, obtemos

$$|f_1(a_0+b_0)| = |f_1(a_0+b_0)-f_1(a_0)+f_1(a_0)| = max\left\{|f_1(a_0 + b_0) - f_1(a_0)|, |f_1(a_0)|\right\} = |f_1(a_0)|,$$

ou seja, é válida a seguinte identidade

$$|f_1(a_0 + b_0)| = |f_1(a_0)|.$$

Fazendo $a_1 = a_0 + b_0$, temos

$$|f(a_1)| < |f(a_0| < |f_1(a_0)|^2 = |f_1(a_1)|^2 = |f^{'}(a_1)|^2,$$

ou ainda,

$$|f(a_1)| < |f^{'}(a_1)|^2.$$

Essa última desigualdade prova que a_1 satisfaz a condição (2.12). Repetindo o processo recursivamente obtemos uma seqüência $a_n = a_{n-1} + b_{n-1}$ tal que para todo $n \in \mathbb{N}$ têm-se

$$|f_1(a_n)| = |f_1(a_0)|,\ f(a_n) + b_n f_1(a_n) = 0,\ |f(a_{n+1})| \leq |b_n^2| = \frac{|f(a_n)|^2}{|f_1(a_n)|^2} = \frac{|f(a_n)|^2}{|f_1(a_0)|^2}.$$

Utilizando a condição (2.12) para a_n, temos

$$|f(a_n)| < |f_1(a_n|^2 = |f_1(a_0)|^2.$$

Portanto, $\dfrac{|f(a_n)|}{|f_1(a_0)|^2} < 1$ e assim

$$|f(a_{n+1})| < |f(a_n|, \text{ para todo } n \in \mathbb{N}_0.$$

Isso prova que a seqüência real $|f(a_n)|$ é decrescente. Como $0 \leq |f(a_n)| \leq 1$, temos que $|f(a_n)| \to 0$ em $\mathbb{R}$ e assim $f(a_n) \to 0$ em $W(k)$. Por outro lado, temos

$$|a_{n+1} - a_n| = |b_n| = \frac{|f(a_n)|}{|f_1(a_n)|} = \frac{|f(a_n)|}{|f_1(a_0)|} \to 0.$$

Portanto, $(a_n)_{n\geq 0}$ é uma seqüência de Cauchy e como $W(k)$ é completo existe $a \in W(k)$ tal que $a_n \to a$, o que implica em $f(a) = 0$. ∎

Lema 2.23. *Suponha que $F(T) = F(t_1, \ldots, t_s)$ é um polinômio em s variáveis com coeficientes em $W(k)$ e que $a \in W(k)^s$ satisfaça a desigualdade*

$$|F(a)| < \left|\frac{\partial F}{\partial t_i}(a)\right|^2, \text{ para algum } i \in \{1, \ldots, s\},$$

onde $|\cdot| = |\cdot|_p$. Então existe $a^* \in W(k)^s$ tal que $F(a^*) = 0$.

Demonstração: Suponha que $a = (a_1, \ldots, a_s)$ e considere $g_i(t) \in W(k)[t]$ definido por

$$g_i(t) = F(a_1, \ldots, a_{i-1}, t, a_{i+1}, \ldots, a_s).$$

Por hipótese, temos

$$|g_i(a_i)| < |g_i'(a_i)|^2.$$

Pelo lema anterior, concluímos que existe $a_i^* \in W(k)$ tal que $g_i(a_i^*) = 0$, ou seja, se $a^* = (a_1, \ldots, a_{i-1}, a_i^*, a_{i+1}, \ldots, a_s)$, então $F(a^*) = 0$. ∎

2.4 O Problema de Waring para $W(k)$

Definição 2.24. Seja $\mathfrak{R}$ um anel comutativo com unidade. Para um inteiro $n > 1$ definimos $g_{\mathfrak{R}}(n)$ como o menor inteiro s para o qual cada elemento de $\mathfrak{R}$ é a uma soma de s n-ésimas potências de elementos de $\mathfrak{R}$, se tal inteiro existir, ou ∞ caso contrário.

O problema de Waring para $\mathfrak{R}$ consiste em decidir se $g_{\mathfrak{R}}(n)$ é finito e estimá-lo, para todo $n \in \mathbb{N}$. No que segue, faremos uma análise deste problema em $W(k)$.

