Universidade de Brasilia
Instituto de Ciencias Exatas
Departamento de Matemática

Somas Exponenciais e Resolução de Equações sobre Corpos Finitos

Vinicius Facó Ventura Vieira

Setembro de 2010

Agradecimentos

- Gostaria de agradecer primeiramente à minha familia, sempre presente e sempre fornecendo apoio mental, psicológico, financeiro e sentimental;
- Gostaria de agradecer ao meu Professor Orientador Hemar Godinho pela paciência e pela disponibilidade no desenvolvimento desse trabalho;
- Devo agradecimentos aos Professores Michael Knapp e Diego Marques por aceitarem participar da banca examinadora e pelas correções nessa Dissertação de Mestrado;
- Aos colegas Laura Lobato, Felipe Batista, Mayra Madeira e Luciana Ventura pelo fornecimento do material e da bibliografia necessários para o desenvolvimento desse trabalho;
- Aos colegas de estudos em Teoria Dos Números na UnB;
- Aos professores Marcelo Furtado, Pavel Zalesski, Carlos Carrion, Ary Medino, Nigel Pitt, Alexei Krassilnilkov pela minha formação na pós-graduação;
- Ao professor Lineu Neto por me introduzir no mundo da Teoria dos Números;
- Aos amigos Jaqueline Godoy, Vanessa Soares, Henrique Roscoe, Ismael Sobrinho, Paloma Baltoré pelas noites mal-dormidas e horas intermináveis de estudo, mas principalmente pelo companheirismo.

Resumo

Vamos fazer um estudo sobre somas exponenciais e vamos obter uma generalização do problema de Waring, tentando achar condições para que um determinado tipo de equação tenha solução em corpos finitos de tamanho $q = p^f$. Para isso, vamos expor primeiramente uma série de resultados básicos sobre corpos finitos e números $p-$ádicos, a fim de acharmos a solubilidade de nossas equações por meio do estudo de somas exponenciais.

Palavras-chave: somas exponenciais; corpos finitos; numeros $p-$ádicos; representantes de Teichmüller; peso em relação a p de um inteiro; problema de Waring .

Abstract

We are going to make a brief study on exponencial sums and we are also going to obtain a general case of Waring's problem, trying to find conditions so a special kind of equation has solution in a finite field of $q = p^f$ elements. For that, we will expose a series of basic results involving finite fields and $p-$adic numbers, intending to find the solvability of our equations using several results involving exponential sums.

Key Words: exponential sums; finite fields; $p-$adic numbers; Teichmüller representatives; $p-$weight degree; Waring's problem.

Índice

Introdução

Achar soluções para equações polinomiais é um problema que tem atraido a atenção de vários matemáticos há muitas décadas. Diversos resultados importantes nesse sentido já foram obtidos, mas, em geral, é extremamente difícil achar condições que garantem a solubilidade de uma equação polinomial. Algumas boas estimativas sobre o número de soluções de equações polinomiais, são dadas no caso de equações polinomiais diagonais.

Em 1935, C. Chevalley provou uma conjectura enunciada por E. Artin: se $F(X_1, \ldots, X_m)$ é um polinômio homogêneo de grau $d < m$ sobre um corpo finito $\mathbb{F}_q$ com $q = p^f$ elementos, então $F = 0$ tem uma solução não-trivial. Chevalley mostrou ainda que a conjectura também é válida quando substituimos a hipótese de homogeneidade de F pela hipótese mais fraca de que F apenas não tenha termo constante. Logo após, E. Warning, com as mesmas hipóteses, mostrou que a característica do corpo divide o número de zeros de F. Vários resultados mais precisos foram obtidos fazendo uma boa estimativa da valorização $p-$ádica da soma exponencial associada ao polinômio. Em 1964 ([2]), Ax desenvolveu uma técnica $p-$ádica que obteve resultados inéditos. Ele provou que se b é igual a $\lceil \frac{m}{d} \rceil - 1$, onde $\lceil a \rceil$ é o menor inteiro maior ou igual a a, então o número de soluções não-singulares de $F = 0$ é divisível por q^b. Esse resultado também foi obtido com uma boa estimativa da valorização $p-$ádica da soma exponencial associada a F.

O resultado de Ax foi posteriormente estendido, por ele mesmo, para um sistema de polinômios. Sejam

$$F_i(X_1, \ldots, X_m),$$

para $i = 1, \ldots, r$, uma coleção de polinômios sobre $\mathbb{F}_q$ de grau d_i respectivamente e seja

$$\lambda = \left\lceil \frac{m - \sum_{i=1}^{r} d_i}{\sum_{i=1}^{r} d_i} \right\rceil .$$

Assim o número de zeros do sistema de polinômios é divisível por q^λ. Em 1971 ([16]), N. Katz melhorou os resultados de Ax, mostrando que, sob as mesmas hipóteses, o número de zeros do sistema de polinômios é divisível por q^μ, onde

$$\mu = \left\lceil \frac{m - \sum_{i=1}^{r} d_i}{\max_{1 \leq i \leq r} \{d_i\}} \right\rceil .$$

Ambos os resultados de Ax e Katz foram obtidos por meio de uma estimativa da valorização $p-$ádica da soma exponencial associada aos polinômios.

Em 1946, Lászlo Rédei formulou a seguinte conjectura:

Conjectura de Rédei 1. *Seja p um primo, $\mathbb{F}_p$ o corpo com p elementos e $F \in \mathbb{F}_p[X_1, \ldots, X_n]$ um polinômio não constante com $gr(F) < rank(F)$, onde $rank(F) = \dim_V$ e V é o subespaço gerado pelas derivadas parciais de F. Então $F = 0$ tem solução.*

De fato, essa conjectura é falsa, mas existem infinitas famílias de polinômios que satisfazem tal conjectura, como foi mostrado em 1956 por Carlitz([3]):

Teorema de Carlitz 1. *Seja d um divisor de $p-1$ e $a_i \in \mathbb{F}_q^*$, para $i = 1, \ldots, d$. Se $G(X_1, \ldots, X_d)$ é um polinômio sobre $\mathbb{F}_q$ com $\partial(G) < d$, então a equação $a_1X_1^d + \cdots + a_dX_d^d + G(X_1, \ldots, X_d) = 0$ tem solução sobre $\mathbb{F}_q$.*

Recentemente, em 2006([8]), Felszeghy estendeu esse resultado mostrando que $a_1X_1^d + \cdots + a_nX_n^d + G(X_1, \ldots, X_n) = 0$ tem solução em $\mathbb{F}_q$ para $n \geq \left\lfloor \frac{p-1}{\lceil \frac{p-1}{d} \rceil} \right\rfloor$, quando $\partial(G) < d$. Nesse resultado, a condição de d ser um divisor de $p-1$ não é necessária.

Aqui, vamos também calcular a valorização $p-$ádica da soma exponencial associada ao polinômio como forma de obter uma estimativa do número soluções de $F = 0$, mas, em nossos estudos, o objetivo será melhorar o resultado de Carlitz acima, para então, acharmos as condições necessárias para estudarmos o problema de Waring.

O problema de Waring consiste em achar, para d fixo, o número mínimo de variáveis tal que a equação $X_1^d + \cdots + X_n^d = \beta$ tem solução para todo número natural β. Esse número mínimo de variáveis é chamado de Número de Waring associado a d. O problema de Waring já foi considerado para equações sobre corpos finitos e há várias estimativas para o número de Waring nesses casos, como as obtidas por S.V. Konyagin, I. Shporlinski e A. Winterhof([18, 19, 26]), muitas vezes obtidas como consequência de boas estimativas de valor absoluto das somas de Gauss([19, 13]).

Em nossos estudos vamos considerar a seguinte generalização do problema de Waring: Dado um polinômio $F(X)$ sobre $\mathbb{F}_q$, queremos achar o número mínimo de variáveis tal que

$$F(X_1) + \cdots + F(X_n) = \beta$$

tenha solução sobre $\mathbb{F}_q$ para todo $\beta \in \mathbb{F}_q$. O problema também pode ser considerado da seguinte forma: Dados polinômios $F_1(X_1), \ldots, F_n(X_n)$ sobre $\mathbb{F}_q$, queremos achar condições tais que todo $\beta \in \mathbb{F}_q$ possa ser escrito como

$$\beta = F_1(x_1) + \cdots + F_n(x_n),$$

onde $x_1, \ldots, x_n \in \mathbb{F}_q$.

Esse problema já foi estudado por Carlitz([4]) e por Cochrane([6]) para um corpo finito de tamanho primo. Carlitz provou que, dados polinômios $F_1(X_1), \ldots, F_n(X_n)$ sobre $\mathbb{F}_p$ de grau, respectivamente, $d_1, \ldots, d_n$, todo elemento $\beta \in \mathbb{F}_p$, forneceu

$$\sum_{i=1}^{n} \left\lceil \frac{p-1}{d_i} \right\rceil + t > p,$$

onde t é o número de polinômios que não são de grau $p-1$ nem da forma $\alpha(X_i - \beta)^{(1/2)(p-1)} + \lambda$.

Cochrane usou estimativas de somas exponenciais para mostrar que $F(X_1) + \cdots + F(X_n) = \beta$ tem solução para todo $\beta \in \mathbb{F}_|$, sempre que $\partial(F(X_1)) + \cdots + \partial(F(X_n)) \geq log(p)$, onde o valor absoluto da soma exponencial correspondente a cada $\partial(F(X_i))$ é menor ou igual a $p(1 - \partial(F(X_i)))$.

Nossos resultados vão se estender para $\mathbb{F}_q$, quando os dois resultados acima apenas se aplicam para $\mathbb{F}_p$. Nosso objetivo será achar condições para que $\beta \in \mathbb{F}_q$ possam ser escritos como

$$\beta = F_1(x_1) + \cdots + F_n(x_n),$$

assim provaremos o seguinte teorema, o qual fornecerá tais condições:

Teorema 1 (Castro,Rubio,Vega)**.** *Seja $d_i > 1$ um divisor de $p-1$, $a_i \in \mathbb{F}_q^*$ e $F_i(X) = a_i X_i^{d_i} + G_i(X_i)$ polinômios sobre $\mathbb{F}_q$ para $i = 1, \ldots, n$. Suponha que $\sum_{i=1}^{n} 1/d_i$ seja um inteiro. Se $\omega_p(G_i) < d_i$, então todo $\beta \in \mathbb{F}_q$ pode ser escrito como*

$$\beta = F_1(x_1) + \cdots + F_n(x_n),$$

para $x_1, \ldots, x_n \in \mathbb{F}_q$.

Capítulo 1

Corpos Finitos

Num primeiro momento, focaremos nossos estudos nos conceitos básicos sobre corpos finitos. Também daremos definições importantes para nosso estudo posterior, como conjugado e traço, por exemplo.

Nessa seção, iremos estudar também teoremas importantes e motivadores envolvendo corpos finitos e polinômios sobre corpos finitos, como o Teorema de Chevalley, por exemplo. Mas antes vamos começar relembrando a definição de uma extenção de um corpo.

1.1 Conceitos e Definições Básicas

Definição 1. *Seja $\mathbb{K}$ um corpo e $\mathbb{F}$ um subcorpo de $\mathbb{K}$, diremos que $\mathbb{K}$ é uma extensão de $\mathbb{F}$. Denotaremos o grau desta extensão como sendo $[\mathbb{K} : \mathbb{F}]$, onde o grau desta extensão será igual a dimensão de $\mathbb{K}$ sobre $\mathbb{F}$ como espaço vetorial.*

Seja p um primo inteiro e seja $\mathbf{I}$ o ideal gerado por p. Temos que $\mathbb{Z}/\mathbf{I}$ é um corpo e $\mathbb{Z}/\mathbf{I} = \{\ \overline{0}, \overline{1}, ..., \overline{p-1}\ \}$. Temos que $\mathbb{F}_p = \{0, 1, 2, ..., p-1\}$ com as operações de adição e multiplicação módulo p é um corpo isomorfo a $\mathbb{Z}/\mathbf{I}$.

Definição 2. *Seja $\boldsymbol{D}$ um domínio de integridade. Chamaremos de característica de $\boldsymbol{D}$ o menor $n \in \mathbb{N}$ tal que $nd = 0$, $\forall d \in \boldsymbol{D}$. Se tal n não existe diremos que a característica é zero. Denotaremos a característica de $\boldsymbol{D}$ como $char(\boldsymbol{D})$.*

Observe que, n não pertence a $\mathbf{D}$ necessariamente, pois definimos $nd = \underbrace{d + d + d + .. + d}_{n\ vezes}$.

Definição 3. *Seja $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ um polinômio. Chamaremos de $f'(x)$ a derivada formal de $f(x)$, que será definida por:*

$$f'(x) = a_1 + 2a_2x + ... + na_nx^{n-1}$$

.

Lema 1.1. *Seja $f(x)$ um polinômio. Temos que $f(x)$ tem raizes múltiplas se, e somente se, $f(x)$ e $f'(x)$ tem fator comum de grau maior ou igual a 1.*

Demonstração. Por um lado, se $f(x)$ tem raizes múltiplas, então, $f(x)$ pode ser escrito da forma $f(x) = (x-\alpha)^m g(x)$, onde α é uma raiz de $f(x)$ e $m \geq 1$. Portanto, temos que $f'(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x)$. Reciprocamente, suponha, por contradição, que $f(x)$ não tenha nenhuma raiz múltipla, ou seja, $f(x) = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ com $\alpha_i \neq \alpha_j$ se $i \neq j$ e $f'(\alpha_i) \neq 0$, $\forall i, j \in \{ 0, 1, 2, ..., n \}$, considerando que estamos fatorando $f(x)$ em seu corpo de decomposição. Logo

$$f'(x) = (x-\alpha_2)(x-\alpha_3)...(x-\alpha_n) + ... + (x-\alpha_1)(x-\alpha_2)...(x-\alpha_{n-1}),$$

o que é uma contradição, pois $f(x)$ e $f'(x)$ tem fator comum de grau maior ou igual a 1. □

1.2 Corpo Finito com $q = p^m$ elementos

Seja $\mathbb{F}_q$ o corpo finito com q elementos. Então existe p primo tal que $\mathbb{F}_p \subset \mathbb{F}_q$ e $[\mathbb{F}_q : \mathbb{F}_p\ ] = m$, $m \in \mathbb{N}$.

Lema 1.2. *Dadas as condições acima, temos que $q = p^m$*

Demonstração. Temos aqui um problema simples de análise combinatória. Basta observar que como o grau da extenção é igual a m, então a dimensão de $\mathbb{F}_q$ sobre $\mathbb{F}_p$ como espaço vetorial é igual a m por definição, logo uma base de $\mathbb{F}_q$ sobre $\mathbb{F}_p$ terá m elementos. Seja $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ tal base. Portanto os elementos de $\mathbb{F}_q$ são da forma

$$a_1\alpha_1 + a_2\alpha_2 + ... + a_m\alpha_m,$$

onde $a_i \in \mathbb{F}_p, \forall i = 1, 2, ..., m$. Portanto é possível gerar p^m elementos distintos, logo $p^m = q$. □

Lema 1.3. *$\mathbb{F}_q$ é o corpo de decomposição de $f(x) = x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. Temos que para todo elemento $a \in \mathbb{F}_q$ não-nulo, $a^q = a$, logo $a^{q-1} = 1$. Além disso, temos que $f'(x) = qx^{q-1} - 1 = -1$, pois $q \equiv 0 \pmod{p}$. Com isso, temos que as raizes de $f(x)$ são todas distintas, e existem no máximo $gr(f(x)) = q$ raizes, pois $f(x)$ e $f'(x)$ não tem fator em comum de grau maior ou igual a 1. Portanto $\mathbb{F}_q$ contem todas as raizes de $f(x)$. □

1.3 Conjugados

Agora vamos encaminhar nossos estudos no propósito de definir os conjugados de um elemento em $\mathbb{F}_{p^m}$ em relação a $\mathbb{F}_p$. Os conjugados terão sua importância para o estudo do

Traço de uma extensão , conceito que será utilizado em nossos estudos posteriormente. Mas primeiramente, analisaremos alguns teoremas e lemas que nos darão uma fundamentação suficiente para que o estudo sobre conjugados apareça naturalmente.

Teorema 1.4. *Sejam $\mathbb{F}_{p^m}$ e $\mathbb{F}_{p^n}$ dois corpos finitos de tamanho, p^m e p^n, respectivamente. Temos que $\mathbb{F}_{p^m}$ é subcorpo de $\mathbb{F}_{p^n}$ se, e somente se, $m|n$.*

Demonstração. Por uma lado, suponha que $\mathbb{F}_{p^m}$ é subcorpo de $\mathbb{F}_{p^n}$ e que $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = r$. Portanto, temos que:

$$p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^r = p^{mr} = (p^m)^r,$$

logo $m|n$. Reciprocamente, temos que, se $n = mr$, então

$$p^n - 1 = (p^m)^r - 1 = (p^m - 1)(p^{m(r-1)} + \cdots + p^m + 1)$$

$$\Rightarrow (p^n - 1) = (p^m - 1)t$$

$$\Rightarrow x^{p^n-1} - 1 = x^{(p^m-1)t} - 1 = (x^{p^m-1} - 1)(x^{(p^m-1)(t-1)} + \cdots + 1)$$

$$\Rightarrow x^{p^n} - x = (x^{p^m} - x)g(x)$$

portanto, todas as raizes de $x^{p^m} - x$ são também raizes de $x^{p^n} - x$, logo $\mathbb{F}_{p^m}$ é subcorpo de $\mathbb{F}_{p^n}$ □

Lema 1.5. *Seja $f(x)$ um polinômio sobre $\mathbb{F}_q$, irredutível de grau m. Então $f(x)$ divide $x^{q^n} - x$ se, e somente se, $m|n$.*

Demonstração. Por um lado, se $f(x)$ divide $x^{q^n} - x$, então, temos que $f(x)g(x) = x^{q^n} - x$, portanto se α é uma raiz de $f(x)$ então α também será raiz de $x^{q^n} - x$. Então temos que, $\alpha^{q^n} - \alpha = 0$. Todas as raizes de $f(x)$ são raizes de $x^{q^n} - x$, portanto, o corpo de decomposição de $f(x)$ é um subcorpo do corpo de decomposição de $x^{q^n} - x$, logo, pelo Teorema 1.4, temos que $m|n$. Reciprocamente, temos que se $m|n$, então, pelo Teorema 1.4, $\mathbb{F}_{q^m}$ é subcorpo de $\mathbb{F}_{q^n}$. Agora, seja α uma raiz de $f(x)$, logo, como $f(x)$ tem grau m, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Portanto, temos que, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Com isso, temos que $\mathbb{F}_q(\alpha)$ é subcorpo de $\mathbb{F}_{q^n}$, logo todas as raizes de $f(x)$ são raizes de $x^{q^n} - x$, logo $x^{q^n} - x = f(x)g(x)$. Portanto, $f(x)|x^{q^n} - x$. □

Nesse próximo teorema, veremos pela primeira vez os conjugados de α, o que significa que estamos completando praticamente toda a base necessária para a introdução da definição do que serão os conjugados.

Teorema 1.6. *Seja $f(x)$ um polinômio irredutível de grau m com coeficientes em $\mathbb{F}_q$ e $\alpha \in \mathbb{F}_{q^m}$ uma raiz de $f(x)$. Então todas as raizes de $f(x)$ são dadas por:*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

e tais raizes são duas a duas distintas.

Demonstração. Vamos escrever $f(x)$ da seguinte forma:

$$f(x) = a_0 + a_1x + \cdots + a_mx^m$$

com isso temos que para $x = \alpha^q$, $f(x)$ será igual a:

$$f(\alpha^q) = a_m(\alpha^q)^m + \cdots + a_1\alpha^q + a_0,$$

mas como $a_i \in \mathbb{F}_q$, para todo $i \in \{0, 1, \ldots, m\}$, então temos que ${a_1}^q = a_1$, logo:

$$\begin{aligned} f(\alpha^q) &= {a_m}^q(\alpha^q)^m + \cdots + {a_0}^q \\ &= (a_m\alpha^m + \cdots + a_1\alpha + a_0)^q \\ &= (f(\alpha))^q \\ &= 0, \end{aligned}$$

pois α é raiz de $f(x)$. Repetindo o mesmo processo feito para α^q para $\alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$, verificamos que todos são raizes de $f(x)$, como $\alpha^{q^m} = \alpha$, então temos m raizes. Basta, agora, mostrar que são distintas. Suponhamos, por contradição, que não são distintas, logo para algum j e r, tais que $0 \leq j, r \leq m-1$, temos que:

$$\begin{aligned} \alpha^{q^j} &= \alpha^{q^r} \\ \Rightarrow (\alpha^{q^j})^{q^{m-r}} &= (\alpha^{q^r})^{q^{m-r}} \\ \Rightarrow \alpha^{q^{m-r+j}} &= \alpha^{q^m} = \alpha \end{aligned}$$

e $m - r + j \leq m - 1 < m$, o que é um absurdo, pois, pelo lema anterior, $m | m - r + j$. Portanto, $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ são m raizes distintas duas a duas. □

Corolário 1.7. *Sejam $f(x)$ e $g(x)$ dois polinômios irredutíveis de grau m com coeficientes em $\mathbb{F}_q[x]$, então $f(x)$ e $g(x)$ possuem o mesmo corpo de decomposição.*

Agora, já temos um embasamento suficiente para definirmos o que vem a ser um conjugado.