Teorema 2.25. *Seja $n \in \mathbb{N}$ tal que $n = p^t d$, com $mdc(p, d) = 1$. Se $a \equiv x_1^n + \cdots + x_s^n \, (mod\, p^{2t+1})$, $x_1, \ldots, x_s \in W(k)$ e algum x_i é uma unidade, então existem $y_1, \ldots, y_s \in W(k)$ com $a = y_1^n + \cdots + y_s^n$.*

Demonstração: Por hipótese, temos que $X = (x_1, \ldots, x_s) \in W(k)^s$ satisfaz $a \equiv x_1^n + \cdots + x_s^n (\mathrm{mod}\, p^{2t+1})$. Defina

$$F(T) = F(t_1, \ldots, t_s) = t_1^n + \cdots + t_{i-1}^n + t_i^n + t_{i+1}^n + \cdots + t_s^n - a.$$

Assim, temos $F(X) \equiv 0 \, (\mathrm{mod}\, p^{2t+1})$, onde $t_i = x_i$ é uma unidade em $W(k)$, ou seja, $x_i \in U(W(k))$. Logo $|F(X)|_p \leq \xi^{2t+1}$, onde $0 < \xi < 1$. Por outro lado, temos

$$\frac{\partial F}{\partial t_i}(X) = n x_i^{n-1} \Rightarrow \frac{\partial F}{\partial t_i}(X) \equiv 0 \, (\mathrm{mod}\, p^t) \Rightarrow \left|\frac{\partial F}{\partial t_i}(X)\right|_p^2 = \xi^{2t}.$$

Logo, temos $|F(X))|_p < \left|\dfrac{\partial F}{\partial t_i}(X)\right|_p^2$ e pelo Lema 2.23 existem $x_1, \ldots, x_i^*, \ldots, x_s \in W(k)$, tais que $F(x_1, \ldots, x_i^*, \ldots, x_s) = 0$, ou seja, $y_1^n + \cdots + y_i^n + \cdots + y_s^n = a$, onde $y_j = x_j$,

para todo $j \neq i$, e $y_i = x_i^*$. ∎

No que segue, vamos assumir n como no Teorema 2.25.

Corolário 2.26. *Se a é uma unidade, então para qualquer representação $a \equiv x_1^n + \cdots + x_s^n \,(mod\, p^{2t+1})$ algum x_i será uma unidade, e mais, cada unidade em $W(k)$ é a soma de, no máximo, $g_{W_l(k)}(n)$ n-ésimas potências, onde $W_l(k) = W(k)/p^l W(k)$ é o anel dos vetores truncados de Witt.*

Demonstração: Se a é uma unidade, então na representação $a \equiv x_1^n + \cdots + x_s^n (\mathrm{mod}\, p^{2t+1})$ algum dos x_i's será uma unidade. De fato, se nenhum dos x_i's for uma unidade então teremos que a não é uma unidade, ou seja, uma contradição. Assim, pelo Teorema 2.25 temos que existem $y_1, \ldots, y_s \in W(k)$ tais que $a = y_1^n + \cdots + y_s^n$ e, se olharmos para os y_i's em $W_l(k)$ vemos que a será escrito como s ou menos n-ésimas potências, ou seja, cada unidade de $W(k)$ é soma de, no máximo, $g_{W_l(k)}(n)$ n-ésimas potências. ∎

Corolário 2.27. *Se a não é uma unidade, então $a-1$ é uma unidade e é uma soma de, no máximo, $g_{W_l(k)}(n)$ n-ésimas potências.*

Demonstração: Seja $a \equiv x_1^n + \cdots + x_s^n (\mathrm{mod}\, p^{2t+1})$, onde $x_1, \ldots, x_s \in W(k)$, tal que a não seja uma unidade em $W(k)$. Suponhamos que $a-1$ não seja uma unidade em $W(k)$. Assim, $a - 1 \equiv x_1^n + \cdots + x_s^n - 1 \,(\mathrm{mod}\, p^{2t+1})$ e pelo menos um dos x_i's deve ser uma unidade para podermos cancelar o -1, de modo que, $\sum_{i=1}^{s} x_i^n$ é uma unidade, ou seja, uma contradição. Sendo $a-1$ uma unidade, então para qualquer representação $a - 1 \equiv y_1^n + \cdots + y_s^n \,(\mathrm{mod}\, p^{2t+1})$, o Teorema 2.25 nos garante a existência de $z_1, \ldots, z_s \in W(k)$ tais que $a - 1 = \sum_{i=1}^{s} z_i^n$. Agora, se olharmos para os z_i's em $W_l(k)$, temos que $a - 1 \equiv \sum_{i=1}^{s} z_i^n \,(\mathrm{mod}\, p^l)$, ou seja, $a-1$ é uma soma de, no máximo, $g_{W_l(k)}(n)$ n-ésimas potências. ∎

Definiremos uma importante função que nos ajudará a demonstrar alguns resultados. Esta idéia foi introduzida por Bovey para $\mathbb{Z}_p$(ver [2]).