Definição 4. *Seja $\alpha \in \mathbb{F}_{q^n}$. Os conjugados de α em relação a $\mathbb{F}_q$ são :*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$$

Exemplo 1. *Seja $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ e $\alpha \in \mathbb{F}_{16}$ raiz de $f(x)$*

- *os conjugados de α em relação a $\mathbb{F}_2$ são: $\alpha, \alpha^2, \alpha^4, \alpha^8$.*
- *os conjugados de α em relação a $\mathbb{F}_4$ são: α, α^4*

Observe que, uma vez que os automorfismos de $\mathbb{F}_{q^m}$ que fixam $\mathbb{F}_q$ são $\sigma_1, \sigma_2, \ldots, \sigma_{m-1}$ onde $\sigma_j(\alpha) = \alpha^{q^j}, \forall \alpha \in \mathbb{F}_{q^m}, j = 1, 2, \ldots, m-1$, então podemos definir os conjugados de α em relação a $\mathbb{F}_q$ como os automorfismos de $\mathbb{F}_{q^m}$ que fixam $\mathbb{F}_q$. De forma análoga, podemos efetuar isso para qualquer extensão finita de corpos. Ou seja, dada uma extensão finita $\mathbb{K} \subset \mathbb{K}(\alpha)$, temos que os conjugados de α em relação a $\mathbb{K}$ serão os automorfismos de $\mathbb{K}(\alpha)$ que fixam $\mathbb{K}$. Esta definição será muito importante no futuro, quando iremos tratar de extensões finitas do corpo dos número racionais $p-$ádicos $\mathbb{Q}_p$.

Seja $f(x) \in \mathbb{F}_q[x]$ o polinômio minimal de $\alpha \in \mathbb{F}_{q^m}$ e $d = gr(f(x))$. Se $d = m$, então os conjugados de α em relação a $\mathbb{F}_q$ são distintos. Se $d < m$ então $d|m$ e $\alpha \in \mathbb{F}_{q^d}$. Neste caso, $\alpha^{q^d} = \alpha$, e assim a lista de conjugados tem a seguinte forma:

$$\underbrace{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}}_{d}, \underbrace{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}}_{d}, \ldots, \underbrace{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}}_{d},$$

ou seja, existem t blocos iguais, onde $m = dt$.

Definição 5. *Seja $f(x) \in \mathbb{K}[x]$ o polinômio minimal de $\alpha \in \mathbb{F}$, onde $gr(f(x)) = d$. Então $d|m$, onde $m = [\mathbb{K} : \mathbb{F}]$. Chamaremos de polinômio característico de α o polinõmio $g(x) = f(x)^{\frac{m}{d}}$. Temos que $g(x) \in \mathbb{K}[x]$.*

Logo, as raizes de $g(x)$ são todos os conjugados de α em relação a $\mathbb{F}_q$. Então:

$$\begin{aligned} g(x) &= (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{m-1}}) \\ &= x^m + a_{m-1}x^{m-1} + \cdots + a_0, \end{aligned}$$

como $g(x) \in \mathbb{K}[x]$, então

$$a_{m-1} = (-1)(\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}),$$

também está em $\mathbb{K}$. Considerando, $\mathbb{K}$ como sendo $\mathbb{F}_{q^m}$, então podemos afirmar que a soma dos conjugados de α em relação a $\mathbb{F}_q$ está em $\mathbb{F}_q$.

1.4 Traço e Norma e suas propriedades

Nessa seção, usaremos o conceito da seção anterior, onde foram definidos os conjugados de um elemento $\alpha \in \mathbb{F}_{q^m}$, para definirmos o que vem a ser traço e norma traço desse mesmo elemento. Racapitulando, temos que, se $p(x) \in \mathbb{F}_q[x]$ é o polinômio minimal de α, então nós definimos $g(x) = p(x)^{\frac{m}{d}}$ como sendo o polinômio característico de α, e também vimos que $g(x) \in \mathbb{F}_q[x]$ e que as raizes de $g(x)$ são os conjugados de α em relação a $\mathbb{F}_q$. Agora, iremos definir formalmente o que é o traço de α.

Definição 6. *Seja $\alpha \in \mathbb{F}_{q^m}$ e $\alpha_j = \alpha^{q^j}, j = 0, 1, \ldots, m-1$, os conjugados de α sobre $\mathbb{F}_q$, então definimos o traço de α a ser a soma desses cojugados, ou seja,*

$$Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) = \sum_{j=0}^{m-1} \alpha_i$$

Lema 1.8. *Seja $\alpha \in \mathbb{F}_{q^m}$, $\alpha_j = \alpha^{q^j}, j = 0, 1, \ldots, m-1$, os conjugados de α sobre $\mathbb{F}_q$ e $g(x)$ o polinômio característico de α. Logo temos que:*

$$Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) = \sum_{j=0}^{m-1} \alpha_i \in \mathbb{F}_q$$

Demonstração. Ja vimos, na seção anterior que $g(x) \in \mathbb{F}_q[x]$, ou seja, $g(x)$ tem coeficientes em $\mathbb{F}_q$. Sabemos também que

$$g(x) = \prod_{j=0}^{m-1} (x - \alpha_j)$$

e que, portanto:

$$g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$$

$$\Rightarrow (-1)a_{m-1} = \sum_{j=0}^{m-1} \alpha_i \in \mathbb{F}_q = Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha)$$

, como a_{m-1} é coeficiente de $g(x)$, então $a_{m-1} \in \mathbb{F}_q$. Portanto,

$$Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$$

□

Vamos estudar agora algumas propriedades importantes do traço:

Teorema 1.9. *Sejam $\alpha, \beta \in \mathbb{F}_{q^m}$, $c \in \mathbb{F}_q$, $\alpha_j = \alpha^{q^j}, j = 0, 1, \ldots, m-1$ e $\beta_j = \beta^{q^j}, j = 0, 1, \ldots, m-1$, os conjugados de α e β, respectivamente. Então temos que:*

1. $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha + \beta) = Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\beta)$
2. $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(c\alpha) = cTr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha)$
3. $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(c) = mc$
4. $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha^q) = Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha)$

Demonstração. 1.

$$Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha + \beta) = \sum_{j=0}^{m-1} (\alpha_j + \beta_j)$$

$$= \sum_{j=0}^{m-1} \alpha_j + \sum_{j=0}^{m-1} \beta_j$$

$$= Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\beta)$$

2.
$$Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(c\alpha) = \sum_{j=0}^{m-1} c\alpha_j$$
$$= c\sum_{j=0}^{m-1} \alpha_j = cTr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha)$$

3.
$$Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(c) = \sum_{j=0}^{m-1} c$$
$$= c\sum_{j=0}^{m-1} 1 = cm$$

4. Aqui, basta observar que os conjugados de α^q são $(\alpha^q), (\alpha^q)^q, \ldots, (\alpha^q)^{q^{m-1}}$, mas temos que $(\alpha^q)^{q^{m-1}} = \alpha^{q^m} = \alpha$, portanto os conjugados de α^q e α são os mesmos, donde
$$Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha^q) = Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha)$$

□

Teorema 1.10. *Seja $\alpha \in \mathbb{F}_{q^m}$. Então $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) = 0$ se, e somente se, existe $\beta \in \mathbb{F}_{q^m}$ tal que $\alpha = \beta^q - \beta$*

Demonstração. Por um lado, temos que se $\alpha = \beta^q - \beta$, então
$$Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\beta^q - \beta)$$
$$= Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\beta^q) - Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\beta) = Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\beta) - Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\beta) = 0$$
Portanto $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) = 0$ Reciprocamente, considere o polinômio $f(x) = x^q - x - \alpha \in \mathbb{F}_{q^m}[x]$ e β uma raiz de $f(x)$. Portanto:
$$0 = Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\beta^q - \beta)$$
$$= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{m-1}}$$
$$= \beta^q - \beta + \beta^{q^2} - \beta^q + \cdots + \beta^{q^m} - \beta^{q^{m-1}}$$
$$= \beta^{q^m} - \beta = 0$$
$$\Rightarrow \beta \in \mathbb{F}_{q^m}$$

□

Agora, vamos definir o que vem a ser a norma de $\alpha \in \mathbb{F}_{q^m}$.

Definição 7. *Sejam $\alpha \in \mathbb{F}_{q^m}$, os conjugados de α em relação a $\mathbb{F}_q$ e $\alpha_i = \alpha^{q^i}, i = 0, 1, \ldots, m-1$. Assim, temos que a norma de $\alpha \in \mathbb{F}_{q^m}$ será definida por:*

$$N(\alpha) = \prod_{i=0}^{m-1} \alpha_i.$$

Lema 1.11. $N(\alpha) \in \mathbb{F}_q$

Demonstração. Seja $g(x)$ o polinômio característico de α, portanto, temos que:

$$g(x) = (x-\alpha)\cdots(x-\alpha^{q^{m-1}})$$

$$= x^m + a_{m-1}x^{m-1} + \cdots + a_0$$

. Como

$$N(\alpha) = \prod_{i=0}^{m-1} \alpha_i = (-1)^m a_0$$

, então

$$N(\alpha) \in \mathbb{F}_q.$$

□

Agora, vamos estudar algumas propriedades da norma de α:

Teorema 1.12. *Sejam $\alpha, \beta \in \mathbb{F}_{q^m}$. Temos que:*

1. $N(\alpha\beta) = N(\alpha)N(\beta)$
2. $N(c) = c^m, \forall c \in \mathbb{F}_q$
3. $N(\alpha^q) = N(\alpha)$

Demonstração. 1. $N(\alpha\beta) = \prod_{i=0}^{m-1} (\alpha\beta)^{q^i} = \prod_{i=0}^{m-1} \alpha^{q^i}\beta^{q^i} = \left[\prod_{i=0}^{m-1} \alpha^{q^i}\right]\left[\prod_{i=0}^{m-1} \beta^{q^i}\right] = N(\alpha)N(\beta)$

2. $N(c) = \prod_{i=0}^{m-1} c^{q^i} = \prod_{i=0}^{m-1} c = c^m$

3. $N(\alpha^q) = \prod_{i=0}^{m-1} (\alpha^q)^{q^i} = \prod_{i=0}^{m-1} \alpha^{q^{i+1}} = \prod_{i=1}^{m} \alpha^{q^i} = \prod_{i=0}^{m-1} \alpha^{q^i}$, pois $\alpha^q = \alpha^{q^m}$.

□

1.5 Aplicações em Corpos Finitos

Agora, vamos direcionar nossos estudos para aplicações importantes envolvendo corpos finitos e resolução de polinômios sobre tais corpos. Vamos enumerar resultados historicamente importantes(como os Teoremas de Chevalley, por exemplo) e que vão ajudar no direcionamento dos nossos estudos para o objetivo principal desta dissertação. A partir deste momento, já podemos notar um relação direta com os teoremas presentes nas conclusões posteriores. Num primeiro momento, vamos estabelecer alguns embasamentos para as demonstrações dos teoremas.

Lema 1.13. *Seja $k \in \mathbb{N}$ e $c \in \mathbb{F}_q$. Então,*

$$\sum_{c \in \mathbb{F}_q} c^k = \begin{cases} -1 & se \quad k \equiv 0(mod(q-1)) \\ 0 & c.c \end{cases}$$

Demonstração. Seja $\beta \in \mathbb{F}_q^*$, tal que $\mathbb{F}_q^* =< \beta >$ então:

$$\sum_{c \in \mathbb{F}_q} c^k = \sum_{j=0}^{q-2} (\beta^j)^k = \sum_{j=0}^{q-2} (\beta^k)^j$$

$$= \frac{(\beta^k)^{q-1} - 1}{\beta^k - 1}$$

se $\beta^k \neq 1$.

- **Caso 1**: Se $k \equiv 0(mod(q-1))$ então $\beta^k = 1$ e

$$\sum_{j=0}^{q-2} (\beta^k)^j = \sum_{j=0}^{q-2} 1 = q - 1 = -1$$

- **Caso 2**:

$$\sum_{j=0}^{q-2} (\beta^k)^j = \frac{(\beta^{q-1})^k - 1}{\beta^k - 1} = 0$$

□

Lema 1.14. *Seja $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ com $gr(f(x_1, x_2, \ldots, x_n)) < n(q-1)$. Então*

$$\sum_{c_1, c_2, \ldots, c_n \in \mathbb{F}_q} f(c_1, \ldots, c_n) = 0$$

Demonstração.

$$\sum_{c_1, c_2, \ldots, c_n \in \mathbb{F}_q} c_1^{k_1} c_2^{k_2} \cdots c_n^{k_n} = \sum_{c_1 \in \mathbb{F}_q} c_1^{k_1} \sum_{c_2 \in \mathbb{F}_q} c_2^{k_2} \cdots \sum_{c_n \in \mathbb{F}_q} c_n^{k_n}$$

, portanto, existe um $k_j < q-1$, onde $j \in \{1, 2, \ldots, n\}$, tal que $q-1$ não divide k_j, logo, pelo lema 1.13,

$$\sum_{c_j \in \mathbb{F}_q} c_j^{k_j} = 0$$

$$\Rightarrow \sum_{c_1, c_2, \ldots, c_n \in \mathbb{F}_q} f(c_1, c_2, \ldots, c_n) = 0$$

□

Teorema 1.15 (Warning)**.** *Seja $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ de grau menor que n. Então o número de soluções de $f(x_1, \ldots, x_n) = 0$ em $\mathbb{F}_q$ é divisível pela característica de $\mathbb{F}_q$.*

Demonstração. Seja o seguinte polinômio $F(x_1, \ldots, x_n) = 1 - f(x_1, \ldots, x_n)^{q-1}$, o qual tem grau menor que $n(q-1)$.

$$F(c_1, \ldots, c_n) = \begin{cases} 0 & \text{se} \quad f(c_1, \ldots, c_n) \neq 0 \\ 1 & \qquad\qquad c.c \end{cases}$$

$$\Rightarrow \sum_{c_1, \ldots, c_n \in \mathbb{F}_q} F(c_1, \ldots, c_n) = N$$

, onde N é o número de soluções de $f(c_1, \ldots, c_n) = 0$ em $\mathbb{F}_q$. Mas, pelo lema 1.14, temos que

$$\sum_{c_1, \ldots, c_n \in \mathbb{F}_q} F(c_1, \ldots, c_n) = 0$$

$$\overset{(N \in \mathbb{N})}{\Rightarrow} N = 0$$

em $\mathbb{F}_q$

$$\Rightarrow N \equiv 0 (mod(char(\mathbb{F}_q)))$$

□

Agora, temos o seguinte Teorema, também muito importante e que é uma consequência do anterior:

Teorema 1.16 (Chevalley)**.** *Seja $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ de grau menor que n e $f(0, \ldots, 0) = 0$, então existe $(c_1, \ldots, c_n) \in \mathbb{F}_q^n \backslash \{\vec{0}\}$ tal que $f(c_1, \ldots, c_n) = 0$.*

Os dois próximos teoremas são generalizações dos dois teoremas anteriores para o caso de $R \in \mathbb{N}$ polinômios.

Teorema 1.17 (Warning)**.** *Sejam $f_1, f_2, \ldots, f_R \in \mathbb{F}_q[x_1, \ldots, x_n]$ com $\sum_{j=0}^{R} gr(f_j) < n$, então o número de soluções do sistema $f_1 = f_2 = \cdots = f_R = 0$ em $\mathbb{F}_q$ é divisível pela característica de $\mathbb{F}_q$.*

Demonstração. Considere $F = (1 - f_1^{q-1}) \cdots (1 - f_R^{q-1})$, temos que:

$$F(c_1, \ldots, c_n) = \begin{cases} 1 & \text{se} \quad f(c_1, \ldots, c_n) = 0 \ \forall \ j = 1, 2, \ldots, R \\ 0 & \qquad\qquad c.c \end{cases}$$

O resto da demonstração é completamente análoga à versão com $R = 1$. □

Teorema 1.18 (Chevalley)**.** *Sejam $f_1, f_2, \ldots, f_R \in \mathbb{F}_q[x_1, \ldots, x_n]$ com $\sum_{j=0}^{R} gr(f_j) < n$. Se $f_j(0, 0, \ldots, 0) = 0, \forall j = 1, \ldots, R$, então existe uma solução não-trivial para o sistema.*

Capítulo 2

Números P-ádicos

Nessa seção vamos expor alguns fatos importantes para o desenvolvimento de nossos estudos sobre números p-ádicos, como as extensões de $\mathbb{Q}_p$ e o grau da classe residual, a valorização de um número racional e o valor absoluto $p-$ádico. Também estudaremos várias consequências importantes, como o peso de um número inteiro e os representantes de Teichmüller.

2.1 Valor Absoluto e Valorização

Nessa seção, iremos começar a direcionar os nossos estudos para a formalização de vários aspectos vistos de forma informal na seção anterior com a finalidade de darmos uma definição formal de $\mathbb{Q}_p$, o corpo dos números racionais $p-$ádicos. Para atingirmos nosso objetivo principal iremos primeiramente estudar os conceitos de valor absoluto e valorização, ambos em um corpo arbitrário qualquer.

Definição 8. *Seja $\mathbb{K}$ um corpo. Um valor absoluto em $\mathbb{K}$ é uma função*

$$|| : \mathbb{K} \longrightarrow \mathbb{R}_+,$$

que satisfaz as seguintes condições :

1. $|x| = 0$ *se, e somente se* $x = 0$
2. $|xy| = |x|\,|y|\,, \forall x, y \in \mathbb{K}$
3. $|x + y| \leq |x| + |y|\,, \forall x, y \in \mathbb{K}$
   Também diremos que um valor absoluto em $\mathbb{K}$ é não-arquimediano se tal satisfaz:
4. $|x + y| \leq max\{|x|\,, |y|\}\,, \forall x, y \in \mathbb{K}$
   Caso contrário, diremos que o valor absoluto é arquimediano.

Proposição 2.1. *Se uma função $|\cdot|$ satisfaz as condições (1), (2) e (4) da definição 8, então $|\cdot|$ é um valor absoluto em $\mathbb{K}$.*

Demonstração. Basta mostrar que (4) $\Rightarrow$ (3). De fato, temos que $\max\{|x|\,|y|\}, \leq |x| + |y|\,, \forall x, y \in \mathbb{K}$, portanto (3) é válida. □

Exemplo 2. *Seja $\mathbb{K} = \mathbb{Q}$ e seja o valor absoluto definido por:*

$$|x| = \begin{cases} -x & se \quad x \leq 0 \\ x & se \quad x > 0 \end{cases}$$

Segue-se que isso é, de fato, um valor absoluto em $\mathbb{Q}$ e é arquimediano.

Temos que o valor absoluto possui as seguintes propriedades:

Proposição 2.2. *Para um valor absoluto $|\cdot|$ qualquer em um corpo arbitrário $\mathbb{K}$, temos que:*

1. $|1| = 1$
2. *Se $x \in \mathbb{K}$ e $|x^n| = 1$, então $|x| = 1$.*
3. $|-1| = 1$
4. *Para todo $x \in \mathbb{K}$, $|-x| = |x|$.*

Demonstração.

1. Temos que
$$|1| = \left|1^2\right| = |1|^2\,,$$
logo $|1| = 1$.
2. Temos que
$$1 = |x^n| = |x|^n\,,$$
logo $|x| = 1$.
3. $|-1|^2 = |(-1)^2| = |1| = 1$, logo $|-1| = 1$.
4. $|-x| = |(-1)(x)| = |-1|\,|x| = |x|$.

□

Proposição 2.3. *Seja $\mathbb{K} = \mathbb{F}_q$ um corpo finito com $q = p^f$ elementos. O único valor absoluto em $\mathbb{K} = \mathbb{F}_q$ é o valor absoluto trivial:*

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

Demonstração. Seja $\mathbb{K} = \mathbb{F}_q$ e seja também

$$||_{\mathbb{K}} : \mathbb{F}_q \to \mathbb{R}_+$$

um valor absoluto. Temos que , para todo $a \in \mathbb{F}_q$ não-nulo, temos que:

$$a^{q-1} = 1 \Rightarrow \left|a^{q-1}\right| = |1|$$

$$\Rightarrow |a|^{q-1} = 1 \Rightarrow |a| = 1.$$

□

Seja $\mathbb{K} = \mathbb{Q}$ e $p \in \mathbb{Z}$ primo. Todo inteiro $n \in \mathbb{Z}$ pode ser escrito como $n = p^{\nu_p(n)}n'$, onde p não divide n' e tal representação é única. Assim podemos definir:

Definição 9. *Seja um primo $p \in \mathbb{Z}$. A valorização $p-$ádica em $\mathbb{Z}$ é a função*

$$\nu_p : \mathbb{Z}^* \longrightarrow \mathbb{R},$$

definida da seguinte forma: para cada $n \in \mathbb{Z}$ não-nulo, seja $\nu_p(n)$ o único inteiro positivo que satisfaz

$$n = p^{\nu_p(n)}n',$$

onde p e n' são primos entre si.

Vamos extender ν_p para os racionais da seguinte forma: se $x = a/b \in \mathbb{Q}$, então,

$$\nu_p(x) = \nu_p(a) - \nu_p(b).$$

Por coveniência, a partir deste momento, vamos definir que $\nu_p(0) = +\infty$. Vamos também observar que a valorização $p-$ádica de $x \in \mathbb{Q}$ também é determinada pela fórmula

$$x = \frac{a}{b}p^{\nu_p(x)},$$

onde p não divide ab.

Temos as seguintes propriedades da valorização $p-$ádica:

Lema 2.4. *Para todo $x, y \in \mathbb{Q}$, temos que*

1. $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
2. $\nu_p(x + y) \geq min\{\nu_p(x), \nu_p(y)\}$.