Definição 2.28. O número $g_{W(k)}(n, r)$ é o menor inteiro s para o qual existem $x_1, \ldots, x_s \in W(k)$ com $v(x_1^n + \cdots + x_s^n) = r$, onde v é a valorização p-ádica em $W(k)$, $n \in \mathbb{N}$.

Observações 2.29.
(a) Obviamente, temos $g_{W(k)}(n, 0) = 1$.

(b) Nas hipóteses do Corolário 2.26, podemos obter, para cada $c \in U(W(k))$, $y_1, \ldots, y_h \in W(k)$ tais que $\sum_{i=1}^{h} y_i^n = cp^t$, com $h \leq g_{W(k)}(n,t)$.

Lema 2.30. *Se $n = p^t d$, com $mdc(p,d) = 1$, $r \leq t$ e $v(x_1^n + \cdots + x_s^n) = r$, então algum x_i é uma unidade em $W(k)$.*

Demonstração: Suponhamos que nenhum dos x_i's seja uma unidade, daí teríamos $r = v(x_1^n + \cdots + x_s^n) \geq n \geq p^t > t$, uma contradição, pois $r \leq t$. Assim, um dos x_i's é uma unidade em $W(k)$. ∎

Teorema 2.31. *Se $n = p^t d$, com $mdc(p,d) = 1$ então $g_{W_{t+1}(k)}(n) \leq g_k(n) \sum_{r=0}^{t} g_{W(k)}(n,r)$.*

Demonstração: O processo será feito por indução sobre t. Para o caso $t = 0$ temos que $g_{W(k)}(n,0) = 1$ e como $W_1(k) = k$ o resultado segue, pois teremos $g_k(n) \leq g_k(n)(g_{W(k)}(n,0))$. Para $t = 1$, queremos mostrar que $g_{W_2(k)}(n) \leq g_k(n)(g_{W(k)}(n,0) + g_{W(k)}(n,1))$, ou seja, $g_{W_2(k)}(n) \leq g_k(n)(1 + g_{W(k)}(n,1))$. Sendo assim, seja $a \in W_2(k)$. Sabemos que para $t = 0$, existem $x_1, \ldots, x_s \in W_2(k)$, $s \leq g_k(n)(g_{W(k)}(n,0))$ com $x_1^{n/p} + \cdots + x_s^{n/p} = a$, onde $n = pd$. Assim, como $(\sigma(x_i))^n \equiv x_i^{n/p} \pmod{p}$, onde σ é o automorfismo inverso de Frobenius de $W(k)$, obtemos $\sum_{i=1}^{s} (\sigma(x_i))^n = a - bp$, para algum $b \in W(k)$. Também, sendo $c \in U(W(k))$, pelo item (b) das Observações 2.29, temos que existem $y_1, \ldots, y_h \in W(k)$ tais que $\sum_{i=1}^{h} y_i^n = cp$, com $h \leq g_{W(k)}(n,1)$. Novamente, pelo caso $t = 0$, temos que existem $z_1, \ldots, z_v \in W(k)$ tais que $\sum_{i=1}^{v} z_i^n \equiv b/c \pmod{p}$, com $v \leq g_k(n)$, ou seja, $\sum_{i=1}^{v} z_i^n = b/c - pm$, $m \in W(k)$. Assim

$$\sum_{i=1}^{s} (\sigma(x_i))^n + \sum_{i=1}^{h} y_i^n \sum_{i=1}^{v} z_i^n = a - bp + cpb/c - cp^2 m,$$

ou seja,

$$\sum_{i=1}^{s} (\sigma(x_i))^n + \sum_{i=1}^{h} y_i^n \sum_{i=1}^{v} z_i^n \equiv a \pmod{p^2}.$$

Logo

$$s + hv \leq g_k(n)(g_{W(k)}(n,0) + g_{W(k)}(n,1)).$$

Agora vamos assumir $t > 0$. Se $a \in W_{t+1}(k)$, então pela hipótese de indução, existem $x_1, \ldots, x_s$ em $W_{t+1}(k)$, $s \leq g_k(n) \sum_{r=0}^{t-1} g_{W(k)}(n,r)$, com $x_1^{n/p} + \cdots + x_s^{n/p} = a$ e, como $(\sigma(x_i))^n \equiv x_i^{n/p} \pmod{p^t}$, onde σ é o automorfismo inverso de Frobenius de $W(k)$, obtemos $\sum_{i=1}^{s} (\sigma(x_i))^n = a - bp^t$, para algum $b \in W(k)$. Também, sendo $c \in U(W(k))$, pelo item (b) das Observações 2.29, temos que existem $y_1, \ldots, y_h \in W(k)$ tais que $\sum_{i=1}^{h} y_i^n = cp^t$, com $h \leq g_{W(k)}(n,t)$. Finalmente, pelo caso $t = 0$, existem $z_1, \ldots, z_v \in W(k)$ tais que $\sum_{i=1}^{v} z_i^n \equiv b/c \pmod{p}$, com $v \leq g_k(n)$, ou seja, $\sum_{i=1}^{v} z_i^n = b/c - pm$, $m \in W(k)$. Segue que