Demonstração. 1. Temos que $x = p^{\nu_p(x)}a/b$, $y = p^{\nu_p(y)}c/d$ e $xy = p^{\nu_p(xy)}e/f$, onde p não divide ab, cd e ef. Portanto,

$$xy = p^{\nu_p(x)}\frac{a}{b}p^{\nu_p(y)}\frac{c}{d} = p^{\nu_p(x)+\nu_p(y)}\frac{ac}{bd} = p^{\nu_p(xy)}\frac{e}{f},$$

como a valorização é única, então

$$\nu_p(xy) = \nu_p(x) + \nu_p(y).$$

2. Temos que
$$x + y = p^{\nu_p(x+y)}\frac{g}{h} = p^{\nu_p(x)}\frac{a}{b} + p^{\nu_p(y)}\frac{c}{d}.$$

Seja $\nu = \min\{\nu_p(x), \nu_p(y)\}$, logo:

$$x + y = p^{\nu_p(x+y)}\frac{g}{h} = p^{\nu_p(x)}\frac{a}{b} + p^{\nu_p(y)}\frac{c}{d}$$

$$= p^{\nu}(p^{\nu_p(x)-\nu}\frac{a}{b} + p^{\nu_p(y)-\nu}\frac{c}{d}),$$

como $\nu_p(x) - \nu \geq 0$ e $\nu_p(y) - \nu \geq 0$, então

$$\nu_p(x + y) = min\left\{\nu_p(x), \nu_p(y)\right\}.$$

□

Definição 10. *Para todo $x \in \mathbb{Q}$, definimos o valor absoluto $p-$ádico de x como sendo*

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

para $x \neq 0$. Para $x = 0$, vamos definir $|x|_p = 0$.

Proposição 2.5. *A função $|\cdot|_p$ é um valor absoluto não-arquimediano em $\mathbb{Q}$.*

Demonstração. Vamos mostrar que a função $||_p$ satisfaz as propriedades $1, 2$ e 4 da definição 8. Logo, temos que:

1. $|x|_p = 0$ se , e somente se, $p^{-\nu_p(x)} = 0$ se , e somente se, $\nu_p(x) = +\infty$ se, e somente se, $x = 0$.
2. $|xy|_p = p^{-\nu_p(xy)} = p^{-\nu_p(x)-\nu_p(y)} = p^{-\nu_p(x)}p^{-\nu_p(y)} = |x|_p |y|_p$
3. Segue diretamente do lema 2.4 (2).

□

2.2 Algumas Propriedades Importantes de $\mathbb{Q}_p$

Aqui, vamos falar brevemente de algumas propriedades de $\mathbb{Q}_p$ e iremos estabelecer uma visão da forma dos elementos desse corpo.

Antes, relembraremos a seguinte definição:

Definição 11. *Seja $\mathbb{K}$ um corpo e $|\cdot|$ um valor absoluto não-arquimediano em $\mathbb{K}$. O subanel*

$$\mathcal{O} = \overline{B}(0,1) = \{x \in \mathbb{K} : |x| \leq 1\}$$

é chamado de anel de valorização de $|\cdot|$. O ideal

$$\mathfrak{p} = B(0,1) = \{x \in \mathbb{K} : |x| < 1\}$$

é chamado de ideal de valorização de $|\cdot|$. O quociente

$$\kappa = \frac{\mathcal{O}}{\mathfrak{p}}$$

é chamado de corpo residual de $|\cdot|$.

Proposição 2.6. *Seja $\mathbb{K} = \mathbb{Q}$ e seja $|\cdot|_p$ o valor absoluto $p-$ádico. Então:*

1. *O anel de valorização associado é $\mathcal{O} = \mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : (p,b) = 1\}$*
2. *o ideal de valorização é $\mathfrak{p} = p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : (p,b) = 1, p|a\}$*
3. *o corpo residual é $\kappa = \mathbb{F}_p$*

Também vamos lembrar algumas propriedades já conhecidas de $\mathbb{Q}_p$:

- existe um valor absoluto $|\cdot|_p$ em $\mathbb{Q}_p$, e $\mathbb{Q}_p$ é completo com relação a esse valor absoluto;
- existe um inclusão $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ cuja imagem é densa em $\mathbb{Q}_p$, e a restrição do valor absoluto $|\cdot|_p$ à $\mathbb{Q}$ coincide com o valor absoluto $p-$ádico.
- os conjuntos
$$\left\{x \in \mathbb{R}_+ : x = |\lambda|_p, \lambda \in \mathbb{Q}\right\}$$
e
$$\left\{x \in \mathbb{R}_+ : x = |\lambda|_p, \lambda \in \mathbb{Q}_p\right\}$$
são ambos iguais ao conjunto $\{p^n : n \in \mathbb{Z}\} \cup \{0\}$.

Observe que a terceira propriedade pode ser reformulada como o seguinte lema:

Lema 2.7. *Para cada $x \in \mathbb{Q}_p$, $x \neq 0$, existe um inteiro $\nu_p(x)$ tal que $|x|_p = p^{-\nu_p(x)}$, ou seja, a valorização $p-$ádica ν_p se extende a $\mathbb{Q}_p$.*

Definição 12. *Vamos definir o anel de inteiros $p-$ádicos como o anel de valorização*

$$\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p : |x|_p \leq 1\right\}.$$

Proposição 2.8. *O anel $\mathbb{Z}_p$ é um anel local (anel que contém um único ideal maximal cujo complemento consiste de elementos invertiveis) cujo ideal maximal é o ideal principal $p\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p : |x|_p < 1\right\}$. Além disso:*

1. $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$
2. *A inclusão $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tem imagem densa, ou seja, dado $x \in \mathbb{Z}_p$ e $n \geq 1$, existe $\alpha \in \mathbb{Z}, 0 \leq \alpha \leq p^n - 1$, tais que $|x - \alpha|_p \leq p^{-n}$. Além disso, tal inteiro α é único.*
3. *Para todo $x \in \mathbb{Z}_p$, existe uma sequência (α_n) convergindo a x da seguinte forma:*
   - *para todo n, $\alpha_n \in \mathbb{Z}$ satisfaz $0 \leq \alpha_n \leq p^n - 1$;*
   - *para todo n, temos que $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$*

   A sequência (α_n) é única.

Demonstração. O fato de $\mathbb{Z}_p$ ser um anel local decorre do fato de ser um anel de valorização. Para mostrar que o ideal principal é $p\mathbb{Z}_p$, basta observar que, pelo lema 2.7:

$$|x|_p < 1 \Longrightarrow |x|_p < \frac{1}{p} \Longrightarrow \left|\frac{x}{p}\right|_p \leq 1 \Longrightarrow x \in p\mathbb{Z}_p$$

1. Decorre diretamente da proposição 2.6
2. Sejam $x \in \mathbb{Z}_p$ e $n \geq 1$. Como $\mathbb{Q}$ é denso em $\mathbb{Q}_p$, temos que existe um $a/b \in \mathbb{Q}$ na bola $B(x, \epsilon)$, de tal forma que:

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

   Basta mostrar então que existe um inteiro, mas para a/b da forma acima, temos que

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

   assim $a/b \in \mathbb{Z}_{(p)}$, ou seja, $(p, b) = 1$. Com isso, existe $b' \in \mathbb{Z}$ tal que $bb' \equiv 1(mod p^n)$, portanto, temos que

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

   Finalmente, basta mostrar que podemos achar um inteiro entre 0 e $p^n - 1$, mas isso decorre diretamente da relação entre congruência modulo potências de p e a valorização $p-$ádica. Escolhendo α como o único inteiro tal que

   $$0 \leq \alpha \leq p^n - 1, \alpha \equiv ab' \pmod{p^n}$$

   que fornece $|x - \alpha|_p \leq p^{-n}$, logo temos o resultado.

3. Decorre diretamente do item anterior (basta aplicar para a sequência de inteiros $n = 1, 2, \ldots$)

□

Agora temos uma visão bastante concreta dos elementos de $\mathbb{Q}_p$ e que forma eles tem. Já temos uma visão extremamente informal de como são esses elementos, então, ja sabemos ao menos como direcionar nossos estudos. Queremos escrever um número racional como uma série de potências em torno de um primo $p \in \mathbb{Z}$.

De fato, seja $x \in \mathbb{Z}_p$, pela proposição 2.8 temos que existe uma sequência (α_n) de inteiros convergindo para x tal que:

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

Vamos agora então tentar o que queriamos, vamos escrever tentar x na base p. Para isso, vamos escrever α_n na base p, assim para reduzirmos esse número módulo p^n vamos "'tirar"' os n últimos dígitos de α_n na base p. Dessa forma, temos que a segunda condição enunciada acima nos diz que os últimos n dígitos de α_n e α_{n+1} são os mesmos. O que nos fornece a sequência:

$$\begin{aligned} a_0 &= b_0 \\ a_1 &= b_0 + b_1 p \\ a_2 &= b_0 + b_1 p + b_2 p^2 \\ &\vdots \\ x &= b_0 + \cdots + b_n p^n + \cdots , \end{aligned}$$

onde $0 \leq b_i \leq p - 1$, para todo $i = 0, 1, \ldots$. Como cada uma das somas parciais dessa soma infinita é igual a α_n e α_n converge para x, então essa soma converge para x, o que nos fornece o seguinte lema;

Lema 2.9. *Seja $x \in \mathbb{Z}_p$ e (α_n) uma sequência como a obtida acima. A série infinita*

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

onde $\alpha_n = b_0 + b_1 p + \cdots + b_n p^n$, converge para x.

Corolário 2.10. *Todo $x \in \mathbb{Z}_p$ pode ser escrito na forma*

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

com $0 \leq b_i \leq p - 1$, para todo $i = 0, 1, \ldots$. Além disso, tal representação é única.

Demonstração. Nos resta provar a unicidade da representação, mas como a sequência (α_n) é única pela proposição 2.8, então os b_n também o serão, assim a representação é de fato única. □

Corolário 2.11. *Todo $x \in \mathbb{Q}_p$ pode ser escrito na forma*

$$x = b_{-n_0}p^{-n_0} + \cdots + b_0 + b_1p + b_2p^2 + \cdots + b_np^n + \cdots$$

$$= \sum_{m \geq -n_0} b_m p^m,$$

com $0 \leq b_m \leq p-1$ e $-n_0 = \nu_p(x)$. Tal representação é única.

Demonstração. Para todo $x \in \mathbb{Q}_p$, podemos escrever x da forma $x = y/p^k$ onde $y \in \mathbb{Z}_p$, com isso, basta dividirmos a série de y em torno de p por p^k e obtemos o resultado. □

2.3 Lema de Hensel e os Representantes de Teichm$\ddot{u}$ller

Aqui, vamos estudar uma das propriedades mais importantes dos números $p-$ádicos, o Lema de Hensel, o qual terá a demonstração apenas de sua primeira forma. Vamos, então, definir o conceito dos representantes de Teichmüller a partir desse Lema de Hensel, os quais serão de grande importância em nossos estudos futuros.

Lema 2.12 (Lema de Hensel(Primeira Forma))**.** *Seja $F(x) = c_0 + c_1x + \cdots + c_nx^n$ um polinômio cujos coeficientes são inteiros $p-$ádicos. Seja $F'(x) = c_1 + 2c_2x + \cdots + nc_nx^{n-1}$ a derivada formal de $F(x)$. Seja $a_0 \in \mathbb{Z}_p$ tal que $F(a_0) \equiv 0 \pmod{p}$ e $F'(a_0) \not\equiv \pmod{p}$. Então existe um único inteiro $p-$ádico a tal que*

$$F(a) = 0$$

e

$$a \equiv a_0 \pmod{p}.$$

Demonstração. Primeiramente, vamos mostrar que existe uma sequência de inteiros racionais $a_1, a_2, a_3, \ldots$ tais que, para todo $n \geq 1$, temos que :

- $F(a_n) \equiv 0 \pmod{p^{n+1}}$
- $a_n \equiv a_{n-1} \pmod{p^n}$
- $0 \leq a_n < p^{n+1}$

Vamos mostrar que tais a_n são únicos e existem por indução sobre n.

Para $n = 1$, seja d_0 o único inteiro em $\{0, 1, \ldots, p-1\}$ congruente a a_0 modulo p. Assim, se um certo a_1 satisfaz as duas últimas condições então $a_1 = d_0 + b_1 p$, onde $0 \leq b_1 \leq p-1$. Vamos agora extender $F(d_0 + b_1 p)$. Assim, temos que:

$$F(a_1) = F(d_0 + b_1 p) = \sum c_i (d_0 + b_1 p)^i$$

$$= \sum (c_i d_0^i + i c_i d_0^{i-1} b_1 p + G)$$

$$\equiv \sum c_i d_0^i + (\sum i c_i d_0^{i-1}) b_1 p (mod p^2) = F(d_0) + F^{'}(d_0) b_1 p,$$

pois $G \equiv 0 \pmod{p^2}$. Como $F(a_0) \equiv 0 \pmod{p}$, podemos escrever $F(d_0) \equiv \alpha p \pmod{p^2}$, para $\alpha \in \{0, 1, \ldots, p-1\}$. Assim para termos

$$F(a_1) \equiv 0 \pmod{p^2}$$

devemos ter

$$\alpha p + F^{'}(d_0) b_1 p \equiv 0 \pmod{p^2} \Rightarrow \alpha + F^{'}(d_0) b_1 \equiv 0 \pmod{p}.$$

Mas tal equação sempre tem solução para b_1, pois, por hipótese, $F^{'}(a_0)$ não é congruente a zero modulo p.Mas pela proposição 2.8 , podemos ecolher $b_1 \in \{0, 1, \ldots, p-1\}$ tal que $b_1 \equiv -\alpha / F^{'}(d_0) \pmod{p}$.Assim b_1 é unicamente determinada.

Vamos supor agora que as tres condições são válidas para todo $a_1, a_2, \ldots, a_{n-1}$. Queremos mostrar que essas tres condições são válidas para a_n e cocluir a nossa indução. Precisamos de $a_n = a_{n-1} + b_n p^n$ com $b_n \in \{0, 1, \ldots, p-1\}$. Dessa forma teremos

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

Como $F(a_{n-1}) \equiv 0 \pmod{p^n}$ por hipótese de indução, então podemos escrever $F(a_{n-1}) \equiv \alpha^{'} p^n \pmod{p^{n+1}}$ e assim temos que:

$$\alpha^{'} p^n + F^{'}(a_{n-1}) b_n p^n \equiv 0 \pmod{p^{n+1}} \Rightarrow \alpha^{'} + F^{'}(a_{n-1}) b_n \equiv 0 \pmod{p}.$$

Como $a_{n-1} \equiv a_0 \pmod{p}$, temos que $F(a_{n-1}) \equiv F(a_0)$ e $F(a_0)$ não é congruente a zero modulo p. Com isso, podemos achar b_n da mesma forma que fizemos no caso $n = 1$, ou seja, resolvendo $-\alpha^{'} / F^{'}(a_{n-1}) \pmod{p}$. Com isso concluimos a indução.

Agora, seja $a = d_0 + b_1 p + b_2 p^2 + \cdots$. Como $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$ para todo n, que implica que o número $p-$ádico $F(a)$ é nulo. Por outro lado, temos que qualquer $a = d_0 + b_1 p + b_2 p^2 + \cdots$ fornece uma sequência única que satisfaz as tres condições do início da demonstração, e a unicidade da sequência implica na unicidade desse a, assim temos o resultado. □

Corolário 2.13. *$\mathbb{Q}_p$ sempre contém as p soluções $a_0, a_1, \ldots, a_{p-1}$ da equação $x^p - x = 0$, onde $a_i \equiv i \pmod{p}$.*

Demonstração. Basta usar o Lema de Hensel para cada $a_0 = 0, 1, \ldots, p-1$ com $F(x) = x^p - x$. □

Definição 13. *As p soluções definidas no corolário 2.13 serão chamadas como os Representantes de Teichmüller de* $\{0, 1, \ldots, p-1\}$.

Com isso, denotando por $\mathbb{T}$ o conjunto dos representantes de Teichmüller, podemos concluir que esses representantes (excluindo o zero) satisfazem a seguinte relação:

$$\sum_{t \in \mathbb{T}^*} t^j = \begin{cases} q-1 & \text{se} \quad j \equiv 0 (mod(q-1)) \\ 0 & \text{se} \quad c.c. \end{cases}$$

Agora se incluirmos o zero nessa soma e convencionarmos $0^0 = 1$, então, temos que:

$$\sum_{t \in \mathbb{T}} t^j = \begin{cases} q & \text{se} \quad j = 0 \\ q-1 & \text{se} \quad j \neq 0, j \equiv 0 (mod(q-1)) \\ 0 & \text{se} \quad c.c. \end{cases}$$

Assim podemos tirar como consequência o caso de várias variáveis, o qual aqui será explicitado na forma do seguinte lema:

Lema 2.14. *Suponha que* $e_1, \ldots, e_m$ *sejam inteiros não negativos e que s desses sejam não-nulos e sejam* $\boldsymbol{t} = (t_1, \ldots, t_m) \in \mathbb{T}^m$ *e* $\boldsymbol{e} = (e_1 \ldots, e_m)$*, então*

$$\sum_{\boldsymbol{t} \in \mathbb{T}^m} t_1^{e_1} \cdots t_m^{e_m} = \begin{cases} (q-1)^s q^{m-s} & se \quad (q-1) | \boldsymbol{e} \\ 0 & se \quad c.c. \end{cases}$$

2.4 Função Peso e Propriedades

Agora, que temos uma definição formal do corpo dos números $p-$ádicos $\mathbb{Q}_p$, podemos concluir que $\mathbb{Q}$ é, de fato, estritamente incluso em $\mathbb{Q}_p$, portanto, podemos afirmar que dado $n \in \mathbb{Z}$, n sempre pode ser escrito na sua forma $p-$ádica, ou seja

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_l p^l = \sum_{j=0}^{l} a_j p^j,$$

onde $a_j \in \{0, 1, \ldots, p-1\}$ para todo $j = 0, \ldots, l$.

Assim definimos o peso de $n \in \mathbb{Z}$ em relação a p como sendo

$$\sigma_p(n) = \sum_{j=0}^{l} a_j.$$

Seja um monômio $X_1^{e_1} \cdots X_n^{e_n}$, vamos definir o peso desse monômio em relação a p como

$$\omega_p(X_1^{e_1} \cdots X_n^{e_n}) = \sigma_p(e_1) + \cdots + \sigma_p(e_n) = \sum_{i=1}^{n} \sigma_p(e_i),$$

assim, podemos denotar o peso em relação a p com respeito a variável X_i do monômio $X_1^{e_1} \cdots X_n^{e_n}$ por

$$\omega_{p,X_i}(X_1^{e_1} \cdots X_n^{e_n}) = \sigma_p(e_i).$$

Seja, agora, um polinômio sobre $\mathbb{F}_q$ definido por $F(X_1, \ldots, X_n) = \sum_{i=1}^{N} a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$, $a_i \neq 0$ para todo i. O peso em relação a p desse polinômio é definido por

$$\omega_p(F) = \max_i \omega_p(X_1^{e_{1i}} \cdots X_n^{e_{ni}}).$$

Agora, da mesma forma que fizemos para um monômio, podemos denotar o peso em relação a p com respeito a uma variável X_i do polinômio F por

$$\omega_{p,X_i} = \max_i \omega_{p,X_i}(X_1^{e_{1i}} \cdots X_n^{e_{ni}}).$$

Proposição 2.15. *Seja $q = p^f$ uma potência inteira de p, onde p é primo. Assim, temos que $\sigma_p(q-1) = f(p-1)$.*

Demonstração. Temos que:

$$q - 1 = p^f - 1 = (p-1)(p^{f-1} + p^{f-2} + \cdots + p + 1)$$

$$= (p-1)p^{f-1} + (p-1)p^{f-2} + \cdots + (p-1)p + (p-1)1$$

Portanto

$$\sigma_p(q-1) = \sum_{i=0}^{f-1} p - 1 = f(p-1).$$

□

Agora, vamos demonstrar algumas propriedades da função peso essenciais para nossos estudos futuros.

Proposição 2.16. *Sejam a, b inteiros não negativos μ um múltiplo positivo de $q-1$ e $q = p^f$, então:*

1. $\sigma_p(ap^k) = \sigma_p(a)$, *para* $k > 0$
2. $\sigma_p(a) + \sigma_p(b) \geq \sigma_p(a+b)$
3. $\sigma_p(a)\sigma_p(b) \geq \sigma_p(ab)$

4. $\sigma_p(\mu) \geq \sigma_p(q-1)$

Demonstração. Os 3 primeiros itens da proposição têm demonstração bastante trivial, logo será apenas apresentada a demonstração do quarto item, de fato, será o item mais importante em nossos estudos posteriores. Temos que, para provarmos o quarto item, é suficiente mostrarmos que se $a > 1$, então existe um $a^{'}$ com $a > a^{'} \geq 1$ e $\sigma_p(a(q-1)) \geq \sigma_p(a^{'}(q-1))$. Mas podemos escrever $a(q-1) = bq + c$, onde $0 \leq c \leq q-1$ e $\sigma_p(bq+c) = \sigma_p(b) + \sigma_p(c)$, usando a primeira propriedade e o fato de que $0 \leq c \leq q-1$. Mas usando isso e a segunda propriedade, temos que

$$\sigma_p(a(q-1)) = \sigma_p(b) + \sigma_p(c) \geq \sigma_p(b+c) = \sigma_p((a-b)(q-1)),$$

com $a > a - b \geq 1$. □

2.5 Ramificação e o Grau da Classe Residual

É facil observar que $\mathbb{Q}_p$ não é um corpo algebricamente fechado (basta ver, por exemplo, que $\sqrt{2} \notin \mathbb{Q}_5$). Por isso, é de nosso interesse estudar as extensões algébricas de $\mathbb{Q}_p$. Num primeiro momento, vamos verificar que a valorização $p-$ádica se extende para uma extensão $\mathbb{K}$ finita e normal de $\mathbb{Q}_p$ de grau n.

Seja $\mathbb{K}$ uma extensão finita de $\mathbb{Q}_p$ e, como vimos anteriormente, $\mathbb{K}$ pode ser visto como um espaço vetorial sobre $\mathbb{Q}_p$. Assim, vamos nos referir a uma norma em um espaço vetorial de forma análogo a que fizemos com corpos, ou seja, um mapa $\|\|_{\mathbb{K}}$ de $\mathbb{K}$ para os numeros reais não-negativos tal que:

1. $\|x\|_{\mathbb{K}} = 0 \Leftrightarrow x = 0$;
2. $\|ax\|_{\mathbb{K}} = \|a\| \|x\|_{\mathbb{K}}, \forall x \in \mathbb{K}, a \in \mathbb{Q}_p$, onde $\|a\|$ denota a norma em $\mathbb{Q}_p$;
3. $\|x+y\|_{\mathbb{K}} \leq \|x\|_{\mathbb{K}} + \|y\|_{\mathbb{K}}$.

Dessa forma, temos que qualquer norma em $\mathbb{K}$ como corpo cuja restrição a $\mathbb{Q}_p$ é uma norma em $\mathbb{Q}_p$, será uma norma em $\mathbb{K}$ como espaço vetorial. Como no caso de corpos, temos que duas normas $\|\|_1$ e $\|\|_2$ em $\mathbb{K}$ como espaço vetorial serão equivalentes se, e somente se, existem constantes positivas c_1 e c_2, tais que, para todo $x \in \mathbb{K}$, temos que: $\|x\|_2 \leq c_1 \|x\|_1$ e $\|x\|_1 \leq c_2 \|x\|_2$.

Teorema 2.17. *Seja $\mathbb{K}$ uma extensão de $\mathbb{Q}_p$ (ou seja, um espaço vetorial sobre $\mathbb{Q}_p$), então todas as normas em $\mathbb{K}$ como espaço vetorial são equivalentes.*

Demonstração. Sejam $\{k_1, \ldots, k_n\}$ uma base de $\mathbb{K}$ e $\|\|_{sup}$ a norma do sup em $\mathbb{K}$, ou seja,

$$\|a_1k_1 + \cdots + a_nk_n\|_{sup} = \max_{1 \leq i \leq n}(\|a_i\|).$$

Seja agora $\|\|\|_{\mathbb{K}}$ uma outra norma qualquer em $\mathbb{K}$.Portanto, para qualquer $x = a_1k_1 + \cdots + a_nk_n$, temos que:

$$\begin{aligned}\|x\|_{\mathbb{K}} &\leq \|a_1\| \|k_1\|_{\mathbb{K}} + \cdots + \|a_n\| \|k_n\|_{\mathbb{K}} \\ &\leq n(\max \|a_i\|) \max \|k_i\|_{\mathbb{K}},\end{aligned}$$

tomando $c_1 = n \max \|k_i\|_{\mathbb{K}}$, temos a inequação $\|\|\|_{\mathbb{K}} \leq c_1 \|\|\|_{sup}$.

Vamos considerar agora o conjunto

$$U = \left\{ x \in \mathbb{K} : \|x\|_{sup} = 1 \right\}.$$

Suponhamos agora, por contradição, que não exista nenhum ϵ positivo tal que $\|x\|_{\mathbb{K}} \geq \epsilon$ para $x \in U$. Assim, temos uma sequencia (x_i) em U tal que $\|x_i\|_{\mathbb{K}} \to 0$. Como U é compacto em relação a norma do sup([17]), então ha uma subsequencia (x_{i_j}) que converge na norma do sup para algum $x \in U$. Mas, para todo j :

$$\|x\|_{\mathbb{K}} \leq \left\|x - x_{i_j}\right\|_{\mathbb{K}} + \left\|x_{i_j}\right\|_{\mathbb{K}} \leq c_1 \left\|x - x_{i_j}\right\|_{sup} + \left\|x_{i_j}\right\|_{\mathbb{K}},$$

pela inequação já provada anteriormente. Mas os dois termos na última equação tendem a 0 quando $j \to \infty$, logo $\|x\|_{\mathbb{K}} = 0$, de forma que $x = 0 \notin U$, o que é uma contradição. Portanto, temos que existe um ϵ positivo, tal que $\|x\|_{\mathbb{K}} \geq \epsilon$ para $x \in U$. Com essa afirmação, temos que na bola de raio 1 da norma do sup U, a norma $\|\|\|_{\mathbb{K}}$ permanece maior que um número positivo ϵ, donde $\|\|\|_{sup} \leq c_2 \|\|\|_{\mathbb{K}}$, em U, onde $c_2 = 1/\epsilon$. Assim, sejam $x = a_1k_1 + \cdots a_nk_n \in \mathbb{K}$ e j tal que $\|a_j\| = max \|a_i\| = \|x\|_{sup}$.Assim $(x/a_j) \in U$, logo

$$\left\| \frac{x}{a_j} \right\|_{\mathbb{K}} \geq \epsilon = \frac{1}{c_2}$$

portanto

$$\|x\|_{sup} = \|a_j\| \leq c_2 \|x\|_{\mathbb{K}}.$$

Dessa forma, temos que, qualquer norma em $\mathbb{K}$ é equivalente à norma do sup. □

Corolário 2.18. *Seja $\mathbb{K}$ uma extensão de $\mathbb{Q}_p$. Então há no máximo uma norma $\|\|\|_{\mathbb{K}}$ de $\mathbb{K}$ como um corpo que extende $\|\|\|$ de $\mathbb{Q}_p$.*

Demonstração. Pelo teorema anterior, temos que duas normas $\|\|\|_1$ e $\|\|\|_2$ são equivalentes em $\mathbb{K}$.Logo $\|\|\|_2 \leq c_1 \|\|\|_1$. Seja $x \in \mathbb{K}$, tal que $\|x\|_1 \neq \|x\|_2$, sem perda de generalidade, suponha $\|x\|_1 < \|x\|_2$. Mas para um N suficientemente grande, temos que $c_1 \left\|x^N\right\|_1 < \left\|x^N\right\|_2$, que é uma contradição. □

Observe que o teorema e o corolário acima podem ser generalizados para extensão de dois corpos quaisquer, mas como aqui vamos apenas nos interessar por extensões de $\mathbb{Q}_p$, restringimos o teorema e o corolário.

Seja σ um automorfismo de $\mathbb{K}$ que fixa $\mathbb{Q}_p$ e seja $||$ um valor absoluto em $\mathbb{K}$. Temos que a função $x \to |\sigma(x)|$ também é um valor absoluto em $\mathbb{K}$ e que fornece o valor absoluto

$p-$ádico sobre $\mathbb{Q}_p$, uma vez que σ fixa $\mathbb{Q}_p$. Mas, como vimos acima, temos que esse valor absoluto é único, logo $|\sigma(x)| = |x|$ para qualquer $x \in \mathbb{K}$. Como vimos anteriormente, a norma é a multiplicação dos automorfismos de $\mathbb{K}$ que fixam $\mathbb{Q}_p$(que são os conjugados), portanto, temos que:

$$\left|\prod_{\sigma} \sigma(x)\right| = |x|^n = |N(x)|\,,$$

onde n é o grau da extensão $\mathbb{K}$ sobre $\mathbb{Q}_p$. Portanto

$$|x| = \sqrt[n]{|N(x)|}.$$

Dessa forma, podemos calcular o valor absoluto em $\mathbb{K}$ de forma mais fácil, pois já conhecemos o valor absoluto $p-$ádico e temos que a norma pertence a $\mathbb{Q}_p$.

Lema 2.19. *Sejam $\mathbb{L}$ e $\mathbb{K}$ extensões finitas de $\mathbb{Q}_p$ da forma $\mathbb{Q}_p \subset \mathbb{L} \subset \mathbb{K}$. suponha que $x \in \mathbb{L}$ e sejam $m = [\mathbb{L} : \mathbb{Q}_p]$ e $n = [\mathbb{K} : \mathbb{Q}_p]$. Então*

$$\sqrt[m]{\left|N_{\mathbb{L}/\mathbb{Q}_p}(x)\right|} = \sqrt[n]{\left|N_{\mathbb{K}/\mathbb{Q}_p}(x)\right|}.$$

Demonstração. Temos que ([21]),

$$N_{\mathbb{K}/\mathbb{L}}(x) = N_{\mathbb{L}/\mathbb{Q}_p}(N_{\mathbb{K}/\mathbb{Q}_p}(x)),$$

e $N_{\mathbb{K}/\mathbb{L}} = x^{[\mathbb{K}:\mathbb{L}]}$. Lembrando que $[\mathbb{K} : \mathbb{Q}_p] = [\mathbb{K} : \mathbb{L}]\,[\mathbb{L} : \mathbb{Q}_p]$(Teorema de Lagrange) o resultado se segue. □

Dessa forma provamos a seguinte proposição:

Proposição 2.20. *Se existe um valor absoluto em $\mathbb{K}$ que extende o valor absoluto $p-$ádico, então tal valor é dado por:*

$$|x| = \sqrt[n]{\left|N_{\mathbb{K}/\mathbb{Q}_p}(x)\right|_p},$$

onde n é o grau da extensão.

Agora é de nosso interesse saber se a fórmula dada pela norma de x nos fornece um valor absoluto, de fato temos que:

Teorema 2.21. *([7])*

Seja $\mathbb{K}/\mathbb{Q}_p$ uma extensão finita de grau n. A função $|| : \mathbb{K} \longrightarrow \mathbb{R}_+$ dada por

$$|x| = \sqrt[n]{\left|N_{\mathbb{K}/\mathbb{Q}_p}(x)\right|_p}$$

é um valor absoluto não-arquimediano em $\mathbb{K}$ que extende o valor absoluto $p-$ádico em $\mathbb{Q}_p$.

Agora que sabemos que $\mathbb{K}$ tem um valor absoluto que extende o valor absoluto $p-$ádico, podemos finalmente expor a seguinte definição:

Definição 14. *Seja $\mathbb{K}$ uma extensão finita de $\mathbb{Q}_p$, e seja $||$ o valor absoluto $p-$ádico em $\mathbb{K}$. Para qualquer $x \in \mathbb{K}, x \neq 0$, vamos definir a valorização $p-$ádica $\nu_p(x)$ como sendo o único número racional satisfazendo*

$$|x| = p^{-\nu_p(x)}.$$

Completamos a definição de maneira formal estabelecendo $\nu_p(0) = +\infty$.

Assim, vamos computar essa valorização definida acima, computando normas, pois:

$$\nu_p(x) = \frac{1}{n}\nu_p(N_{\mathbb{K}/\mathbb{Q}_p}(x)).$$

Proposição 2.22. *A valorização $p-$ádica ν_p é um homomorfismo do grupo multiplicativo $\mathbb{K}$ para o grupo aditivo $\mathbb{Q}$. A imagem desse homomorfismo é da forma $\frac{1}{e}\mathbb{Z}$, onde e é um divisor de $n = [\mathbb{K} : \mathbb{Q}_p]$.*

Demonstração. Ja sabemos que tal valorização é um homomorfismo usando a fórmula acima(pois de fato é uma valorização!) e também sabemos que a imagem está contida em $\frac{1}{n}\mathbb{Z}$, também pela expressão acima. Seja agora d/e(com $(d, e) = 1$) na imagem, de tal forma que o denominador e é o maior possível. Como d e e são co-primos, então existem r e s tais que $rd = 1 + se$, então

$$r \cdot \frac{d}{e} = \frac{1 + se}{e} = \frac{1}{e} + s$$

está na imagem, uma vez que $s \in \mathbb{Z}$ está na imagem, dai $1/e$ também está na imagem. Pela escolha de e como o maior possível, então a imagem é de fato $\frac{1}{e}\mathbb{Z}$. □

Agora podemos definir o seguinte:

Definição 15. *Seja $\mathbb{K}/\mathbb{Q}_p$ uma extensão finita, e seja $e = e(\mathbb{K}/\mathbb{Q}_p)$ o único inteiro positivo como definido na demonstração da proposição anterior. Vamos chamar tal inteiro e de índice de ramificação de $\mathbb{K}$ sobre $\mathbb{Q}_p$. Vamos dizer que a extensão $\mathbb{K}/\mathbb{Q}_p$ é não-ramificada se $e = 1$. Vamos chamá-la de ramificada se $e > 1$ e totalmente ramificada se $e = n$, onde n é o grau da extensão. Finalmente, vamos escrever $f = f(\mathbb{K}/\mathbb{Q}_p) = n/e$ e vamos chamar tal $f = f(\mathbb{K}/\mathbb{Q}_p)$ como grau da classe residual.*

Definição 16. *Seja $\mathbb{K}/\mathbb{Q}_p$ uma extensão finita e seja e seu índice de ramificação. Vamos definir um elemento $\pi \in \mathbb{K}$ como um uniformizador se $\nu_p(\pi) = 1/e$.*

O seguinte lema será importante para a demonstração do próximo teorema:

Lema 2.23. *([11])Uma sequência (a_n) em $\mathbb{Q}_p$ é uma sequência de Cauchy se, e somente se, satisfaz*

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

Sejam agora $\mathcal{O}_{\mathbb{K}}$ e $\mathfrak{p}_{\mathbb{K}}$ o anel de valorização de $\mathbb{K}$ e seu ideal maximal, respectivamente, e seja

$$\kappa = \mathcal{O}_{\mathbb{K}}/\mathfrak{p}_{\mathbb{K}}$$

o anel residual. Dessa forma temos que:

Proposição 2.24. *Seja $\pi \in \mathbb{K}$ um uniformizador, então:*

1. *$\pi \in \mathbb{K}$ é o gerador do ideal $\mathfrak{p}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{K}}$, que é principal.*
2. *Qualquer elemento $x \in \mathbb{K}$ pode ser escrito na forma $x = u\pi^{e\nu_p(x)}$, onde $u \in \mathcal{O}_{\mathbb{K}}$ é uma unidade e tem valorização em relação a p nula.*
3. *O corpo residual κ é uma extensão finita de $\mathbb{F}_p$ com grau menor ou igual ao grau da extensão $\mathbb{K}/\mathbb{Q}_p$.Mais especificamente, sendo f o grau da classe residual, temos que $[\kappa : \mathbb{F}_p] = f$, ou seja, o corpo residual κ é isomorfo ao corpo finito com p^f elementos.*

Demonstração. Para provar a primeira propriedade, basta observar que:

$$x \in \mathfrak{p}_{\mathbb{K}} \Rightarrow \nu_p(x) > 0 \Rightarrow \nu_p(x) \geq 1/e,$$

pois pela proposição 2.22, temos que a imagem da valorização $p-$ádica é da forma $\frac{1}{e}\mathbb{Z}$. Assim, temos que

$$x \in \mathfrak{p}_{\mathbb{K}} \Rightarrow \nu_p(\pi^{-1}x) \geq 0 \Rightarrow \pi^{-1}x \in \mathcal{O}_{\mathbb{K}}$$
$$\Rightarrow x \in \pi\mathcal{O}_{\mathbb{K}}.$$

Assim, temos que π gera $\mathfrak{p}_{\mathbb{K}}$.

A prova do segundo item é análoga. Vamos observar que, também pela proposição 2.22, temos que a imagem da valorização $p-$ádica de $x \in \mathbb{K}$, é da forma $\nu_p(x) = \frac{1}{e}s$, onde $s \in \mathbb{Z}$. Assim, temos que:

$$x \in \mathbb{K} \Rightarrow \nu_p(x) = \frac{1}{e}s =$$
$$= s\nu_p(\pi) = \nu_p(\pi^s) =$$
$$= \nu_p(u) + \nu_p(\pi^s) = \nu_p(u\pi^{e\nu_p(x)}),$$

onde u é tal que $\nu_p(u) = 0$. Para a prova do terceiro item, vamos recordar que os elementos de $\kappa = \mathcal{O}_{\mathbb{K}}/\mathfrak{p}_{\mathbb{K}}$ são classes laterais $a + \mathfrak{p}_{\mathbb{K}}$. Vamos observar que, se a e b estão em $\mathbb{Z}_p$, então as classes laterais $a + \mathfrak{p}_{\mathbb{K}}$ e $b + \mathfrak{p}_{\mathbb{K}}$ são a mesma classe lateral se, e somente se, $a - b \in \mathfrak{p}_{\mathbb{K}} \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Dessa forma temos a inclusão

$$\frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \longrightarrow \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}_{\mathbb{K}}}$$

$$a(p\mathbb{Z}_p) \longrightarrow a\mathfrak{p}_{\mathbb{K}}$$

para $a \in \mathbb{Z}_p$. Como $\mathbb{Z}_p/p\mathbb{Z}_p$ é isomorfo ao corpo finito com p elementos, então κ é uma extensão de $\mathbb{F}_p$. Agora resta-nos mostrar que tal extensão é finita e tem grau menor que $n = [\mathbb{K} : \mathbb{Q}_p]$.

De fato, seja, para $i = 1, 2, \ldots, n+1$, um mapa

$$\mathcal{O}_{\mathbb{K}} \longrightarrow \kappa$$

$$a_i \longrightarrow \overline{a_i}.$$

Como o grau de $\mathbb{K}$ sobre $\mathbb{Q}_p$ como espaço vetorial é igual a n, então $a_1, a_2, \ldots, a_{n+1}$ devem ser linearmente dependentes sobre $\mathbb{Q}_p$, ou seja:

$$a_1 b_1 + \cdots + a_{n+1} b_{n+1} = 0, b_i \in \mathbb{Q}_p.$$

Podemos assumir, sem perda de generalidade, que todos $b_i \in \mathbb{Z}_p$, mas que pelo menos um deles não está em $p\mathbb{Z}_p$. Com isso temos que:

$$\overline{a_1}\overline{b_1} + \cdots + \overline{a_{n+1}}\overline{b_{n+1}} = 0.$$

Mas como pelo menos um dos $\overline{b_i}$ não está em $p\mathbb{Z}_p$, então há um $\overline{b_i}$ diferente de zero, assim temos que $\overline{a_1}, \ldots, \overline{a_{n+1}}$ são linearmente dependentes sobre $\mathbb{F}_p$.

Sejam agora os elementos

$$a_1, a_2, \ldots, a_f,$$

$$\pi a_1, \pi a_2, \ldots, \pi a_f,$$

$$\pi^2 a_1, \pi^2 a_2, \ldots, \pi^2 a_f,$$

$$\ldots$$

$$\pi^{e-1} a_1, \pi^{e-1} a_2, \ldots, \pi^{e-1} a_f,$$

onde e e f são, respectivamente, o índice de ramificação e o grau da classe residual. Vamos agora provar que isso é uma base de $\mathbb{K}$ sobre $\mathbb{Q}_p$. Seja, então $x \in \mathcal{O}_{\mathbb{K}}$, de forma análoga ao que fizemos acima, temos que, $\overline{x}$ pode ser escrito como uma combinação dos $\overline{a}_j$, assim

$$x = x_{0,1} a_1 + x_{0,2} a_2 + \cdots + x_{0,f} a_f + \pi l_1,$$

onde $x_{0,j} \in \mathbb{Z}_p$ e $l_1 \in \mathcal{O}_{\mathbb{K}}$.

Agora, aplicando o mesmo processo a $l_1\pi$, obtemos:

$$x = x_{0,1} a_1 + x_{0,2} a_2 + \cdots + x_{0,f} a_f +$$

$$+ x_{1,1} \pi a_1 + x_{1,2} \pi a_2 + \cdots + x_{1,f} \pi a_f +$$

$$+ l_2 \pi^2,$$

onde $l_2 \in \mathcal{O}_{\mathbb{K}}$.

Repetindo o mesmo processo e vezes e lembrando que π^e e p tem a mesma valorização, temos que

$$x = x_{0,1} a_1 + x_{0,2} a_2 + \cdots + x_{0,f} a_f +$$

$$+ x_{1,1} \pi a_1 + x_{1,2} \pi a_2 + \cdots + x_{1,f} \pi a_f +$$

$$\ldots$$

$$+x_{e-1,1}\pi^{e-1}a_1 + x_{e-1,2}\pi^{e-1}a_2 + \cdots + x_{e-1,f}\pi^{e-1}a_f +$$
$$+px^{'},$$

onde $x_{i,j} \in \mathbb{Z}_p$ e $x^{'} \in \mathcal{O}_{\mathbb{K}}$.

Vamos aplicar o mesmo processo para $x^{'}$, mas reduzindo modulo p em vez de π. Isolando cada um dos novos coeficientes e tomando o limite, podemos usar o lema 2.23. Dessa forma, teremos x escrito como combinação linear da base dos elementos de nossa base. Para mostrar a independência, basta aplicar um processo análogo ao usado acima ainda nessa mesma demonstração do terceiro item desse teorema.

□

Agora, vamos fornecer a primeira forma do Lema de Hensel para o anel de inteiros $\mathcal{O}_{\mathbb{K}}$.

Lema 2.25. *Seja $\mathbb{K}/\mathbb{Q}_p$ uma extensão finita de grau n e seja π um uniformizador. Seja $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathcal{O}_{\mathbb{K}}[X]$. Suponha que exista um $\alpha_1 \in \mathcal{O}_{\mathbb{K}}$ tal que*

$$F(\alpha_1) \equiv 0 \pmod{\pi}$$

e

$$F^{'}(\alpha_1) \not\equiv 0 \pmod{\pi}.$$

Assim, existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que

$$\alpha \equiv \alpha_1 \pmod{\pi}$$

e

$$F(\alpha) = 0.$$

Demonstração. Aqui, vamos observar que como visto na definição 12, temos que $\mathbb{Z}_p$ é o anel de valorização de $\mathbb{Q}_p$. Mas também temos que $\mathcal{O}_{\mathbb{K}}$ é o anel de valorização de $\mathbb{K}$. Vamos observar também que, pela proposição 2.8, temos que o ideal principal de $\mathbb{Z}_p$ é o ideal gerado pelo seu elemento primo p, $p\mathbb{Z}_p$, assim como o ideal principal de $\mathcal{O}_{\mathbb{K}}$ é o ideal gerado pelo seu elemento primo(o uniformizador) π, $\mathfrak{p}_{\mathbb{K}}$. Assim, podemos fazer essa demonstração de forma idêntica à demostração da primeira forma do Lema de Hensel dada anteriormente, mas agora fezendo reduções módulo π, ao inves de p. □

Agora, de forma análoga ao que fizemos para concluir o corolário 2.13, temos que podemos inferir o seguinte corolário:

Corolário 2.26. *Sejam $\mathbb{K}/\mathbb{Q}_p$ uma extensão finita de grau n e f o grau da classe residual. Então o grupo multiplicativo $\mathcal{O}_{\mathbb{K}}^{\times}$ contém o grupo cíclico das $(p^f - 1)-$ésimas raizes da unidade.*

Assim, temos que $\mathbb{K}$ contém todas as $(p^f - 1)-$ésimas raizes da unidade, ou seja, $\mathbb{K}$ contém as soluções de $x^{p^f} - x = 0$. Mais uma vez de forma análoga ao que fizemos antes, podemos agora definir quais são os representantes de Teichmüller em $\mathbb{K}$, pois para a no corpo residual de $\mathbb{K}$, temos um $a^{'} \in \mathbb{K}$ tal que $(a^{'})^{p^f} = a^{'}$ e $a^{'} \equiv a \pmod{\pi}$. Assim:

Definição 17. *Sejam $a^{'} \in \mathbb{K}$ tal que $(a^{'})^{p^f} = a^{'}$ e $a^{'} \equiv a \pmod{\pi}$ e f o grau da classe residual, onde $a \in \kappa$, o corpo residual de $\mathbb{K}$. Vamos definir tal $a^{'}$ como o representante de Teichmüller de a. E vamos denotar por*

$$\mathbb{T} = \left\{ a^{'} \in \mathbb{K} : (a^{'})^{p^f} = a^{'} \right\}$$

o conjunto dos representantes de Teichmüller.

Com isso, denotando por $\mathbb{T}$ o conjunto dos representantes de Teichmüller de $\mathbb{F}_q$, podemos concluir que esses representantes (excluindo o zero) satisfazem a seguinte relação:

$$\sum_{t \in \mathbb{T}^*} t^j = \begin{cases} q-1 & \text{se} \quad j \equiv 0 (mod(q-1)) \\ 0 & \text{se} \quad c.c. \end{cases}$$

Agora se incluirmos o zero nessa soma e convencionarmos $0^0 = 1$, então, temos que:

$$\sum_{t \in \mathbb{T}} t^j = \begin{cases} q & \text{se} \quad j = 0 \\ q-1 & \text{se} \quad j \neq 0, j \equiv 0 (mod(q-1)) \\ 0 & \text{se} \quad c.c. \end{cases}$$

Assim podemos tirar como consequência o caso de várias variáveis, o qual aqui será explicitado na forma do seguinte lema:

Lema 2.27. *Suponha que $e_1, \ldots, e_m$ sejam inteiros não negativos e que s desses sejam não-nulos e sejam $\boldsymbol{t} = (t_1, \ldots, t_m) \in \mathbb{T}^m$ e $\boldsymbol{e} = (e_1 \ldots, e_m)$, então*

$$\sum_{\boldsymbol{t} \in \mathbb{T}^m} t_1^{e_1} \cdots t_m^{e_m} = \begin{cases} (q-1)^s q^{m-s} & se \quad (q-1) | \boldsymbol{e} \\ 0 & se \quad c.c. \end{cases}$$

Teorema 2.28. *Para cada f, existe uma única extensão não-ramificada de grau f, a qual pode ser obtida pela adjunção de uma $(p^f - 1)-$ésima raiz primitiva da unidade.*

Demonstração. Existência: Temos que $\mathbb{F}_{p^f}^* =< \overline{\alpha} >$ é ciclico, logo $\mathbb{F}_p(\overline{\alpha})$ é uma extensão de $\mathbb{F}_p$ de grau f, ou seja, tem um polinômio minimal de $\overline{\alpha}$ sobre $\mathbb{F}_p$. Seja

$$\overline{g}(X) = X^f + \overline{a}_{f-1} X^{f-1} + \cdots + \overline{a}_0.$$

Para cada $j = 0, 1, \ldots, f-1, f$, seja $a_j \in \mathbb{Z}_p$ que se reduz a $\overline{a}_j$ módulo p. Assim, temos o seguinte polinômio

$$g(X) = X^f + a_{f-1} X^{f-1} + \cdots + a_0,$$

que é irredutível em $\mathbb{Q}_p$ (caso contrário, $\overline{g}(X)$ não seria irredutível, pois poderíamos fatorizar $g(X)$ como o produto de polinômios em $\mathbb{Z}_p$ que daria uma fatorização de $\overline{g}(X)$ quando reduzissimos $g(X)$ módulo p). Seja, então $\alpha \in \overline{\mathbb{Q}}_p$ uma raiz de $g(X)$, assim, temos que $\mathbb{Q}_p(\alpha)$ é uma extensão de grau f de $\mathbb{Q}$. Mas a classe lateral $\alpha + \mathfrak{p}_{\mathbb{Q}_p(\alpha)}$ é uma raiz

do polinômio irredutível $\overline{g}(X)$, ou seja, $\kappa_{\mathbb{Q}_p(\alpha)}$ é uma extensão de $\mathbb{F}_p$ de grau f. Portanto, $\mathbb{Q}_p(\alpha)$ é uma extensão não-ramificada de $\mathbb{Q}_p$, e a existência está provada.

Unicidade: Seja $\mathbb{K}$ uma extensão não-ramificada de $\mathbb{Q}_p$, assim $[\mathbb{K}:\mathbb{Q}_p] = f$, onde f é o grau da classe residual. Sabemos que $\kappa = \mathcal{O}_{\mathbb{K}}/\mathfrak{p}_{\mathbb{K}} = \mathbb{F}_{p^f}$, e seja $\overline{\alpha} \in \mathbb{F}_{p^f}$ o gerador do grupo multiplicativo $\mathbb{F}_{p^f}^{\times}$ tal que $\alpha_0 \in \mathcal{O}_{\mathbb{K}}$ é um elemento que se reduz a $\overline{\alpha}$ módulo π, onde π é um uniformizador (e, portanto, gerador de $\mathfrak{p}_{\mathbb{K}}$).

Pela versão dada acima do Lema de Hensel, temos que existe $\alpha \in \mathcal{O}_{\mathbb{K}}$, $\alpha \equiv \alpha_0 (mod \pi)$ tal que $\alpha^{p^f-1}-1 = 0$. Mas, sejam $\overline{\alpha}, \overline{\alpha}^2, \ldots, \overline{\alpha}^{p^f-1}$ as reduções módulo $\mathfrak{p}_{\mathbb{K}}$ de $\alpha, \alpha^2, \ldots, \alpha^{p^f-1}$, respectivamente. Como $\overline{\alpha}, \overline{\alpha}^2, \ldots, \overline{\alpha}^{p^f-1}$ são distintos, então $\alpha, \alpha^2, \ldots, \alpha^{p^f-1}$ também o são. Portanto α é uma $(p^f-1)-$ésima raiz da unidade, assim $[\mathbb{Q}_p(\alpha):\mathbb{Q}_p] \geq f$.

Mas, pelo corolário 2.26, $\mathbb{K}$ contém α, assim $\mathbb{Q}_p(\alpha) \subset \mathbb{K}$. Logo, $f = [\mathbb{K}:\mathbb{Q}_p] \geq [\mathbb{Q}_p(\alpha):\mathbb{Q}_p] \geq f$, ou seja, $\mathbb{K} = \mathbb{Q}_p(\alpha)$. A unicidade se segue.

□

Capítulo 3

Somas Exponenciais e Aplicações

3.1 Soma Exponencial

Como ja mencionamos anteriormente, as Somas Exponenciais são uma ferramenta extremamente útil na hora de calcularmos o número de soluções de um dado polinômio sobre $\mathbb{F}_q$, onde $q = p^f$ e f é inteiro. Mas antes de darmos uma definição formal de Soma Exponencial, devemos definir o que vem a ser um caráter aditivo.

Definição 18. *Seja $\mathbb{F}_q$ o corpo finito com q elementos. Diremos que Ψ é um caráter aditivo sobre $\mathbb{F}_q$ se Ψ é um homomorfismo de $\mathbb{F}_q$ para $\mathbb{C}$, tal que $\Psi(x) = \exp(\frac{2i\pi Tr(x)}{p})$ $\forall x \in \mathbb{F}_q$. Assim, temos que $\Psi(x+y) = \Psi(x)\Psi(y)$ $\forall x, y \in \mathbb{F}_q$.*

Definição 19. *Seja, agora, um polinômio $F(x_1, x_2, ..., x_m)$ em $\mathbb{F}_q[X_1, X_2, ..., X_m]$. Temos que a Soma Exponencial de Ψ associada a $F(X_1, X_2, ..., X_m)$ será definida aqui por:*

$$S(F) = \sum_{x_1, x_2, ..., x_m \in \mathbb{F}_q} \Psi(F(x_1, x_2, ..., x_m)),$$

onde Ψ é um carater aditivo não-trivial sobre $\mathbb{F}_q$.

Observação:A partir deste ponto, quando nos referirmos à divisibilidade de uma soma exponencial estaremos nos referindo à valorização $p-$ádica (ou $\pi-$ádica, conforme menção) de tal soma exponencial.

Observe que, como Ψ é um caráter aditivo, se $F(x_1, x_2, ..., x_m) = G(x_1, x_2, ..., x_m) + \beta$ onde $G(0, 0, ..., 0) = 0$, então

$$S(F) = \sum_{x_1, x_2, ..., x_m \in \mathbb{F}_q} \Psi(F(x_1, x_2, ..., x_m))$$

$$= \sum_{x_1, x_2, ..., x_m \in \mathbb{F}_q} \Psi(G(x_1, x_2, ..., x_m) + \beta) = \Psi(\beta) \sum_{x_1, x_2, ..., x_m \in \mathbb{F}_q} \Psi(G(x_1, x_2, ..., x_m)),$$

portanto o termo constante não afetará a divisibilidade da soma exponencial, com isso, de agora em diante, consideraremos que $F(x_1, x_2, ..., x_m)$ contém todas as variáveis e não possui termo constante.

Assim, temos então $\mathbb{K}$ como sendo a extensão única e não-ramificada de $\mathbb{Q}_p$ de grau f. Sejam $q = p^f$, $\mathcal{O}_{\mathbb{K}}$ e $\mathfrak{p}_{\mathbb{K}}$, respectivamente, o anel de valorização e seu ideal maximal. $\mathbb{K}$ pode ser obtido pela adjunção de uma $(q-1)$-ésima raiz primitiva da unidade em $\mathbb{Q}_p$. Denotemos $\mathbb{T}$ como o conjunto dos representantes de Teichm*ü*ller de $\mathbb{F}_q$ em $\mathbb{K}$. Seja ξ uma p-ésima raiz primitiva da unidade e seja $\mathbb{K}(\xi)$ a extensão de grau $p-1$ sobre $\mathbb{K}$.

Temos que o polinômio

$$F(x) = \frac{(x+1)^p - 1}{x}$$

é um polinômio minimal para $\xi - 1$. Assim, teremos que $N_{\mathbb{K}(\xi)/\mathbb{Q}_p}(\xi - 1) = p$, portanto $|\xi - 1| = p^{-1/(p-1)}$. Com isso,

$$\nu_p(\xi - 1) = \frac{1}{p-1}.$$

Assim, temos que $\pi = \xi - 1$ é um uniformizador. Sejam também $\mathcal{O}_{\mathbb{K}(\xi)}$ o anel de inteiros de $\mathbb{K}(\xi)$ e $\mathfrak{p}_{\mathbb{K}(\xi)}$ o ideal maximal correspondente gerado por π. Temos que $[\mathbb{K}(\xi) : \mathbb{Q}_p] = (p-1)f$ e

$$\mathbb{F}_q \cong \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}_{\mathbb{K}}} \cong \frac{\mathcal{O}_{\mathbb{K}(\xi)}}{\mathfrak{p}_{\mathbb{K}(\xi)}}.$$

3.2 Limitação da Divisibilidade de uma Soma Exponencial

No próximo momento vamos direcionar nossos estudos em busca de uma limitação da divisibilidade em π da soma exponencial de um polinômio. Antes disso, vamos achar um modo de calcular a valorização com respeito a π, para isso precisaremos do Teorema de Stickelberger e do seguinte lema:

Lema 3.1. *([2]) Existe um polinômio único*

$$C(X) = \sum_{l=0}^{q-1} c(l)X^l \in \mathbb{K}(\xi)[X]$$

de grau $q-1$ tal que:

$$C(t) = \xi^{Tr_{\mathbb{K}}(t)}, \forall t \in \mathbb{T}$$

Onde $Tr_{\mathbb{K}}(t)$ é o traço de $\mathbb{K}$ sobre $\mathbb{Q}_p$. Além disso, os coeficientes de $C(X)$ satisfazem:

$$c(0) = 1,$$

$$(q-1)c(q-1) = -q,$$

$$(q-1)c(j) = g(j), \forall 0 < j < q-1$$

onde $g(j)$ é a soma de Gauss:

$$g(j) = \sum_{t \in \mathbb{T}} t^{-j} \xi^{Tr_{\mathbb{K}}(t)}.$$

Também precisaremos do Teorema de Stickelberger:

Teorema 3.2 (Stickelberger)**.** *([22, 20]) Para $0 \leq j < q-1$:*

$$\frac{g(j)\rho_p(j)}{\pi^{\sigma_p(j)}} \equiv -1 \pmod{\pi},$$

onde $\rho_p(j) = \prod_{m=0}^{n-1} j_m!$ e $j = \sum_{m=0}^{n-1} j_m p^m$.

Agora podemos usar o Teorema de Stickelberger para calcularmos a valorização dos coeficientes de $C(X)$, portanto podemos tirar do Lema 3.1 e do Teorema 3.2 anteriores a seguinte consequência:

Lema 3.3. *Para $\alpha \in \mathbb{K}(\xi)$, seja $\nu_\pi(\alpha)$ a valorização com respeito a π. Então*

$$\nu_\pi(c(j)) = \sigma_p(j).$$

Demonstração. Se $j = 0$, então $c(j) = 1$, portanto $\nu_\pi(c(0)) = \nu_\pi(1) = 0 = \sigma_p(0)$, e o lema está provado. Agora para $0 < j < q-1$ temos que, $(q-1)c(j) = g(j)$. Pelo Teorema de Stickelberger, temos que:

$$\begin{aligned} k\pi &= \frac{g(j)\rho_p(j)}{\pi^{\sigma_p(j)}} + 1 \\ \Rightarrow k\pi^{\sigma_p(j)+1} &= g(j)\rho_p(j) + \pi^{\sigma_p(j)} \\ \Rightarrow k\pi^{\sigma_p(j)+1} - \pi^{\sigma_p(j)} &= g(j)\rho_p(j) \\ \Rightarrow \pi^{\sigma_p(j)}(k\pi - 1) &= g(j)\rho_p(j), \end{aligned}$$

então temos que:

$$\nu_\pi(c(j)) = \sigma_p(j).$$

□

Agora ja podemos achar uma limitação para a divisibilidade em π da soma exponencial de um polinomio usando o seguinte teorema:

Teorema 3.4. *Seja $\mathbb{F}_q$ o corpo finito com $q = p^f$ elementos e seja o polinômio sobre $\mathbb{F}_q$ com N termos e m variáveis dado por:*

$$F(X_1, \ldots, X_m) = \sum_{j=1}^{N} \overline{a_j} X_1^{e_{1j}} \cdots X_m^{e_{mj}}, \overline{a_j} \in \mathbb{F}_q^*.$$

Para um vetor $\vec{v}$, seja $supp(\vec{v})$ o número de entradas não-nulas em $\vec{v}$. Se $S(F)$ é a soma exponencial:

$$S(F(X_1, \cdots, X_m)) = \sum_{(x_1,\ldots,x_m)\in\mathbb{F}_q^m} \Psi(F(x_1, \ldots, x_m)),$$

então:

$$\nu(S(F)) \geq L,$$

onde

$$L = min_{l_1,\ldots,l_N}\{\sum_{j=1}^{N} \sigma_p(l_j) + f(p-1)(m - supp(l_1\vec{e_1} + \cdots + l_N\vec{e_N}))\},$$

onde o mínimo é tomado sobre todos $(l_1, \ldots, l_N) \in \{0, 1, \ldots, q-1\}^N$ tais que $q-1$ divide $l_1\vec{e_1} + \cdots + l_N\vec{e_N}$. Ou seja:

$$L = min_{l_1,\ldots,l_N}\{\sum_{j=1}^{N} \sigma_p(l_j)\}$$

e $(l_1, \ldots, l_N)$ é uma solução para o sistema de equações modulares:

$$e_{11}l_1 + e_{12}l_2 + \cdots + e_{1N}l_N \equiv 0(mod(q-1))$$

$$\vdots$$

$$e_{m1}l_1 + \cdots + e_{mN}l_N \equiv 0(mod(q-1)),$$

onde $\sum_{j=1}^{N} e_{ij}l_j \neq 0$, para $i = 0, \ldots, m$.

Demonstração. Vamos denotar por $a_j \in \mathbb{T}$, o representante de Teichmüller do coeficiente $\overline{a_j} \in \mathbb{F}_q$. Com isso, temos que a soma exponencial $S(F)$ é elevada para:

$$\begin{aligned}
S(F) &= \sum_{(x_1,\ldots,x_m)\in\mathbb{F}_q^m} \Psi(F(x_1, \ldots, x_m)) \\
&= \sum_{(x_1,\ldots,x_m)\in\mathbb{F}_q^m} \Psi(\sum_{j=1}^{N} \overline{a_j} X_1^{e_{1j}} \cdots X_m^{e_{mj}}) \\
&= \sum_{(x_1,\ldots,x_m)\in\mathbb{F}_q^m} \prod_{j=1}^{N} \Psi(\overline{a_j} X_1^{e_{1j}} \cdots X_m^{e_{mj}}) \\
&= \sum_{(x_1,\ldots,x_m)\in\mathbb{F}_q^m} \prod_{j=1}^{N} e^{\frac{2i\pi Tr(\overline{a_j} X_1^{e_{1j}} \cdots X_m^{e_{mj}})}{p}}
\end{aligned}$$

$$= \sum_{(x_1,\ldots,x_m)\in\mathbb{F}_q^m} \prod_{j=1}^{N} (e^{\frac{2i\pi}{p}})^{Tr(\overline{a_j}X_1^{e_{1j}}\cdots X_m^{e_{mj}})} = \sum_{(x_1,\ldots,x_m)\in\mathbb{F}_q^m} \prod_{j=1}^{N} \xi^{Tr(\overline{a_j}X_1^{e_{1j}}\cdots X_m^{e_{mj}})}$$

$$= \sum_{\vec{t}\in\mathbb{T}^m} \prod_{j=1}^{N} \xi^{Tr(a_j(\vec{t})^{\vec{e_j}})} = \sum_{\vec{t}\in\mathbb{T}^m} \prod_{j=1}^{N} C(a_j\vec{t}),$$

pelo Lema 3.1 . Substituindo os coeficientes de $C(X)$, temos que:

$$S(F) = \sum_{\vec{t}\in\mathbb{T}^m} \prod_{j=1}^{N} \sum_{l_j=0}^{q-1} c(l_j) {a_j}^{l_j} (\vec{t})^{l_j\vec{e_j}}$$

$$= \sum_{l_1=0}^{q-1} \cdots \sum_{l_N=0}^{q-1} \sum_{\vec{t}\in\mathbb{T}^m} \left[\prod_{j=1}^{N} c(l_j)\right] \left[\prod_{j=1}^{N} {a_j}^{l_j}\right] (\vec{t})^{l_1\vec{e}_1+\cdots+l_N\vec{e}_N}$$

$$= \sum_{l_1=0}^{q-1} \cdots \sum_{l_N=0}^{q-1} \left[\prod_{j=1}^{N} c(l_j)\right] \left[\sum_{\vec{t}\in\mathbb{T}^m} (\vec{t})^{l_1\vec{e}_1+\cdots+l_N\vec{e}_N}\right] \left[\prod_{j=1}^{N} {a_j}^{l_j}\right].$$

Vamos chamar o termo $\left[\prod_{j=1}^{N} c(l_j)\right] \left[\sum_{\vec{t}\in\mathbb{T}^m} (\vec{t})^{l_1\vec{e}_1+\cdots+l_N\vec{e}_N}\right] \left[\prod_{j=1}^{N} {a_j}^{l_j}\right]$ de T. Agora usando o Lema 2.27 temos que nós podemos restringir o somatório em T para os $(l_1,\ldots,l_N)$ tais que $q-1$ divide o vetor $\sum_j l_j\vec{e}_j$, uma vez que $\sum_{\vec{t}} (\vec{t})^{l_1\vec{e}_1+\cdots+l_N\vec{e}_N}$ é nulo caso contrário. Dessa forma, seja:

$$s = supp(\sum_{j=1}^{N} l_j\vec{e}_j),$$

o número de entradas que são multiplos positivos de $q-1$. Temos que $0 \leq s \leq m$ e

$$\sum_{\vec{t}\in\mathbb{T}^m} (\vec{t})^{l_1\vec{e}_1+\cdots+l_N\vec{e}_N} = (q-1)^s q^{m-s},$$

também pelo lema 2.27. Também temos que a valorização com respeito a π é:

$$\nu_\pi(\sum_{\vec{t}\in\mathbb{T}} (\vec{t})^{l_1\vec{e}_1+\cdots+l_N\vec{e}_N}) = \nu_\pi((q-1)^s q^{m-s}) = f(p-1)(m-s).$$

Por outro lado, pelo Lema 3.3, temos que a valorização de $c(l_j)$ é $\sigma_p(l_j)$, portanto:

$$\nu_\pi(\prod_{j=1}^{N} c(l_j)) = \sum_{j=1}^{N} \nu_\pi(c(l_j)) = \sum_{j=1}^{N} \sigma_p(l_j)$$

Com isso, temos que os coeficientes de $\prod_{j=1}^{N} a_j^{l_j}$ em T têm valorização:

$$\nu_\pi(\prod_{j=1}^{N} c(l_j) \prod_{\vec{t}\in\mathbb{T}^m} (\vec{t})^{l_1\vec{e}_1+\cdots+l_N\vec{e}_N}) = \sum_{j=1}^{N} \sigma_p(l_j) + f(p-1)(m-s)$$

O valor de L definido no enunciado do teorema é a divisibilidade mínima em π dos coeficientes de $a_1^{l_1} \cdots a_N^{l_N}$ tais que $q-1$ divide $\sum_{j=1}^{N} l_j \vec{e}_j$.

Como $\overline{a_j} \neq 0$, então $\nu_\pi(a_j) = 0$. Logo, temos que:

$$\nu_\pi(S(F)) \geq min_{l_1,\ldots,l_N} \nu_\pi(c(l_1)\cdots c(l_N) \sum_{\vec{t}\in\mathbb{T}} (\vec{t})^{l_1\vec{e}_1+\cdots+l_N\vec{e}_N}) = L.$$

□

3.3 Resultados de Carlitz e o Problema de Waring

Seja a seguinte equação $X_1^d + X_2^d + \cdots + X_n^d = \beta$, onde $\beta \in \mathbb{N}$. Como já mencionamos anteriormente, o Problema de Waring consiste em achar o número mínimo de variáveis para que tal equação tenha solução para todo β, esse número mínimo de variáveis será chamado de Número de Waring associado a d. Em nossos estudos, vamos considerar uma generalização para o Problema de Waring em corpos finitos, de fato, seja $F(X)$ um polinômio sobre $\mathbb{F}_q$, queremos achar o número mínimo de variáveis tal que:

$$F(X_1) + \cdots + F(X_n) = \beta$$

tenha solução em $\mathbb{F}_q$ para todo $\beta \in \mathbb{F}_q$. De forma análoga, podemos considerar o problemna da seguinte forma: Dados polinômios $F_1(X_1), \ldots, F_n(X_n)$ sobre $\mathbb{F}_q$, queremos achar condições tais que todo $\beta \in \mathbb{F}_q$ pode ser escrito na forma:

$$\beta = F_1(x_1) + \cdots + F_n(x_n),$$

onde $x_1, \ldots, x_n \in \mathbb{F}_q$. Vamos denotar o número que queremos achar por $\gamma(F, q)$.

O caminho para estudarmos tal generalização do Problema de Waring, será construido por meio de uma outra generalização. Na verdade, iremos, num primeiro momento, generalizar três resultados de Carlitz de 1956([3]) sobre o número de soluções de sistemas de polinômios sobre corpos finitos. Eis o primeiro resultado:

Teorema 3.5. *Se $F(X_1, \ldots, X_n)$ é um polinômio homogêneo de grau n enquanto $G(X_1, \ldots, X_n)$ é um polinômio de grau menor que n, e*

$$\sum_{x_1,\ldots,x_n\in\mathbb{F}_q} F^{q-1}(x_1, \ldots, x_n) \neq 0,$$

então a equação $F(X_1, \ldots, X_n) = G(X_1, \ldots, X_n)$ tem solução sobre $\mathbb{F}_q$.

O resultado do Teorema é bastante forte, mas uma das hipóteses não é tão simples de ser verificada, de fato nem sempre será fácil verificar que $\sum_{\vec{x}\in\mathbb{F}_q^n} F^{q-1} \neq 0$. Temos dois resultados que não precisam de tal hipótese.

Teorema 3.6. *Seja d um divisor de $p-1$ e $a_i \in \mathbb{F}_q^*$ para $i = 1, \ldots, d$. Se $G(X_1, \ldots, X_d)$ é um polinômio sobre $\mathbb{F}_q$ tal que grau$(G) < d$, então a equação $a_1 X_1^d + \cdots + a_n X_n^d + G(X_1, \ldots, X_n) = 0$ tem solução em $\mathbb{F}_q$.*

Corolário 3.7. *Seja d um divisor de $p-1$ e $F_1(X_1), \ldots, F_d(X_d)$ polinômios sobre $\mathbb{F}_q$ de grau d. Então a equação $F_1(X_1) + \cdots + F_d(X_d) = 0$ tem solução em $\mathbb{F}_q$.*

De fato, no corolário acima já podemos inserir um $\beta \in \mathbb{F}_q$ no lugar do 0 e o corolário continua válido, o que já nos direciona para o caminho da generalização que queremos. Na verdade, vamos melhorar a condição do grau dos polinômios e vamos substituir essa hipótese pelo peso desses mesmos polinômios.

3.4 Divisibilidade Exata de uma Soma Exponencial e Solução de Equações

Nessa seção iremos provar teoremas que resultam em uma divisibilidade exata de uma soma exponencial, dessa forma vamos generalizar o corolário de Carlitz e , como consequência teremos a generealização do problema de Waring que queremos. Na verdade, vamos utilizar um lema que relaciona o número de zeros de um sistema de polinômios $P_1(X_1, \ldots, X_n), \ldots, P_t(X_1, \ldots, X_n)$ e a soma exponencial $\sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \Psi(F(x_1, \ldots, x_n))$.

Lema 3.8. *([1]) Sejam $q = p^f$, $P_1(X_1, \ldots, X_n), \ldots, P_t(X_1, \ldots, X_n)$ polinômios sobre $\mathbb{F}_q$ e seja N o número de zeros comuns de $P_1(X_1, \ldots, X_n), \ldots, P_t(X_1, \ldots, X_n)$. Então,*

$$N = p^{-tf} \sum_{x_1,\ldots,x_n,y_1,\ldots,y_t \in \mathbb{F}_q} \Psi(y_1 P_1(x_1, \ldots, x_n) + \cdots + y_t P_t(x_1, \ldots, x_n)).$$

Agora, podemos computar a exata divisibilidade de certas somas exponenciais e o número de soluções das equações relacionadas, dessa forma, podemos garantir que tais equações são solúveis e então podemos obter a generalização do Problema de Waring.

Teorema 3.9. *Seja d_i um divisor de $p-1$ e $a_i \in \mathbb{F}_q^*$ para $i = 1, \ldots, t$. Considere os monômios*

$$(X_{i_1} \cdots X_{i_{n_1}})^{d_1}, (X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2}, \ldots, (X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t}$$

todos com o mesmo grau $d > 1$, suporte disjunto e $1 \leq i_j \leq n = n_t$. Se $G(X_1, \ldots, X_n)$ é um polinômio sobre $\mathbb{F}_q$ com $\omega_p(G) < d$, e

$$F(X_1, \ldots, X_n) = a_1 (X_{i_1} \cdots X_{i_{n_1}})^{d_1} + a_2 (X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2} + \cdots$$

$$+ a_t (X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} + G(X_1, \ldots, X_n),$$

então

$$\nu_\pi(S(F)) = f(p-1) \sum_{i=1}^{t} \frac{1}{d_i}.$$

Demonstração. Sem perda de generalidade, podemos supor que os monômios do enunciado do teorema podem ser escritos da forma:

$$(X_1 \cdots X_{n_1})^{d_1}(X_{n_1+1} \cdots X_{n_2})^{d_2} \cdots (X_{n_{t-1}+1} \cdots X_n)^{d_t},$$

e também podemos supor que $F(0, \ldots, 0) = 0$, pois, como vimos na primeira seção deste capítulo, termo constante não afetará a divisibilidade da soma exponencial de $F(X_1, \ldots, X_n)$. Seja $G(X_1, \ldots, X_n) = \sum_{r=1}^{N} b_r X_1^{e_{1r}} \cdots X_n^{e_{nr}}$.

No teorema que nos forneceu uma limitação para a soma exponencial de $F(X_1, \ldots, X_n)$ da segunda seção deste capítulo, nós associamos um sistema de equações módulo $(q-1)$ ao polinômio $F(X_1, \ldots, X_n)$. Aqui também faremos isso, então temos o seguinte sistema associado a $F(X_1, \ldots, X_n)$:

1)

$$d_1h_1 + e_{1,1}s_1 + e_{1,2}s_2 + \cdots + e_{1,N}s_N \equiv 0(mod(q-1))$$

$$\vdots$$

$$d_1h_1 + e_{n_1,1}s_1 + \cdots + e_{n_1,N}s_N \equiv 0(mod(q-1))$$

2)

$$d_2h_2 + e_{n_1+1,1}s_1 + \cdots + e_{n_1+1,N}s_N \equiv 0(mod(q-1))$$

$$\vdots$$

$$d_2h_2 + e_{n_2,1}s_1 + \cdots + e_{n_2,N}s_N \equiv 0(mod(q-1))$$

$\vdots$

t)

$$d_th_t + e_{n_{t-1}+1,1}s_1 + \cdots + e_{n_{t-1}+1,N}s_N \equiv 0(mod(q-1))$$

$$\vdots$$

$$d_th_t + e_{n,1}s_1 + \cdots + e_{n,N}s_N \equiv 0(mod(q-1))$$

Seja $(h_1, \ldots, h_t, s_1, \ldots, s_N)$ uma solução qualquer e não-trivial para o sistema. Como fizemos no teorema da limitação da divisibilidade da soma exponencial, onde associamos um termo T à solução do sistema, faremos exatamente o mesmo aqui. E da mesma forma, vamos calcular a valorização deste termo. Para isso, sejam $a_j^{'}$ e $b_r^{'}$, respectivamente, os representantes de Teichmüller de $a_j, b_r \in \mathbb{F}_q$ e $\mathbb{T}$ o grupo dos representantes de Teichmüller e vamos lembrar que ξ é uma raiz primitiva da unidade e que $C(X)$ é determinado pelo lema 3.1. Temos, num primeiro momento, que:

$$F(X_1, \ldots, X_n) = a_1(X_{i_1} \cdots X_{i_{n_1}})^{d_1} + a_2(X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2} + \cdots$$

$$+a_t(X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} + G(X_1, \ldots, X_n),$$

portanto, temos que:

$$S(F) = \sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \Psi(F(x_1,\ldots,x_n))$$

$$= \sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \Psi(a_1(x_{i_1}\cdots x_{i_{n_1}})^{d_1} + a_2(x_{i_{n_1+1}}\cdots x_{i_{n_2}})^{d_2} + \cdots$$

$$+a_t(x_{i_{n_{t-1}+1}}\cdots x_{i_n})^{d_t} + G(x_1,\ldots,x_n))$$

$$= \sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \left[\prod_{j=1}^{t} \Psi(a_j(x_{i_{n_{j-1}+1}}\cdots x_{i_{n_j}})^{d_j})\right] [\Psi(G(x_1,\ldots,x_n))]$$

$$= \sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \left[\prod_{j=1}^{t} e^{\frac{2i\pi Tr(a_j(x_{i_{n_{j-1}+1}}\cdots x_{i_{n_j}})^{d_j})}{p}}\right] [\Psi(G(x_1,\ldots,x_n))]$$

$$= \sum_{\mathbf{t}\in\mathbb{T}^n} \left[\prod_{j=1}^{t} \xi^{Tr(a_j^{'}\mathbf{t}^{\vec{d_j}})}\right] \left[\prod_{r=1}^{N} \xi^{Tr(b_r^{'}\mathbf{t}^{\vec{e_r}})}\right]$$

$$= \sum_{\mathbf{t}\in\mathbb{T}^n} \left[\prod_{j=1}^{t} C(a_j^{'}\mathbf{t}^{\vec{d_j}})\right] \left[\prod_{r=1}^{N} C(b_r^{'}\mathbf{t}^{\vec{e_r}})\right]$$

$$= \sum_{\mathbf{t}\in\mathbb{T}^n} \left[\prod_{j=1}^{t} (\sum_{h_j=0}^{q-1} c(h_j)(a_j^{'})^{h_j}\mathbf{t}^{\vec{d_j}h_j})\right] \left[\prod_{r=1}^{N} (\sum_{s_r=0}^{q-1} c(s_r)(b_r^{'})^{s_r}\mathbf{t}^{\vec{e_r}s_r})\right]$$

$$= \sum_{h_1=0}^{q-1}\cdots\sum_{h_t=0}^{q-1}\sum_{s_1=0}^{q-1}\cdots\sum_{s_N=0}^{q-1}\sum_{\mathbf{t}\in\mathbb{T}^n} \left\{\left[\prod_{j=1}^{t} c(h_j)\right]\left[\prod_{j=1}^{t}(a_j^{'})^{h_j}\right]\mathbf{t}^{\vec{d_1}h_1+\cdots+\vec{d_t}h_t}\right\}$$

$$\left\{\left[\prod_{r=1}^{N} c(s_r)\right]\left[\prod_{r=1}^{N}(b_r^{'})^{s_r}\right]\mathbf{t}^{\vec{e_1}s_1+\cdots+\vec{e_N}s_N}\right\}$$

$$= \sum_{h_1=0}^{q-1}\cdots\sum_{h_t=0}^{q-1}\sum_{s_1=0}^{q-1}\cdots\sum_{s_N=0}^{q-1} \left\{\left[\prod_{j=1}^{t} c(h_j)\right]\left[\sum_{\mathbf{t}\in\mathbb{T}^n}\mathbf{t}^{\vec{d_1}h_1+\cdots+\vec{d_t}h_t+\vec{e_1}s_1+\cdots+\vec{e_N}s_N}\right]\left[\prod_{j=1}^{t}(a_j^{'})^{h_j}\right]\right\}$$

$$\left\{\left[\prod_{r=1}^{N} c(s_r)\right]\left[\prod_{r=1}^{N}(b_r^{'})^{s_r}\right]\right\}$$

Assim temos o nosso termo T, e da mesma forma que fizemos no teorema 3.4, vamos calcular a valorização deste termo. Assim temos que:

$$\nu_\pi(T) = \sum_{i=1}^{t}\sigma_p(h_i) + \sum_{i=1}^{N}\sigma_p(s_i) + f(p-1)s,$$

onde s é o número de equações do nosso sistema iguais a zero. Seja $n_0 = 0$ e, para $i = 1,\ldots,t$, seja r_i o número de equações iguais a zero em cada i bloco de $n_i - n_{i-1}$

equações em nosso sistema. Uma vez que d_i é divisor de $p-1$, temos que $d_i \leq p-1$, logo $\sigma_p(d_i) = d_i$.

Agora, vamos aplicar a função peso em relação a p no primeiro bloco de equações do nosso sistema, usando a propriedades da função peso, teremos $n_1 - r_1$ inequações não-nulas. Somando-as e dividindo por $d_1 n_1$, temos:

$$\sigma_p(h_1) + \frac{\sigma_p(e_{1,1}) + \cdots + \sigma_p(e_{n_1,1})}{d_1 n_1}\sigma_p(s_1) + \cdots + \frac{\sigma_p(e_{1,N}) + \cdots + \sigma_p(e_{n_1,N})}{d_1 n_1}\sigma_p(s_N)$$

$$\geq \frac{f(p-1)(n_1 - r_1)}{n_1 d_1}.$$

Repetindo o mesmo processo para um bloco i arbitrário do sistema, obtemos:

$$\sigma_p(h_i) + \frac{\sigma_p(e_{n_{i-1}+1,1}) + \cdots + \sigma_p(e_{n_i,1})}{d_1(n_i - n_{i-1})}\sigma_p(s_1) + \cdots + \frac{\sigma_p(e_{n_{i-1}+1,N}) + \cdots + \sigma_p(e_{n_i,N})}{d_i(n_i - n_{i-1})}\sigma_p(s_N)$$

$$\geq \frac{f(p-1)(n_i - n_{i-1} - r_i)}{(n_i - n_{i-1})d_i}, \forall 1 \leq i \leq t.$$

Lembrando que $d_i(n_i - n_{i-1}) = d$, somamos as inequações dos t blocos e obtemos:

$$\sum_{i=1}^{t}\sigma_p(h_i) + \frac{\sigma(e_{1,1}) + \cdots + \sigma_p(e_{n,1})}{d}\sigma_p(s_1) + \cdots + \frac{\sigma_p(e_{1,N}) + \cdots + \sigma_p(e_{n,N})}{d}\sigma_p(s_N)$$

$$\geq f(p-1)\sum_{i=1}^{t}\frac{n_i - n_{i-1} - r_i}{(n_i - n_{i-1})d_i}$$

Como $\sigma_p(e_{1,k}) + \cdots + \sigma_p(e_{n,k})$ é o peso em relação a p do k-ésimo monômio de G e $\omega_p(G) < d$, então temos que $(\sigma_p(e_{1,k}) + \cdots + \sigma_p(e_{n,k}))/d < 1$. Com isso, temos que:

$$\sum_{i=1}^{t}\sigma_p(h_i) + \sum_{i=1}^{N}\sigma_p(s_i) \geq \sum_{i=1}^{t}\sigma_p(h_i) + \frac{\sigma_p(e_{1,1}) + \cdots + \sigma_p(e_{n,1})}{d}\sigma_p(s_1)$$

$$+ \cdots + \frac{\sigma_p(e_{1,N}) + \cdots + \sigma_p(e_{n,N})}{d}\sigma_p(s_N) \geq f(p-1)\sum_{i=1}^{t}\frac{n_i - n_{i-1} - r_i}{(n_i - n_{i-1})d_i},$$

e,

$$\nu_\pi(T) \geq f(p-1)\left[\sum_{i=1}^{t}\frac{n_i - n_{i-1} - r_i}{(n_i - n_{i-1})d_i} + \sum_{i=1}^{t} r_i\right]$$

$$= f(p-1)\left[\sum_{i=1}^{t}\frac{1}{d_i} + \sum_{i=1}^{t}\frac{r_i\left[(n_i - n_{i-1})d_i - 1\right]}{(n_i - n_{i-1})d_i}\right].$$

Agora, temos que se $s_i \neq 0$ para algum i, a desigualdade é estrita e como $r_i\left[(n_i - n_{i-1})d_i - 1\right] \geq 0$, qualquer solução com $\nu_\pi(T) = f(p-1)\sum_{i=1}^{t} 1/d_i$ é mínima e tem $s_i = 0, \forall i = 1, \ldots, N$. Seja a seguinte solução para o sistema:

$$(\frac{\lambda_1(q-1)}{d_1}, \ldots, \frac{\lambda_t(q-1)}{d_t}, 0, \ldots, 0),$$

onde $0 \leq \lambda_i \leq d_i \forall i = 1, \ldots, t$. Então temos que:

$$\sum_{i=1}^{t} \sigma_p(h_i) + \sum_{i=1}^{N} \sigma_p(s_i) = \sum_{i=1}^{t} \sigma_p(\frac{\lambda_i(q-1)}{d_i})$$

$$= \sum_{i=1}^{t} \sigma_p(\frac{\lambda_i(p-1)}{d_i} \sum_{k=1}^{f} p^{f-k}) = f(p-1)\sum_{i=1}^{t} \frac{\lambda_i}{d_i},$$

e,

$$\nu_\pi(T) = f(p-1)\left[\sum_{i=1}^{t} \frac{\lambda_i}{d_i} + s\right],$$

onde s é o número de equações no sistema iguais a zero para esta solução.

Se $\lambda_i = 1\ \forall i = 1, \ldots, t$, então nenhuma das equações do sistema é nula e $\nu_\pi(T) = f(p-1)\sum_{i=1}^{t} 1/d_i$. Além disso, $((q-1)/d_1, \ldots, (q-1)/d_t, 0, \ldots, 0)$ é uma solução mínima. Qualquer solução mínima deve ser da forma $(\lambda_1(q-1)/d_1, \ldots, \lambda_t(q-1)/d_t, 0, \ldots, 0)$ e $\sum_{i=1}^{t}(r_i\left[(n_i - n_{i-1})d_i - 1\right])/(n_i - n_{i-1})d_i = 0$. Como $r_i\left[(n_i - n_{i-1})d_i - 1\right] \geq 0$, a soma é nula se, e somente se, $n_i - n_{i-1} = d_i = 1$ ou $r_i = 0\ \forall i = 1, \ldots, t$. Se $r_i \neq 0$ para algum i, então $n_i - n_{i-1} = d_i = 1$, portanto F tem grau 1, mas isso é uma contradição. Se $r_i = 0\ \forall i = 1, \ldots, t$, então $\lambda_i \geq 1\ \forall i$, $\nu_\pi(T) = f(p-1)\sum_{i=1}^{t} \lambda_i/d_i$, e isto é uma solução mínima se, e somente se, $\lambda_i = 1\ \forall i$. Com isso, $((q-1)/d_1, \ldots, (q-1)/d_t, 0, \ldots, 0)$ é a única solução mínima e $\nu_\pi(F) = f(p-1)\sum_{i=1}^{t} 1/d_i$. □

Temos dois corolários imediátos desse teorema.

Corolário 3.10. *Seja d um divisor de $p-1$, $nd > 1$ e $a \in \mathbb{F}_q^*$. Se $G(X_1, \ldots, X_n)$ é um polinômio sobre $\mathbb{F}_q$ com $\omega_p(G) < dn$, e*

$$F(X_1, \ldots, X_n) = aX_1^d \cdots X_n^d + G(X_1, \ldots, X_n),$$

então $\nu_\pi(S(F)) = f(p-1)/d$.

Corolário 3.11. *Seja $d \neq 1$ um divisor de $p-1$ e $a \in \mathbb{F}_q^*$. Se $F(X) = aX^d + b_1X^{d_1} + \cdots + b_rX^{d_r}$ é um polinômio sobre $\mathbb{F}_q$, onde $\sigma_p(d_i) < d$ para todo i, então $\nu_\pi(S(F)) = f(p-1)/d$. Portanto $S(F) \neq 0$.*

Agora que podemos calcular o valor exato da valorização de uma soma exponencial de um polinômio sobre $\mathbb{F}_q$, teremos como consequência, a possibilidade de calcularmos a divisibilidade exata do número de soluções de um sistema de polinômios sobre $\mathbb{F}_q$ por meio do seguinte teorema:

Teorema 3.12. *Seja d_i um divisor de $p-1$ e $a_i \in \mathbb{F}_q^*$ para $i = 1, \ldots, t$. Suponha que $\sum_{i=1}^{t} 1/d_i$ é inteiro e sejam os monômios:*

$$(X_{i_1} \cdots X_{i_{n_1}})^{d_1}, (X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2}, \ldots, (X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t},$$

todos com o mesmo grau $d > 1$, suporte disjunto e $1 \leq i_j \leq n = n_t$. Se $G(X_1, \ldots, X_n) = \sum_{r=1}^{N} b_r X_1^{e_{1r}} \cdots X_n^{e_{nr}}$ é um polinômio tal que $b_r \in \mathbb{F}_q$ para $r = 1, \ldots, N$ com $\omega_p(G) < d$ e

$$F(X_1, \ldots, X_n) = a_1(X_{i_1} \cdots X_{i_{n_1}})^{d_1} + a_2(X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2}$$

$$+ \cdots + a_t(X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} + G(X_1, \ldots, X_n),$$

então $p^{f(\sum_{i=1}^{t} 1/d_i - 1)}$ é a divisibilidade exata do número de soluções de $F = 0$. Em particular, o polinômio F tem solução sobre $\mathbb{F}_q$.

Demonstração. Seja:

$$F'(X_1, \ldots, X_n, Y) = y(F(X_1, \ldots, X_n)) =$$

$$= y(a_1(X_{i_1} \cdots X_{i_{n_1}})^{d_1} + a_2(X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2}$$
$$+ \cdots + a_t(X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} + G(X_1, \ldots, X_n)).$$

Pelo Lema 3.8, temos que o número de soluções de $F = 0$ é igual a $p^{-f} S(F')$, onde $S(F')$ é a soma exponencial do polinômio F'. Assim para descobrirmos a divisibilidade do número de soluções de $F = 0$, basta computarmos o valor da soma exponencial de F'. Para isso, vamos seguir os mesmos passos que fizemos para acharmos a divisibilidade da soma exponencial de F no teorema anterior, ou seja, vamos, num primeiro momento, associar um sistema de equações modulares ao polinômio F', depois vamos associar um termo T à solução e vamos calcular a valorização desse termo.

Temos o seguinte sistema associado a F', que será o mesmo sistema de F com a última equação adicional :

1)

$$d_1 h_1 + e_{1,1} s_1 + e_{1,2} s_2 + \cdots + e_{1,N} s_N \equiv 0 (mod(q-1))$$

$$\vdots$$

$$d_1 h_1 + e_{n_1,1} s_1 + \cdots + e_{n_1,N} s_N \equiv 0 (mod(q-1))$$

2)

$$d_2 h_2 + e_{n_1+1,1} s_1 + \cdots + e_{n_1+1,N} s_N \equiv 0 (mod(q-1))$$

$$\vdots$$

$$d_2 h_2 + e_{n_2,1} s_1 + \cdots + e_{n_2,N} s_N \equiv 0 (mod(q-1))$$

$\vdots$

t)

$$d_t h_t + e_{n_{t-1}+1,1} s_1 + \cdots + e_{n_{t-1}+1,N} s_N \equiv 0 (mod(q-1))$$

$$\vdots$$

$$d_t h_t + e_{n,1} s_1 + \cdots + e_{n,N} s_N \equiv 0 (mod(q-1))$$

$t+1$)

$$h_1 + \cdots + h_t + s_1 + \cdots + s_N \equiv 0 (mod(q-1))$$

Além disso, temos que achar o termo T associado à solução desse sistema. Sejam $a_j^{'}, b_r^{'} \in \mathbb{T}$ os representantes de Teichmüller respectivamente de $a_j, b_r \in \mathbb{F}_q$, $\mathbb{T}$ o conjunto dos representantes de Teichmüller de $\mathbb{F}_q$, ξ uma raiz p-ésima primitiva da unidade e Ψ um caráter aditivo. Temos que:

$$S(F^{'}) = \sum_{x_1,\ldots,x_n,y \in \mathbb{F}_q} \Psi(F^{'}(x_1,\ldots,x_n,y))$$

$$= \sum_{x_1,\ldots,x_n,y \in \mathbb{F}_q} \Psi(y(F(x_1,\ldots,x_n))$$

$$= \sum_{x_1,\ldots,x_n,y \in \mathbb{F}_q} \Psi(\sum_{j=1}^{t} y(a_j(x_{i_{n_{j-1}+1}} \cdots x_{i_{n_j}})^{d_j}) + \sum_{r=1}^{N} y b_r x_1^{e_{1r}} \cdots x_n^{e_{nr}})$$

$$= \sum_{x_1,\ldots,x_n,y \in \mathbb{F}_q} \left[\prod_{j=1}^{t} \Psi(y a_j(x_{i_{n_{j-1}+1}} \cdots x_{i_{n_j}})^{d_j})\right] \left[\prod_{r=1}^{N} \Psi(y b_r x_1^{e_{1r}} \cdots x_N^{e_{nr}})\right]$$

$$= \sum_{x_1,\ldots,x_n,y \in \mathbb{F}_q} \left[\prod_{j=1}^{t} (e^{\frac{2i\pi}{p}})^{Tr(y a_j(x_{i_{n_{j-1}+1}} \cdots x_{i_{n_j}})^{d_j})}\right] \left[\prod_{r=1}^{N} (e^{\frac{2i\pi}{p}})^{Tr(y b_r x_1^{e_{1r}} \cdots x_n^{e_{nr}})}\right]$$

$$= \sum_{x_1,\ldots,x_n,y \in \mathbb{F}_q} \left[\prod_{j=1}^{t} \xi^{Tr(y a_j(x_{i_{n_{j-1}+1}} \cdots x_{i_{n_j}})^{d_j})}\right] \left[\prod_{r=1}^{N} \xi^{Tr(y b_r x_1^{e_{1r}} \cdots x_n^{e_{nr}})}\right]$$

$$= \sum_{\mathbf{t} \in \mathbb{T}^n, u \in \mathbb{T}} \left[\prod_{j=1}^{t} C(u a_j^{'} \mathbf{t}^{d_j})\right] \left[\prod_{r=1}^{N} C(u b_r^{'} \mathbf{t}^{\mathbf{e}_r})\right],$$

onde $C(X)$ é o polinômio definido no lema 3.1 e $\mathbf{e} = (e_1, \ldots, e_n)$. Portanto:

$$S(F^{'}) = \sum_{\mathbf{t} \in \mathbb{T}^n, u \in \mathbb{T}} \left[\prod_{j=1}^{t} \sum_{h_j=0}^{q-1} c(h_j)(u a_j^{'})^{h_j} \mathbf{t}^{h_j d_j}\right] \left[\prod_{r=1}^{N} \sum_{s_r=0}^{q-1} c(s_r)(u b_r^{'})^{s_r} \mathbf{t}^{s_r \mathbf{e}_r}\right]$$

$$= \sum_{h_1=0}^{q-1} \cdots \sum_{h_t=0}^{q-1} \sum_{s_1=0}^{q-1} \cdots \sum_{s_r=0}^{q-1} \left\{ \left[\prod_{j=1}^{t} c(h_j) \right] \left[\sum_{\mathbf{t}\in\mathbb{T}^n, u\in\mathbb{T}} u^{h_j+s_r} \mathbf{t}^{h_1 d_1 + \cdots + h_t d_t + s_1 \mathbf{e}_1 + \cdots + s_N \mathbf{e}_N} \right] \left[\prod_{j=1}^{t} (a_j^{'})^{h_j} \right] \right\}$$

$$\left\{ \left[\prod_{r=1}^{N} c(s_r) \right] \left[\prod_{r=1}^{N} (b_r^{'})^{s_r} \right] \right\}.$$

Assim, temos nosso termo T, assim seguindo os mesmos passos do teorema 3.9, achamos:

$$\nu_p(T) \geq f(p-1) \left[\sum_{i=1}^{t} \frac{1}{d_i} + \sum_{i=1}^{t} \frac{r_i \left[(n_i - n_{i-1}) d_i - 1 \right]}{(n_i - n_{i-1}) d_i} + \alpha \right],$$

onde $\alpha = 1$ se $h_1 + \cdots + h_t + s_1 + \cdots + s_N = 0$ e $\alpha = 0$ caso contrário. Se nós tivermos $s_i \neq 0$ para algum i, então temos:

$$\nu_\pi(T) \geq f(p-1) \left[\sum_{i=1}^{t} \frac{1}{d_i} + \sum_{i=1}^{t} \frac{r_1 \left[(n_i - n_{i-1}) d_i - 1 \right]}{(n_i - n_{i-1}) d_i} + \alpha \right].$$

Além disso, temos que:

$$\sum_{i=1}^{t} \frac{r_i \left[(n_i - n_{i-1}) d_i - 1 \right]}{(n_i - n_{i-1}) d_i} + \alpha \geq 0$$

e temos que qualquer solução com $\nu_\pi(T) = f(p-1) \sum_{i=1}^{t} 1/d_i$ é mínima e tem $s_i = 0$ $\forall i = 1, \ldots, N$. Temos também que:

$$(\frac{\lambda_1(q-1)}{d_1}, \ldots, \frac{\lambda_t(q-1)}{d_t}, 0, \ldots, 0)$$

é uma solução para o nosso sistema se, e somente se, $\sum_{i=1}^{t} \lambda_i/d_i \in \mathbb{Z}$. Como $\sum_{i=1}^{t} 1/d_i$ é inteiro, então:

$$(\frac{q-1}{d_1}, \ldots, \frac{q-1}{d_t}, 0, \ldots, 0),$$

é uma solução mínima. Qualquer outra solução mínima deve ter a forma

$$(\frac{\lambda_1(q-1)}{d_1}, \ldots, \frac{\lambda_t(q-1)}{d_t}, 0, \ldots, 0)$$

e

$$\sum_{i=1}^{t} \frac{r_i \left[(n_i - n_{i-1}) d_i - 1 \right]}{(n_i - n_{i-1}) d_i} + \alpha = 0.$$

Logo, temos que:

$$\nu_\pi(T) = f(p-1) \left[\sum_{i=1}^{t} \frac{\lambda_i}{d_i} \right],$$

mas isso é uma solução mínima se, e somente se, $\lambda_i = 1$ para todo $i = 1, \ldots, t$. Com isso ,

$$(\frac{q-1}{d_1}, \ldots, \frac{q-1}{d_t}, 0, \ldots, 0)$$

é a única solução mínima para o sistema. Assim, temos que:

$$\nu_\pi(T) = f(p-1)\left[\sum_{i=1}^{t} \frac{1}{d_i}\right],$$

lembrando que o número de soluções de $F = 0$ é $p^{-f}S(F')$, temos que $p^{f(\sum_{i=1}^{t} 1/d_i - 1)}$ é a exata divisibilidade do número de soluções de $F = 0$. □

Como corolário desse teorema, podemos obter uma generalização do segundo resultado de Carlitz exposto na seção anterior, de fato, vamos substituir a condição do grau do polinômio pelo peso em relação a p. Assim teremos:

Corolário 3.13. *Seja $d > 1$ um divisor de $p-1$ e $a_i \in \mathbb{F}_q^*$ para $i = 1, \ldots, d$. Se $G(X_1, \ldots, X_d)$ é um polinômio sobre $\mathbb{F}_q$ com $\omega_p(G) < d$, então a equação*

$$a_1 X_1^d + \cdots + a_d X_d^d + G(X_1, \ldots, X_d) = 0$$

tem solução sobre $\mathbb{F}_q$.

Exemplo 3. *Seja*

$$F(X_1, \ldots, X_7) = X_1^7 + X_2^7 + \cdots + X_7^7 + \sum_{k<j} a_{k,j} X_k X_j + X_1^{29^k+1} + \cdots + X_7^{29^k+1}$$

sobre $\mathbb{F}_{29^f}$. Então a equação $F = \beta$ tem solução para todo $\beta \in \mathbb{F}_{29^f}$.

Para encaminhar nossos estudos no sentido do nosso objetivo, vamos agora usar uma hipótese sobre o valor parcial peso em relação a p de monômios do polinômio estudado a fim de calcular o valor exato da divisibilidade da nossa soma exponencial. Esse resultado está explícito no teorema a seguir.

Teorema 3.14. *Seja $d_i > 1$ um divisor de $p-1$ e $a_i \in \mathbb{F}_q^*$ para $i = 1, \ldots, n$. Sejam $G_1, \ldots, G_N$ monômios. Se $G(X_1, \ldots, X_n) = G_1 + \cdots + G_N$ é um polinômio sobre $\mathbb{F}_q$ com $\sum_{i=1}^{n} \omega_{p,X_i}(G_j)/d_i < 1$ para $j = 1, \ldots, N$, e $F = a_1 X_1^{d_1} + \cdots + a_n X_n^{d_n} + G(X_1, \ldots, X_n)$, então*

$$\nu_\pi(S(F)) = f(p-1)\sum_{i=1}^{n} \frac{1}{d_i}.$$

Demonstração. Seja $G(X_1, \ldots, X_n) = \sum_{r=1}^{N} b_r X_1^{d_{1r}} \cdots X_n^{d_{nr}}$. Podemos supor, sem perda de generalidade, que $G(0, \ldots, 0) = 0$, pois, como vimos, termo constante não afeta a divisibilidade da soma exponencial. Temos o seguinte sistema de equações modulares associada ao polinômio F:

$$d_1h_1 + d_{11}s_1 + \cdots + d_{1N}s_N \equiv 0(mod(q-1))$$
$$\vdots$$
$$d_nh_n + d_{n1}s_1 + \cdots + d_{nN}s_N \equiv 0(mod(q-1)).$$

Seja $(h_1, \ldots, h_n, s_1, \ldots, s_N)$ uma solução para o sistema. Aplicando a função peso em relação a p em cada uma das equações do nosso sistema obtemos:

$$\sigma_p(d_i)\sigma_p(h_i) + \sigma_p(d_{i1})\sigma_p(s_1) + \cdots + \sigma_p(d_{iN})\sigma_p(s_N) \geq \alpha_i\sigma_p(q-1) = \alpha_i f(p-1),$$

onde $\alpha_i = 0$ ou $\alpha_i = 1$.

Como $d_i \leq p-1$, então $\sigma_p(d_i) = d_i$. Dividindo a inequação acima por d_i temos que

$$\sigma_p(h_i) + \frac{\sigma_p(d_{i1})}{d_i}\sigma_p(s_1) + \cdots + \frac{\sigma_p(d_{iN})}{d_i}\sigma_p(s_N) \geq \frac{\alpha_i f(p-1)}{d_i}$$

para $i = 1, \ldots, n$.

Pela definição de peso de um monômio em relação a p com respeito a uma variável X_i, temos que $\sum_{i=1}^{n}\sigma_p(d_{ij}) = \sum_{i=1}^{n}\omega_{p,X_i}(G_j)$, para todo $j = 1, \ldots, N$. Lembrando que $\sum_{i=1}^{n}\omega_{p,X_i}(G_j)/d_i < 1$ por hipótese, vamos somar todas as inequações para obter:

$$\sum_{i=1}^{n}\sigma_p(h_i) + \sum_{i=1}^{N}\sigma_p(s_i) \geq$$

$$\sum_{i=1}^{n}\sigma_p(h_i) + \sum_{i=1}^{n}\frac{\sigma_p(d_{i1})}{d_i}\sigma_p(s_1) + \cdots + \sum_{i=1}^{n}\frac{\sigma_p(d_{iN})}{d_i}\sigma_p(s_N) \geq f(p-1)\sum_{i=1}^{n}\frac{\alpha_i}{d_i}.$$

Sendo $\sum_{i=1}^{n}(1-\alpha_i)$ o número de equações iguais a zero em nosso sistema e T o termo associado à solução (da mesma forma que nos outros teoremas), então temos que:

$$\nu_\pi(T) = \sum_{i=1}^{n}\sigma_p(h_i) + \sum_{i=1}^{N}\sigma_p(s_i) + f(p-1)\sum_{i=1}^{n}(1-\alpha_i)$$

Assim, temos que:

$$\nu_\pi(T) \geq f(p-1)\left[\sum_{i=1}^{n}\frac{\alpha_i}{d_i} + \sum_{i=1}^{n}(1-\alpha_i)\right]$$

$$= f(p-1)\left[\sum_{i=1}^{n}\frac{1}{d_i} + \sum_{i=1}^{n}\frac{(1-\alpha_i)(d_i-1)}{d_i}\right].$$

Seguindo exatamente o mesmo raciocínio da demonstração do teorema 3.9, temos que, se $s_i \neq 0$ para algum i, então a desigualdade acima é estrita e , como $(1-\alpha_i)(d_i-1) \geq 0$, então qualquer solução com

$$\nu_\pi(T) = f(p-1)\sum_{i=1}^{n}\frac{1}{d_i}$$

é mínima e tem $s_i = 0$ para todo i.

Seja a seguinte solução para o nosso sistema:

$$(\frac{q-1}{d_1}, \ldots, \frac{q-1}{d_n}, 0, \ldots, 0)$$

Temos que, para essa solução:

$$\sum_{i=1}^{n}\sigma_p(h_i) + \sum_{i=1}^{N}\sigma_p(s_i) = f(p-1)\sum_{i=1}^{n}\frac{1}{d_i}.$$

Portanto, essa solução é mínima. Qualquer outra solução com $s_1 = \cdots = s_N = 0$ tem $h_i = \lambda_i(q-1)/d_i$ para $0 \leq \lambda_i \leq d_i$ e

$$\nu_\pi(T) = \sum_{i=1}^{n}\sigma_p(h_i) + \sum_{i=1}^{N}\sigma_p(s_i) + f(p-1)s = f(p-1)\left[\sum_{i=1}^{n}\frac{\lambda_i}{d_i} + s\right],$$

onde s é o número de equações iguais a zero em nosso sistema para $(\frac{\lambda_1(q-1)}{d_1}, \ldots, \frac{\lambda_n(q-1)}{d_n}, 0, \ldots, 0)$. Para essa solução ser mínima deveremos ter $\sum_{i=1}^{n}(1-\alpha_i)(d_i-1) = 0$. Se $1-\alpha_i \neq 0$ para algum i, então $d_i = 1$, o que, por hipótese, é uma contradição. Se $1-\alpha_i = 0$ para todo i, então $\nu_\pi(T) = f(p-1)\sum_{i=1}^{n}\lambda_i/d_i$, que é mínima se, e somente se, $\lambda_i = 1$ para todo i.

Assim

$$(\frac{q-1}{d_1}, \ldots, \frac{q-1}{d_n}, 0, \ldots, 0),$$

é a única solução mínima e

$$\nu_\pi(T) = f(p-1)\sum_{i=1}^{n}\frac{1}{d_i}.$$

□

Capítulo 4

Uma Generalização do Problema de Waring

Neste capítulo, finalmente chegaremos ao nosso último objetivo e daremos uma generealização do problema de Waring. Como já mencionamos anteriormente, o problema de Waring consiste em achar o número de Waring, o qual é definido da seguinte forma:

Definição 20. *Seja a seguinte equação*

$$X_1^d + \cdots + X_n^d = \beta, \beta \in \mathbb{N}$$

Vamos chamar de Número de Waring associado a d, o número mínimo de variáveis tal que a equação acima tem solução em $\mathbb{Z}$ para todo $\beta \in \mathbb{N}$.

Em nossos estudos, vamos nos preocupar com um problema um pouco diferenciado. Dado um polinômio $F(X)$ sobre $\mathbb{F}_q$, vamos tentar achar o número mínimo de variáveis tal que

$$F(X_1) + \cdots + F(X_n) = \beta$$

tem solução em $\mathbb{F}_q$ para todo $\beta \in \mathbb{F}_q$. Vamos denotar esse número por $\gamma(F, q)$. De forma análoga, podemos considerar o seguinte problema: Dados polinômios $F_1(X), \ldots, F_n(X)$ todos sobre $\mathbb{F}_q$, queremos achar condições tais que todo $\beta \in \mathbb{F}_q$ possa ser escrito como

$$\beta = F_1(x_1) + \cdots + F_n(x_n),$$

onde $x_1, \ldots, x_n \in \mathbb{F}_q$.

É fácil observar que a segunda versão do nosso problema é mais razoável, tendo em vista os resultados expostos até aqui, de fato, para acharmos as condições necessárias para a solução do nosso problema vamos, num primeiro momento, precisar do seguinte resultado:

Teorema 4.1 (Castro,Rubio,Vega)**.** *Seja $d_i > 1$ um divisor de $p-1$ e $a_i \in \mathbb{F}_q$ para $i = 1, \ldots, n$. Suponha que $\sum_{i=1}^n 1/d_i$ é inteiro, e sejam $G_1, \ldots, G_N$ monômios. Se $G(X_1, \ldots, X_n) =$*

$G_1 + \cdots + G_N$ é um polinômio sobre $\mathbb{F}_q$ com $\sum_{i=1}^{n} \omega_{p,X_i}(G_j)/d_i < 1$ para $j = 1, \ldots, N$, e $F(X_1, \ldots, X_n) = a_1X_1^{d_1} + \cdots + a_nX_n^{d_n} + G(X_1, \ldots, X_n)$, então a exata divisibilidade do número de soluções de $F = 0$ é $p^{f(\sum_{i=1}^{n} 1/d_i - 1)}$. Em particular, a equação $F = 0$ tem solução em $\mathbb{F}_q$

Demonstração. A demonstração desse teorema é análoga a demonstração do teorema 3.12. De fato, queremos achar algumas condições tais que tenhamos alguma informação sobre o número de soluções de $F = 0$, mas já sabemos, pelo lema 3.8, que o número de soluções de $F = 0$ é $p^{-f}S(F^{'})$, onde

$$\begin{aligned} F^{'} &= yF \\ &= y(a_1X_1^{d_1} + \cdots + a_nX_n^{d_n} + G(X_1, \ldots, X_n)) \\ &= y(a_1X_1^{d_1} + \cdots + a_nX_n^{d_n} + G_1 + \cdots + G_N), \end{aligned}$$

onde $y \in \mathbb{F}_q$ e $G_i = b_iX_1^{d_{1i}} \cdots X_n^{d_{ni}}$ para $i = 1, \ldots, N$.

Basta, portanto, computar o valor de $S(F^{'})$. Para isso, vamos seguir os mesmos passos que foram executados anteriormente, ou seja, vamos associar um sistema de equações modulares a $F^{'}$, um termo T associado à solução desse sistema e, então, vamos achar a valorização desse termo T.

Num primeiro momento, temos que o sistema associado a $F^{'}$ é o mesmo de F com a equação adicional $h_1 + \cdots + h_n + s_1 + \cdots + s_N \equiv 0(mod(q-1))$, então, temos o seguinte sistema de equações modulares associado a $F^{'}$:

$$d_1h_1 + d_{11}s_1 + \cdots + d_{1N}s_N \equiv 0(mod(q-1))$$

$$\vdots$$

$$d_nh_n + d_{n1}s_1 + \cdots + d_{nN}s_N \equiv 0(mod(q-1))$$

$$h_1 + \cdots + h_n + s_1 + \cdots + s_N \equiv 0(mod(q-1))$$

Seja $(h_1, \ldots, h_n, s_1, \ldots, s_N)$ uma solução qualquer para o sistema, vamos então calcular o termo T associado a essa solução. Sejam $a_j^{'}$ e $b_r^{'}$, respectivamente, os representantes de Teichmüller de $a_j, b_r \in \mathbb{F}_q$ e $\mathbb{T}$ o grupo dos representantes de Teichmüller, $\mathbf{d}_r = (d_{1r}, \ldots, d_{nr})$ para $r = 1, \ldots, N$ e vamos lembrar que ξ é uma raiz primitiva da unidade e que $C(X)$ é determinado pelo lema 3.1. Temos que:

$$S(F^{'}) = \sum_{x_1,\ldots,x_n,y \in \mathbb{F}_q} \Psi(F^{'}(x_1, \ldots, x_n, y))$$

$$= \sum_{x_1,\ldots,x_n,y\in\mathbb{F}_q} \Psi(y(F(x_1,\ldots,x_n)))$$

$$= \sum_{x_1,\ldots,x_n,y\in\mathbb{F}_q} \Psi(y(a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}+G_1+\cdots+G_N))$$

$$= \sum_{x_1,\ldots,x_n,y\in\mathbb{F}_q} \Psi(\sum_{j=1}^{n} ya_jx_j^{d_j}+\sum_{r=1}^{N} yb_rx_1^{d_{1r}}\cdots x_n^{d_{nr}})$$

$$= \sum_{x_1,\ldots,x_n,y\in\mathbb{F}_q} \left[\Psi(\sum_{j=1}^{n} ya_jx_j^{d_j})\right]\left[\Psi(\sum_{r=1}^{N} yb_rx_1^{d_{1r}}\cdots x_n^{d_{nr}})\right]$$

$$= \sum_{x_1,\ldots,x_n,y\in\mathbb{F}_q} \left[\prod_{j=1}^{n} \Psi(ya_jx_j^{d_j})\right]\left[\prod_{r=1}^{N} \Psi(yb_rx_1^{d_{1r}}\cdots x_n^{d_{nr}})\right]$$

$$= \sum_{x_1,\ldots,x_n,y\in\mathbb{F}_q} \left[\prod_{j=1}^{n} (e^{\frac{2\pi i}{p}})^{Tr(ya_jx_j^{d_j})}\right]\left[\prod_{r=1}^{N} (e^{\frac{2\pi i}{p}})^{Tr(yb_rx_1^{d_{1r}}\cdots x_n^{d_{nr}})}\right]$$

$$= \sum_{\mathbf{t}\in\mathbb{T}^n,t\in\mathbb{T}} \left[\prod_{j=1}^{n} \xi^{Tr(ta_j'\mathbf{t}^{d_j})}\right]\left[\prod_{r=1}^{N} \xi^{Tr(tb_r'\mathbf{t}^{\mathbf{d}_r})}\right]$$

$$= \sum_{\mathbf{t}\in\mathbb{T}^n,t\in\mathbb{T}} \left[\prod_{j=1}^{n} C(ta_j'\mathbf{t}^{d_j})\right]\left[\prod_{r=1}^{N} C(tb_r'\mathbf{t}^{\mathbf{d}_r})\right]$$

$$= \sum_{\mathbf{t}\in\mathbb{T}^n,t\in\mathbb{T}} \left\{\prod_{j=1}^{n}\left[\sum_{h_j=0}^{q-1} c(h_j)(ta_j')^{h_j}(\mathbf{t})^{d_jh_j}\right]\right\}\left\{\prod_{r=1}^{N}\left[\sum_{s_r=0}^{q-1} c(s_r)(tb_r')^{s_r}(\mathbf{t})^{\mathbf{d}_rs_r}\right]\right\}$$

$$= \sum_{h_1=0}^{q-1}\cdots\sum_{h_n=0}^{q-1}\sum_{s_1=0}^{q-1}\cdots\sum_{s_N=0}^{q-1}\sum_{\mathbf{t}\in\mathbb{T}^n,t\in\mathbb{T}} \left\{\left[\prod_{j=1}^{n} c(h_j)\right]\left[\prod_{j=1}^{n}(ta_j')^{h_j}\right](\mathbf{t})^{d_1h_1+\cdots+d_nh_n}\right\}$$

$$\left\{\left[\prod_{r=1}^{N} c(s_r)\right]\left[\prod_{r=1}^{N}(tb_r')^{s_r}\right](\mathbf{t})^{\mathbf{d}_1s_1+\cdots+\mathbf{d}_Ns_N}\right\}$$

$$= \sum_{h_1=0}^{q-1} \cdots \sum_{h_n=0}^{q-1} \sum_{s_1=0}^{q-1} \cdots \sum_{s_N=0}^{q-1} \left\{ \left[\prod_{j=1}^{n} c(h_j) \right] \left[\sum_{\mathbf{t}\in\mathbb{T}^n, t\in\mathbb{T}} (\mathbf{t})^{d_1h_1+\cdots+d_nh_n+\mathbf{d}_1s_1+\cdots+\mathbf{d}_Ns_N} \right] \left[\prod_{j=1}^{n} (ta_j^{'})^{h_j} \right] \right\}$$

$$\left\{ \left[\prod_{r=1}^{N} c(s_r) \right] \left[\prod_{r=1}^{N} (tb_r^{'})^{s_r} \right] \right\}$$

Assim, temos agora nosso termo T, portanto, usando o lema 2.27 e o lema 3.3, temos que

$$\nu_\pi(T) = \sum_{j=1}^{n} \sigma_p(h_j) + \sum_{r=1}^{N} \sigma_p(s_r) + f(p-1)k,$$

onde k é o número de equações iguais a zero em nosso sistema.

Agora, aplicando a função peso em relação a p em uma das primeiras n equações e usando a proposição 2.16 obtemos:

$$\sigma_p(d_i)\sigma_p(h_i) + \sigma_p(d_{i1})\sigma_p(s_1) + \cdots + \sigma_p(d_{iN})\sigma_p(s_N) \geq \alpha_i\sigma_p(q-1) = \alpha_i f(p-1),$$

onde $\alpha_i = 0$ ou $\alpha_i = 1$ para $i = 1, \ldots, n$.

Como $d_i \leq p-1$, $\sigma_p(d_i) = d_i$. Dividindo a desigualdade acima por d_i, obtemos agora:

$$\sigma_p(h_i) + \frac{\sigma_p(d_{i1})}{d_i}\sigma_p(s_1) + \cdots + \frac{\sigma_p(d_{iN})}{d_i}\sigma_p(s_N) \geq \frac{\alpha_i f(p-1)}{d_i},$$

para $i = 1, \ldots, n$.

Sabendo que $\sum_{i=1}^{n} \sigma_p(d_{ij}) = \sum_{i=1}^{n} \omega_{p,X_i}(G_j)$ para $j = 1, \ldots, N$, somando as n primeiras desigualdades obtidas do sistema e usando o fato que $\sum_{i=1}^{n} \omega_{p,X_i}(G_j)/d_i < 1$, temos

$$\sum_{i=1}^{n} \sigma_p(h_i) + \sum_{r=1}^{N} \sigma_p(s_r) \geq$$

$$\sum_{i=1}^{n} \sigma_p(h_i) + \sum_{i=1}^{n} \frac{\sigma_p(d_{i1})}{d_i}\sigma_p(s_1) + \cdots + \sum_{i=1}^{n} \frac{\sigma_p(d_{iN})}{d_i}\sigma_p(s_N) \geq f(p-1)\sum_{i=1}^{n} \frac{\alpha_i}{d_i}$$

Agora, se $\sum_{i=1}^{n}(1-\alpha_i)$ é o número de equações iguais a zero no bloco das primeiras n equações em nosso sistema e $\alpha = 1$ se $h_1 + \cdots + h_n + s_1 + \cdots + s_N = 0$ e $\alpha = 0$ caso contrário, então

$$k = \sum_{i=1}^{n}(1-\alpha_i) + \alpha.$$

Portanto, temos que:

$$\nu_\pi(T) \geq f(p-1)\left[\sum_{i=1}^{n}\frac{\alpha_i}{d_i}+\sum_{i=1}^{n}(1-\alpha_i)+\alpha\right]$$

$$= f(p-1)\left[\sum_{i=1}^{n}\frac{1}{d_i}+\sum_{i=1}^{n}\frac{(1-\alpha_i)(d_i-1)}{d_i}+\alpha\right].$$

Agora, temos que se $s_i \neq 0$ para algum i, teremos desigualdade estrita acima, e como

$$\sum_{i=1}^{n}\frac{(1-\alpha_i)(d_i-1)}{d_i}+\alpha \geq 0,$$

então qualquer solução de nosso sistema que fornece $\nu_\pi(T) = f(p-1)\sum_{i=1}^{n} 1/d_i$ é mínima e tem $s_i = 0$ para todo $i = 1, \ldots, N$.

Temos que

$$(\frac{q-1}{d_1}, \ldots, \frac{q-1}{d_n}, 0, \ldots, 0)$$

é uma solução, pois, por hipótese, $\sum_{i=1}^{n} 1/d_i \in \mathbb{Z}$. Qualquer outra solução mínima deve ter a forma

$$(\frac{\lambda_1(q-1)}{d_1}, \ldots, \frac{\lambda_n(q-1)}{d_n}, 0, \ldots, 0)$$

e

$$\sum_{i=1}^{n}\frac{(1-\alpha_i)(d_i-1)}{d_i}+\alpha = 0.$$

Portanto,

$$\nu_\pi(T) = f(p-1)\left[\sum_{i=1}^{n}\frac{\lambda_i}{d_i}\right],$$

logo tal solução é mínima se, e somente se, $\lambda_i = 1$ para todo $i = 1, \ldots, n$. Com isso

$$(\frac{q-1}{d_1}, \ldots, \frac{q-1}{d_n}, 0, \ldots, 0)$$

é a única solução mínima. Assim, temos que

$$\nu_\pi(T) = f(p-1)\sum_{i=1}^{n}\frac{1}{d_i}.$$

Logo a exata divisibilidade do número N de soluções de $F = 0$ é $p^{f(\sum_{i=1}^{n} 1/d_i - 1)}$, pois $N = p^{-f}S(F')$. □

Exemplo 4. *Seja* $F(X_1, \ldots, X_7) = X_1^{10} + \cdots + X_4^{10} + X_5^5 + X_6^5 + X_7^5 + X_1X_2X_3 + X_4X_5X_6X_7$ *sobre* $\mathbb{F}_{31}$. *Então* $F = \beta$ *tem solução para todo* $\beta \in \mathbb{F}_{31^f}$.

Temos que o seguinte corolário generaliza o corolário 3.7:

Corolário 4.2. *Seja $d > 1$ um divisor de $p-1$, e suponha que n/d é inteiro. Se $F_i(X_i) = a_i X_i^d + G_i(X_i)$ é um polinômio sobre $\mathbb{F}_q$ com $\omega_p(G_i) < d$ para todo i, então a divisibilidade exata do número de soluções de $F_1(X_1) + \cdots + F_n(X_n) = 0$ é $p^{f(n/d-1)}$. Em particular, a equação tem solução sobre $\mathbb{F}_q$.*

Exemplo 5. *Seja $p > 5$, $d = (p-1)/2$, e considere o polinômio*

$$F(X_1, \ldots, X_d) = X_1^d + \cdots + X_d^d + X_1^{p^i+1} + \cdots + X_d^{p^i+1}$$

sobre $\mathbb{F}_q$. Então $F = \beta$ tem solução sobre $\mathbb{F}_q$ para cada $\beta \in \mathbb{F}_q$.

Se $q = p^{2i}$, então a equação $X_1^{p^i+1} + \cdots + X_d^{p^i+1} = \beta$ não tem solução para todo $\beta \in \mathbb{F}_{p^{2i}} \backslash \mathbb{F}_{p^i}$. Mas com o corolário acima, os termos extras em $X_1^d + \cdots + X_d^d + X_1^{p^i+1} + \cdots + X_d^{p^i+1} = \beta$ garantem que a equação adicionada deles tem solução para todo $\beta \in \mathbb{F}_{p^{2i}}$.

Agora, poderemos finalmente provar o seguinte teorema, o qual é, de fato, uma consequência imediata do teorema anterior e justamente fornece as condições necessárias que procurávamos para a nossa generalização do problema de Waring.

Teorema 4.3 (Castro,Rubio,Vega)**.** *Seja $d_i > 1$ um divisor de $p-1$, $a_i \in \mathbb{F}_q^*$ e $F_i(X) = a_i X_i^{d_i} + G_i(X_i)$ polinômios sobre $\mathbb{F}_q$ para $i = 1, \ldots, n$. Suponha que $\sum_{i=1}^n 1/d_i$ seja um inteiro. Se $\omega_p(G_i) < d_i$, então todo $\beta \in \mathbb{F}_q$ pode ser escrito como*

$$\beta = F_1(x_1) + \cdots + F_n(x_n),$$

para $x_1, \ldots, x_n \in \mathbb{F}_q$.

Demonstração. A demonstração é trivial. Basta notar que, pelo teorema 4.1, temos que, para todo $\beta \in \mathbb{F}_q$

$$a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} + G_1(x_1) + \cdots + G_n(x_n) - \beta = 0$$

tem solução em $\mathbb{F}_q$. Assim o resultado se segue. □

Exemplo 6. *Sejam $F_1(X) = X_1^6 + X_1^{17}$, $F_2(X) = X_2^3 + X_2^{14}$, $F_3(X) = X_3^2 + X_3$ todos sobre $\mathbb{F}_{13^f}$. Então todo $\beta \in \mathbb{F}_{13^f}$ pode ser escrito como $\beta = x_1^6 + x_1^{17} + x_2^3 + x_2^{14} + x_3^2 + x_3$.*

Corolário 4.4. *Seja $F(X) = aX^d + G(X)$ um polinômio sobre $\mathbb{F}_q$, onde $d \neq 1$ divide $p-1$. Se $\omega_p(G) < d$, então $\gamma(F, q) \leq d$.*

Exemplo 7. *Seja $F(X) = X^3 + aX^{p^i+1}$ sobre $\mathbb{F}_q$ onde 3 divide $p-1$. Então $\gamma(F, q) \leq 3$. Usando Maple podemos obter $\gamma(x^3 + x^8, 49) = 2$ e $\gamma(x^3 + x^{14}, 169) = 2$. Podemos, também, observar que $\gamma(x^8, 49)$ e $\gamma(x^{14}, 169)$ não existem.*

Exemplo 8. *Seja $F(X) = X^4 + a_1 X^{p^{i_1}+p^{j_1}+1} + a_2 X^{p^{i_2}+p^{j_2}+1} + \cdots + a_n X^{p^{i_n}+p^{j_n}+1}$ sobre $\mathbb{F}_{29^f}$, então $\gamma(F, 29^f) \leq 4$.*

Referências Bibliográficas

[1] Adolphson and Sperber. p-adic estimates for exponential sums and the of chevalley-warning. *Ann. Sci. Ecole Norm. Sup.*, 20:545–556, 1987.

[2] Ax. Zeros of polynomials over finite fields. *Amer. J. Math.*, 86:255–261, 1964.

[3] Carlitz. Solvability of certain equations in a finite field. *Quart J. Math.*, 7:3–4, 1956.

[4] Mills Carlitz, Lewis and Straus. Polynomials over finite fields with minimal value sets. *Mathematika*, 8:121–130, 1961.

[5] Rubio Castro and Vega. Divisibility of exponential sums and solvability of certain equations over finite fields. *Quart. J. Math.*, 00:1–13, 2007.

[6] Pinner Cochrane and Rosenhouse. Bounds on exponential sums and the polynomial waring problem mod p. *J.London Math. Soc.*, 67:319–336, 2003.

[7] Hirzebruch Ebbinghaus, Hermes. *Numbers*. Springer-Verlag, 1991.

[8] Felszeghy. On the solvability of some special equations over finite fields. *Publ. Math. Debrecen*, 68:15–23, 2006.

[9] Garcia and Lequain. *Elementos de Álgebra*. IMPA : Projeto Euclides, 3 ed., 2005.

[10] Gonçalves. *Introdução à Álgebra*. IMPA : Projeto Euclides, 4 ed., 2006.

[11] Gouvêa. *p-adic Numbers: An Introduction*. Springer-Verlag, 2 ed., 1997.

[12] Hardy and Wright. *An Introduction to the Theory of Numbers*. Oxford: Oxford University Press, 6 ed., 2008.

[13] Heath-Brown and Konyagin. New bounds for gauss sums derived from kth powers, and for heilbronn's exponential sum. *Quart. J. Math.*, 51:221–235, 2000.

[14] Herstein. *Tópicos de Álgebra*. Editora Polígono S.A., 1970.

[15] Ireland and Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 2 ed., 1990.

[16] Katz. On a theorem of ax. *Amer. J. Math.*, 93:485–499, 1971.

[17] Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions.* Springer-Verlag, 2 ed., 1984.

[18] Konyagin. Estimates for gaussian sums and waring's problem modulo a prime. *Proc. Steklov Inst. Math.*, 01:105–117, 1994.

[19] Konyagin and Shparlinski. *Character Sums with Exponential Functions and Their Applications.* Cambridge University Press, Vol.136, 1999.

[20] Lang. *Cyclotomic Fields.* Springer, New york, 1978.

[21] Lidl and Niederreiter. *Finite Fields.* Cambridge: Cambridge University Press, 1997.

[22] Moreno. *Algebraic Curves Over Finite Fields.* Cambridge University Press, 1991.

[23] Castro Moreno, Shum and Kumar. Tight bounds for chevalley-warning- ax type estimates with improved applications. *Proc. London Math.Soc.*, 88:545–564, 2004.

[24] Soares Shokranian and Godinho. *Teoria dos Números.* Editora Universidade de Brasília, 2 ed., 1999.

[25] Soares. *Coleção Matemática Universitária: Cálculo em uma Variável Complexa.* IMPA, 4 ed., 2006.

[26] Winterhof. On waring's problem in finite fields. *Acta Arith.*, LXXXVII.2:171–177, 1998.