$$\sum_{i=1}^{s} (\sigma(x_i))^n + \sum_{i=1}^{h} y_i^n \sum_{i=1}^{v} z_i^n = a - bp^t + cp^t b/c + cp^{t+1} m,$$

ou seja,

$$\sum_{i=1}^{s} (\sigma(x_i))^n + \sum_{i=1}^{h} y_i^n \sum_{i=1}^{v} z_i^n \equiv a \pmod{p^{t+1}}.$$

Portanto,

$$s + hv \leq g_k(n) \sum_{r=0}^{t-1} g_{W(k)}(n,r) + g_k(n) g_{W(k)}(n,t) = g_k(n) \sum_{r=0}^{t} g_{W(k)}(n,r),$$

que é o desejado. ∎

Além do problema de Waring, existem outras aplicações para $W(k)$, como por exemplo no estudo de variedades algébricas sobre um corpo de característica positiva [10], na teoria de grupos algébricos comutativos [11], [12], e na teoria de grupos formais [13].

Uma outra aplicação seria em problemas clássicos como o de sistemas de formas aditivas com coeficientes em $W(k)$, o qual tem sido bastante estudado para $\mathbb{Z}_p$.

Para uma abordagem quando $W(k)$ é ramificado pode-se consultar [16].

Referências Bibliográficas

[1] E. Witt, *Zyklische Körper und Algebren der characteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassem-körper der charakteristik p*, J. Reine Angew. Math., 176 (1936) 126-140

[2] J. D. Bovey, *A note on Waring's problem in p-adic fields*, Acta Arith. 29 (1976) 343-351.

[3] J. F. Voloch, *On the p-adic Waring's problem*, Acta Arith. 90 (1999) 91-95

[4] A. Garcia and J. F. Voloch, *Fermat curves over finite fields*, J. Number Theory (1988) 345-356.

[5] I. Chowla, *On Waring's problem (mod p)*, Proc. Nat. Sci. India, A, 12 (1943) 195-220.

[6] M. M. Dodson, *On Waring's problem in p-adic fields*, Acta Arith. 22 (1973) 315-327.

[7] M. M. Dodson and A. Tietäväinen, *A note on Warig's problem in $GF[p]$*, Acta Arith. to appear.

[8] G. H. Hardy and J. E. Littlewood, *Some problems 'Partitio Numerorum' (IV): The singular series in Waring's problem and the value of the number $G(k)$*, Math. Zeitschr. 12 (1922) 161-188.

[9] Foutaine, preprint, available at `http://www.math.ku.dk/~kiming/lecture_notes/2000-fontaine/witt.pdf`.

[10] D. Mumford, *Lectures on curves on an algebraic surface*, Princeton Univ. Press (1966).

[11] J. P. Serre, *Groupes algébrique et corps des classes*, Hermann (1959).

[12] M. Demazure, P. Gabriel, *Groupes algébriques*, **1**, North-Holland (1971).

[13] J. Dieudonné, *Groupes de Lie et hyperalgébres de Lie sur un corps de charactéristique* $p > 0$ *VII*, Math. Ann., **134** (1957) 114-133.

[14] J. P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[15] J. W. S. Cassels, *Local Fields*, Cambridge University Press, 1986.

[16] M. J. Greenberg, *Lectures on Forms in Many Variables*, University of California, Santa Cruz, 1969.

[17] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966.

[18] S. Shokranian, M. Soares e H. Godinho, *Teoria dos Números*, Editora Universidade de Brasília, 2ª ed., 1999.

[19] O. Zariski and P. Samuel, *Commutative Algebra*, V. II, Springer-Verlag, 1960.

[20] M. D. Larsen and P. J. McCarthy, *Multiplicative Theory of Ideals*, Academic Press, New York and London, 1971.

[21] I. G. Macdonald and M. F. Atiyah, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, University of Oxford, 1969.

[22] P. J. McCarthy, *Algebraic Extensions of Fields*, Chelsea Publishing Company, New York, University of Kansas, 1976.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo