Hugo Rodrigues Teixeira

Generalização dos Teoremas de Chevalley-Warning e Ax-Katz

Belo Horizonte
2021

Hugo Rodrigues Teixeira

Generalização dos Teoremas de Chevalley-Warning e Ax-Katz

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, como parte dos requisitos para a obtenção do título de Mestre em Matemática.

Universidade Federal de Minas Gerais - UFMG

Orientador: Fabio Enrique Brochero Martínez

Belo Horizonte
2021

Teixeira, Hugo Rodrigues.

T266p Generalização dos Teoremas de Chevalley-Warning e Ax-Katz [manuscrito] / Hugo Rodrigues Teixeira.– 2021.
79 f. il.

Orientador: Fabio Enrique Brochero Martínez.
Dissertação (mestrado) - Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática.
Referências: f.79.

1. Matemática – Teses. 2. Corpos finitos (Algebra) – Teses. 3. Somas de Gauss – Teses. 4. Somas de Jacobi – Teses. I. Brochero Martínez, Fabio Enrique. II. Universidade Federal de Minas Gerais; Instituto de Ciências Exatas, Departamento de Matemática. III.Título.

CDU 51(043)

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa
CRB 6ª Região nº 1510

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
COLEGIADO DO CURSO DE GRADUAÇÃO / PÓS-GRADUAÇÃO EM MATEMÁTICA

FOLHA DE APROVAÇÃO

Generalização dos Teoremas de Chevalley-Warning e Ax-Katz

HUGO RODRIGUES TEIXEIRA

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

Prof. Fabio Enrique Brochero Martínez

UFMG

Prof. Hemar Godinho

UnB

Prof. John William MacQuarrie

UFMG

Prof. Sávio Ribas

UFOP

Belo Horizonte, 30 de abril de 2021.

Documento assinado eletronicamente por **Fabio Enrique Brochero Martinez**, **Professor do Magistério Superior**, em 30/04/2021, às 16:22, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Hemar Teixeira Godinho**, **Usuário Externo**, em 30/04/2021, às 16:26, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **John William Macquarrie**, **Professor do Magistério Superior**, em 30/04/2021, às 16:27, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Sávio Ribas**, **Usuário Externo**, em 30/04/2021, às 16:27, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0696511** e o código CRC **C7AF2A48**.

Referência: Processo nº 23072.221611/2021-84 SEI nº 0696511

Agradecimentos

Primeiramente gostaria de agradecer ao Professor Fabio Brochero por aceitar ser meu orientador. Obrigado por sua paciência, atenção e por sua confiança em mim.

Agradeço à minha família, em especial aos meus pais e ao meu irmão, por apoiarem todas as minhas decisões e me ajudarem a superar todos os problemas encontrados no caminho.

Agradeço aos Pilantras, ao Bonde e às Rolezeiras por serem meus amigos e estarem comigo sempre.

Agradeço à todos os professores, em especial aos professores Alberto Sarmiento, Carmen Rosa e Seme Gebara Neto, por todos os ensinamentos.

Agradeço à Aline e sua família por me incentivarem diariamente e por todos os momentos de descontração.

Por último, agradeço à CAPES pelo apoio financeiro.

Resumo

Nesta dissertação, apresentaremos algumas generalizações dos Teoremas de Ax-Katz e Chevalley-Warning. O objetivo delas é encontrar a maior potência do primo p que divide o número de soluções de um sistema polinomial sobre o corpo $\mathbb{F}_q$, com $char(\mathbb{F}_q) = p$. Apresentaremos também algumas propriedades das somas de Gauss e de Jacobi, para obter a congruência de Stickelberger, e faremos uma introdução aos números p-ádicos, conceitos necessários para a prova do Teorema de Ax.

Palavras-chave: Corpos finitos, Teorema de Chevalley-Warning, Teorema de Ax-Katz, Soma de Gauss, Soma de Jacobi, Congruência de Stickelberger, Números p-ádicos.

Abstract

In this dissertation, we will present some generalizations of the Ax-Katz and Chevalley-Warning Theorems. Their goal is to find the greatest power of the prime p that divides the number of solutions of a polynomial system over $\mathbb{F}_q$, with $char(\mathbb{F}_q) = p$. We will also present some properties of Gauss and Jacobi sums, in order to obtain Stickelberger's congruence, and an introduction to the p-adic numbers, concepts needed in the proof of Ax's Theorem.

Keywords: Finite Fields, Ax-Katz Theorem, Chevalley-Warning Theorem, Gauss Sum, Jacobi Sum, Stickelberger's Congruence, p-adic Numbers.

Sumário

1 Introdução

Ao longo da dissertação, denotaremos por $\mathbb{F}_q$ o corpo com $q = p^f$ elementos, onde p é um primo ímpar e f um inteiro positivo.

Dado um polinômio com n variáveis e coeficientes no corpo finito $\mathbb{F}_q$, uma pergunta natural é: qual é o número de elementos em $\mathbb{F}_q^n$ que são raízes desse polinômio? Para polinômios de grau 2 é possível encontrar uma fórmula que responde essa pergunta, como veremos no Capítulo 2. Entretanto, para polinômios de grau arbitrário não é conhecida uma fórmula geral que soluciona esta pergunta.

Em 1935, Claude Chevalley [Chev35] contribuiu de maneira significativa para a solução desse problema. No mesmo ano, seu resultado foi melhorado por Ewald Warning com o Teorema de Chevalley-Warning ([War35]), que apresentaremos no Capítulo 3. Com ele descobrimos que o número de soluções do sistema polinomial é um múltiplo da característica do corpo base, caso a soma dos graus dos polinômios seja menor que o número de variáveis.

Anos depois, em 1964, James Ax obteve um resultado ainda melhor com as mesmas condições. O Teorema de Ax ([Ax64]) diz que o número de soluções é divisível por uma potência do número de elementos do corpo. Essa potência foi aprimorada por Nicholas Katz em 1971, o que atualmente é conhecido como o Teorema de Ax-Katz ([Ka71]). Este resultado será provado no Capítulo 9 desta dissertação.

Para demonstrar Teorema de Ax precisaremos de algumas ferramentas que serão discutidas nos Capítulos 4 a 8. No Capítulo 4 serão introduzidos caracteres aditivos e multiplicativos sobre $\mathbb{F}_q$ e as somas de Gauss e Jacobi associadas a eles. Em seguida, no Capítulo 5, serão apresentadas propriedades dos anéis de inteiros de $\mathbb{Q}(\zeta_m)$, onde ζ_m denota uma raiz m-ésima da unidade. Com essas propriedades, no Capítulo 6, obteremos a Congruência de Stickelberger (Teorema 6.18), que relaciona somas de Gauss e os resíduos módulo um ideal primo do anel de inteiros de $\mathbb{Q}(\zeta_p)$. Essa congruência será fundamental para a demonstração do Teorema de Ax.

O último ingrediente necessário para a prova do Teorema de Ax-Katz são os números p-ádicos, que serão apresentado no Capítulo 8. Eles são definidos a partir de uma valoração que relaciona cada número inteiro à maior potência do primo p que o divide. Essa valoração pode ser estendida para o corpo dos números racionais e ela determina uma norma não arquimediana, denominada norma p-ádica. Fazendo o completamento dos racionais com respeito a essa norma obtemos o corpo $\mathbb{Q}_p$. Os elementos de valoração positiva de $\mathbb{Q}_p$ formam um anel local e, fazendo o quociente desse anel pelo seu ideal maximal, obtemos um corpo isomorfo a $\mathbb{F}_p$. Tomando extensões algébricas de $\mathbb{Q}_p$, de maneira análoga, construímos um corpo isomorfo a $\mathbb{F}_q$.

Os Teoremas de Chevalley-Warning e Ax-Katz têm sido generalizados de várias maneiras ao longo dos anos. No Capítulo 10 apresentaremos algumas das generalizações presentes no artigo [BBC19], de 2017, que envolvem tomar graus parciais dos polinômios bem como composição com outras funções polinomiais.

2 Funções de segundo grau sobre $\mathbb{F}_q$

Dados $b \in \mathbb{F}_q$ e $g \in \mathbb{F}_q[x_1, \cdots, x_n]$ polinômio de grau 2, qual é o número de elementos $(c_1, \cdots, c_n)$ em $\mathbb{F}_q^n$ tais que $g(c_1, \cdots, c_n) = b$? Neste capítulo seguiremos o caminho apresentado no livro [LN], dividindo este problema em casos e, no final, apresentaremos uma fórmula que responderá a essa pergunta.

Para todo $g \in \mathbb{F}_q[x_1, \cdots, x_n]$, polinômio com coeficientes em $\mathbb{F}_q$, e $b \in \mathbb{F}_q$, denotaremos por $N(g = b) = \#\{(a_1, \cdots, a_n) \in \mathbb{F}_q^n \mid g(a_1, \cdots, a_n) = b\}$. Precisaremos do seguinte caracter.

Definição 2.1. *Se $b \in \mathbb{F}_q$, definimos*

$$\mathcal{X}(b) = \begin{cases} 1, & \textit{se } b \textit{ é um quadrado em } \mathbb{F}_q^* \\ -1, & \textit{se } b \textit{ não é um quadrado em } \mathbb{F}_q^* \\ 0, & \textit{se } b = 0. \end{cases}$$

$\mathcal{X}$ será chamado de o caracter quadrático sobre $\mathbb{F}_q$.

Como $\mathbb{F}_q^*$ é cíclico ([LN] Capítulo 1.2), se $a, b \in \mathbb{F}_q^*$ e γ é um gerador de $\mathbb{F}_q^*$, temos que $a = \gamma^s$ e $b = \gamma^t$, para certos s e t naturais. Assim, analisando as possibilidades de paridade para s, t e $s+t$, podemos concluir que $\mathcal{X}(\gamma^{s+t}) = \mathcal{X}(\gamma^s)\mathcal{X}(\gamma^t)$, ou seja, $\mathcal{X}$ é multiplicativo.

Definição 2.2. *Definimos $\mathcal{V}(b)$ como:*

$$\mathcal{V}(b) = \begin{cases} -1, & \textit{se } b \neq 0 \\ q-1, & \textit{se } b = 0. \end{cases}$$

Com isso, podemos mostrar o teorema a seguir.

Teorema 2.3. *Seja $g : \mathbb{F}_q^n \to \mathbb{F}_q$ definida por $g(x_1, \cdots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$, onde $a_1, \cdots, a_n \in \mathbb{F}_q^*$. Se $b \in \mathbb{F}_q$, então*

$$N(g(x_1, \cdots, x_n) = b) = \begin{cases} q^{n-1} + q^{\frac{n-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{n}{2}}a_1 \cdots a_n), & \textit{se } n \textit{ é par} \\ q^{n-1} + q^{\frac{n-1}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}a_1 \cdots a_n b), & \textit{se } n \textit{ é ímpar.} \end{cases}$$

Demonstração. Dividiremos esta demonstração em casos.

Caso 1: Começaremos com o caso $n = 1$, isto é, uma função da forma $g(x) = ax^2$.

$$N(ax^2 = b) = N\left(x^2 = \frac{b}{a}\right) = \begin{cases} 1, & \text{se } b = 0 \\ 2, & \text{se } \frac{b}{a} \text{ é um quadrado e } b \neq 0 \\ 0, & \text{se } \frac{b}{a} \text{ não é um quadrado.} \end{cases}$$

Ou, equivalentemente,

$$N(ax^2 = b) = 1 + \mathcal{X}\left(\frac{b}{a}\right) = 1 + \mathcal{X}(ab).$$

Caso 2: Agora, com a solução do caso anterior, vamos tomar uma função com duas variáveis. Portanto, seja $g(x_1, x_2) = a_1x_1^2 + a_2x_2^2$, com $a_1, a_2 \in \mathbb{F}_q^*$.

$$\begin{aligned}
N(a_1x_1^2 + a_2x_2^2 = b) &= \sum_{c_1+c_2=b} N(a_1x_1^2 = c_1)N(a_2x_2^2 = c_2) \\
&= \sum_{c_1+c_2=b} \left(1 + \mathcal{X}\left(\frac{c_1}{a_1}\right)\right)\left(1 + \mathcal{X}\left(\frac{c_2}{a_2}\right)\right) \\
&= \sum_{c_1+c_2=b} 1 + \mathcal{X}\left(\frac{c_1}{a_1}\right) + \mathcal{X}\left(\frac{c_2}{a_2}\right) + \mathcal{X}\left(\frac{c_1c_2}{a_1a_2}\right) \\
&= \sum_{c_1+c_2=b} 1 + \sum_{c_1+c_2=b} \mathcal{X}\left(\frac{c_1}{a_1}\right) + \sum_{c_1+c_2=b} \mathcal{X}\left(\frac{c_2}{a_2}\right) \\
&\quad + \sum_{c_1+c_2=b} \mathcal{X}\left(\frac{c_1c_2}{a_1a_2}\right).
\end{aligned}$$

Como $\frac{c_1}{a_1}$ e $\frac{c_2}{a_2}$ percorrem todos os elementos de $\mathbb{F}_q$, então $\sum_{c_1+c_2=b} \mathcal{X}\left(\frac{c_1}{a_1}\right) = \sum_{c_1+c_2=b} \mathcal{X}\left(\frac{c_2}{a_2}\right) = 0$, já que a quantidade de quadrados não nulos é igual à quantidade de não quadrados em $\mathbb{F}_q$ (para concluir isso, basta observar que o kernel de $g(x) = x^2$ aplicada no grupo multiplicativo $\mathbb{F}_q^*$ é o conjunto $\{-1, 1\}$ e, pelo Teorema do Isomorfismo de Grupos ([LN] Capítulo 1.1), temos que $|Im(g)| = \frac{|\mathbb{F}_q^*|}{2}$). Portanto

$$\begin{aligned}
N(a_1x_1^2 + a_2x_2^2 = b) &= q + \mathcal{X}(a_1a_2) \sum_{c_1+c_2=b} \mathcal{X}(c_1c_2) \\
&= q + \mathcal{X}(a_1a_2) \sum_{c\in\mathbb{F}_q^*} \mathcal{X}(c(b-c)) \\
&= q + \mathcal{X}(a_1a_2) \sum_{c\in\mathbb{F}_q^*} \mathcal{X}(c^2)\mathcal{X}\left(\frac{b}{c} - 1\right) \\
&= q + \mathcal{X}(a_1a_2) \sum_{c\in\mathbb{F}_q^*} \mathcal{X}\left(\frac{b}{c} - 1\right).
\end{aligned}$$

Se $b \neq 0$, então

$$N(a_1x_1^2 + a_2x_2^2 = b) = q + \mathcal{X}(a_1a_2)\big[\big(\sum_{d\in\mathbb{F}_q} \mathcal{X}(d)\big) - \mathcal{X}(-1)\big] = q - \mathcal{X}(-a_1a_2).$$

Se $b = 0$, então

$$N(a_1x_1^2 + a_2x_2^2 = b) = q + \mathcal{X}(a_1a_2) \sum_{c\in\mathbb{F}_q^*} \mathcal{X}(-1) = q + (q-1)\mathcal{X}(-a_1a_2).$$

Das duas relações anteriores, concluímos que

$$N(a_1x_1^2 + a_2x_2^2 = b) = q + \mathcal{V}(b)\mathcal{X}(-a_1a_2).$$

Caso 3: Por indução sobre o número de variáveis, suponhamos que o teorema é valido para menos do que n variáveis. Portanto, seja $g(x_1, \cdots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$, com $a_1, \cdots, a_n \in \mathbb{F}_q^*$.

Primeiramente, se n é ímpar, $n-1$ é par e, pela hipótese de indução, vale que

$$\begin{aligned}
N\left(\sum_{i=1}^{n} a_ix_i^2 = b\right) &= \sum_{c_1+c_2=b} N(a_1x_1^2 + \cdots + a_{n-1}x_{n-1}^2 = c_1)N(a_nx_n^2 = c_2) \\
&= \sum_{c_1+c_2=b} (q^{n-2} + q^{\frac{n-3}{2}}\mathcal{V}(c_1)\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_{n-1})) \\
&\qquad \cdot \left(1 + \mathcal{X}\left(\frac{c_2}{a_n}\right)\right) \\
&= \sum_{c_1+c_2=b} q^{n-2} + \sum_{c_1+c_2=b} q^{n-2}\mathcal{X}\left(\frac{c_2}{a_n}\right) \\
&\qquad + \sum_{c_1+c_2=b} q^{\frac{n-3}{2}}\mathcal{V}(c_1)\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_{n-1}) \\
&\qquad + \sum_{c_1+c_2=b} q^{\frac{n-3}{2}}\mathcal{V}(c_1)\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_{n-1})\mathcal{X}\left(\frac{c_2}{a_n}\right).
\end{aligned}$$

Observemos que $\sum_{c_1+c_2=b}\mathcal{V}(c_1) = 0$ e $\sum_{c_1+c_2=b}\mathcal{X}\left(\frac{c_2}{a_n}\right) = 0$, uma vez que c_1 e $\frac{c_2}{a_n}$ percorrem todos os elementos de $\mathbb{F}_q$. Observemos também que $\mathcal{X}(\frac{c_2}{a_n}) = \mathcal{X}(c_2a_n)$, pois se a^{-1} é um quadrado, então a também é. Assim,

$$\begin{aligned}
N\left(\sum_{i=1}^{n} a_ix_i^2 = b\right) &= \sum_{c_1+c_2=b} q^{n-2} + \sum_{c_1+c_2=b} q^{\frac{n-3}{2}}\mathcal{V}(c_1)\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_nc_2) \\
&= q^{n-1} + \sum_{c\in\mathbb{F}_q} q^{\frac{n-3}{2}}\mathcal{V}(b-c)\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_nc) \\
&= q^{n-1} + (q-1)q^{\frac{n-3}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_nb) \\
&\qquad - \sum_{c\in\mathbb{F}_q\setminus\{b\}} q^{\frac{n-3}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_nc) \\
&= q^{n-1} + (q-1)q^{\frac{n-3}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_nb) \\
&\qquad + q^{\frac{n-3}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_nb) \\
&= q^{n-1} + q^{\frac{n-1}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_nb).
\end{aligned}$$

Por outro lado, se n é par, $n-2$ também é. Logo, pela hipótese de indução, temos

$$
\begin{aligned}
N\left(\sum_{i=1}^{n} a_i x_i^2 = b\right) &= \sum_{c_1+c_2=b} N\left(\sum_{i=1}^{n-2} a_i x_i^2 = c_1\right) N(a_{n-1}x_{n-1}^2 + a_n x_n^2 = c_2)\\
&= \sum_{c_1+c_2=b} (q^{n-3} + q^{\frac{n-4}{2}}\mathcal{V}(c_1)\mathcal{X}((-1)^{\frac{n-2}{2}}a_1\cdots a_{n-2}))\\
&\qquad \cdot (q + \mathcal{V}(c_2)\mathcal{X}(-a_{n-1}a_n))\\
&= \sum_{c_1+c_2=b} q^{n-2} + \sum_{c_1+c_2=b} q^{\frac{n-2}{2}}\mathcal{V}(c_1)\mathcal{X}((-1)^{\frac{n-2}{2}}a_1\cdots a_{n-2})\\
&\qquad + \sum_{c_1+c_2=b} q^{n-3}\mathcal{V}(c_2)\mathcal{X}(-a_{n-1}a_n)\\
&\qquad + \sum_{c_1+c_2=b} q^{\frac{n-4}{2}}\mathcal{V}(c_1)\mathcal{V}(c_2)\mathcal{X}((-1)^{\frac{n}{2}}a_1\cdots a_n)\\
&= q^{n-1} + q^{\frac{n-4}{2}}\mathcal{X}((-1)^{\frac{n}{2}}a_1\cdots a_n)\sum_{c\in\mathbb{F}_q}\mathcal{V}(c)\mathcal{V}(b-c)
\end{aligned}
$$

Observemos que se $b=0$, então

$$
\begin{aligned}
\sum_{c\in\mathbb{F}_q}\mathcal{V}(c)\mathcal{V}(b-c) &= \mathcal{V}(0)^2 + \sum_{c\in\mathbb{F}_q^*}\mathcal{V}(c)\mathcal{V}(-c)\\
&= (q-1)^2 + (q-1)\\
&= (q-1)q\\
&= \mathcal{V}(b)q.
\end{aligned}
$$

Se $b\neq 0$, então

$$
\begin{aligned}
\sum_{c\in\mathbb{F}_q}\mathcal{V}(c)\mathcal{V}(b-c) &= -2(q-1) + \sum_{c\in\mathbb{F}_q\setminus\{0,b\}}\mathcal{V}(c)\mathcal{V}(b-c)\\
&= -2(q-1) + q - 2\\
&= -q\\
&= \mathcal{V}(b)q.
\end{aligned}
$$

Portanto,

$$
\begin{aligned}
N\left(\sum_{i=1}^{n} a_i x_i^2 = b\right) &= q^{n-1} + q^{\frac{n-4}{2}}\mathcal{X}((-1)^{\frac{n}{2}}a_1\cdots a_n)\mathcal{V}(b)q\\
&= q^{n-1} + q^{\frac{n-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{n}{2}}a_1\cdots a_n).
\end{aligned}
$$

Assim, concluímos que

$$
N\left(\sum_{i=1}^{n} a_i x_i^2 = b\right) = \begin{cases} q^{n-1} + q^{\frac{n-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{n}{2}}a_1\cdots a_n), & \text{se } n \text{ é par}\\ q^{n-1} + q^{\frac{n-1}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}a_1\cdots a_n b), & \text{se } n \text{ é ímpar.}\end{cases}
$$

$\square$

Exemplo 2.4. *Sejam $\mathbb{F}_{13} \cong \frac{\mathbb{Z}}{13\mathbb{Z}}$ o corpo com 13 elementos e*

$$g(x_1, x_2) = 7x_1^2 + 5x_2^2,$$

polinômio em $\mathbb{F}_{13}[x_1, x_2]$. Tomando $b = 2$, vamos encontrar o número de soluções para $g(x_1, x_2) = 2$. Aplicando o teorema anterior, temos:

$$\begin{aligned} N(g(x_1, x_2) = 2) =& 13 + \mathcal{V}(2)\mathcal{X}((-1) \cdot 7 \cdot 5) \\ =& 13 - \mathcal{X}(4) \\ =& 12. \end{aligned}$$

Portanto temos 12 soluções em $\mathbb{F}_{13}$ para $g(x_1, x_2) = 2$.

Exemplo 2.5. *Sejam $\mathbb{F}_{13} \cong \frac{\mathbb{Z}}{13\mathbb{Z}}$ o corpo com 13 elementos e*

$$g(x_1, x_2, x_3, x_4, x_5) = 3x_1^2 + 2x_2^2 + 10x_3^2 + 8x_4^2 + x_5^2,$$

polinômio em $\mathbb{F}_{13}[x_1, x_2, x_3, x_4, x_5]$. Desejamos encontrar o número de soluções para $g(x_1, x_2, x_3, x_4, x_5) = 6$. Nesse caso, pelo teorema anterior, como $n = 5$, temos:

$$\begin{aligned} N(g(x_1, x_2, x_3, x_4, x_5) = 6) =& 13^{5-1} + 13^{\frac{5-1}{2}}\mathcal{X}((-1)^{\frac{5-1}{2}} \cdot 3 \cdot 2 \cdot 10 \cdot 8 \cdot 1 \cdot 6) \\ =& 13^4 + 13^2\mathcal{X}(7). \end{aligned}$$

Como 7 não é um quadrado em $\mathbb{F}_{13}$, então $\mathcal{X}(7) = -1$ e

$$\begin{aligned} N(g(x_1, x_2, x_3, x_4, x_5) = 6) =& 13^4 - 13^2 \\ =& 28.392. \end{aligned}$$

Assim, temos 28.392 soluções em $\mathbb{F}_{13}^5$ para $g(x_1, x_2, x_3, x_4, x_5) = 6$.

Definição 2.6. *Se $g \in \mathbb{F}_q[x_1, \cdots, x_n]$ é um polinômio homogêneo de grau 2 (todos os seus monômios têm grau 2) ou o polinômio nulo, dizemos que g é uma forma quadrática em n variáveis.*

Duas formas quadráticas g e h são ditas equivalentes se g pode ser transformada em h por uma mudança linear de variáveis em $\mathbb{F}_q$.

Para toda forma quadrática $g(x_1, \cdots, x_n) = \sum_{1 \leq i,j \leq n} a_{i,j}x_ix_j$, associamos a matriz $A_{n\times n}$ cuja entrada (i, j) é o coeficiente $a_{i,j}$ de g, para todo $1 \leq i, j \leq n$.

Se $char(\mathbb{F}_q) \neq 2$, então $2^{-1} \in \mathbb{F}_q$. Assim, podemos reescrever $a_{i,j}x_ix_j$ como $2^{-1}a_{i,j}x_ix_j + 2^{-1}a_{i,j}x_jx_i$, para todo $1 \leq i < j \leq n$. Desta maneira temos que a matriz A associada à g é simétrica.

Para o próximo resultado, precisamos encontrar uma forma quadrática equivalente à $g(x_1, \cdots, x_n) = \sum_{1 \leq i,j \leq n} a_{i,j}x_ix_j$ cuja matriz associada seja diagonal. Para isso, precisamos da seguinte proposição:

Proposição 2.7. *Seja $g(x_1, \cdots, x_n) = \sum_{1 \leq i,j \leq n} a_{i,j} x_i x_j$ uma forma quadrática não nula sobre $\mathbb{F}_q$, com $char(\mathbb{F}_q)$ ímpar. Então existe uma mudança linear de variáveis $(x_1, \cdots, x_n) \overset{\mathcal{L}}{\mapsto} (y_1, \cdots, y_n)^t = B^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, com $B \in GL(\mathbb{F}_q, n)$, tal que $g \circ \mathcal{L}^{-1}(y_1, \cdots, y_n) = \tilde{g}(y_1, \cdots, y_n) = ay_1^2 + g(y_2, \cdots, y_n)$, com $a \neq 0$.*

Demonstração. Sem perda de generalidade, podemos assumir $a_{i,j} = a_{j,i}$, já que $char(\mathbb{F}_q) \neq 2$. Seja $A = (a_{i,j}) \in M_{n \times n}$ a matriz simétrica que determina a forma quadrática, isto é

$$g(x_1, \cdots, x_n) = (x_1, \cdots, x_n) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Sejam $a \in \mathbb{F}_q^*$ um elemento não nulo da imagem de g sobre $\mathbb{F}_q^n$ e $(c_1, \cdots, c_n) \in \mathbb{F}_q^n$ tais que $g(c_1, \cdots, c_n) = a$. Denotemos por $B = \begin{pmatrix} c_1 & b_{1,2} & \cdots & b_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_n & b_{n,2} & \cdots & b_{n,n} \end{pmatrix}$ de tal forma que $B \in GL(\mathbb{F}_q, n)$. Isso é possível pois $(c_1, \cdots, c_n) \neq 0$.

Observemos que

$$\begin{aligned} B^t A B &= \begin{pmatrix} c_1 & \cdots & c_n \\ b_{1,2} & \cdots & b_{n,2} \\ \vdots & \ddots & \vdots \\ b_{1,n} & \cdots & b_{n,n} \end{pmatrix} \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} c_1 & b_{1,2} & \cdots & b_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_n & b_{n,2} & \cdots & b_{n,n} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i,j} a_{i,j} c_i c_j & \cdots & \tilde{a}_{1,n} \\ \vdots & \ddots & \vdots \\ \tilde{a}_{n,1} & \cdots & \tilde{a}_{n,n} \end{pmatrix} = \begin{pmatrix} a & \cdots & \tilde{a}_{1,n} \\ \vdots & \ddots & \vdots \\ \tilde{a}_{n,1} & \cdots & \tilde{a}_{n,n} \end{pmatrix}, \end{aligned}$$

para $(\tilde{a}_{i,j})$ apropriados. Observemos que $B^t A B$ também é simétrica. Logo

$$\begin{aligned} \tilde{g}(y_1, y_2, \cdots, y_n) =& (y_1, y_2, \cdots, y_n) B^t A B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \\ =& a y_1^2 + 2(\tilde{a}_{1,2} y_1 y_2 + \cdots + \tilde{a}_{1,n} y_1 y_n) + \tilde{g}(y_2, \cdots, y_n) \\ =& a \left(y_1 + \frac{\tilde{a}_{1,2} y_2 + \cdots + \tilde{a}_{1,n} y_n}{a} \right)^2 + g(y_2, \cdots, y_n). \end{aligned}$$

Fazendo a mudança de variáveis $y_1 \mapsto \left(y_1 + \frac{\tilde{a}_{1,2} y_2 + \cdots + \tilde{a}_{1,n} y_n}{a} \right) = \tilde{y}_1$, temos

$$\tilde{g}(\tilde{y}_1, y_2, \cdots, y_n) = a \tilde{y}_1^2 + g(y_2, \cdots, y_n).$$

$\square$

Do resultado anterior, concluímos que toda forma quadrática sobre $\mathbb{F}_q$ com $char(\mathbb{F}_q) \neq 2$ é equivalente a uma forma quadrática diagonal, ou seja, se $g(X) = X^tAX$, existe $B \in GL(\mathbb{F}_q, n)$ tal que $\tilde{g}(Y) = Y^tB^tABY$, onde $B^tAB = \begin{pmatrix} d_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_n \end{pmatrix}$.

Observação 2.8. *Se $g(c_1, \cdots, c_n) = 0$ para todo $(c_1, \cdots, c_n) \in \mathbb{F}_q^n$, então a matriz associada a forma quadrática é a matriz nula.*

Com isso, chegamos ao seguinte resultado:

Teorema 2.9. *Seja $g(x_1, \cdots, x_n) = \sum_{1 \leq i,j \leq n} a_{i,j}x_ix_j$ forma quadrática sobre $\mathbb{F}_q$ com $char(\mathbb{F}_q) \neq 2$ e seja A a matriz simétrica associada a g com $\det(A) \neq 0$. Então*

$$N(g(x_1, \cdots, x_n) = b) = \begin{cases} q^{n-1} + q^{\frac{n-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{n}{2}}\det(A)), & \textit{se } n \textit{ é par} \\ q^{n-1} + q^{\frac{n-1}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}\det(A)b), & \textit{se } n \textit{ é ímpar.} \end{cases}$$

Demonstração. Pela Proposição 2.7, existe uma forma quadrática diagonal, $\tilde{g}$, equivalente a g dada por $\tilde{g}(X) = X^tB^tABX = \sum_{i=1}^{n} d_ix_i^2$. Além disso, do Teorema 2.3, temos que

$$N(g(x_1, \cdots, x_n) = b) = N(\tilde{g}(x_1, \cdots, x_n) = b) = \begin{cases} q^{n-1} + q^{\frac{n-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{n}{2}}d_1 \cdots d_n), & \text{se } n \text{ é par} \\ q^{n-1} + q^{\frac{n-1}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}d_1 \cdots d_nb), & \text{se } n \text{ é ímpar.} \end{cases}$$

Notemos que $d_1 \cdots d_n = \det(B^tAB) = \det(B)^2 \det(A)$, portanto,

$$\mathcal{X}(c_1 \cdots c_n) = \mathcal{X}(\det(B)^2 det(A)) = \mathcal{X}(\det(A)).$$

Logo

$$N(g(x_1, \cdots, x_n) = b) = \begin{cases} q^{n-1} + q^{\frac{n-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{n}{2}}\det(A)), & \text{se } n \text{ é par} \\ q^{n-1} + q^{\frac{n-1}{2}}\mathcal{X}((-1)^{\frac{n-1}{2}}\det(A)b), & \text{se } n \text{ é ímpar.} \end{cases}$$

□

Desta forma o número de soluções de g depende apenas do determinante de sua matriz associada A.

Exemplo 2.10. *Novamente, seja $\mathbb{F}_{13}$ o corpo com 13 elementos e tomemos $b = 7$ e $g(x_1, x_2, x_3) = 2x_1^2 + 3x_2^2 + 5x_3^2 + 7x_1x_2 + 8x_1x_2 + 9x_2x_3$ um polinômio em $\mathbb{F}_{13}[x_1, x_2, x_3]$. Aplicaremos o teorema anterior para encontrar o número de soluções para $g(x_1, x_2, x_3) = 7$.*

Para isso, observemos que a matriz simétrica associada ao polinômio $g(x_1, x_2, x_3)$ é

$$A = \begin{pmatrix} 2 & 10 & 4 \\ 10 & 3 & 11 \\ 4 & 11 & 5 \end{pmatrix}$$

e que $\det(A) = 3 \neq 0$.

Portanto,

$$\begin{aligned} N(g(x_1,x_2,x_3)=7) =& 13^2+13\cdot \mathcal{X}((-1)\cdot \det(A)\cdot 7)\\ =& 13^2+13\cdot\mathcal{X}(5)\\ =& 13^2-13\\ =& 156. \end{aligned}$$

Assim, existem 156 *soluções para* $g(x_1,x_2,x_3)=7$ *em* $\mathbb{F}_{13}^3$*.*

Uma pergunta imediata é: o que acontece quando $\det(A)=0$?

Teorema 2.11. *Seja* $g(x_1,\cdots,x_n)=\sum_{1\le i,j\le n} a_{i,j}x_ix_j$ *uma forma quadrática sobre* $\mathbb{F}_q$*, com* $char(\mathbb{F}_q)\neq 2$ *e matriz associada* $A=(a_{i,j})$ *de posto* k*. Seja* $B\in GL(\mathbb{F}_q,n)$ *tal que* $B^tAB=\begin{pmatrix}\tilde{A} & 0\\ 0 & 0\end{pmatrix}$*, onde* $\tilde{A}\in GL(\mathbb{F}_q,k)$*. Então*

$$N(g(x_1,\cdots,x_n)=b)=\begin{cases} q^{n-1}+q^{\frac{2n-k-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{k}{2}}\det(\tilde{A})), & \textit{se } k \textit{ é par}\\ q^{n-1}+q^{\frac{2n-k-1}{2}}\mathcal{X}((-1)^{\frac{k-1}{2}}\det(\tilde{A})b), & \textit{se } k \textit{ é ímpar.}\end{cases}$$

Demonstração. Sabemos pela Proposição 2.7 que existe uma forma quadrática $\tilde{g}=X^tB^tABX=\sum_{i=1}^k d_ix_i^2$ equivalente a g. Notemos que $\tilde{g}$ possui $n-k$ variáveis livres e seus coeficientes formam a matriz diagonal $\tilde{A}$.

Pelo teorema anterior, sabemos que

$$N(\sum_{i=1}^k c_ix_i^2=b)=\begin{cases} q^{k-1}+q^{\frac{k-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{k}{2}}\det(\tilde{A})), & \text{se } k \text{ é par}\\ q^{k-1}+q^{\frac{k-1}{2}}\mathcal{X}((-1)^{\frac{k-1}{2}}\det(\tilde{A})b), & \text{se } k \text{ é ímpar.}\end{cases}$$

Como cada uma das $n-k$ variáveis livres pode assumir q valores, basta multiplicar o número de soluções anterior por q^{n-k}. Logo, concluímos que

$$N(g(x_1,\cdots,x_n)=b)=\begin{cases} q^{n-1}+q^{\frac{2n-k-2}{2}}\mathcal{V}(b)\mathcal{X}((-1)^{\frac{k}{2}}\det(\tilde{A})), & \text{se } k \text{ é par}\\ q^{n-1}+q^{\frac{2n-k-1}{2}}\mathcal{X}((-1)^{\frac{k-1}{2}}\det(\tilde{A})b), & \text{se } k \text{ é ímpar.}\end{cases}$$

□

Exemplo 2.12. *Mais uma vez, seja* $\mathbb{F}_{13}$ *o corpo com* 13 *elementos e tomemos* $b=2$ *e* $g(x_1,x_2,x_3)=x_1^2+4x_2^2+3x_3^2+6x_1x_2+x_1x_3+9x_2x_3$*, polinômio em* $\mathbb{F}_{13}[x_1,x_2,x_3]$*. Nesse caso a matriz associada à* g *é*

$$A=\begin{pmatrix}1 & 3 & 7\\ 3 & 4 & 11\\ 7 & 11 & 3\end{pmatrix},$$

com $\det(A) = 0$ *e posto* 2. *Tomando* $B = \begin{pmatrix} 1 & 10 & 12 \\ 0 & 1 & 11 \\ 0 & 0 & 1 \end{pmatrix}$, *temos*

$$\begin{pmatrix} 1 & 0 & 0 \\ 10 & 1 & 0 \\ 12 & 11 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 & 7 \\ 3 & 4 & 11 \\ 7 & 11 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 10 & 12 \\ 0 & 1 & 11 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Assim, $\tilde{A} = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}$ *e*

$$\begin{aligned} N(g(x_1, x_2, x_3) = 2) = & 13^2 + 13 \cdot \mathcal{V}(2) \cdot \mathcal{X}((-1) \cdot \det(\tilde{A})) \\ = & 13^2 + 13 \\ = & 182. \end{aligned}$$

Portanto existem 182 *soluções para* $g(x_1, x_2, x_3) = 2$ *em* $\mathbb{F}_{13}^3$.

Observação 2.13. *Se char*$(\mathbb{F}_q) = 2$, *não podemos assumir que a matriz de coeficientes da forma quadrática é simétrica, uma vez que* 2^{-1} *não está definido em* Fq. *Assim, não conseguimos transformar as formas quadráticas em formas diagonais e, portanto, os teoremas deste capítulo não são válidos para esse caso. Entretanto é possível obter resultados similares, como os Teoremas 6.30 e 6.32 de [LN].*

O número de soluções da forma quadrática $g(x_1, \cdots, x_n) = 0$ é divisível por $q^{\left\lfloor \frac{n-1}{2} \right\rfloor}$. Em geral, impondo algumas condições sobre g, mostra-se que o número de soluções de $g = 0$ em $\mathbb{F}_q^n$ é sempre um múltiplo de q^s, com s adequado, como será mostrado no Capítulo 9 desta dissertação. Uma versão fraca disso será mostrada no próximo capítulo.

3 Teorema de Chevalley-Warning

A pergunta respondida no capítulo anterior para polinômios de segundo grau também pode ser feita para polinômios de grau n e, mais ainda, para um sistema de polinômios de grau n. Seja $\mathcal{S} = \{(c_1, \cdots, c_n) \in \mathbb{F}_q^n \mid f_i(c_1, \cdots, c_n) = 0,\ \forall\ 1 \leq i \leq r\}$, o conjunto de zeros de um sistema, com $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ polinômios quaisquer.

Os Teoremas de Chevalley-Warning e Ax-Katz são uma resposta parcial a esta pergunta, quando o número de variáveis é maior que a soma dos graus dos polinômios, como veremos a seguir. Nossas referências principais são os artigos [Ax64], [Ka71] e [BBC19]. O objetivo é encontrar a maior potência do inteiro q que divide $|\mathcal{S}|$, impondo algumas condições para os polinômios $f_1, \cdots, f_r$.

Começaremos com o Teorema de Chevalley-Warning, mas antes precisamos de algumas propriedades do corpo $\mathbb{F}_q$.

Proposição 3.1. *Seja $l \in \mathbb{Z}_{\geq 0}$. Então* $\sum_{x \in \mathbb{F}_q} x^l = \begin{cases} -1, & \textit{se } (q-1)|l \textit{ e } l > 0 \\ 0, & \textit{caso contrário.} \end{cases}$ *Como convenção tomamos $0^0 = 1$.*

Demonstração. Se $l = 0$, então $\sum_{x \in \mathbb{F}_q} x^l = \sum_{x \in \mathbb{F}_q} 1 = 0$. Se $q-1$ divide l e $l \neq 0$, então $\sum_{x \in \mathbb{F}_q} x^l = \sum_{x \in \mathbb{F}_q^*} 1 = -1 + \sum_{x \in \mathbb{F}_q} 1 = -1$.

Suponhamos que $(q-1)$ não divide l. Sejam $M = \sum_{x \in \mathbb{F}_q} x^l$. Como $\mathbb{F}_q^*$ é um grupo cíclico de ordem $q-1$, existe um elemento de ordem $q-1$, portanto seja r tal elemento. Temos que

$$r^l M = r^l \sum_{x \in \mathbb{F}_q} x^l = \sum_{x \in \mathbb{F}_q} (rx)^l = M,$$

uma vez que rx percorre todos os elementos de $\mathbb{F}_q$. Portanto $r^l M - M = M(r^l - 1) = 0$, mas $r^l \neq 1$, pois l não divide $q-1$, logo $M = 0$, concluindo a prova. $\square$

Proposição 3.2. *Seja $F(x_1, \cdots, x_n) \in \mathbb{F}_q[x_1, \cdots, x_n]$ um polinômio de grau menor que $n(q-1)$. Então $\sum_{(x_1, \cdots, x_n) \in \mathbb{F}_q^n} F(x_1, \cdots, x_n) \equiv 0 \pmod{p}$.*

Demonstração. Podemos escrever

$$F(x_1, \cdots, x_n) = \sum_{\sum_{i=1}^n \alpha_i < n(q-1)} a_{(\alpha_1, \cdots, \alpha_n)} x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Então, somando sobre todos os $(x_1, \cdots, x_n)$ em $\mathbb{F}_q^n$, temos

$$\begin{aligned} \sum_{(x_1, \cdots, x_n) \in \mathbb{F}_q^n} F(x_1, \cdots, x_n) &= \sum_{\sum_{i=1}^n \alpha_i < n(q-1)} a_{(\alpha_1, \cdots, \alpha_n)} \sum_{(x_1, \cdots, x_n) \in \mathbb{F}_q^n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \\ &= \sum_{\sum_{i=1}^n \alpha_i < n(q-1)} a_{(\alpha_1, \cdots, \alpha_n)} \Big(\sum_{x_1 \in \mathbb{F}_q} x_1^{\alpha_1} \Big) \cdots \Big(\sum_{x_n \in \mathbb{F}_q} x_n^{\alpha_n} \Big). \end{aligned}$$

Como $\sum_{i=1}^{n} \alpha_i < n(q-1)$, existe $1 \leq i \leq n$ tal que $\alpha_i < (q-1)$ e, consequentemente, não é múltiplo positivo de $q-1$. Assim, para tal i, $\sum_{x_i \in \mathbb{F}_q} x_i^{\alpha_i} = 0$ pela Proposição 3.1. Como isto é válido para todo monômio, concluímos que $\sum_{(x_1,\cdots,x_n)\in\mathbb{F}_q^n} F(x_1,\cdots,x_n) \equiv 0 \pmod p$.

□

Teorema 3.3 (Chevalley-Warning)**.** *Sejam* $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ *tais que* $d = \deg(f_1) + \cdots + \deg(f_r) < n$. *Se*

$$\mathcal{S} = \{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid f_j(x_1, \cdots, x_n) = 0, \ \forall 1 \leq j \leq r\},$$

então $|\mathcal{S}| \equiv 0 \pmod p$.

Demonstração. Primeiramente, para simplificar a notação, denotaremos por $X = (x_1, \cdots, x_n)$. Agora definimos a função $N(X) = \prod_{i=1}^{r}(1 - f_i(X)^{q-1})$. Observemos que, para $1 \leq i \leq r$ e para $X_0 \in \mathbb{F}_q^n$ fixo, se $f_i(X_0) = 0$, então $f_i(X_0)^{q-1} = 0$ e se $f_i(X_0) \neq 0$, então $f_i(X_0)^{q-1} = 1$. Com isso, temos que

$$N(X_0) = \begin{cases} 1, & \text{se } f_i(X_0) = 0, \ \forall 1 \leq i \leq r \\ 0, & \text{caso contrário.} \end{cases}$$

Ou seja, somando sobre $\mathbb{F}_q^n$, $\sum_{X\in\mathbb{F}_q^n} N(X) \equiv |\mathcal{S}| \pmod p$. Logo, basta mostrar que $\sum_{X\in\mathbb{F}_q^n} N(X) \equiv 0 \pmod p$. Notemos que

$$\begin{aligned} \sum_{X\in\mathbb{F}_q^n} N(X) &= \sum_{X\in\mathbb{F}_q^n} \prod_{i=1}^{r} (1 - f_i(X)^{q-1}) \\ &= \sum_{(j_1,\cdots,j_r)\in\{0,1\}^r} \sum_{X\in\mathbb{F}_q^n} (-1)^{j_1+\cdots+j_r} \prod_{i=1}^{r} f_i(X)^{(q-1)j_i} \end{aligned}$$

e $\deg(\prod_{i=1}^{r} f_i(X)^{(q-1)j_i}) < n(q-1)$. Assim, pela Proposição 3.2, temos o resultado.

□

Observemos que a condição $\sum \deg(f_i) < n$ é necessária, como mostra o seguinte exemplo:

Exemplo 3.4. *Sejam* $\{\alpha_1, \cdots, \alpha_n\}$ *base de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$ *e* $f(x_1, \cdots, x_n) = \prod_{j=0}^{n-1}(\alpha_1^{q^j} x_1 + \cdots + \alpha_n^{q^j} x_n)$.

Seja τ *o automorfismo de Frobenius sobre* $\mathbb{F}_{q^n}$ *tal que* $\tau(b) = b^q$. *Observemos que o corpo fixado por* τ *é* $\mathbb{F}_q$. *Por um abuso de notação, denotaremos também por* τ *o homomorfismo sobre* $\mathbb{F}_{q^n}[x_1, \cdots, x_n]$ *tal que* $\tau(\sum a_{\vec{i}} X^{\vec{i}}) = \sum \tau(a_{\vec{i}}) X^{\vec{i}}$, *onde* $\vec{i} = (i_1, \cdots, i_n)$ *e* $X^{\vec{i}} = x_1^{i_1} \cdots x_n^{i_n}$. *Observemos também que o anel fixado por* τ *é* $\mathbb{F}_q[x_1, \cdots, x_n]$. *Assim,*

$$\tau(f(x_1, \cdots, x_n)) = f(x_1, \cdots, x_n),$$

ou seja, $f(x_1, \cdots, x_n) \in \mathbb{F}_q[x_1, \cdots, x_n]$ *e* $\deg(f) = n$.

Se $(c_1, \cdots, c_n) \in \mathbb{F}_q^n$ *é tal que* $f(c_1, \cdots, c_n) = 0$, *então existe* $0 \leq j \leq n-1$ *tal que* $\alpha_1^{q^j} c_1 + \cdots + \alpha_n^{q^j} c_n = 0$. *Aplicando* τ *a quantidade necessária de vezes, temos que* $\alpha_1 c_1 + \cdots + \alpha_n c_n = 0$, *mas* $\{\alpha_1, \cdots, \alpha_n\}$ *é base, assim* $c_1 = \cdots = c_n = 0$ *é a única solução.*

Corolário 3.5. *Sejam* $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ *tais que* $d = \deg(f_1) + \cdots + \deg(f_r) < n$ *e sejam* $g_1, \cdots, g_n \in \mathbb{F}_q[x]$ *polinômios de permutação. Se* $\mathcal{S} = \{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid f_j(g_1(x_1), \cdots, g_n(x_n)) = 0,\ \forall 1 \leq j \leq r\} \neq \emptyset$, *então* $|\mathcal{S}| \equiv 0 \pmod p$.

Demonstração. Como $g_1, \cdots, g_n$ são polinômios de permutação e, portanto, representam funções bijetivas de $\mathbb{F}_q$ em $\mathbb{F}_q$, existem funções inversas $g_1^{-1}, \cdots, g_n^{-1} \in \mathbb{F}_q[x]$. Assim, para cada solução $(x_1, \cdots, x_n)$ de $f_1 = \cdots = f_r = 0$, existe uma solução de $f_1(g_1(x_1), \cdots, g_n(x_n)) = \cdots = f_1(g_1(x_1), \cdots, g_n(x_n)) = 0$ dada por $(g_1^{-1}(x_1), \cdots, g_n^{-1}(x_n))$. Portanto, como $d < n$, pelo Teorema de Chevalley-Warning vale que $|\mathcal{S}| \equiv 0 \pmod p$. □

No que segue, o objetivo é, usando as mesmas hipóteses sobre o grau e o número de variáveis do Teorema de Chevalley-Warning, limitar inferiormente o número de soluções do sistema. Para isso precisamos dos seguintes resultados que podem ser encontrados na seção 6.1 de [LN].

Definição 3.6. *Se* $W \subset \mathbb{F}_q^n$ *é um subespaço vetorial e* $\vec{a} \in \mathbb{F}_q^n$ *é um vetor, dizemos que* $W_1 = W + \vec{a}$ *é um subespaço afim e* $dim_{\mathbb{F}_q}(W_1) = dim_{\mathbb{F}_q}(W)$. *Dizemos que* $W_1 = W + \vec{a}$ *e* $W_2 = W + \vec{b}$ *são paralelos se* $W_1 \cap W_2 = \emptyset$, *que é equivalente a* $a - b \notin W$.

Proposição 3.7. *Se* $W_1 \subset \mathbb{F}_q^n$ *é um subespaço afim de dimensão d, então existem* $a_i \in \mathbb{F}_q^n$, *com* $i = 2, \cdots, q^{n-d}$, *tal que* $W_i = W + a_i$ *são subespaços afins distintos e paralelos a* W_1 *e* $\bigcup_{i=1}^{q^{n-d}} W_i = \mathbb{F}_q^n$

Demonstração. Suponha que, para $s < q^{n-d}$, existam $a_2, \cdots, a_s \in \mathbb{F}_q^n$ tais que $W_2, \cdots, W_s$ sejam subespaços afins distintos paralelos a W_1. Como $|\bigcup_{i=1}^{s} W_i| = sq^d < q^n$, exite um elemento $b \in \mathbb{F}_q^n$ tal que $b \notin \bigcup_{i=1}^{s} W_i$. Assim $W_1 + b$ é subespaço afim.

Se $\beta \in W_1 + b \cup W_1$, então $\beta = w + b$, para algum $w \in W_1$, logo $\beta - b = w \in W_1$. Mas $\beta \in W_1$, o que implica $b \in W_1$, absurdo! Se $\beta \in W_1 + b \cup W_i$, para algum $i = 2, \vdots s$, então $\beta = w + a_i$, para algum $w \in W_1$, logo $\beta - a_i \in W_1$. Analogamente, $\beta - b \in W_1$, portanto $\beta - a_i - \beta + b = b - a_i \in W_1$ e $b - a_i + a_i = b \in W_i$, absurdo! Assim, temos que W_i são subespaços afins distintos e paralelos a W_1.

Para obter a igualdade $\bigcup_{i=1}^{q^{n-d}} W_i = \mathbb{F}_q^n$, basta notar que $|W_i| = q^d$ para todo $i = 1, \cdots, q^{n-d}$.

□

Lema 3.8. *Sejam* $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$, $d = \deg(f_1) + \cdots + \deg(f_r)$ *e* $\mathcal{S} = \{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid f_j(x_1, \cdots, x_n) = 0, \forall 1 \leq j \leq r\}$. *Se* W_1 *e* W_2 *espaços afins paralelos de dimensão d, então* $|W_1 \cap \mathcal{S}| \equiv |W_2 \cap \mathcal{S}| \pmod p$.

Demonstração. Realizando uma mudança variáveis, podemos supor que $W_1 = \{(c_1, \cdots, c_n) \in \mathbb{F}_q^n \mid c_1 = \cdots = c_{n-d} = 0)\}$ e $W_2 = \{(c_1, \cdots, c_n) \in \mathbb{F}_q^n \mid c_1 = 1; c_2 = \cdots = c_{n-d} = 0\}$ e sejam $g_1, \cdots, g_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ as funções obtidas a partir das mudanças de variáveis. Como a mudança de variáveis é afim, temos que $\deg(g_i) = \deg(f_i)$.

Seja $G(x_1, \cdots, x_n) = (-1)^{n-d}(x_1^{q-2} + \cdots + x_1 + 1)(x_2^{q-1} - 1) \cdots (x_{n-d}^{q-1} - 1)$. Assim,

$$G(x_1, \cdots, x_n) = \begin{cases} -1, & \text{se } (x_1, \cdots, x_n) \in W_1 \\ 1, & \text{se } (x_1, \cdots, x_n) \in W_2 \\ 0, & \text{caso contrário.} \end{cases}$$

Definimos a função $H(x_1, \cdots, x_n) = (1 - g_1^{q-1}) \cdots (1 - g_r^{q-1}) G(x_1, \cdots, x_n)$. Logo,

$$H(x_1, \cdots, x_n) = \begin{cases} -1, & \text{se } (x_1, \cdots, x_n) \in W_1 \cap S \\ 1, & \text{se } (x_1, \cdots, x_n) \in W_2 \cap S \\ 0, & \text{caso contrário} \end{cases}$$

e $\deg(H) = (q-1)d + (n-d-1)(q-1) + q - 2 = n(q-1) - 1 < n(q-1)$. Portanto, pela Proposição 3.2

$$\sum_{(c_1, \cdots, c_n) \in \mathbb{F}_q^n} H(c_1, \cdots, c_n) \equiv 0 \equiv |W_2 \cap \mathcal{S}| - |W_1 \cap \mathcal{S}| \pmod{p}.$$

□

Teorema 3.9 (Warning [War35]). *Sejam $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ e $d = \deg(f_1) + \cdots + \deg(f_r)$ tal que $d < n$. Se $\mathcal{S}$ é o conjunto solução de $f_1 = \cdots = f_r = 0$ e $|\mathcal{S}| \neq 0$, então $|\mathcal{S}| \geq q^{n-d}$.*

Demonstração. Primeiramente, suponhamos que exista W_1, subespaço afim de $\mathbb{F}_q^n$, tal que $|\mathcal{S} \cap W_1| \not\equiv 0 \pmod{p}$ e $dim(W_1) = d$. Em particular, notemos que $|W_1 \cap \mathcal{S}| \geq 1$. Se, para $i = 2, \cdots, q^{n-d}$, $W_i = W_1 + a_i$ são espaços afins distintos paralelos a W_1 com $dim(W_i) = d$, pelo Lema 3.8, $|W_i \cap \mathcal{S}| \equiv |W_1 \cap \mathcal{S}| \pmod{p}$, então $|W_2 \cap \mathcal{S}| \geq 1$. Como $\mathbb{F}_q^n = \bigcup_{i=1}^{q^{n-d}} W_i$, temos que $|\mathcal{S}| = |\bigcup_{i=1}^{q^{n-d}} (W_i \cap \mathcal{S})| \geq q^{n-d}$.

Agora, suponhamos que para todo W subespaço afim de $\mathbb{F}_q^n$, com $dim(W) = d$, temos $|W \cap \mathcal{S}| \equiv 0 \pmod{p}$.

Afirmação: existe $1 \leq k \leq d$ tal que $|W \cap \mathcal{S}| \equiv 0 \pmod{p}$, para todo W subespaço afim de $\mathbb{F}_q^n$ com $dim(W) = k$, e $|W' \cap \mathcal{S}| \not\equiv 0 \pmod{p}$ para algum W' com $dim(W') = k - 1$.

De fato, tomando $k = 1$, $dim(W') = 1 - 1 = 0$, logo W' é um ponto. Como $\mathcal{S} \neq \emptyset$ existe W' tal que $|W' \cap \mathcal{S}| = 1$. Logo existe $k \geq 1$ que satisfaz tal propriedade.

Seja U plano afim tal que $dim(U) = k - 1$ e $|U \cap \mathcal{S}| \not\equiv 0 \pmod{p}$. Seja $\mathcal{W} = \{W \mid W$ é plano afim com $dim(W) = k$ e $U \subset W\}$.

Se $W \in \mathcal{W}$, então $|W \cap \mathcal{S}| \equiv 0 \pmod{p}$. Por outro lado, $|W \cap \mathcal{S}| = |U \cap \mathcal{S}| + |(W \setminus U) \cap \mathcal{S}|$ e $|U \cap \mathcal{S}| \not\equiv 0 \pmod{p}$ e $|(W \setminus U) \cap \mathcal{S}| \not\equiv 0 \pmod{p}$.

Se $W_1, W_2 \in \mathcal{W}$, então $dim(W_1 \cap W_2) \leq k-1$ e $W_1 \cap W_2 \supset U$. Mas $dim(U) = k-1$, portanto $W_1 \cap W_2 = U$. Assim,

$$|\mathcal{S}| \geq |U \cap \mathcal{S}| + \sum_{W \in \mathcal{W}} |(W \setminus U) \cap \mathcal{S}| \geq (p-1) + |\mathcal{W}|.$$

Fazendo uma mudança linear de variáveis, podemos supor que $U = \{(c_1, \cdots, c_n) \in \mathbb{F}_q^n \mid c_1 = \cdots = c_{n-k+1} = 0\}$. Logo, combinatorialmente, temos que $|\mathcal{W}| = \frac{q^{n-k+1}-1}{q-1} = q^{n-k} + q^{n-k-1} + \cdots + 1 > q^{n-d}$ e, consequentemente, $|\mathcal{S}| \geq q^{n-d}$. $\square$

Observação 3.10. *Existem casos onde o número de soluções do sistema é* q^{n-d}.

Tomando $g(x_1, \cdots, x_d) := \prod_{i=0}^{n-1} (\alpha_1^{q^i} x_1 + \cdots + \alpha_d^{q^i} x_d)$, *em que* $(\alpha_1, \cdots, \alpha_n)$ *é base de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$, *e* $f(x_1, \cdots, x_n) := g(x_1, \cdots, x_d)$. *Como* $f(c_1, \cdots, c_n) = 0 \Leftrightarrow c_1 = \cdots = c_d = 0$, *então a quantidade de soluções de* $f(x_1, \cdots, x_n) = 0$ *é* q^{n-d}.

4 Soma de Gauss

Antes de seguir para o Teorema de Ax-Katz, precisaremos de um resultado conhecido como Congruência de Stickelberger. Para obter este resultado utilizaremos duas somas de caracteres sobre $\mathbb{F}_q$ denominadas soma de Gauss e soma de Jacobi. Neste capítulo, apresentaremos tais somas e algumas de suas propriedades fundamentais. Os resultados presentes neste capítulo encontram-se no Capítulo 8 de [IR].

Ao longo dos próximos capítulos, denotaremos por ζ_m uma raiz m-ésima da unidade e $Tr : \mathbb{F}_q \to \frac{\mathbb{Z}}{p\mathbb{Z}}$ a função traço definida por $Tr(x) = x + x^p + \cdots + x^{p^{f-1}}$. Denotamos por $\psi : \mathbb{F}_q \to \mathbb{C}^*$ o caracter aditivo $\psi(x) = \zeta_p^{Tr(x)}$, $\chi : \mathbb{F}_q \to \mathbb{C}^*$ um caracter multiplicativo qualquer de $\mathbb{F}_q^*$ e $\mathbf{1} : \mathbb{F}_q^* \to \mathbb{C}^*$ o caracter trivial dado por $\mathbf{1}(a) = 1$, para todo $a \in \mathbb{F}_q^*$. Estendemos χ em 0 de tal forma que $\chi(0) = 1$ se $\chi = \mathbf{1}$ e $\chi(0) = 0$ caso contrário. Notemos que $\chi^{q-1} = \mathbf{1}$ em $\mathbb{F}_q^*$, logo χ tem ordem coprima com p.

Definição 4.1 (Soma de Gauss). *Definimos a soma de Gauss do caracter χ como*

$$g(\chi) = \sum_{a \in \mathbb{F}_q} \chi(a)\psi(a).$$

Podemos verificar de maneira direta que $g(\mathbf{1}) = 1$ e que $g(\chi) \in \mathbb{Q}(\zeta_{pm})$ se χ tem ordem m.

Lema 4.2. *Sejam χ um caracter multiplicativo e $g(\chi)$ a sua soma de Gauss. Então:*

a) $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$;

b) Se $\chi \neq \mathbf{1}$, então $g(\chi)\overline{g(\chi)} = q$;

c) Se $\chi \neq \mathbf{1}$, então $g(\chi)g(\overline{\chi}) = \chi(-1)q$.

Demonstração. a) Como $\overline{\chi}(-1) = \chi(-1)$, segue que

$$\begin{aligned}
\chi(-1)\overline{g(\chi)} =& \chi(-1)\overline{\sum_{a \in \mathbb{F}_q} \chi(a)\psi(a)} = \chi(-1)\sum_{a \in \mathbb{F}_q} \overline{\chi}(a)\overline{\psi}(a) \\
=& \chi(-1)\sum_{a \in \mathbb{F}_q} \overline{\chi}(a)\psi(a)^{-1} = \sum_{a \in \mathbb{F}_q} \chi(-1)\overline{\chi}(a)\psi(-a) \\
=& \sum_{a \in \mathbb{F}_q} \overline{\chi}(-a)\psi(-a) = g(\overline{\chi}).
\end{aligned}$$

b) Se $\chi \neq \mathbf{1}$, então vale que

$$\begin{aligned}
g(\chi)\overline{g(\chi)} &= \sum_{a,b\neq 0} \chi(ab^{-1})\psi(a-b) \quad \text{tomando } ab^{-1}=c\\
&= \sum_{b,c\neq 0} \chi(c)\psi(bc-b)\\
&= \sum_{b\neq 0} \chi(1)\psi(0) + \sum_{c\neq 1}\chi(c)\sum_{b\neq 0}\psi(b(c-1))\\
&= q-1+\sum_{c\neq 0,1}\chi(c)(-1)\\
&= q.
\end{aligned}$$

c) Pelo item a), $g(\chi)g(\overline{\chi}) = g(\chi)\chi(-1)\overline{g(\chi)}$ e, pelo item b), $g(\chi)\chi(-1)\overline{g(\chi)} = \chi(-1)q$.

□

Definição 4.3 (Soma de Jacobi)**.** *Dados χ_1 e χ_2 caracteres multiplicativos, definimos a soma de Jacobi dos caracteres χ_1 e χ_2 como:*

$$J(\chi_1,\chi_2) = \sum_{a\in\mathbb{F}_q} \chi_1(a)\chi_2(1-a).$$

Verifica-se de forma direta que se m é o mínimo múltiplo comum das ordens de χ_1 e χ_2, então $J(\chi_1,\chi_2)$ é inteiro algébrico em $\mathbb{Q}(\zeta_m)$.

Lema 4.4. *São válidos*

a) $J(\mathbf{1},\mathbf{1}) = q$;

b) $J(\mathbf{1},\chi) = J(\chi,\mathbf{1}) = 0$, *se* $\chi \neq \mathbf{1}$;

c) $J(\chi,\overline{\chi}) = -\chi(-1)$ *se* $\chi \neq \mathbf{1}$;

d) $J(\chi_1,\chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$ *se* $\chi_1 \neq \mathbf{1}$, $\chi_2 \neq \mathbf{1}$ *e* $\chi_1\chi_2 \neq \mathbf{1}$.

Demonstração.

a) $J(\mathbf{1},\mathbf{1}) = \sum_{a\in\mathbb{F}_q} \mathbf{1}(a)\mathbf{1}(1-a) = \sum_{a\in\mathbb{F}_q} 1 = q$.

b) $J(\chi,\mathbf{1}) = J(\mathbf{1},\chi) = \sum_{a\in\mathbb{F}_q} \mathbf{1}(a)\chi(1-a) = \sum_{a\in\mathbb{F}_q} \chi(1-a) = \sum_{b\in\mathbb{F}_q}\chi(b) = 0$.

c)

$$J(\chi,\overline{\chi}) = \sum_{a\in\mathbb{F}_q} \chi(a)\overline{\chi}(1-a) = \sum_{a\in\mathbb{F}_q\setminus\{1\}} \chi(a(1-a)^{-1}).$$

Se $a(1-a)^{-1} = c$, então $a = c(1+c)^{-1}$ para todo $c \neq -1$. Assim $J(\chi,\overline{\chi}) = \sum_{c\in\mathbb{F}_q\setminus\{-1\}}\chi(c) = -\chi(-1)$.

d)

$$g(\chi_1)g(\chi_2) = \sum_{a,b\in\mathbb{F}_q} \chi_1(a)\chi_2(b)\psi(a+b) = \sum_{x\in\mathbb{F}_q}\big(\sum_{a\in\mathbb{F}_q}\chi_1(a)\chi_2(x-a)\big)\psi(x).$$

Se $x = 0$, então

$$\sum_{a \in \mathbb{F}_q} \chi_1(a)\chi_2(-a) = \chi_1(-1) \sum_{a \in \mathbb{F}_q} \chi_1(-a)\chi_2(-a) = 0.$$

Se $x \neq 0$, tomando $a = xa'$ temos

$$\begin{aligned}\sum_{a \in \mathbb{F}_q} \chi_1(a)\chi_2(x-a) = &\sum_{a' \in \mathbb{F}_q} \chi_1(xa')\chi_2(x-xa') \\ =&\chi_1(x)\chi_2(x)J(\chi_1,\chi_2).\end{aligned}$$

Portanto

$$g(\chi_1)g(\chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(x)J(\chi_1,\chi_2)\psi(x) = J(\chi_1,\chi_2)g(\chi_1\chi_2).$$

□

Corolário 4.5. *Se χ_1 e χ_2 são caracteres cuja ordem divide de m, então $\frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$ é um inteiro algébrico em $\mathbb{Q}(\zeta_m)$.*

A Congruência de Stickelberger associa somas de Gauss de caracteres em $\mathbb{F}_q$ com elementos em ideais primos do anel de inteiros de uma extensão ciclotômica dos racionais. Neste momento apresentaremos algumas propriedades das somas de Gauss que ajudaram a localizá-las nesses ideais.

Se m é um inteiro com $(m,p) = 1$, então $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ ([Wash] Capítulo 2). Assim, tomando $(b,m) = 1$, definimos $\pi_b \in Gal(\mathbb{Q}(\zeta_p,\zeta_m);\mathbb{Q})$ como $\pi_b : \zeta_p \mapsto \zeta_p$ e $\pi_b : \zeta_m \mapsto \zeta_m^b$. No que segue, para todo $a \in \mathbb{Q}(\zeta_p,\zeta_m)$, denotamos por a^{π_b} o elemento $\pi_b(a)$. Esta notação será muito útil e prática nos resultados seguintes.

Lema 4.6. *Se χ é um caracter multiplicativo cuja ordem divide m, então*

$$\frac{g(\chi)^b}{g(\chi)^{\pi_b}} = g(\chi)^{b-\pi_b} \in \mathbb{Q}(\zeta_m)$$

e $g(\chi)^m \in \mathbb{Q}(\zeta_m)$.

Demonstração. Sabemos que $g(\chi)^{b-\pi_b} \in \mathbb{Q}(\zeta_m,\zeta_p)$. Seja $(c,p) = 1$ e tomemos $\tau_c : \mathbb{Q}(\zeta_m,\zeta_p) \to \mathbb{Q}(\zeta_m,\zeta_p)$ automorfismo que fixa $\mathbb{Q}$ tal que $\tau_c : \zeta_m \mapsto \zeta_m$ e $\tau_c : \zeta_p \mapsto \zeta_p^c$ ([Wash] Capítulo 2). Precisamos mostrar que $\tau_c(g(\chi)^{b-\pi_b}) = g(\chi)^{b-\pi_b}$ para todo c.

De fato,

$$\begin{aligned} g(\chi)^{\tau_c} &= \sum_{a\in\mathbb{F}_q} \tau_c(\chi(a))\tau_c(\psi(a)) \\ &= \sum_{a\in\mathbb{F}_q} \chi(a)\psi(a)^c \\ &= \sum_{a\in\mathbb{F}_q} \chi(a)\psi(ca) \quad \text{tomando} \quad ca = b \\ &= \sum_{b\in\mathbb{F}_q} \chi\big(bc^{-1}\big)\psi(b) \\ &=\chi(c)^{-1}g(\chi). \end{aligned}$$

Portanto, $(g(\chi)^b)^{\tau_c} = (g(\chi)^{\tau_c})^b = \chi(c)^{-b}g(\chi)^b$.

Por outro lado,

$$\begin{aligned} g(\chi)^{\pi_b} &= \sum_{a\in\mathbb{F}_q} \pi_b(\chi(a))\pi_b(\psi(a)) \\ &= \sum_{a\in\mathbb{F}_q} \chi(a)^b\psi(a) \\ &= \sum_{a\in\mathbb{F}_q} \chi^b(a)\psi(a) \\ &=g(\chi^b). \end{aligned}$$

Logo, $(g(\chi)^{\pi_b})^{\tau_c} = (g(\chi^b))^{\tau_c} = \chi(c)^{-b}g(\chi^b)$. Assim,

$$\begin{aligned} (g(x)^{b-\pi_b})^{\tau_c} &=\chi(c)^{-b}g(\chi)^b\chi(c)^b g(\chi^b)^{-1} \\ &=g(\chi)^b g(\chi^b)^{-1} \\ &=g(\chi)^b g(\chi)^{-\pi_b} \\ &=g(\chi)^{b-\pi_b}, \end{aligned}$$

portanto $g(\chi)^{b-\pi_b} \in \mathbb{Q}(\zeta_m)$. □

Lema 4.7. *Se χ é um caracter multiplicativo sobre $\mathbb{F}_q^*$, então $g(\chi^p) = g(\chi)$.*

Demonstração. $g(\chi^p) = \sum_{a\in\mathbb{F}_q} \chi^p(a)\psi(a) = \sum_{a\in\mathbb{F}_q} \chi(a^p)\zeta_p^{Tr(a)}$. Observemos que $a \mapsto a^p$ é um automorfismo em $\mathbb{F}_q$ e, além disso, $Tr(a) = Tr(a^p)$. Portanto $g(\chi^p) = \sum_{a\in\mathbb{F}_q} \chi(a^p)\zeta_p^{Tr(a^p)} = \sum_{a\in\mathbb{F}_q} \chi(a)\zeta_p^{Tr(a)} = g(\chi)$. □

Como uma aplicação das somas de Gauss e de Jacobi e de suas propriedades, estimaremos a seguir o número de soluções de $X^d + Y^d = 1$ com $X, Y \in \mathbb{F}_q$. Primeiramente assumamos que $d|(q-1)$. Como $\mathbb{F}_q^*$ é cíclico de ordem $q-1$, existe um caracter χ de ordem d, que será fixado no resto do capítulo. A ciclicidade de $\mathbb{F}_q^*$ implica que $\chi(u) = 1$ se, e somente se, u é uma potência d-ésima em $\mathbb{F}_q$.

Definição 4.8. *Para $u \in \mathbb{F}_q^*$, definimos $N_d(u) = \#\{x \in \mathbb{F}_q \mid x^d = u\}$.*

Verifica-se que $N_d(u) = \begin{cases} 1, & \text{se } u = 0 \\ 0, & \text{se } u \text{ não é uma potência } d\text{-ésima} \\ d, & \text{se } u \neq 0 \text{ e } u \text{ é uma potência } d\text{-ésima.} \end{cases}$

Proposição 4.9. $N_d(u) = \sum_{a=0}^{d-1} \chi^a(u)$.

Demonstração. Se $u = 0$, como $\chi^a(0) = 0$ para $a \neq 0$ e $\chi^0(0) = 1$, então $\sum_{a=0}^{d-1} \chi^a(0) = 1 = N_d(0)$.

Se u não é uma potência d-ésima, então $\chi(u) \neq 1$. Assim, se $S = \sum_{a=0}^{d-1} \chi^a(u)$, temos que $\chi(u)S = \sum_{a=0}^{d-1} \chi^{a+1}(u) = \sum_{a=1}^{d} \chi^a(u) = S$. Logo $S(\chi(u) - 1) = 0$ o que implica que $S = 0$.

Se u é uma potência d-ésima, então $\sum_{a=0}^{d-1} \chi^a(u) = 1 + \cdots + 1 = d = N_d(u)$. □

Desta forma, para determinar o número de soluções de $X^d + Y^d = 1$ em $\mathbb{F}_q$, basta usar a proposição anterior da seguinte forma

$$\begin{aligned} N(X^d + Y^d = 1) &= \sum_{u \in \mathbb{F}_q} N_d(u) N_d(1-u) \\ &= \sum_{u \in \mathbb{F}_q} \sum_{i=0}^{d-1} \chi^i(u) \sum_{j=0}^{d-1} \chi^j(1-u) \\ &= \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} \sum_{u \in \mathbb{F}_q} \chi^i(u)\chi^j(1-u) \\ &= \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} J(\chi^i, \chi^j) \\ &= q + \sum_{i=1}^{d-1} \sum_{j=1}^{d-1} J(\chi^i, \chi^j) \\ &= q - \sum_{i=1}^{d-1} \chi^i(-1) + \sum_{\substack{i,j=1 \\ i+j \neq d}}^{d-1} J(\chi^i, \chi^j) \\ &= q + 1 - N_d(-1) + \sum_{\substack{i,j=1 \\ i+j \neq d}}^{d-1} J(\chi^i, \chi^j). \end{aligned}$$

Observemos que $|g(\chi)| = \sqrt{g(\chi)\overline{g(\chi)}} = \sqrt{q}$ se $\chi \neq 1$. Portanto, pelo Lema 4.4 d), $|J(\chi^i, \chi^j)| = \frac{|g(\chi^i)g(\chi^j)|}{|g(\chi^i\chi^j)|} = \sqrt{q}$. Assim, pela desigualdade triangular,

$$|N(X^d + Y^d = 1) + N_d(-1) - q - 1| = \Big| \sum_{\substack{i,j=1 \\ i+j \neq d}}^{d-1} J(\chi^i, \chi^j) \Big| \leq (d-1)(d-2)\sqrt{q}.$$

Agora assumamos $d \nmid (q-1)$ e seja $e = (d, (q-1))$. Nesse caso, $x \mapsto x^{\frac{d}{e}}$ é uma bijeção de $\mathbb{F}_q$. Assim, tomando $\tilde{X} = X^{\frac{d}{e}}$ basta resolver $\tilde{X}^e + \tilde{Y}^e = 1$. Portanto $N(X^d + Y^d = 1) = N(X^e + Y^e = 1)$, logo $|N(X^e + Y^e = 1) + N_e(-1) - q - 1| \leq (e-1)(e-2)\sqrt{q} \leq (d-1)(d-2)\sqrt{q}$.

Este resultado é um caso particular da cota obtida por Hasse-Weil para curvas sobre corpos finitos (Teorema 6.37 [LN]).

5 Elemento de Stickelberger

Este capítulo apresentará alguns resultados presentes no Capítulo 14 de [IR], sobre o anel de inteiros de algumas extensões ciclotômicas dos racionais que serão úteis para definir o caracter utilizado na Congruência de Stickelberger.

Seja M uma extensão abeliana finita de $\mathbb{Q}$. Pelo Teorema de Kronecker-Weber ([Wash], capítulo 14), sabemos que $M \subseteq \mathbb{Q}(\zeta_m)$, para algum número natural m, que podemos supor mínimo com esta propriedade.

Assim, $G := Gal(M, \mathbb{Q})$ pode ser visto como um grupo quociente de $Gal(\mathbb{Q}(\zeta_m), \mathbb{Q}) \cong \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$ e, para todo $(a, m) = 1$, temos que $\tau_a \in G$ é definido pela relação $\tau_a(\zeta_m) = \zeta_m^a$.

Definição 5.1. *Definimos $\mathbb{Z}[G]$ como o anel do grupo G com coeficientes em $\mathbb{Z}$. Assim, se $\alpha \in \mathbb{Z}[G]$, então $\alpha = \sum_{\tau_i \in G} a_i \tau_i$, com $a_i \in \mathbb{Z}$. Com isso, para todo $k \in M$, definimos*

$$k^{\sum_{\tau_i \in G} a_i \tau_i} = \prod_{\tau_i \in G} (k^{\tau_i})^{a_i}.$$

Definição 5.2 (Elemento e ideal de Stickelberger)**.** *Seja $\mathcal{R}$ o conjunto completo de invertíveis $\pmod{m}$. Definimos o elemento de Stickelberger como*

$$\Theta = \Theta(M) = \sum_{a \in \mathcal{R}} \left\{ \frac{a}{m} \right\} \tau_a^{-1} \in \mathbb{Q}[G],$$

onde $\{\alpha\}$ representa a parte fracionária de α e $\mathbb{Q}[G]$ é a álgebra de grupo racional do grupo G. O ideal de Stickelberger é definido como $I(M) = \mathbb{Z}[G] \cap \Theta\mathbb{Z}[G]$.

Lema 5.3. *Sejam $M = \mathbb{Q}(\zeta_m)$ e $J = \langle c - \tau_c \mid mdc(c, m) = 1 \rangle$ ideal em $\mathbb{Z}[G]$. Se $\beta \in \mathbb{Z}[G]$, então $\beta\Theta \in \mathbb{Z}[G]$ se, e somente se, $\beta \in J$.*

Demonstração. Primeiro vamos mostrar que $\beta\Theta \in \mathbb{Z}[G]$ para todo β gerador de J. Observemos que no caso em que $\beta = c - \tau_c$, com $(c, m) = 1$, temos que

$$(c - \tau_c)\Theta = (c - \tau_c)\Big(\sum_{a \in \mathcal{R}} \left\{ \frac{a}{m} \right\} \tau_a^{-1} \Big) = \sum_{a \in \mathcal{R}} c \left\{ \frac{a}{m} \right\} \tau_a^{-1} - \sum_{a \in \mathcal{R}} \left\{ \frac{a}{m} \right\} \tau_c \tau_a^{-1}.$$

Reparemos que se $s \in \mathbb{N}$ é tal que $\tau_a^{-1}(\zeta_m) = \zeta_m^s$, então $\zeta_m = \tau_a(\zeta_m^s) = \zeta_m^{as}$, logo $as \equiv 1 \pmod{m}$ e $s \equiv a^{-1} \pmod{m}$. Assim, $\tau_a^{-1} = \tau_{a^{-1}}$ e

$$\begin{aligned}(c - \tau_c)\Theta &= \sum_{a \in \mathcal{R}} c \left\{ \frac{a}{m} \right\} \tau_a^{-1} - \sum_{a \in \mathcal{R}} \left\{ \frac{a}{m} \right\} \tau_{c^{-1}}^{-1} \tau_a^{-1}, \quad \text{tomando } c^{-1}a = b \\ &= \sum_{a \in \mathcal{R}} c \left\{ \frac{a}{m} \right\} \tau_a^{-1} - \sum_{b \in \mathcal{R}} \left\{ \frac{bc}{m} \right\} \tau_b^{-1}.\end{aligned}$$

Observemos que $b \mapsto bc$ é automorfismo em $\mathbb{Z}_m^*$, uma vez que $(c, m) = 1$. Assim

$$\begin{aligned}(c - \tau_c)\Theta &= \sum_{a \in \mathcal{R}} c \left\{\frac{a}{m}\right\} \tau_a^{-1} - \left\{\frac{ac}{m}\right\} \tau_a^{-1} \\ &= \sum_{a \in \mathcal{R}} \left(c \left\{\frac{a}{m}\right\} - \left\{\frac{ac}{m}\right\}\right) \tau_a^{-1}.\end{aligned}$$

Agora se $a = \tilde{a}m + \tilde{r}$, onde $0 \leq \tilde{r} < m$, então $ac = \tilde{a}cm + \tilde{r}c$. Portanto $\left\{\frac{a}{m}\right\} = \frac{\tilde{r}}{m}$ e $\left\{\frac{ac}{m}\right\} = \left\{\frac{\tilde{r}c}{m}\right\}$, logo

$$c \left\{\frac{a}{m}\right\} - \left\{\frac{ac}{m}\right\} = \frac{c\tilde{r}}{m} - \left\{\frac{c\tilde{r}}{m}\right\} = \left\lfloor \frac{c\tilde{r}}{m} \right\rfloor \in \mathbb{Z}.$$

Concluímos que $\beta\Theta \in \mathbb{Z}[G]$.

Por outro lado, suponhamos que $\beta\Theta \in \mathbb{Z}[G]$. Seja $\beta = \sum_a x_a \tau_a$, com $1 \leq a \leq m$ e $(a, m) = 1$, $x_a \in \mathbb{Z}$ e $\tau_a \in G$. Logo

$$\begin{aligned}\beta\Theta &= \left(\sum_a x_a \tau_a\right) \left(\sum_c \left\{\frac{c}{m}\right\} \tau_c^{-1}\right) \\ &= \sum_a \sum_c x_a \left\{\frac{c}{m}\right\} \tau_c^{-1} \tau_a, \quad \text{tomando } b \equiv ca^{-1} \pmod{m} \\ &= \sum_a \sum_b x_a \left\{\frac{ba}{m}\right\} \tau_b^{-1} \\ &= \sum_b \left(\sum_a x_a \left\{\frac{ba}{m}\right\}\right) \tau_b^{-1} \in \mathbb{Z}[G],\end{aligned}$$

desta forma $\sum_a x_a \left\{\frac{ba}{m}\right\} \in \mathbb{Z}$ para todo b.

Se $b = 1$, então $\sum_a x_a \left\{\frac{a}{m}\right\} \in \mathbb{Z}$ e, desta forma, $\sum_a x_a \frac{a}{m} \in \mathbb{Z}$. Logo $\sum_a x_a a \equiv 0 \pmod{m}$. Além disso,

$$\begin{aligned}((1 + m) - \tau_{1+m})(\zeta_m) &= (1 + m)(\zeta_m) - \tau_{1+m}(\zeta_m) \\ &= \zeta_m + m\zeta_m - \zeta_m^{1+m} \\ &= m\zeta_m,\end{aligned}$$

portanto $m \in J$ e, consequentemente, $\sum_a x_a a \in J$. Com isso, $\sum_a x_a \tau_a = \sum_a x_a(\tau_a - a) + \sum_a x_a a \in J$ e temos que $\beta \in J$. $\square$

Uma consequência direta desse lema é que $I(M) = J\Theta$.

Agora, seja K uma extensão finita de $\mathbb{Q}$ de grau n e seja $\mathcal{O}_K$ o anel de inteiros algébricos de K.

Definição 5.4. *Dizemos que I é um ideal fracionário de K se existe $n \in \mathbb{N} \setminus \{0\}$ tal que nI é um ideal de $\mathcal{O}_K$.*

Definição 5.5. *Seja $A \subset \mathcal{O}_K$ um ideal, definimos $N(A) := \left|\frac{\mathcal{O}_K}{A}\right|$.*

Para provar a próxima proposição, precisaremos do Teorema Chinês do Resto para anéis.

Teorema 5.6 (Teorema Chinês do Resto)**.** *Seja R um anel comutativo com identidade e $A_1, A_2, \cdots, A_g$ ideais tais que $A_i + A_j = R$ se $i \neq j$. Seja $A = A_1 A_2 \cdots A_g$. Então*

$$\frac{R}{A} \cong \frac{R}{A_1} \oplus \frac{R}{A_2} \oplus \cdots \oplus \frac{R}{A_g}.$$

Demonstração. Seja ψ_i a função natural de R em $\frac{R}{A_i}$ e definamos $\psi : R \to \frac{R}{A_1} \oplus \cdots \oplus \frac{R}{A_g}$ como $\psi(r) = (\psi_1(r), \cdots, \psi_g(r))$. Mostraremos que ψ é sobrejetiva e que $\ker(\psi) = A$.

Para mostrar que ψ é sobrejetiva, basta mostrar que, para qualquer $a_1, \cdots, a_g \in R$, o sistema $x \equiv a_i \pmod{A_i}$, $i = 1, \cdots, g$, tem solução.

Observemos que $(A_1 + A_2)(A_1 + A_3) \cdots (A_1 + A_g) = R$. Expandindo o produto, temos que todos os termos estão em A_1 com exceção do último. Assim, $A_1 + A_2 A_3 \cdots A_g = R$, logo existem $u_1 \in A_1$ e $v_1 \in A_2 \cdots A_g$ tais que $u_1 + v_1 = 1$. Portanto $v_1 \equiv 1 \pmod{A_1}$ e $v_1 \equiv 0 \pmod{A_i}$, se $i \neq 1$.

Analogamente, para todo $j = 2, \cdots, g$, existe v_j tal que $v_j \equiv 1 \pmod{A_j}$ e $v_j \equiv 0 \pmod{A_i}$, se $i \neq j$. Verifica-se diretamente que $x = a_1 v_1 + a_2 v_2 + \cdots + a_g v_g$ é solução do sistema.

Agora basta mostrar que $\ker(\psi) = A$. Claramente, temos que $\ker(\psi) = A_1 \cap \cdots \cap A_g$, portanto gostaríamos de provar que o produto dos ideais é igual a interseção. Para isso, utilizaremos uma indução sobre o número de ideais.

Para $g = 2$, como $A_1 + A_2 = R$ por hipótese, existem $a_1 \in A_1$ e $a_2 \in A_2$ tais que $a_1 + a_2 = 1$. Se $a \in A_1 \cap A_2$, então $a = aa_1 + aa_2 \in A_1 A_2$ e $A_1 \cap A_2 \subset A_1 A_2$. Como $A_1 A_2 \subset A_1 \cap A_2$, temos a igualdade.

Agora suponhamos que $g > 2$ e que a afirmação vale quando temos $g - 1$ ideais. Assim, $A_1 \cap A_2 \cap \cdots \cap A_g = A_1 \cap A_2 A_3 \cdots A_g$. Entretanto, pela primeira parte desta demonstração, sabemos que $A_1 + A_2 A_3 \cdots A_g = R$, logo $A_1 \cap A_2 A_3 \cdots A_g = A_1 A_2 A_3 \cdots A_g$, como queríamos provar. □

Definição 5.7. *Um domínio de integridade é um domínio de Dedekind se satisfaz as seguintes propriedades:*

a) É um domínio Noetheriano;

b) É integralmente fechado;

c) Todo ideal primo é maximal.

Em um domínio de Dedekind, se I e J são ideais, dizemos que $I|J$ se, e somente se, $J \subseteq I$.

Proposição 5.8. *Se $A, B \subset \mathcal{O}_K$ são ideais, então $N(AB) = N(A)N(B)$.*

Demonstração. Se A e B são relativamente primos (*i.e.* $A + B = \mathcal{O}_K$), então, pelo Teorema Chinês do Resto, $\frac{\mathcal{O}_K}{AB} \cong \frac{\mathcal{O}_K}{A} \oplus \frac{\mathcal{O}_K}{B}$, logo $N(AB) = N(A)N(B)$.

Como $\mathcal{O}_K$ é domínio de Dedekind , seus ideais podem ser escritos como o produto de ideais primos de maneira única ([IR], capítulo 12). Portanto, para provar o caso em que A e B não são coprimos, basta mostrar a seguinte afirmação.

Afirmação: Se $\mathcal{P}$ é um ideal primo, então $N(\mathcal{P}^\alpha) = N(\mathcal{P})^\alpha$, para todo $\alpha \in \mathbb{N}$.

Provaremos a afirmação por indução sobre α. Para $\alpha = 1$ o resultado é trivial. Suponhamos $\alpha > 1$ e que a afirmação vale para $\alpha - 1$. Nesse caso, $\frac{\mathcal{O}_K}{\mathcal{P}^\alpha}$ tem $\frac{\mathcal{P}^{\alpha-1}}{\mathcal{P}^\alpha}$ como ideal e, pelo Teorema do Isomorfismo de anéis, $\frac{\frac{\mathcal{O}_K}{\mathcal{P}^\alpha}}{\frac{\mathcal{P}^{\alpha-1}}{\mathcal{P}^\alpha}} \cong \frac{\mathcal{O}_K}{\mathcal{P}^{\alpha-1}}$. Pela hipótese de indução $\left|\frac{\mathcal{O}_K}{\mathcal{P}^{\alpha-1}}\right| = N(\mathcal{P})^{\alpha-1}$.

Como $\mathcal{P}^\alpha \subset \mathcal{P}^{\alpha-1}$, tomamos $a \in \mathcal{P}^{\alpha-1} \setminus \mathcal{P}^\alpha$. Assim, definindo $\mathcal{I} = (a) + \mathcal{P}^\alpha$, temos que $\mathcal{P}^{\alpha-1} | \mathcal{I}$ e $\mathcal{I} | \mathcal{P}^\alpha$. Portanto $\mathcal{I}$ deve ser uma potência de $\mathcal{P}$, mas $\mathcal{P}^\alpha \neq \mathcal{I}$, logo $\mathcal{I} = \mathcal{P}^{\alpha-1}$.

Seja $\eta : \mathcal{O}_K \to \frac{\mathcal{P}^{\alpha-1}}{\mathcal{P}^\alpha}$ o homomorfismo tal que $\beta \mapsto \beta a + \mathcal{P}^\alpha$. Então $\ker(\eta) = \{\beta \in \mathcal{O}_K \mid \beta a \in \mathcal{P}^\alpha\}$. Observemos que $\mathcal{P}^\alpha | (\beta a)$ e $\mathcal{P}^{\alpha-1} | (a)$. Por outro lado, $\mathcal{P}^\alpha \nmid (a)$, logo $\mathcal{P} | (\beta)$ e $\beta \in \mathcal{P}$, o que implica que $\ker(\eta) = \mathcal{P}$ e, pelo Teorema do Isomorfismo, temos que $\frac{\mathcal{O}_K}{\mathcal{P}} \cong \frac{\mathcal{P}^{\alpha-1}}{\mathcal{P}^\alpha}$.

Assim, $N(\mathcal{P}^\alpha) = \left|\frac{\mathcal{O}_K}{\mathcal{P}^\alpha}\right| = \left|\frac{\mathcal{O}_K}{\mathcal{P}^{\alpha-1}}\right| \left|\frac{\mathcal{P}^{\alpha-1}}{\mathcal{P}^\alpha}\right| = \left|\frac{\mathcal{O}_K}{\mathcal{P}^{\alpha-1}}\right| \left|\frac{\mathcal{O}_K}{\mathcal{P}}\right| = N(\mathcal{P})^{\alpha-1} N(\mathcal{P}) = N(\mathcal{P})^\alpha$, como queríamos provar. □

Definição 5.9. *Seja $\mathcal{I}$ um ideal, dizemos que $a \equiv b \pmod{\mathcal{I}}$ se, e somente se, $a - b \in \mathcal{I}$.*

A partir desse momento vamos supor K uma extensão Galoisiana de grau n de $\mathbb{Q}$ e denotaremos por G o grupo de automorfismos $Gal(K, \mathbb{Q})$. Sabe-se que $|G| = n$.

Definição 5.10. *Se P é um ideal primo e A um ideal, então definimos $ord_P(A)$ como o menor inteiro t, não negativo, tal que $P^t \supset A$ e $P^{t+1} \not\supseteq A$. Denominamos o inteiro t por índice de ramificação de P.*

Proposição 5.11. *Seja $p \in \mathbb{Z}$ um primo, $\mathcal{P}_1$ e $\mathcal{P}_2$ ideais primos em $\mathcal{O}_K$, tal que $(p) \subset \mathcal{P}_1 \cap \mathcal{P}_2$. Então existe $\tau \in G$ tal que $\tau(\mathcal{P}_1) = \mathcal{P}_2$.*

Demonstração. Suponhamos que $\mathcal{P}_2 \notin \{\tau(\mathcal{P}_1) \mid \tau \in G\}$. Portanto, existe $\alpha \in \mathcal{O}_K$ tal que $\alpha \equiv 0 \pmod{\mathcal{P}_2}$ e $\alpha \equiv 1 \pmod{\tau(\mathcal{P}_1)}$ para todo $\tau \in G$. Mas $N(\alpha) = \prod_{\tau \in G} \tau(\alpha) \in \mathcal{P}_2 \cap \mathbb{Z} = (p)$.

Por outro lado, $\tau^{-1}(\alpha) \equiv \tau^{-1}(1) \pmod{\mathcal{P}_1}$ implica que $\tau^{-1}(\alpha) \equiv 1 \pmod{\mathcal{P}_1}$. Assim, $N(\alpha) \equiv 1 \pmod{\mathcal{P}_1}$ e $\tau(\alpha) - 1 \in \mathcal{P}_1 \cap \mathbb{Z} = (p)$, o que é absurdo! Logo existe $\tau \in G$ tal que $\tau(\mathcal{P}_1) = \mathcal{P}_2$. □

Proposição 5.12. *Se $\mathcal{I}$ é um ideal em $\mathcal{O}_K$, então $\prod_{\tau \in G} \tau(\mathcal{I}) = (N(\mathcal{I}))$.*

Demonstração. Como ambos os lados da igualdade são multiplicativos, basta provar para $\mathcal{I} = \mathcal{P}$ um ideal primo. Nesse caso, sejam $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$ e $N(\mathcal{P}) = p^f$, onde p é primo e sejam $\{\mathcal{P}_1, \cdots, \mathcal{P}_s\}$ os elementos distintos do conjunto $\{\tau_i(\mathcal{P}) \mid 1 \leq i \leq n\}$. Assim

$$\prod_{\tau \in G} \tau(\mathcal{P}) = \mathcal{P}_1^u \cdots \mathcal{P}_s^u$$

e $[K:\mathbb{Q}] = n = su$.

Sabemos que $(p) \subset \mathcal{P}$ e, como $p \in \mathbb{Z}$, $\tau((p)) = (p)$. Portanto $(p) \subset \tau_i(\mathcal{P})$ para todo $1 \leq i \leq n$, logo $(p) = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_s^{e_s}$. Aplicando τ_i nos dois lados da igualdade, temos que $(p) = \tau_i(\mathcal{P}_1)^{e_1} \cdots \tau_i(\mathcal{P}_s)^{e_s}$. Se $\mathcal{P}_i = \tau_i(\mathcal{P}_1)$, então, pela unicidade da fatoração em ideais primos, $e_1 = e_i$. Mais ainda, pela Proposição 5.11, $e_1 = \cdots = e_s = e$ e, com isso, $(p) = \mathcal{P}_1^e \cdots \mathcal{P}_s^e$.

Afirmamos que $\left|\frac{\mathcal{O}_K}{(p)}\right| = p^n$. Para isso basta notar que todo elemento de $\mathcal{O}_K$ pode ser escrito como combinação linear de elementos da base de K sobre $\mathbb{Q}$. Portanto todo elemento de $\frac{\mathcal{O}_K}{(p)}$ é representado de modo único por elementos do tipo $\sum_{i=1}^n x_i a_1$, onde a_i é um elemento da base de K sobre $\mathbb{Q}$ e $x_i \in \mathbb{Z}$ é tal que $0 \leq x_i < p$.

Portanto, como τ é automorfismo, $N(\mathcal{P}) = N(\mathcal{P}_i) = p^f$, logo

$$p^n = N(p) = N(\mathcal{P}_1)^e \cdots N(\mathcal{P}_s)^e = p^{efs}.$$

Assim $su = n = efs$ e $u = ef$. Ou seja,

$$\prod_{\tau \in G} \tau(\mathcal{P}) = (\mathcal{P}_1 \cdots \mathcal{P}_s)^{ef} = (p)^f = (p^f) = (N(\mathcal{P})),$$

como queríamos provar. $\square$

Segue diretamente desta demonstração a seguinte proposição:

Proposição 5.13. *Sejam $p \in \mathbb{Z}$ um número primo e $P_1, \cdots, P_s$ os ideais primos em $\mathcal{O}_K$ que contêm p. Sejam e_i e f_i, respectivamente, o índice de ramificação e o grau de tais ideais, para $i = 1, \cdots, s$. Então $e_1 = e_2 = \cdots = e_s$ e $f_1 = f_2 = \cdots = f_s$. Se e e f denotam tais valores, então $efs = n$.*

Proposição 5.14. *Sejam $\alpha \in \mathcal{O}_K$ e $A = (\alpha)$. Então $N(A) = |N(\alpha)|$.*

Demonstração. $(N(A)) = \prod_{\tau\in G} \tau(A) = \prod_{\tau\in G} \tau((\alpha)) = \prod_{\tau\in G}(\tau(\alpha)) = \prod_{\tau\in G}(\tau(\alpha)) = (N(\alpha))$. Com isso concluímos que $N(A) = uN(\alpha)$, onde u é uma unidade. Como $N(A), N(\alpha) \in \mathbb{Z}$ e $N(A)$ é positivo por definição, então $u = \pm 1$ e $N(A) = |N(\alpha)|$. $\square$

Definição 5.15. *Se m é um inteiro, definimos D_m como $D_m := \mathcal{O}_{\mathbb{Q}(\zeta_m)}$ o anel de inteiros de $\mathbb{Q}(\zeta_m)$.*

Observação 5.16. *D_m é um anel de inteiros, logo é um domínio de Dedekind. Portanto, se $\mathcal{P}$ é um ideal primo de D_m, com $p \in \mathcal{P}$ primo, então $\mathcal{P}$ é um ideal maximal e $\frac{D_m}{\mathcal{P}}$ é um corpo de característica p.*

Seja $\mathcal{P} \subset D_m$ um ideal primo tal que $m \notin \mathcal{P}$ e seja $q = N(\mathcal{P}) = \left|\frac{D_m}{\mathcal{P}}\right|$. Como $x^m - 1 = \prod_{i=1}^m (x - \zeta_m^i)$, dividindo por $x - 1$, temos

$$x^{m-1} + \cdots + x + 1 = \prod_{i=1}^{m-1} (x - \zeta_m^i).$$

Tomando $x = 1$, concluímos que $m = \prod_{i=1}^{m-1}(1 - \zeta_m^i)$ e $\overline{m} = \prod_{i=1}^{m-1}\overline{(1 - \zeta_m^i)}$ em $\frac{D_m}{\mathcal{P}}$, onde $\overline{a}$ representa a classe módulo $\mathcal{P}$.

Como $\overline{m} \neq 0$, então $\zeta_m^i \neq 1$ para todo $1 \leq i \leq m-1$. Portanto $\langle \zeta_m \rangle$ é subgrupo de $(\frac{D_m}{\mathcal{P}})^*$ e, com isso, $|\langle \zeta_m \rangle| = m$ divide $\left|(\frac{D_m}{\mathcal{P}})^*\right| = q - 1$.

Proposição 5.17. *Seja $\alpha \in D_m$ tal que $\alpha \notin \mathcal{P}$. Então existe $j \in \mathbb{N}$ único $\pmod m$ tal que $\alpha^{\frac{q-1}{m}} \equiv \zeta_m^j \pmod{\mathcal{P}}$.*

Demonstração. Se $\alpha = 1$, basta tomar $j = m$ e temos o resultado. Suponhamos $\alpha \neq 1$. Como $\left(\frac{D_m}{\mathcal{P}}\right)^*$ é grupo multiplicativo com $q - 1$ elementos, então $\alpha^{q-1} \equiv 1 \pmod{\mathcal{P}}$ e $\prod_{j=1}^{m-1}(\alpha^{\frac{q-1}{m}} - \zeta_m^j) \equiv 0 \pmod{\mathcal{P}}$. Portanto existe $1 \leq j \leq m-1$ tal que $\alpha^{\frac{q-1}{m}} - \zeta_m^j \equiv 0 \pmod{\mathcal{P}}$.

Se existe $i \neq j$ tal que $\alpha^{\frac{q-1}{m}} \equiv \zeta_m^i \pmod{\mathcal{P}}$, então $\zeta_m^{j-i} - 1 \equiv 0 \pmod{\mathcal{P}}$. Mas $(\zeta_m^{j-i} - 1)$ é divisor de (m) e $\mathcal{P}$ simultaneamente, absurdo! Logo ζ^j é único. $\square$

Com a Proposição 5.17, podemos definir o símbolo de resto da potência m-ésima, que será a base para a construção do caracter utilizado na Congruência de Stickelberger. A seguir veremos também algumas propriedades úteis desse símbolo.

Definição 5.18. *Seja $\alpha \in D_m$ e $\mathcal{P}$ um ideal primo tal que $m \notin \mathcal{P}$. Definimos o símbolo de resto da potência m-ésima como*

$$\left(\frac{\alpha}{\mathcal{P}}\right)_m = \begin{cases} 0, & se\ \alpha \in \mathcal{P} \\ \zeta_m^j, & se\ \alpha \notin \mathcal{P}\ e\ \alpha^{\frac{N(\mathcal{P})-1}{m}} \equiv \zeta_m^j \pmod{\mathcal{P}} \end{cases}$$

Tomando $m = 2$ temos o símbolo de Legendre.

Proposição 5.19.

a) Se $\alpha \notin \mathcal{P}$, então $\left(\frac{\alpha}{\mathcal{P}}\right)_m = 1$ se, e somente se, $x^m \equiv \alpha \pmod{\mathcal{P}}$ tem solução em D_m;

b) $\left(\frac{\alpha}{\mathcal{P}}\right)_m = \alpha^{\frac{N(\mathcal{P})-1}{m}} \pmod{\mathcal{P}}$;

c) $\left(\frac{\alpha\beta}{\mathcal{P}}\right)_m = \left(\frac{\alpha}{\mathcal{P}}\right)_m \left(\frac{\beta}{\mathcal{P}}\right)_m$;

d) Se $\alpha \equiv \beta \pmod{\mathcal{P}}$, então $\left(\frac{\alpha}{\mathcal{P}}\right)_m = \left(\frac{\beta}{\mathcal{P}}\right)_m$.

Demonstração. As proposições b), c) e d) são aplicações diretas da definição. Portanto provaremos apenas a proposição a).

Suponhamos primeiramente que $x^m \equiv \alpha \pmod{\mathcal{P}}$ tem solução $x_0 \notin \mathcal{P}$. Nesse caso,

$$\begin{aligned} \alpha^{\frac{N(\mathcal{P})-1}{m}} &\equiv (x_0^m)^{\frac{N(\mathcal{P})-1}{m}} \\ &\equiv x_0^{N(\mathcal{P})-1} \\ &\equiv x_0^{q-1} \equiv 1 \pmod{\mathcal{P}}. \end{aligned}$$

Por outro lado, observemos que $\left(\frac{D_m}{\mathcal{P}}\right)^* = \mathbb{F}_q^*$ é um grupo cíclico de ordem $q - 1$. Seja θ um gerador de $\mathbb{F}_q^*$. Logo $\theta^m, \theta^{2m}, \cdots, \theta^{\frac{q-1}{m}m}$ são raízes distintas de $F(x) = x^{\frac{q-1}{m}} - 1 \in$

$\mathbb{F}_q[x]$. Portanto, se $\overline{\alpha} \in \left(\frac{D_m}{\mathcal{P}}\right)^*$ é tal que $\overline{\alpha}^{\frac{q-1}{m}} = 1$, então $\overline{\alpha}$ é uma solução de $F(x)$ e, consequentemente, existe $1 \leq l \leq \frac{q-1}{m}$ tal que $\overline{\alpha} = \theta^{lm} = (\theta^l)^m$. Assim, $\overline{x} = \theta^l$ é uma solução de $x^m \equiv \alpha \pmod{\mathcal{P}}$. $\square$

Corolário 5.20. $\left(\frac{\zeta_m}{\mathcal{P}}\right)_m = \zeta_m^{\frac{N(\mathcal{P})-1}{m}}$.

Definição 5.21. *Seja $A \subset D_m$ um ideal tal que $m \notin A$ e seja $A = \mathcal{P}_1 \cdots \mathcal{P}_n$ a fatoração em ideais primos de A. Para $\alpha \in D_m$, definimos o símbolo de resto de potência m-ésima como $\left(\frac{\alpha}{A}\right)_m := \left(\frac{\alpha}{\mathcal{P}_1}\right)_m \left(\frac{\alpha}{\mathcal{P}_2}\right)_m \cdots \left(\frac{\alpha}{\mathcal{P}_n}\right)_m$.*

Proposição 5.22. *a) $\left(\frac{\alpha\beta}{A}\right)_m = \left(\frac{\alpha}{A}\right)_m \left(\frac{\beta}{A}\right)_m$;*

b) $\left(\frac{\alpha}{AB}\right)_m = \left(\frac{\alpha}{A}\right)_m \left(\frac{\alpha}{B}\right)_m$;

c) Se α é primo com A e $x^m \equiv \alpha \pmod{A}$ tem solução, então $\left(\frac{\alpha}{A}\right)_m = 1$.

Demonstração. Mais uma vez, as proposições a) e b) são aplicações diretas da definição e da Proposição 5.19. Assim, provaremos apenas o item c) da proposição.

Se $x^m \equiv \alpha \pmod{A}$ tem solução, então, como α e A são coprimos, $x^m \equiv \alpha \pmod{\mathcal{P}_i}$ tem solução para todo $1 \leq i \leq n$. Assim, pela Proposição 5.19, $\left(\frac{\alpha}{\mathcal{P}_i}\right)_m = 1$ para todo $1 \leq i \leq n$ e $\left(\frac{\alpha}{A}\right)_m = \prod_{i=1}^n \left(\frac{\alpha}{\mathcal{P}_i}\right)_m = 1$. $\square$

Proposição 5.23. *Seja $A \subset D_m$ um ideal tal que $\alpha \notin A$. Seja $\tau \in G$, então $\left(\frac{\alpha}{A}\right)_m^\tau = \left(\frac{\alpha^\tau}{A^\tau}\right)_m$.*

Demonstração. Como $\left(\frac{\alpha}{A}\right)_m = \left(\frac{\alpha}{\mathcal{P}_1}\right)_m \cdots \left(\frac{\alpha}{\mathcal{P}_n}\right)_m$ e τ é uma função multiplicativa, basta provar a proposição para $A = \mathcal{P}$ ideal primo. Nesse caso, $\left(\frac{\alpha}{\mathcal{P}}\right)_m \equiv \alpha^{\frac{N(\mathcal{P})-1}{m}} \pmod{\mathcal{P}}$, logo $\left(\frac{\alpha}{\mathcal{P}}\right)_m^\tau \equiv \left(\alpha^{\frac{N(\mathcal{P})-1}{m}}\right)^\tau \pmod{\mathcal{P}^\tau}$. Por outro lado, $\left(\frac{\alpha^\tau}{\mathcal{P}^\tau}\right)_m \equiv (\alpha^\tau)^{\frac{N(\mathcal{P})-1}{m}} \pmod{\mathcal{P}^\tau}$ por definição. Como τ é automorfismo, $\left(\alpha^{\frac{N(\mathcal{P})-1}{m}}\right)^\tau = (\alpha^\tau)^{\frac{N(\mathcal{P})-1}{m}}$, portanto $\left(\frac{\alpha}{\mathcal{P}}\right)_m^\tau = \left(\frac{\alpha^\tau}{\mathcal{P}^\tau}\right)_m$. $\square$

Observação 5.24. *Lembrando que, se l é um primo ímpar e ζ_l é uma raiz l-ésima da unidade, como $x^{l-1} + x^{l-2} + \cdots + x + 1 = \prod_{j=1}^{l-1}(x - \zeta_l^j)$, então $l = \prod_{j=1}^{l-1}(1 - \zeta_l^j) \in D_l$. Notemos que $\frac{1-\zeta_l^i}{1-\zeta_l}$ é uma unidade em D_l, pois $\frac{1-\zeta_l^{ij}}{1-\zeta_l^i}$, com $ij \equiv 1 \pmod{l}$, é o seu inverso. Com isso, podemos escrever $l = u(1-\zeta_l)^{l-1}$ onde u é uma unidade em D_l.*

Definição 5.25. *Seja $\alpha \in D_l$, onde l é um primo ímpar. Dizemos que α é primário se satisfaz as seguinte propriedades:*

a) Não é uma unidade;

b) É coprimo com l;

c) É congruente a um número racional módulo $(1-\zeta_l)^2$.

Proposição 5.26. *Seja $\alpha \in D_l$, com l primo. Existe um inteiro c, único módulo l, tal que $\zeta_l^c \alpha$ é primário.*

Demonstração. Seja $\lambda_l = 1 - \zeta_l$, então $\lambda_l^{l-1} = ul$, onde u é uma unidade em D_l, e $(l) = (\lambda_l^{l-1})$. Como $1 \equiv \zeta_l \pmod{\lambda_l}$, tomando $\alpha = \sum_{j=0}^{l-1} a_j \zeta_l^j$, com $a_j \in \mathbb{Z}$, temos $\alpha \equiv \sum_{j=0}^{l-1} a_j \equiv a \pmod{\lambda_l}$ e $\frac{\alpha - a}{\lambda_l} \in D_l$. Pelo mesmo argumento, existe um $b \in \mathbb{Z}$ tal que $\frac{\alpha - a}{\lambda_l} \equiv b \pmod{\lambda_l}$, logo $\alpha - a \equiv \lambda_l b \pmod{\lambda_l^2}$ e $\alpha \equiv a + b\lambda_l \pmod{\lambda_l^2}$.

Como $\zeta_l = 1 - \lambda_l$, temos $\zeta_l^c = (1 - \lambda_l)^c \equiv 1 - c\lambda_l \pmod{\lambda_l^2}$. Assim $\zeta_l^c \alpha = (a + b\lambda_l)(1 - c\lambda_l) \equiv a + (b - ac)\lambda_l \pmod{\lambda_l^2}$. Como $(a, l) = 1$, basta tomar c tal que $b \equiv ac \pmod{l}$. $\square$

6 Relação e Congruência de Stickelberger

Neste capítulo demonstraremos a Relação e a Congruência de Stickelberger como no Capítulo 14 de [IR]. Para isso, utilizaremos as seguintes notações: sejam $\mathcal{X} : \mathbb{F}_q^* \to \mathbb{C}$ um caracter multiplicativo de ordem m e $\psi : \mathbb{F}_q \to \mathbb{C}$ o caracter aditivo dado por $\psi(a) = \zeta_p^{Tr(a)}$. Estendemos χ em zero de tal forma que $\chi(0) = 0$ se $\chi \neq \mathbf{1}$ e $\mathbf{1}(0) = 1$. Como no capítulo anterior, a soma de Gauss de χ é definida como $g(\mathcal{X}) = \sum_{t \in \mathbb{F}_q} \mathcal{X}(t)\psi(t)$.

Para todo $t \in \mathbb{F}_q \cong \frac{D_m}{\mathcal{P}}$, definimos $\mathcal{X}_{\mathcal{P}} : \mathbb{F}_q \to \mathbb{C}$ da seguinte maneira:

$$\mathcal{X}_{\mathcal{P}}(t) = \begin{cases} 0, & \text{se } t = 0 \\ \left(\frac{\gamma}{\mathcal{P}}\right)_m^{-1}, & \text{onde } \gamma \in D_m \text{ é tal que } \overline{\gamma} = t \in \frac{D_m}{\mathcal{P}}. \end{cases}$$

Com isso, definimos a soma de Gauss para um ideal primo de D_m como $g(\mathcal{P}) := g(\mathcal{X}_{\mathcal{P}}, \psi)$ e $\Phi(\mathcal{P}) := g(\mathcal{P})^m$.

Proposição 6.1. *a) $g(\mathcal{P}) \in \mathbb{Q}(\zeta_m, \zeta_p)$;*

b) $|g(\mathcal{P})|^2 = q$;

c) $\Phi(\mathcal{P}) \in \mathbb{Q}(\zeta_m)$.

Demonstração. a) Como $\mathcal{X}_{\mathcal{P}}(t) \in \mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_m, \zeta_p)$ e $\psi(t) \in \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_m, \zeta_p)$, para todo $t \in \mathbb{F}_q$, segue que $g(\mathcal{P}) \in \mathbb{Q}(\zeta_m, \zeta_p)$.

b) A demonstração é uma aplicação direta do Lema 4.2 c).

c) Basta mostrar que $(g(\mathcal{P})^m)^{\tau_i} = g(\mathcal{P})^m$, para todo τ_i automorfismo de $\mathbb{Q}(\zeta_m, \zeta_p)$ que fixa $\mathbb{Q}(\zeta_m)$, ou seja, para $\tau_i : \begin{matrix} \zeta_m \mapsto \zeta_m \\ \zeta_p \mapsto \zeta_p^i \end{matrix}$, com $i = 1, \cdots, p-1$.

Assim,

$$\begin{aligned} g(\mathcal{P})^{m\tau_i} &= \left(\sum_{t \in \mathbb{F}_q} \mathcal{X}_{\mathcal{P}}(t)\psi(t)\right)^{m\tau_i} = \left(\sum_{t \in \mathbb{F}_q} \mathcal{X}_{\mathcal{P}}(t)\psi(t)^{\tau_i}\right)^m \\ &= \left(\sum_{t \in \mathbb{F}_q} \mathcal{X}_{\mathcal{P}}(t)\psi(t)^i\right)^m = \left(\sum_{t \in \mathbb{F}_q} \mathcal{X}_{\mathcal{P}}(t)\psi(ti)\right)^m. \end{aligned}$$

Tomando $s = ti$, notemos que s percorre todo $\mathbb{F}_q$, assim

$$g(\mathcal{P})^{m\tau_i} = \left(\sum_{t \in \mathbb{F}_q} \mathcal{X}_{\mathcal{P}}(si^{-1})\psi(s)\right)^m = \left(\mathcal{X}_{\mathcal{P}}(i^{-1}) \sum_{t \in \mathbb{F}_q} \mathcal{X}_{\mathcal{P}}(s)\psi(s)\right)^m.$$

Como $\mathcal{X}_{\mathcal{P}}(i)$ é uma raiz m-ésima da unidade, $g(\mathcal{P})^{m\tau_i} = g(\mathcal{P})^m$, como queríamos provar. □

Para demonstrar a Congruência de Stickelberger, além das somas de Gauss, precisaremos de alumas propriedades da função que será definida a seguir.

Definição 6.2. *Seja* $0 \leq a \leq q-1$ *tal que* $a = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$*, definimos* $\sigma_p(a) = a_0 + a_1 + \cdots + a_{f-1}$*. Se* $a \geq q$*, então* $\sigma_p(a) = \sigma_p(t)$*, tal que* $a \equiv t \pmod{q}$ *e* $0 \leq t \leq q-1$

Lema 6.3. *Se* $a \in \mathbb{Z}$*, então* $\sigma_p(a) = (p-1)\sum_{i=0}^{f-1}\{\frac{p^i a}{q-1}\}$*, onde* $\{x\}$ *é a parte fracionária de* x*.*

Demonstração. Seja $a = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$. Observemos que $p^i a \equiv a_{f-i} + a_{f-i+1}p + \cdots + a_{f-i-1}p^{f-1} \pmod{q-1}$, para $i = 0, 1, \cdots, f-1$. Assim,

$$\begin{aligned}
\sum_{i=0}^{f-1}\left\{\frac{p^i a}{q-1}\right\} &= \sum_{i=0}^{f-1}\frac{a_{f-i} + a_{f-i+1}p + \cdots + a_{f-i-1}p^{f-1}}{q-1} \\
&= \frac{1}{q-1}\sum_{j=0}^{f-1}\left(\sum_{i=0}^{f-1} a_i\right)p^j = \frac{\sigma_p(a)}{q-1}\sum_{j=0}^{f-1}p^j = \frac{\sigma_p(a)}{q-1}\frac{q-1}{p-1}.
\end{aligned}$$

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

Lema 6.4. $\sum_{a=1}^{q-2}\sigma_p(a) = \frac{(q-2)(p-1)f}{2}$.

Demonstração. Para cada $1 \leq a \leq q-2$, com $a = (a_{f-1}\cdots a_1 a_0)_p$ na base p, podemos definir $b = (b_{f-1}\cdots b_1 b_0)_p$ tal que $b_i = (p-1-a_i)$. Notemos que se a percorre todos os inteiros entre 1 e $q-2$, b também percorre, porém no sentido contrário. Além disso, notemos que $\sigma_p(a) + \sigma_p(b) = \sigma_p(a+b) = (p-1)f$. Assim, $\sum_{i=1}^{q-2}\sigma_p(a) = \frac{1}{2}\sum_{i=1}^{q-2}(\sigma_p(a) + \sigma_p(b)) = \frac{1}{2}\sum_{i=1}^{q-2}(p-1)f = \frac{(q-2)(p-1)f}{2}$. □

A partir deste momento tomaremos ideais em vários anéis de inteiros diferentes. Para facilitar o entendimento fixaremos o seguinte diagrama:

$$\begin{array}{lcc}
\mathscr{P} \subset D_{(q-1)p} & \to & D_{(q-1)p}/\mathscr{P} \\
| & & | \\
\mathcal{P} \subset D_{q-1} & \to & D_{q-1}/\mathcal{P} \\
| & & | \\
P \subset D_m & \to & D_m/P \\
| & & | \\
p \subset \mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z}
\end{array}$$

Assim, p é um primo e $p\mathbb{Z}$ é o ideal gerado por p em $\mathbb{Z}$, m é um natural tal que $p \nmid m$ e P é o ideal primo em D_m, tal que $P \cap \mathbb{Z} = p\mathbb{Z}$ e $f = ord_m(p)$ é o menor inteiro tal que $p^f \equiv 1 \pmod{m}$. Também denotaremos por $\mathcal{P}$ um ideal primo em D_{q-1} que contém P e por $\mathscr{P}$ um ideal primo em $D_{(q-1)p}$ que contém $\mathcal{P}$.

Relembrando a Definição 5.10, se P é um ideal primo e A um ideal, então definimos $ord_P(A)$ como o menor inteiro t, não negativo, tal que $P^t \supset A$ e $P^{t+1} \not\supseteq A$. Denominamos o inteiro t por índice de ramificação de P.

Se P é um ideal em D_m tal que $P \cap \mathbb{Z} = p\mathbb{Z}$, dizemos que P se ramifica se $ord_P(p) > 1$. As proposições a seguir culminarão no Lema 6.8, que estabelece os índices de ramificação de $\mathscr{P}$. A Congruência de Stickelberger é uma congruência módulo $\mathscr{P}$, assim, esses índices serão amplamente utilizados.

Proposição 6.5. *Se p é um primo tal que $p \nmid m$, então todo ideal primo P em D_m que contém p não se ramifica.*

Demonstração. Se P se ramifica, então $(p) \subset P^2$. Seja $w \in P \setminus P^2$. Observemos que podemos escrever $w = a_0 + a_1\zeta_m + a_2\zeta_m^2 + \cdots + a_l\zeta_m^l$, com $a_i \in \mathbb{Z}$ e $l \leq \varphi(m)$. Como $p \nmid m$, então existe n tal que $p^n \equiv 1 \pmod m$, portanto, usando do fato de que $a^p \equiv a \pmod p$, para todo $a \in \mathbb{Z}$, temos

$$\begin{aligned} w^{p^n} \equiv & (a_0 + a_1\zeta_m + a_2\zeta_m^2 + \cdots + a_l\zeta_m^l)^{p^n} \pmod p \\ \equiv & a_0^{p^n} + (a_1\zeta_m)^{p^n} + (a_2\zeta_m^2)^{p^n} + \cdots + (a_l\zeta_m^l)^{p^n} \pmod p \\ \equiv & a_0 + a_1\zeta_m + a_2\zeta_m^2 + \cdots + a_l\zeta_m^l \pmod p \\ \equiv & a_0 + a_1\zeta_m + a_2\zeta_m^2 + \cdots + a_l\zeta_m^l \equiv w \pmod{P^2} \end{aligned}$$

Mas, como $w^{p^n} \in P^2$, concluímos que $w \in P^2$, absurdo! Logo P não se ramifica. $\square$

Proposição 6.6. *Sejam P um ideal primo em D_m e $P \cap \mathbb{Z} = p\mathbb{Z}$. Se p é ímpar, então P se ramifica se, e somente se, $p|m$.*

Demonstração. Pela proposição anterior, sabemos que $p \nmid m$ implica que P não se ramifica. Suponhamos que p é ímpar e que $p|m$. Nesse caso temos que $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_m)$. Primeiramente mostraremos que (p) se ramifica em D_p.

Temos $\frac{\zeta_p - 1}{\zeta_p^i - 1} \in D_p$ se $(i,p) = 1$. De fato, observe que, como $(i,p) = 1$, pelo Teorema de Bezout ([Apo] Capítulo 1.3) existem $a, b \in \mathbb{Z}$ tais que $ai + bp = 1$, logo

$$\frac{\zeta_p^{ai+bp} - 1}{\zeta_p^i - 1} = \frac{\zeta_p^{ai} - 1}{\zeta_p^i - 1} = \zeta_p^{i(a-1)} + \cdots + \zeta_p^i + 1 \in D_p.$$

Pela Observação 5.24, $p = u(1-\zeta_p)^{p-1}$, onde u é uma unidade em D_p, logo $(p) = (1-\zeta_p)^{p-1}$.

Se $(1-\zeta_p) = P_1P_2\cdots P_t$, com P_i ideais primos em D_m, não necessariamente distintos, então $(p) = (P_1P_2\cdots P_t)^{p-1}$. Como $p - 1 > 1$, todo ideal primo em D_m que contém p se ramifica. $\square$

Proposição 6.7. *Sejam p um primo tal que $p \nmid m$ e D o anel de inteiros de $\mathbb{Q}(\zeta_p, \zeta_m)$. Então*

$$(p) = (P_1P_2\cdots P_s)^{p-1},$$

onde P_i, com $i = 1, \cdots, g$, são ideais primos distintos de grau f e $s = \frac{\varphi(m)}{f}$.

Demonstração. Como $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_p, \zeta_m)$, sabemos pela demonstração da proposição anterior que todos os ideais primos em D que contêm p têm índice de ramificação divisível por $p-1$. Logo

$$(p) = (P_1 P_2 \cdots P_{s'})^{e'(p-1)},$$

onde P_i são ideais primos distintos em D. Sabemos também, pela Proposição 5.13, que cada P_i tem o mesmo grau, que denotamos por f', e que $f's'e'(p-1) = \varphi(pm)$.

Por outro lado, fatorando (p) em D_m, temos

$$(p) = \tilde{P}_1 \tilde{P}_2 \cdots \tilde{P}_s,$$

onde $\tilde{P}_i$ são ideais primos de grau f em D_m. Mais uma vez pela Proposição 5.13, temos que $s = \frac{\varphi(m)}{f}$.

Observando a fatoração de $\tilde{P}_i$ em D e comparando-a com a fatoração de (p) em D, é concluímos que $f' \geq f$ e $s' \geq s$. Assim

$$(p-1)\varphi(m) = \varphi(pm) = e'(p-1)f's' \geq e'(p-1)f\frac{\varphi(m)}{f}.$$

Segue então que $1 \geq e'$, logo $e' = 1$, $f = f'$ e $s' = s = \frac{\varphi(m)}{f}$, concluindo a prova. □

Lema 6.8. *a) $ord_{\mathscr{P}}(pD_{(q-1)p}) = p-1$;*

b) $ord_{\mathscr{P}}(\lambda_p) = 1$, onde $\lambda_p = 1 - \zeta_p$;

c) $ord_{\mathscr{P}}(PD_{(q-1)p}) = p-1$.

Demonstração. a) Este item segue diretamente da Proposição 6.7, assumindo $m = q-1$.

b) Pelo item a), $ord_{\mathscr{P}}(pD_{(q-1)p}) = p-1$. Na demonstração da Proposição 6.6, concluímos que $(p) = (\lambda_p)^{p-1}$, com isso, segue que $(\mathscr{P}_1\mathscr{P}_2 \cdots \mathscr{P}_s)^{p-1} = pD_{(q-1)p} = (pD_p)D_{(q-1)p} = \lambda_p^{p-1}D_{(q-1)p}$. Logo $ord_{\mathscr{P}}(\lambda_p) = 1$.

c) Pela Proposição 5.13, $pD_{q-1} = PP_2 \cdots P_s$, onde $s = \frac{\varphi(q-1)}{f}$ e P_i são ideais primos em D_{q-1}. Por outro lado, pela Proposição 6.7, $pD_{p(q-1)} = (\mathscr{P}\mathscr{P}_2 \cdots \mathscr{P}_s)^{p-1}$, onde $g = \frac{\varphi(q-1)}{f}$. Como $pD_{p(q-1)} = (pD_{q-1})D_{p(q-1)}$, segue que $PP_2 \cdots P_s D_{p(q-1)} = (\mathscr{P}\mathscr{P}_2 \cdots \mathscr{P}_s)^{p-1}$, onde todos os $\mathscr{P}_i$ são primos distintos e $P, P_2, \cdots, P_s$ são primos dois a dois. Assim, $PD_{p(q-1)} = \mathscr{P}^{p-1}$, concluindo a prova.

□

Lema 6.9. $\frac{D_m}{P} \cong \frac{D_{q-1}}{\mathcal{P}}$.

Demonstração. Sabemos que $\frac{D_m}{P}$ é um corpo com $q = p^f$ elementos. Suponhamos que $\left|\frac{D_{q-1}}{\mathcal{P}}\right| = p^{f'}$, então f' é minimal tal que $p^{f'} \equiv 1 \pmod{q-1}$, ou seja, $(p^{f'}-1)|(p^f-1)$. Portanto $f' = f$. □

Definição 6.10. *Seja $\alpha \in D_{q-1}$, definimos*

a) $\left(\frac{\alpha}{\mathcal{P}}\right) = 0$ *se* $\alpha \in \mathcal{P}$*;*

b) Se $\alpha \notin \mathcal{P}$, $\left(\frac{\alpha}{\mathcal{P}}\right)$ *é a única raiz* $(q-1)$*-ésima da unidade tal que* $\alpha - \zeta_{q-1}^{j} \in \mathcal{P}$.

O seguinte lema pode ser concluído diretamente da definição.

Lema 6.11. *Para todo α e β em D_{q-1}, vale*

a) $\left(\frac{\alpha\beta}{\mathcal{P}}\right) = \left(\frac{\alpha}{\mathcal{P}}\right)\left(\frac{\beta}{\mathcal{P}}\right)$*;*

b) Se $\alpha - \beta \in \mathcal{P}$*, então* $\left(\frac{\alpha}{\mathcal{P}}\right) = \left(\frac{\beta}{\mathcal{P}}\right)$*;*

c) Se $\alpha \in D_m$, $\left(\frac{\alpha}{\mathcal{P}}\right)^{\frac{q-1}{m}} = \left(\frac{\alpha}{\mathcal{P}}\right)_m$.

E com isso, podemos definir o seguinte caracter.

Definição 6.12. *Como* $\frac{D_{q-1}}{\mathcal{P}} \cong \mathbb{F}_q$*, se* $t \in \mathbb{F}_q$ *definimos* $\omega(t) = \left(\frac{\gamma}{\mathcal{P}}\right)$*, onde* $t = \overline{\gamma} \in \frac{D_{q-1}}{\mathcal{P}}$.

Assim, como $\omega(\overline{\zeta}_{q-1}^{i}) = \left(\frac{\zeta_{q-1}^{i}}{\mathcal{P}}\right) = \zeta_{q-1}^{i}$, temos que ω é um caracter de ordem $q-1$.

Definição 6.13. *Para cada* $a \in \mathbb{Z}_{\geq 0}$*, definimos* $g_a = g(\omega^{-a}, \psi)$*. Observemos que* $g(\mathcal{P}) = g_{\frac{q-1}{m}}$.

Teorema 6.14. $ord_{\mathscr{P}}(g_a) = \sigma_p(a)$.

Demonstração. Provaremos primeiro para $a = 1$.

$$g_1 = \sum_{t \in \mathbb{F}_q} \omega(t)^{-1} \zeta_p^{Tr(t)} = \sum_{t \in \mathbb{F}_q} \omega(t)^{-1} (1 - \lambda_p)^{Tr(t)}.$$

Observemos que $ord(\overline{\zeta}_{q-1}) = q-1$, portanto $\mathbb{F}_q^* = \langle \overline{\zeta}_{q-1} \rangle$. Assim

$$g_1 = \sum_{i=1}^{q-1} \omega(\overline{\zeta}_{q-1}^{i})^{-1} (1 - \lambda_p)^{Tr(\overline{\zeta}_{q-1}^{i})} = \sum_{i=1}^{q-2} \zeta_{q-1}^{-i} (1 - \lambda_p)^{m_i},$$

onde $m_i \equiv Tr(\overline{\zeta}_{q-1}^{i}) \pmod{p}$.

Notemos que $(1-\lambda_p)^{m_i} = \sum_{j=0}^{m_i} \binom{m_i}{j} (-\lambda_p)^{m_i - j} \equiv 1 - m_i \lambda_p \pmod{\mathscr{P}^2}$. Portanto

$$\begin{aligned} g_1 &\equiv \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} (1 - m_i \lambda_p) \pmod{\mathscr{P}^2} \\ &\equiv (-\sum_{i=0}^{q-2} m_i \zeta_{q-1}^{-i}) \lambda_p \pmod{\mathscr{P}^2} \\ &\equiv -\lambda_p \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} (\zeta_{q-1}^{i} + \zeta_{q-1}^{ip} + \cdots + \zeta_{q-1}^{ip^{f-1}}) \pmod{\mathscr{P}^2} \\ &\equiv -\lambda_p (q-1) \equiv \lambda_p \pmod{\mathscr{P}^2}, \end{aligned}$$

já que $\sum_{i=0}^{q-2} \zeta_{q-1}^{i(p^j - 1)} = 0$, para todo $1 \leq j \leq q-2$, e $\sum_{i=0}^{q-2} \zeta_{q-1}^{0} = q - 1$.

Portanto, $g_1 \equiv \lambda_p \pmod{\mathscr{P}^2}$, o que implica que $g_1 \equiv \lambda_p \pmod{\mathscr{P}}$ e, como $ord_{\mathscr{P}}(\lambda_p) = 1$, concluímos que

$$ord_{\mathscr{P}}(g_1) = 1 = \sigma_p(1).$$

Seja $\theta(a) = ord_{\mathscr{P}}(g_a)$. Sabemos que $\theta(1) = 1$. Vamos mostrar agora que $\theta(a+b) \leq \theta(a) + \theta(b)$ quando $1 \leq a, b, a+b \leq q-1$.

Do Lema 4.4 d), temos que

$$ord_{\mathscr{P}}(g_a g_b) = ord_{\mathscr{P}}(J(\omega^{-a}, \omega^{-b})g_{a+b}) = ord_{\mathscr{P}}(J(\omega^{-a}, \omega^{-b})) + ord_{\mathscr{P}}(g_{a+b}).$$

Portanto $\theta(a+b) \leq \theta(a) + \theta(b)$. Mais ainda, como $J(\omega^{-a}, \omega^{-b}) \in \mathbb{Q}(\zeta_{q-1})$, pelo Lema 6.8 c) $ord_{\mathscr{P}}(J(\omega^{-a}, \omega^{-b})) = p-1$, logo $\theta(a) + \theta(b) \equiv \theta(a+b) \pmod{p-1}$.

Agora vamos mostrar que $\theta(pa) = \theta(a)$.

$$g_{pa} = \sum_{t \in \mathbb{F}_q} \omega(t)^{-pa} \psi(t) = \sum_{t \in \mathbb{F}_q} \omega(t^p)^{-a} \psi(t).$$

Notemos que $Tr(t^p) = Tr(t)$ e $t \mapsto t^p$ é automorfismo em $\mathbb{F}_q$, logo

$$g_{pa} = \sum_{t \in \mathbb{F}_q} \omega(t^p)^{-a} \psi(t^p) = \sum_{t \in \mathbb{F}_q} \omega(t)^{-a} \psi(t) = g_a.$$

Portanto $\theta(pa) = \theta(a)$.

Concluímos então que para todo $1 \leq a \leq p-1$, $\theta(a) = a = \sigma_p(a)$ e, em geral, se $a = a_0 + a_1 p + \cdots + a_{f-1} p^{f-1}$, então $\theta(a) \leq \theta(a_0) + \theta(a_1) + \cdots + \theta(a_{f-1})$ e $\theta(a) \equiv \theta(a_0) + \theta(a_1) + \cdots + \theta(a_{f-1}) \pmod{p-1}$. Ou seja, $\theta(a) \leq \sigma_p(a)$ e $\theta(a) \equiv \sigma_p(a) \pmod{p-1}$.

Por fim, basta mostrar que $\sum_{a=1}^{q-2} \theta(a) = \frac{(p-1)(p-2)f}{2} = \sum_{a=1}^{q-2} \sigma_p(a)$ e teremos $\theta(a) = \sigma_p(a)$.

Para isso, pelo Lema 4.2 b), $g_a g_{q-1-a} = \omega(-1)^a q$, logo

$$\begin{aligned} \theta(g_a) + \theta(g_{q-1-a}) &= ord_{\mathscr{P}}(g_a) + ord_{\mathscr{P}}(g_{q-1-a}) = ord_{\mathscr{P}}(\omega(-1)^a q) \\ &= ord_{\mathscr{P}}(q) = ord_{\mathscr{P}}(p) \cdot f = (p-1)f. \end{aligned}$$

Somando em a,

$$\sum_{a=1}^{q-2} \theta(g_a) + \theta(g_{q-1-a}) = (p-1)(q-2)f.$$

Observemos que $\sum_{a=1}^{q-2} \theta(g_a) = \sum_{a=1}^{q-2} \theta(g_{q-1-a})$, logo $\sum_{a=1}^{q-2} \theta(a) = \frac{(p-1)(q-2)f}{2}$. □

Corolário 6.15. $ord_P(\Phi(P)) = \frac{m}{p-1} \sigma_p\left(\frac{q-1}{m}\right)$.

Demonstração. Pelo Lema 6.8 c), $ord_{\mathscr{P}}(\Phi(P)) = (p-1) ord_P(\Phi(P))$. Mas $ord_{\mathscr{P}}(\Phi(P)) = ord_{\mathscr{P}}(g(P)^m) = m\sigma_p\left(\frac{q-1}{m}\right)$, já que $g(P) = g(\mathcal{X}_P, \psi) = g_{\frac{q-1}{m}}$. Portanto $ord_P(\Phi(P)) = \frac{m}{p-1} \sigma_p\left(\frac{q-1}{m}\right)$. □

Sabemos, pela Proposição 6.1 c), que $|\Phi(P)|^2 = q^m = p^{fm}$, portanto $(p) \subset \Phi(P)$. Assim, todo ideal primo na decomposição de $\Phi(P)$ deve conter p. Mais ainda, notemos que se P' é um ideal primo que contém p, então existe automorfismo τ de $\frac{\mathbb{Q}(\zeta_m)}{\mathbb{Q}}$ tal que $P' = P^{\tau^{-1}}$. Definimos então $P_t := P^{\tau_t^{-1}}$ para $1 \leq t \leq m$, com $(m,t) = 1$.

Lema 6.16. $ord_{P_t}(\Phi(P)) = \frac{m}{p-1}\sigma_p\left(t\frac{q-1}{m}\right)$.

Demonstração. Seja t' tal que $t' \equiv t \pmod m$ e $t' \equiv 1 \pmod p$. Como $(m,p) = 1$, tal sistema sempre tem solução pelo Teorema Chinês do Resto e, como $t' \equiv t \pmod m$, $P_t = P_{t'}$.

Seja $\alpha = ord_{P_{t'}}(\Phi(P))$, então $\Phi(P) = (P^{\tau_{t'}^{-1}})^\alpha L$ e $\Phi(P)^{\tau_{t'}} = P^\alpha L^{\tau_{t'}}$, onde L é um produto de ideais primos distintos de $P_{t'}$. Logo, $\alpha = ord_P(\Phi(P)^{\tau_{t'}})$. Assim, $g(P)^{\tau_{t'}} = \left(\sum_{r\in\mathbb{F}_q} \mathcal{X}_P(r)\psi(r)\right)^{\tau_{t'}} = \sum_{r\in\mathbb{F}_q} \mathcal{X}_P(r)^t\psi(r)$. Como $\Phi(P) = g(P)^m$, concluímos que $\Phi(P)^{\tau_t} = \left(\sum_{r\in\mathbb{F}_q} \mathcal{X}_P(r)^t\psi(r)\right)^m = g_u^m$, com $u = t\frac{q-1}{m}$. Portanto $ord_P(\Phi(P)^{\tau_t}) = ord_P(g_u^m) = \frac{m}{p-1}\sigma_p\left(t\frac{q-1}{m}\right)$. □

Teorema 6.17 (Relação de Stickelberger)**.** *Seja P um ideal primo de D_m tal que $m \notin P$ e $P \cap \mathbb{Z} = p\mathbb{Z}$. Então*

$$\Phi(P) = P^{\sum_{t\in T} t\tau_t^{-1}},$$

onde $T = \{t \in \mathbb{N} \mid 1 \leq t \leq m-1$ e $(t,m) = 1\}$.

Demonstração. Seja

$$G(P) = \{\tau \in Gal(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \mid P^\tau = P\}$$

o subgrupo de $Gal(\mathbb{Q}(\zeta_m) : \mathbb{Q})$ que fixa P, também conhecido como estabilizador de P. Sabe-se que $\tau_p \in G(P)$ e $\langle\tau_p\rangle \subseteq G(P)$. Pela Proposição 5.11, para cada ideal primo P_i que contém p, existe um automorfismo em $Gal(\mathbb{Q}(\zeta_m) : \mathbb{Q})$ que leva P em P_i. Portanto, se s é o número de ideais primos que contêm p, então $s \cdot |G(P)| = |Gal(\mathbb{Q}(\zeta_m) : \mathbb{Q})| = \varphi(m)$. Logo, como f é o menor inteiro tal que $p^f \equiv 1 \pmod m$, pelas Proposições 5.13 e 6.6, segue que $|\langle\tau_p\rangle| = f = \frac{\varphi(m)}{s} = |G(P)|$. Portanto $G(P)$ é cíclico gerado por τ_p.

Denotamos por $\{t_1, t_2, \cdots, t_s\}$ um conjunto de representantes de $\frac{\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*}{\langle p\rangle}$, isto é, para todo $1 \leq t \leq m$, com $(t,m) = 1$, existem $1 \leq i \leq s$ e $0 \leq j \leq f-1$ únicos tais que $t \equiv t_i p^j \pmod m$.

Assim, pelo lema anterior, tomando $\alpha_i = \frac{m}{p-1}\sigma_p(t_i\frac{q-1}{m})$, temos que

$$\Phi(P) = \prod_{i=1}^{s}\left(P^{\tau_{t_i}^{-1}}\right)^{\alpha_i} = P^{\sum_{i=1}^{s}\alpha_i\tau_{t_i}^{-1}} = P^\Lambda.$$

Usando o Lema 6.4,

$$\Lambda = m\sum_{i=1}^{s}\sum_{j=0}^{f-1}\left\{\frac{p^j t_i}{m}\right\}\tau_{t_i}^{-1}\tau_{p^j}^{-1} = m\sum_T\left\{\frac{t}{m}\right\}\tau_t^{-1} = \sum_T t\tau_t^{-1},$$

onde $T = \{t \in \mathbb{N} \mid 1 \leq t \leq m$ e $(t,m) = 1\}$. □

Reparemos que $\Lambda = m\Theta$, onde Θ é o Elemento de Stickelberger da Definição 5.2.

A seguinte relação será utilizada na demonstração do Teorema de Ax.

Teorema 6.18 (Congruência de Stickelberger)**.** *Seja $0 \leq a \leq q-1$ um número inteiro tal que $(a_{f-1}\cdots a_1 a_0)_p = \sum_{j=0}^{f-1} a_j p^j$ é sua representação na base p. Se $\sigma_p(a) = \sum_{i=0}^{f-1} a_i$, $\rho_p(a) = \prod_{i=0}^{f-1} a_i!$ e $\lambda = -\lambda_p = \zeta_p - 1$, então*

$$\frac{g_a \rho_p(a)}{\lambda^{\sigma_p(a)}} \equiv -1 \pmod{\mathscr{P}}.$$

Demonstração. Primeiramente provaremos este teorema para $1 \leq a \leq p-1$. Sejam ω o caracter multiplicativo de $\mathbb{F}_q$, como na Definição 6.12, e $1 \leq n, r \leq q-1$. Observemos que $J(\omega^{-n}, \omega^{-r}) = J(\omega^{q-1-n}, \omega^{q-1-r})$. Portanto,

$$\begin{aligned} J(\omega^{q-1-n}, \omega^{q-1-r}) &= \sum_{t \in \mathbb{F}_q} \omega(t)^{q-1-n} \omega(1-t)^{q-1-r} \\ &\equiv \sum_{\mu} \mu^{q-1-n}(1-\mu)^{q-1-r} \pmod{\mathcal{P}}, \end{aligned}$$

onde μ percorre todas as classes residuais não nulas módulo $\mathcal{P}$. Assim,

$$\begin{aligned} J(\omega^{q-1-n}, \omega^{q-1-r}) &\equiv \sum_{\mu} \mu^{q-1-n}(1-\mu)^{q-1-r} \pmod{\mathcal{P}} \\ &\equiv \sum_{\mu} \mu^{q-1-n} \Big(\sum_{k=0}^{q-1-r} \binom{q-1-r}{k} (-\mu)^k \Big) \pmod{\mathcal{P}} \\ &\equiv \sum_{\mu} \sum_{k=0}^{q-1-r} (-1)^k \binom{q-1-r}{k} \mu^{k+q-1-n} \pmod{\mathcal{P}} \\ &\equiv \sum_{k=0}^{q-1-r} (-1)^k \binom{q-1-r}{k} \sum_{\mu} \mu^{k+q-1-n} \pmod{\mathcal{P}}. \end{aligned}$$

Pela Proposição 3.1, segue que

$$\sum_{\mu} \mu^{k+q-1-n} = \begin{cases} 0 \pmod{\mathcal{P}}, & \text{se } (q-1) \nmid (k-n) \\ -1 \pmod{\mathcal{P}}, & \text{se } (q-1) | (k-n). \end{cases}$$

Como $(q-1)|(k-n)$ se, e somente se, $k = n$, temos que

$$\begin{aligned} J(\omega^{q-1-n}, \omega^{q-1-r}) &\equiv (-1)^{n+1} \binom{q-1-r}{n} \pmod{\mathcal{P}} \\ &\equiv (-1)^{n+1} \frac{(q-1-r)\cdots(q-n-r)}{n!} \pmod{\mathcal{P}} \\ &\equiv (-1)^{n+1}(-1)^n \frac{(1+r)\cdots(n+r)}{n!} \pmod{\mathcal{P}} \\ &\equiv -\frac{(r+n)!}{n!r!} \pmod{\mathcal{P}}. \end{aligned}$$

Portanto, se $1 < a \leq p-1$, vale que $J(\omega^{-1}, \omega^{-(a-1)}) \equiv -a \pmod{\mathcal{P}}$. Mais ainda, do Lema 4.4, sabemos que $g_n g_r = J(w^{-n}, \omega^{-r}) g_{r+n}$, logo,

$$g_a \equiv -\frac{1}{a} g_{a-1} g_1 \pmod{\mathcal{P}}.$$

Aplicando este processo indutivamente, obtemos

$$g_a \equiv \frac{(-1)^{a-1}}{a!} g_1^a \pmod{\mathcal{P}}.$$

Agora vamos calcular g_1^a módulo $\mathscr{P}^{a+1}$. Notemos que $\sum_\mu \omega^{-1}(\mu) = 0$, assim temos que

$$\begin{aligned} g_1 &= \sum_\mu \omega^{-1}(\mu) \zeta_p^{Tr(\mu)} \\ &= \sum_\mu \omega^{-1}(\mu)(\zeta_p^{Tr(\mu)} - 1) \end{aligned}$$

Dividindo por $\lambda_p = 1 - \zeta_p$ e lembrando que $\frac{\zeta_p^r - 1}{1-\zeta_p} \equiv -r \pmod{\lambda_p}$ e que $ord_{\mathscr{P}}(\lambda_p) = 1$, temos

$$\begin{aligned} \frac{g_1}{\lambda_p} &= \sum_\mu \omega^{-1}(\mu) \frac{(\zeta_p^{Tr(\mu)} - 1)}{1 - \zeta_p} \\ &\equiv -\sum_\mu \omega^{-1}(\mu) Tr(\mu) \pmod{\mathscr{P}} \\ &\equiv -\sum_\mu \mu^{-1}(\mu + \mu^p + \cdots + \mu^{p^{f-1}}) \pmod{\mathscr{P}} \\ &\equiv -(q-1) \equiv 1 \pmod{\mathscr{P}}. \end{aligned}$$

Notemos que última igualdade foi utilizado que $\sum_\mu \mu^j = 0$, para todo $j \neq 0$ e $\sum_\mu 1 = q-1$. Portanto $g_1^a \equiv \lambda_p^a \pmod{\mathscr{P}^{a+1}}$ e

$$g_a \equiv \frac{(-1)^{a+1} \lambda_p^a}{a!} \pmod{\mathscr{P}^{a+1}}.$$

Agora, se $1 \leq a \leq p-1$ e $k \in \mathbb{Z}_{>0}$, então $g_{p^k a} = \sum_\mu \omega(\mu)^{-p^k a} \zeta_p^{Tr(\mu)} = \sum_\mu \omega(\mu^{p^k})^{-a} \zeta_p^{Tr(\mu^{p^k})} = g_a$, logo

$$g_{p^k a} \equiv \frac{(-1)^{a+1} \lambda_p^a}{a!} \pmod{\mathscr{P}^{a+1}}$$

e, de outra forma,

$$\frac{g_{p^k a}}{\lambda_p^a} \equiv \frac{(-1)^{a+1}}{a!} \pmod{\mathscr{P}}.$$

Já obtemos a congruência para números entre 1 e $p-1$ e para múltiplos de p. Agora iremos provar para $1 \leq a \leq q-1$, utilizando sua representação na base p, $(a_{f-1} \cdots a_1 a_0)_p$, e o Lema 4.4. A prova segue por indução sobre o número de algarismos não nulos de a na base p.

Assim, se $a = p^k a_k + p^l a_l$, com $1 \leq a_k, a_l \leq p-1$ e $0 \leq k < l$, então, pelo Lema 4.4,

$$g_a = g_{p^k a_k + p^l a_l} = \frac{g_{p^k a_k} g_{p^l a_l}}{J(\omega^{-p^k a_k}, \omega^{-p^l a_l})}.$$

Notemos que,

$$\begin{aligned} J(\omega^{-p^k a_k}, \omega^{-p^l a_l}) &\equiv -\frac{(p^k a_k + p^l a_l)!}{(p^k a_k)!(p^l a_l)!} \\ &\equiv -\frac{(p^k a_k + p^l a_l) \cdots (1 + p^l a_l)}{(p^k a_k)!} \pmod{\mathscr{P}} \\ &\equiv -\frac{(p^k a_k)!}{(p^k a_k)!} \equiv -1 \pmod{\mathscr{P}}. \end{aligned} \tag{6.1}$$

Portanto

$$\begin{aligned} \frac{g_a}{\lambda_p^{a_k + a_l}} &= \frac{g_{a_k}}{\lambda_p^{a_l}} \frac{g_{a_l}}{\lambda_p^{a_l}} \frac{1}{J(\omega^{-p^k a_k}, \omega^{-p^l a_l})} \\ &\equiv \frac{(-1)^{a_k+1}}{a_k!} \frac{(-1)^{a_l+1}}{a_l!} (-1) \pmod{\mathscr{P}} \\ &\equiv \frac{(-1)^{\sigma_p(a)+1}}{\rho_p(a)} \pmod{\mathscr{P}}. \end{aligned}$$

Suponhamos agora que o resultado vale se a tem $s-1$ algarismos não nulos na base p. Suponhamos que a tem s algarismos não nulos na base p e $a = b + p^l a_l$, com $p^l > b$ e $1 \leq a_l \leq p-1$. Assim, temos $g_a = \frac{g_b g_{p^l a_l}}{J(w^{-b}, \omega^{-p^l a_l})}$ e, analogamente à (6.1),

$$J(w^{-b}, \omega^{-p^l a_l}) \equiv -1 \pmod{\mathscr{P}}.$$

Portanto,

$$\begin{aligned} \frac{g_a}{\lambda_p^{\sigma_p(a)}} &= \frac{g_b}{\lambda_p^{\sigma_p(b)}} \frac{g_{a_l}}{\lambda_p^{a_l}} \frac{1}{J(\omega^{-b}, \omega^{-p^l a_l})} \\ &\equiv \frac{(-1)^{\sigma_p(b)+1}}{\rho_p(b)} \frac{(-1)^{a_l+1}}{a_l!} (-1) \pmod{\mathscr{P}} \\ &\equiv \frac{(-1)^{\sigma_p(a)+1}}{\rho_p(a)} \pmod{\mathscr{P}}, \end{aligned}$$

como queríamos provar. $\square$

7 Reciprocidade de Eisenstein

Com a Relação de Stickelberger temos o necessário para a demonstração da Reciprocidade de Eisenstein, como é mostrado na seção 14.5 de [IR]. A Reciprocidade de Eisenstein é um teorema importante no estudo dos corpos ciclotômicos, entretanto, esse resultado não será utilizado nos demais capítulos. Assim, não há mal em pular diretamente para o Capítulo 8, onde apresentaremos os números e corpos p-ádicos.

Utilizaremos as mesmas notações do capítulo anterior, tomando m um inteiro positivo e ζ_m uma raiz m-ésima da unidade.

Lema 7.1. *Se m é um natural ímpar, então as únicas raízes da unidade em $\mathbb{Q}(\zeta_m)$ são $\pm\zeta_m^j$ com $j = 1, \cdots, m$.*

Demonstração. Seja $\theta \in \mathbb{Q}(\zeta_m)$ uma raiz da unidade. Assim, $\theta = \sum_{j=1}^{\varphi(m)} a_j \zeta_m^j$ e $\theta^k = 1$ para algum $k \neq 0$. Provaremos que k divide m.

Se $4|k$, então $\theta^{\frac{k}{4}} = \pm\sqrt{-1} \in \mathbb{Q}(\zeta_m)$ e $\mathbb{Q}(i) \subset \mathbb{Q}(\zeta_m)$. Notemos que $2 = (1+i)^2\left(\frac{1-i}{1+i}\right)$ e $\left(\frac{1-i}{1+i}\right)$ é uma unidade em $\mathbb{Q}(i)$, logo 2 se ramifica em $\mathbb{Q}(i)$. Mas, pela demonstração do Lema 6.8, 2 não se ramifica em $\mathbb{Q}(\zeta_m)$, pois $2 \nmid m$. Absurdo! Portanto $4 \nmid k$.

Se $2|k$, podemos escrever $k = 2k_0$ e $\theta = \pm\zeta_{k_0}^j$, portanto, podemos assumir k ímpar. Como $\theta \in \mathbb{Q}(\zeta_m)$, temos $\mathbb{Q}(\theta) \subset \mathbb{Q}(\zeta_m)$. Assim, existe uma raiz l-ésima da unidade em $\mathbb{Q}(\zeta_m)$, para $l = mmc(k, m)$. Ou seja, $\mathbb{Q}(\zeta_l) \subseteq \mathbb{Q}(\zeta_m)$. Porém, reparemos que $[\mathbb{Q}(\zeta_l) : \mathbb{Q}] = \varphi(l) = \varphi(m\frac{k}{(m,k)}) \geq \varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$. Logo $l = m$ e $k|m$. □

Lema 7.2. *Seja K uma extensão galoisiana de grau n de $\mathbb{Q}$ e seja $Gal(K : \mathbb{Q}) = \{\tau_i : K \to K,\ \text{para } i = 1, \cdots, n\}$ o grupo de Galois da extensão K. Se $\alpha \in \mathcal{O}_K$ é tal que $|\tau_i(\alpha)| \leq 1$ para todo $1 \leq i \leq n$, então α é uma raiz da unidade.*

Demonstração. Para todo $l \in \mathbb{N}$, definamos $f_l(x) = \prod_{i=1}^{n}(x - \tau_i(\alpha^l))$. Como α é um inteiro algébrico, então $f_l(x) \in \mathbb{Z}[x]$. Notemos que

$$(-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \tau_{i_1}(\alpha^l) \cdots \tau_{i_j}(\alpha^l) = a_{j,l}$$

é o coeficiente de x^j em $f_l(x)$.

Assim, $|a_{j,l}|$ é inteiro e $|a_{j,l}| \leq \sum_{i_1 < \cdots < i_j} |\tau_{i_1}(\alpha^l)| \cdots |\tau_{i_j}(\alpha^l)| \leq \binom{n}{j}$, logo só existe um número finito de $a_{j,l}$, ou seja, existem infinitos l_i tais que $f_{l_1}(x) = f_{l_i}(x)$, com $l_1 < l_2 < \cdots < l_i < \cdots$. Observemos que os polinômios $f_{l_j}(x)$ têm as mesmas raízes, não necessariamente na mesma ordem, mas como existem infinitos l_j podemos garantir que há dois destes com raízes na mesma ordem. Assim, podemos tomar $l_s < l_r$ tais que $\alpha^{l_r} = \alpha^{l_s}$. Logo $\alpha^{l_r - l_s} = 1$ e α é uma raiz da unidade. □

Definição 7.3. *Seja $A \subset D_m$ ideal tal que A e (m) são coprimos. Se $A = P_1 \cdots P_n$, definimos $\Phi(A) = \Phi(P_1) \cdots \Phi(P_n)$, onde $\Phi(P) = g(P)^m$.*

Proposição 7.4. *Sejam A e B ideais em D_m coprimos com (m) e $\alpha \in D_m$ coprimo com m. Se $\gamma = \sum_{(t,m)=1} t\tau_t^{-1}$, então*

a) $\Phi(AB) = \Phi(A)\Phi(B)$;

b) $|\Phi(A)|^2 = (N(A))^m$;

c) $(\Phi(A)) = A^\gamma$;

d) $\Phi((\alpha)) = \epsilon(\alpha)\alpha^\gamma$, onde $\epsilon(\alpha)$ é uma unidade em D_m.

Demonstração. a) Este item é uma consequência direta da definição;

b) $|\Phi(A)|^2 = |\Phi(P_1) \cdots \Phi(P_n)|^2 = \prod_{j=1}^n |\Phi(P_j)|^2 = \prod_{j=1}^n |g(P_j)^m|^2 = \prod_{j=1}^n |g(P_j)^2|^m$. Como $|g(P_j)|^2 = |\frac{D_m}{(P_j)}|$, então $\prod_{j=1}^n |\frac{D_m}{(P_j)}|^m = N(A)^m$;

c) $\Phi(A) = \Phi(P_1 \cdots P_n) = \Phi(P_1) \cdots \Phi(P_n)$. Pela Relação de Stickelberger, $\Phi(P_1) \cdots \Phi(P_n) = P_1^\gamma \cdots P_n^\gamma = (P_1 \cdots P_n)^\gamma$;

d) Pela parte c), $(\Phi((\alpha))) = (\alpha)^\gamma = (\alpha^\gamma)$, logo $\Phi((\alpha))$ e α^γ diferem por uma unidade e $\Phi((\alpha)) = \epsilon(\alpha)\alpha^\gamma$, onde $\epsilon(\alpha)$ é uma unidade.

□

Para simplificar a notação, denotaremos $\Phi((\alpha))$ apenas por $\Phi(\alpha)$.

Lema 7.5. *Sejam $A \subseteq D_m$ um ideal coprimo com m e $\tau : \mathbb{Q}(\zeta_m) \to \mathbb{Q}(\zeta_m)$ um automorfismo que fixa $\mathbb{Q}$. Então $\Phi(A)^\tau = \Phi(A^\tau)$.*

Demonstração. $g(P) = \sum_{\alpha \in \frac{D_m}{P}} \left(\frac{\alpha}{P}\right)^{-1} \zeta_p^{Tr(\alpha)}$.

Seja $\overline{\tau} : \mathbb{Q}(\zeta_m, \zeta_p) \to \mathbb{Q}(\zeta_m, \zeta_p)$ um automorfismo tal que $\overline{\tau}|_{\mathbb{Q}(\zeta_m)} = \tau$ e $\overline{\tau}|_{\mathbb{Q}(\zeta_p)} = id$.

$$g(P)^{\overline{\tau}} = \sum_{\alpha \in \frac{D_m}{P}} \left(\left(\frac{\alpha}{P}\right)_m^{-1} \right)^{\overline{\tau}} \zeta_p^{Tr(\alpha)} = \sum_{\alpha \in \frac{D_m}{P}} \left(\frac{\alpha^\tau}{P^\tau}\right)_m^{-1} \zeta_p^{Tr(\alpha)}.$$

Reparemos que $Tr(\alpha) = Tr(\alpha^\tau)$, portanto,

$$g(P)^{\overline{\tau}} = \sum_{\alpha \in \frac{D_m}{P}} \left(\frac{\alpha^\tau}{P^\tau}\right)_m^{-1} \zeta_p^{Tr(\alpha^\tau)} = g(P^\tau).$$

Assim, como $g(P) \in \mathbb{Q}(\zeta_m)$, segue que $g(P)^\tau = g(P)^{\overline{\tau}} = g(P^\tau)$ e, como g e τ são multiplicativas, $g(A)^\tau = g(A^\tau)$. □

Lema 7.6. *Para $\alpha \in D_m$, vale que $|\alpha^\gamma|^2 = |N(\alpha)|^m$.*

Demonstração. Notemos que $\tau_{-1}(\zeta_m) = \zeta_m^{-1} = \overline{\zeta}_m$. Logo $|\alpha^\gamma|^2 = \alpha^\gamma\overline{\alpha^\gamma} = \alpha^\gamma\alpha^{\gamma\tau_{-1}} = \alpha^{\gamma(1+\tau_{-1})}$.

Por outro lado,

$$\begin{aligned}\tau_{-1}\gamma = \tau_{-1}\sum_{\substack{(t,m)=1\\1\leq t\leq m}} t\tau_t^{-1} &= \sum_{\substack{(t,m)=1\\1\leq t\leq m}} t\tau_{-t}^{-1}\\ &= \sum_{\substack{(t,m)=1\\1\leq t\leq m}} t\tau_{m-t}^{-1}.\end{aligned}$$

Notemos que se t percorre todos os coprimos com m entre 1 e m, $m-t$ também percorre. Assim, escrevendo $t = m-(m-t)$, temos

$$\begin{aligned}\tau_{-1}\gamma = \sum_{\substack{(t,m)=1\\1\leq t\leq m}} t\tau_{m-t}^{-1} &= m\sum_{\substack{(t,m)=1\\1\leq t\leq m}} \tau_{m-t}^{-1} - \sum_{\substack{(t,m)=1\\1\leq t\leq m}} (m-t)\tau_{m-t}^{-1}\\ &= m\sum_{\substack{(t,m)=1\\1\leq t\leq m}} \tau_{m-t}^{-1} - \gamma,\end{aligned}$$

logo, $\gamma(1+\tau_{-1}) = m\sum_{\substack{(t,m)=1\\1\leq t\leq m}} \tau_t$. Portanto $|\alpha^\gamma|^2 = \alpha^{m\sum\tau_t} = N(\alpha)^m$. □

Proposição 7.7. *Seja $\alpha \in D_m$ tal que α é coprimo com m. Então $\Phi(\alpha) = \epsilon(\alpha)\alpha^\gamma$, onde $\epsilon(\alpha) = \pm\zeta_m^i$.*

Demonstração. Da Proposição 7.4 d), sabemos que $\Phi(\alpha) = \epsilon(\alpha)\alpha^\gamma$. Tomando o módulo ao quadrado,

$$|\Phi(\alpha)|^2 = |\epsilon(\alpha)|^2|\alpha^\gamma|^2 = |\epsilon(\alpha)|^2|N(\alpha)|^m.$$

Da Proposição 7.4 b), $|\Phi(\alpha)|^2 = |N(\alpha)|^m$, ou seja, $|\epsilon(\alpha)|^2 = 1$. Mais ainda, podemos usar o Lema 7.5 e este mesmo raciocínio para obter $|\tau(\epsilon(\alpha))| = 1$ para todo τ automorfismo de $\mathbb{Q}(\zeta_m)$. Portanto, os Lemas 7.1 e 7.2 nos garantem que $\epsilon(\alpha) = \pm\zeta_m^i$. □

Proposição 7.8. *Sejam $P, P' \subseteq D_m$ ideais primos e coprimos com m e sejam $N(P)$ e $N(P')$ primos entre si. Então $\left(\frac{\Phi(P)}{P'}\right)_m = \left(\frac{N(P')}{P}\right)_m$.*

Demonstração. Seja $q' = p'^{f'} = N(P')$ e ψ um caracter aditivo. Portanto $q' \equiv 1 \pmod{m}$

e

$$\begin{aligned} g(P)^{q'} &\equiv \sum_{t\in\mathbb{F}_q} \mathcal{X}_P(t)^{q'}\psi(t)^{q'} \pmod{p'} \\ &\equiv \sum_{t\in\mathbb{F}_q} \mathcal{X}_P(t)\psi(q't) \pmod{p'} \\ &\equiv \sum_{t\in\mathbb{F}_q} \mathcal{X}_P(q')^{-1}\mathcal{X}_P(q't)\psi(q't) \pmod{p'} \\ &\equiv \mathcal{X}_P(q')^{-1}g(P) \pmod{p'} \\ &\equiv \left(\frac{q'}{P}\right)_m g(P) \pmod{p'}, \end{aligned}$$

lembrando que $\mathcal{X}_P(a) = \left(\frac{a}{P}\right)_m^{-1}$. Como $g(P)$ é primo com P', temos que $g(P)^{q'-1} \equiv \left(\frac{q'}{P}\right)_m \pmod{P'}$.

Assim, $\left(\frac{\Phi(P)}{P'}\right)_m \equiv \Phi(P)^{\frac{q'-1}{m}} = g(P)^{q'-1} \equiv \left(\frac{q'}{P}\right)_m \equiv \left(\frac{N(P')}{P}\right)_m \pmod{P'}$. Se $\left(\frac{\Phi(P)}{P'}\right)_m \equiv \zeta_m^i \pmod{P'}$ e $\left(\frac{N(P')}{P}\right)_m \equiv \zeta_m^j \pmod{P'}$, podemos assumir sem perda de generalidade que $i \leq j$, logo $(\zeta_m^i - \zeta_m^j) = \zeta_m^i(\zeta_m^{j-i} - 1) \in P'$. Se $i \neq j$, temos que $(\zeta_m^{j-i} - 1) \in P'$ é um divisor de m e $m \notin P'$, absurdo! Portanto $i = j$ e $\left(\frac{\Phi(P)}{P'}\right)_m = \left(\frac{N(P')}{P}\right)_m$, como queríamos provar. □

Corolário 7.9. *Se A e B são ideais em D_m coprimos com m e $N(A)$ e $N(B)$ são coprimos, então $\left(\frac{N(B)}{A}\right)_m = \left(\frac{\Phi(A)}{B}\right)_m$.*

Demonstração. O resultado é imediato por multiplicatividade. □

Corolário 7.10. *Sejam A e B como no corolário anterior e $A = (\alpha)$. Então $\left(\frac{\epsilon(\alpha)}{B}\right)_m \left(\frac{\alpha}{N(B)}\right)_m = \left(\frac{N(B)}{\alpha}\right)_m$.*

Demonstração. Primeiro, notemos que

$$\left(\frac{N(B)}{A}\right)_m = \left(\frac{\Phi(A)}{B}\right)_m = \left(\frac{\epsilon(\alpha)}{B}\right)_m \left(\frac{\alpha^\gamma}{B}\right)_m.$$

Em seguida, observemos que

$$\left(\frac{\alpha^{t\tau_t^{-1}}}{B}\right)_m = \left(\frac{\alpha^{\tau_t^{-1}}}{B}\right)_m^t = \left(\frac{\alpha^{\tau_t^{-1}}}{B}\right)_m^{\tau_t} = \left(\frac{\alpha}{B^{\tau_t}}\right)_m.$$

Finalmente,

$$\left(\frac{N(B)}{\alpha}\right)_m = \left(\frac{\epsilon(\alpha)}{B}\right)_m \prod_{\substack{1\leq t\leq m \\ (t,m)=1}} \left(\frac{\alpha}{B^{\tau_t}}\right)_m = \left(\frac{\epsilon(\alpha)}{B}\right)_m \left(\frac{\alpha}{N(B)}\right)_m.$$

□

A partir de agora tomaremos $m = l$, um primo ímpar.

Lema 7.11. *Se $A \subset D_l$ é um ideal coprimo com l, então $\Phi(A) \equiv \pm 1 \pmod{l}$.*

Demonstração. É suficiente mostrar que $\Phi(P) \equiv -1 \pmod{l}$ para P ideal primo. Temos

$$\begin{aligned}\Phi(P) = g(P)^l &= \left(\sum_{t\in\mathbb{F}_q} \mathcal{X}_P(t)\psi(t)\right)^l \\ &\equiv \sum_{t\in\mathbb{F}_q} \mathcal{X}_P(t)^l\psi(t)^l \pmod{l} \\ &\equiv \sum_{t\in\mathbb{F}_q} \mathcal{X}_P(t)^l\psi(lt) \pmod{l}.\end{aligned}$$

Notemos que $\mathcal{X}_P(t)$ é igual a 0 se $t = 0$, e igual a uma raiz l-ésima da unidade se $t \neq 0$, portanto

$$\begin{aligned}\Phi(P) &\equiv \sum_{t\in\mathbb{F}_q^*} \psi(lt) \pmod{l} \\ &\equiv -1 \pmod{l},\end{aligned}$$

uma vez que $\sum_{t\in\mathbb{F}_q} \psi(t) = 0$ e $\psi(0) = 1$. □

Para o próximo lema, precisamos lembrar da seguinte definição do Capitulo 5:

Definição 7.12. *Dizemos que $\alpha \in D_l$ é primário se α é primo com l e $\alpha \equiv x \pmod{(1-\zeta_l)^2}$ para algum $x \in \mathbb{Z}$.*

Lema 7.13. *Se $\alpha \in D_l$ é primário, então $\epsilon(\alpha) = \pm 1$.*

Demonstração. Lembrando que $l = u(1-\zeta_l)^{l-1}$, onde u é uma unidade de D_l, assim os únicos fatores primos de l são $(1-\zeta_l)$. Tomando $\tau \in Gal(\mathbb{Q}(\zeta_l);\mathbb{Q})$, temos que τ fixa l, portanto $(1-\zeta_l)^\tau = (1-\zeta_l)$. Mais ainda, $(1-\zeta_l)^\gamma \subseteq (1-\zeta_l)$.

Como $\Phi(\alpha) = \epsilon(\alpha)\alpha^\gamma$, pelo Lema 7.11, $\epsilon(\alpha)\alpha^\gamma \equiv \pm 1 \pmod{l}$. Como α é primário, $\alpha \equiv x \pmod{(1-\zeta_l)^2}$ para algum $x \in \mathbb{Z}$. Portanto,

$$\alpha^\gamma \equiv x^\gamma \equiv x^{1+\cdots+(l-1)} = x^{\frac{l(l-1)}{2}} \pmod{(1-\zeta_l)^2},$$

mas $x^{\frac{l-1}{2}} \equiv \pm 1 \pmod{l}$, logo $x^{\frac{l-1}{2}} \equiv \pm 1 \pmod{(1-\zeta_l)^2}$ e

$$\alpha^\gamma \equiv (\pm 1)^l \equiv \pm 1 \pmod{(1-\zeta_l)^2}.$$

Segue então que $\epsilon(\alpha) \equiv \pm 1 \pmod{(1-\zeta_l)^2}$. Da Proposição 7.7, sabemos que $\epsilon(\alpha) = \pm\zeta_l^j$. Além disso, é fácil ver que $\zeta_l^j \equiv 1 \pmod{1-\zeta_l}$, portanto $\zeta_l^j \equiv 1 \pmod{(1-\zeta_l)^2}$. Basta mostrar que l divide j. Temos

$$0 \equiv (\zeta_l^j - 1) \pmod{(1-\zeta_l)^2},$$

dividindo por $1 - \zeta_l$,

$$\begin{aligned} 0 &\equiv (\zeta_l^{j-1} + \cdots + \zeta_l + 1) \pmod{1-\zeta_l} \\ 0 &\equiv j \pmod{1-\zeta_l}, \end{aligned}$$

logo $l | j^{l-1}$, mas l é primo, assim $l|j$ e $\epsilon(\alpha) = \pm 1$. □

Proposição 7.14. *Sejam $\alpha \in D_l$ primário, B um ideal primo com l e $N(B)$ primo com α. Então $\left(\frac{\alpha}{N(B)}\right)_l = \left(\frac{N(B)}{\alpha}\right)_l$.*

Demonstração. Já provamos até aqui que

$$\left(\frac{N(B)}{\alpha}\right)_l = \left(\frac{\epsilon(\alpha)}{B}\right)_l \left(\frac{\alpha}{N(B)}\right)_l = \left(\frac{\pm 1}{B}\right)_l \left(\frac{\alpha}{N(B)}\right)_l.$$

Portanto, resta mostrar que $\left(\frac{\epsilon(\alpha)}{B}\right)_l = 1$. Como l é ímpar, $(\pm 1)^l = \pm 1$, assim

$$\left(\frac{\epsilon(\alpha)}{B}\right)_l = \left(\frac{\pm 1}{B}\right)_l = \left(\frac{(\pm 1)^l}{B}\right)_l = \left(\frac{\pm 1}{B}\right)_l^l = 1,$$

como queríamos provar. □

Teorema 7.15 (Reciprocidade de Eisenstein)**.** *Sejam l um primo ímpar, $a \in \mathbb{Z}$ primo com l e $\alpha \in D_l$ primário. Se a e α são coprimos, então $\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l$.*

Demonstração. Como os dois lados da igualdade são multiplicativos, basta mostrar para $a = p$ primo em D_l. Seja P um ideal primo contendo p e $N(P) = q = p^f$. Pela proposição anterior, $\left(\frac{\alpha}{N(P)}\right)_l = \left(\frac{N(P)}{\alpha}\right)_l$, logo, $\left(\frac{\alpha}{p^f}\right)_l = \left(\frac{p^f}{\alpha}\right)_l$ e $\left(\frac{\alpha}{p}\right)_l^f = \left(\frac{p}{\alpha}\right)_l^f$.

Notemos que $f|(l-1)$, logo $(f, l) = 1$, portanto, existem $a, b \in \mathbb{Z}$ tais que $af + bl = 1$. Como $\left(\frac{\alpha}{p}\right)_l^l = \left(\frac{p}{\alpha}\right)_l^l = 1$, concluímos que $\left(\frac{\alpha}{p}\right)_l^{af+bl} = \left(\frac{p}{\alpha}\right)_l^{af+bl}$ e, finalmente,

$$\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l.$$

□

8 Corpos p-ádicos

As demonstrações do Teorema de Ax e da generalização final dos Teoremas de Ax-Katz e Chevalley-Warning se baseiam na relação existente entre $\mathbb{F}_q$ e uma extensão do corpo dos números p-ádicos. Portanto, neste capítulo introduziremos a norma p-ádica e, a partir dos números racionais, construiremos o corpo p-ádico para então encontrar tal relação. Os resultados apresentados neste capítulo podem ser encontrados em [Rob] e em [BBC19].

Definição 8.1. *a) Dado $(\mathcal{A}, +, \cdot)$ anel, dizemos que $(\mathcal{A}, ||\cdot||)$ é uma norma se $||\cdot|| : \mathcal{A} \to \mathbb{R}$ é uma função com as seguintes propriedades:*

1) $||a|| \geq 0$;

2) $||a|| = 0$ *se, e somente se,* $a = 0$;

3) $||a + b|| \leq ||a|| + ||b||$;

4) $||ab|| = ||a|| \cdot ||b||$.

b) Dada uma norma $|| \cdot ||$ denotamos por $d(a, b) = ||a - b||$ a métrica associada a $|| \cdot ||$.

c) Dizemos que $|| \cdot ||$ é não arquimediana se $||a + b|| \leq \max\{||a||, ||b||\}$.

Definição 8.2. *Para $n \in \mathbb{Z}^*$, dizemos que a valoração de n, denotada por $\upsilon_p(n)$, é a maior potência de p que divide n. Denotamos a valoração em 0 por $\upsilon_p(0) = \infty$.*

A definição da função υ_p pode ser estendida para os números racionais de tal forma que $\upsilon_p(\frac{a}{b}) = \upsilon_p(a) - \upsilon_p(b)$.

Teorema 8.3. *Para cada p primo e $\alpha > 1$, a função $|| \cdot ||_{p,\alpha} : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ definida por $a \mapsto \alpha^{-\upsilon_p(a)}$ é uma norma.*

Demonstração. 1) $||a||_{p,\alpha} = \alpha^{-\upsilon_p(a)} \geq 0$.

2) $||a||_{p,\alpha} = 0 \Leftrightarrow \alpha^{-\upsilon_p(a)} = 0 \Leftrightarrow \upsilon_p(a) = \infty \Leftrightarrow a = 0$.

3) $||a + b||_{p,\alpha} = \alpha^{-\upsilon_p(a+b)}$. Consideramos dois casos

- Se $\upsilon_p(a) < \upsilon_p(b)$

$$\upsilon_p(a + b) = \upsilon_p(a) \text{ e } ||a + b||_{p,\alpha} = \alpha^{-\upsilon_p(a)} \leq \max\{||a||_{p,\alpha}, ||b||_{p,\alpha}\}.$$

- Se $\upsilon_p(a) = \upsilon_p(b)$

$$\upsilon_p(a + b) \geq \upsilon_p(a) \text{ e } ||a + b||_{p,\alpha} \leq \alpha^{-\upsilon_p(a)} = \max\{||a||_{p,\alpha}, ||b||_{p,\alpha}\}.$$

4) $||ab||_{p,\alpha} = \alpha^{-\upsilon_p(ab)} = \alpha^{-\upsilon_p(a)}\alpha^{-\upsilon_p(b)} = ||a||_{p,\alpha}||b||_{p,\alpha}$.

Logo $|| \cdot ||_{p,\alpha}$ é uma norma não arquimediana. □

Tomando p primo e $\alpha > 1$, $d_{p,\alpha}(a,b) = ||a-b||_{p,\alpha}$ define uma métrica e um espaço topológico. Uma pergunta natural é qual a relação dos espaços topológicos definidos por $d_{p,\alpha}$ e $d_{p,\beta}$ para $\alpha, \beta > 1$? A seguinte proposição responderá esta pergunta.

Proposição 8.4. *Para p primo e α e β reais maiores que 1, $d_{p,\alpha}$ e $d_{p,\beta}$ definem a mesma topologia.*

Demonstração. Basta mostrar que um aberto de uma topologia pode ser coberto por abertos da outra.

Sejam $a \in \mathbb{Q}$, $r > 0$ e $B_\alpha(a,r) = \{c \in \mathbb{Q} \mid ||a-c||_{p,\alpha} < r\}$. Se $c \in B_\alpha(a,r)$, queremos encontrar $\delta > 0$ tal que $B_\beta(c,\delta) \subseteq B_\alpha(a,r)$.

Mas $x \in B_\beta(c,\delta)$ equivale a $||c-x||_{p,\beta} < \delta$, ou seja, $\beta^{-\upsilon_p(c-x)} < \delta$ e $\upsilon_p(c-x) > -\log_\beta \delta$. Por outro lado, $x \in B_\alpha(a,r)$ implica que $\upsilon_p(a-x) > -\log_\alpha r$.

Como $\upsilon_p(a-x) = \upsilon_p((a-c)+(c-x)) \geq \min\{\upsilon_p(a-c), \upsilon_p(c-x)\}$, queremos que $-\log_\beta \delta$ seja maior que $-\log_\alpha r$. Assim, tomando $\delta < \beta^{\log_\alpha r}$ temos que $B_\beta(c,\delta) \subseteq B_\alpha(a,r)$ e as topologias são iguais. □

Definição 8.5. *Tomando $a \in \mathbb{Q}$ e $\alpha = p$, dizemos que $||a||_p := p^{\upsilon_p(a)}$ é a norma p-ádica de a.*

Definição 8.6. *Seja $\{x_n\}_n$ uma sequência de racionais. Dizemos que $\{x_n\}_n$ é uma sequência de Cauchy com respeito à norma p-ádica se, para todo $\varepsilon > 0$, existe $N > 0$ tal que $||x_n - x_m||_p < \varepsilon$ para todo $n, m > N$.*

Tomemos $\mathcal{C}_p$, o conjunto das sequências de Cauchy formada por números racionais com respeito à norma p-ádica, e $\sim$ a relação de equivalência tal que $\{x_n\} \sim \{y_n\}$ se, para todo $\varepsilon > 0$, existe $N > 0$ tal que $||y_n - x_m||_p < \varepsilon$ para todo $n, m > N$. Definimos $\mathbb{Q}_p := \mathcal{C}_p/\sim$ como o completamento p-ádico dos racionais. Estendemos a função υ_p em $\mathbb{Q}_p$, definindo-a como $\upsilon_p(x) = \lim_{n\to\infty} \upsilon_p(a_n)$, para todo $x \in \mathbb{Q}_p$ tal que $\lim_{n\to\infty} a_n = x$, com $\{a_n\}_n \in \mathcal{C}_p$.

Teorema 8.7. *Sejam $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid \upsilon_p(x) \geq 0\}$ e $\mathcal{I}_p := \{x \in \mathbb{Q}_p \mid \upsilon_p(x) > 0\}$. Então $\mathbb{Z}_p$ é um anel e $\mathcal{I}_p$ é o seu único ideal maximal.*

Demonstração. Sejam $\mathcal{A} \subseteq \mathbb{Z}_p$ um ideal e $\mathcal{C}$ a imagem de $\mathcal{A}$ pela aplicação υ_p. Sejam n_0 o elemento mínimo de $\mathcal{C}$ e $a \in \mathcal{A}$ tal que $\upsilon_p(a) = n_0$.

Se $n_0 = 0$ e $b \in \mathbb{Z}_p$ então $\upsilon_p(ba^{-1}) = \upsilon_p(b) \geq 0$, portanto, $ba^{-1} \in \mathbb{Z}_p$. Assim $b = (ba^{-1})a \in \mathcal{A}$ pois $\mathcal{A}$ é ideal, logo $\mathcal{A} = \mathbb{Z}_p$.

Se $n_0 \geq 1$, então para todo $c \in \mathcal{A}$ tem-se $\upsilon_p(c) \geq 1$. Assim $\upsilon_p(cp^{-1}) \geq 0$, segue que, $cp^{-1} \in \mathbb{Z}_p$ e, desta forma, $c = (cp^{-1})p \in \mathcal{I}_p$. Portanto $\mathcal{A} \subseteq \mathcal{I}_p$ e $\mathcal{I}_p$ é ideal maximal. □

Dada uma extensão de $\mathbb{Q}_p$ de grau n, a chamaremos de $\mathbb{K}$, temos n homomorfismos de $\mathbb{K}$ em $\overline{\mathbb{K}}$ que fixam $\mathbb{Q}_p$ e permutam as raízes do polinômio minimal que define a extensão $\overline{\mathbb{K}}$. Se $\tau_i : \mathbb{K} \to \overline{\mathbb{K}}$, com $i = 1, \cdots, n$, são tais homomorfismos, definimos a função

$N_{\mathbb{K}|\mathbb{Q}_p} : \mathbb{K} \to \mathbb{Q}_p$ como $N_{\mathbb{K}|\mathbb{Q}_p}(\alpha) = \prod_{i=1}^{n} \tau_i(\alpha)$. Com isso, queremos estender a valoração υ_p de $\mathbb{Q}_p$ para $\mathbb{K}$.

Seja $\mathcal{V}_p : \mathbb{K} \to \mathbb{Q}$ tal que $\mathcal{V}_p|_{\mathbb{Q}_p} = \upsilon_p$ e $\mathcal{V}_p(\alpha) = \mathcal{V}_p(\tau_i(\alpha))$, para todo $i = 1, \cdots, n$, e para todo $\alpha \in \mathbb{K}$. Assim, notemos que

$$\upsilon_p(N_{\mathbb{K}|\mathbb{Q}_p}(\alpha)) = \mathcal{V}_p(N_{\mathbb{K}|\mathbb{Q}_p}(\alpha)) = \mathcal{V}_p(\prod_{i=1}^{n} \tau_i(\alpha)) = \sum_{i=1}^{n} \mathcal{V}_p(\tau_i(\alpha)) = n \cdot \mathcal{V}_p(\alpha).$$

Portanto, podemos definir a extensão de υ_p para $\mathbb{K}$, como

$$\mathcal{V}_p(\alpha) = \frac{1}{n}\upsilon_p(N_{\mathbb{K}|\mathbb{Q}_p}(\alpha)).$$

Por abuso de notação, denotaremos por υ_p a extensão de υ_p.

Seja π o elemento em $\mathbb{K}$ com a menor valoração positiva. Definimos $\mathcal{O}_{\mathbb{K}} = \{a \in \mathbb{K} \mid \upsilon_p(a) \geq 0\}$, o anel de inteiros de $\mathbb{K}$ e $\mathcal{M}_{\mathbb{K}} = \pi\mathcal{O}_{\mathbb{K}} = \{a \in \mathcal{O}_{\mathbb{K}} \mid \upsilon_p(a) > 0\}$, o seu ideal maximal. Denotamos por $k = \frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}}$ o corpo residual de $\mathbb{K}$.

Em particular, se $a \in \mathcal{O}_{\mathbb{K}}$, então $\upsilon_p(pa) = \upsilon_p(p) + \upsilon_p(a) = 1 + \upsilon(a) \geq 1$, logo $pa \in \mathcal{M}_{\mathbb{K}}$. Ou seja, k é um corpo de característica p e $\mathbb{F}_p \subset k$.

Definição 8.8. *Definimos o grau residual de $\mathbb{K}$ como o inteiro*

$$f = [k : \mathbb{F}_p].$$

Definimos também o índice de ramificação de $\mathbb{K}$ como o inteiro

$$e = [\upsilon_p(\mathbb{K}^*) : \upsilon_p(\mathbb{Q}_p^*)] = [\upsilon_p(\mathbb{K}^*) : \mathbb{Z}],$$

onde $\upsilon_p(\mathbb{K}^*)$ $\upsilon_p(\mathbb{Q}_p^*)$ são os grupos gerados pela valoração de $\mathbb{K}^*$ e $\mathbb{Q}_p^*$.

Reparemos que, para todo $a \in \mathbb{K}^*$, temos que $a^e \in \mathbb{Q}_p^*$, pela definição do inteiro e. Em particular, $\pi^e \in \mathbb{Q}_p^*$ e $\upsilon_p(\pi^e) > 0$, portanto $\upsilon_p(\pi^e) \geq 1$. Mostraremos que $\upsilon_p(\pi^e) = 1$.

Se $\upsilon_p(\pi^e) > 1$, então $\upsilon_p\left(\frac{\pi^e}{p}\right) > 0$ e $\upsilon_p(\pi) = \upsilon_p(\pi^e\pi^{-(e-1)}) > \upsilon_p(p\pi^{-(e-1)})$. Se $\upsilon_p(p\pi^{-(e-1)}) \leq 0$, então $\upsilon_p(p) \leq \upsilon_p(\pi^{(e-1)}) < \upsilon_p\left(\frac{p}{\pi}\right)$, absurdo! Logo $\upsilon_p(\pi) > \upsilon_p(p\pi^{-(e-1)}) > 0$, mas π é mínimo, absurdo! Assim, $\upsilon_p(\pi^e) = 1$ e $\upsilon_p(\pi) = \frac{1}{e}$.

Proposição 8.9. *Se $\mathbb{K}$ é uma extensão de grau n sobre $\mathbb{Q}_p$, com índice de ramificação e, corpo residual k e grau residual f, então vale que $e \leq n$ e $f \leq n$.*

Demonstração. Sejam $x_1, x_2 \in \mathbb{K}^*$ e $a_1, a_2 \in \mathbb{Q}_p$, tais que

$$\upsilon_p(a_1x_1) = \upsilon_p(a_2x_2) \neq 0.$$

Então $\upsilon_p(x_1) = \upsilon_p\left(\frac{a_2}{a_1}\right) + \upsilon_p(x_2)$, logo x_1 e x_2 pertencem à mesma classe em $\frac{\mathbb{K}^*}{\mathcal{O}_{\mathbb{K}}^*}$. Consequentemente, se $\sum a_ix_i$ é uma soma finita com x_i em classes distintas, então não teremos valuações iguais entre os termos da soma e $\sum a_ix_i \neq 0$ para todo $a_i \in \mathbb{Q}_p^*$.

Assim, tomando $\{\pi, \pi^2, \cdots, \pi^e\}$, temos e classes distintas em $\frac{\mathbb{K}^*}{\mathbb{Q}_p^*}$ e linearmente independentes. Logo $e = [\mathbb{K}^* : \mathbb{Q}_p^*] \leq \dim_{\mathbb{Q}_p} \mathbb{K} = n$.

Sejam $\overline{v}_1, \cdots, \overline{v}_{n+1} \in k^*$ classes distintas e sejam $v_1, \cdots, v_{n+1}$ seus representantes em $\mathbb{K}$. Como $n + 1 > n = \dim_{\mathbb{Q}_p} \mathbb{K}$, segue que

$$a_1 v_1 + \cdots + a_{n+1} v_{n+1} = 0,$$

para algum conjunto de $a_i \in \mathbb{Q}_p$, não todos nulos.

Sem perda de generalidade, podemos assumir que $a_i \in \mathbb{Z}_p$, para todo $i = 1, \cdots, n+1$, mas nem todos pertencem a $p\mathbb{Z}_p$. Assim, tomando a classe em k, temos que $\overline{a}_i \in \mathbb{F}_p$ não são todos nulos e

$$\overline{a}_1 \overline{v}_1 + \cdots + \overline{a}_{n+1} \overline{v}_{n+1} = 0.$$

Logo $\overline{v}_1, \cdots, \overline{v}_{n+1}$ são linearmente dependentes sobre $\mathbb{F}_p$ e $f = [k : \mathbb{F}_p] \leq n$.

□

Proposição 8.10. *Se $\mathbb{K}$ é uma extensão de grau n sobre $\mathbb{Q}_p$, com índice de ramificação e, corpo residual k e grau residual f, então vale que $e \cdot f = n$*

Demonstração. Sejam $s_1, \cdots, s_f \in \mathcal{O}_{\mathbb{K}}$, tais que $\overline{s}_1, \cdots, \overline{s}_f \in k$ formam uma base de k sobre $\mathbb{F}_p$. Gostaríamos de mostrar que o conjunto $\{s_i \pi^j\}$, com $i = 1, \cdots, f$ e $j = 0, \cdots, e-1$, é uma base de k sobre $\mathbb{Q}_p$.

Afirmação: Os elementos $\{s_i \pi^j\}$, com $i = 1, \cdots, f$ e $j = 0, \cdots, e-1$, são $\mathbb{Q}_p$-linearmente independentes.

De fato, tomemos

$$\sum_{\substack{1 \leq i \leq f \\ 0 \leq j < e}} c_{ij} s_i \pi^j = \sum_{0 \leq j < e} x_j \pi^j,$$

onde $x_j = \sum_{1 \leq i \leq f} c_{ij} s_i$ e $c_{ij} \in \mathbb{Q}_p$. Para cada j fixado, existe $l(j) = l$ tal que $\upsilon_p(c_{lj}) \leq \upsilon_p(c_{ij})$, para todo $i = 1, \cdots, f$. Assim,

$$\frac{x_j}{c_{lj}} = \sum_{1 \leq i \leq f} \left(\frac{c_{ij}}{c_{lj}} \right) s_i = \sum_{1 \leq i \leq f} \lambda_i s_i,$$

onde $\upsilon_p(\lambda_i) \geq 0$, para todo $i = 1, \cdots, f$ e $\upsilon_p(\lambda_l) = 0$.

Tomando a classe em k, como $\{\overline{s}_i\}$ são linearmente independentes sobre k, segue que

$$0 \neq \sum_{1 \leq i \leq f} \overline{\lambda}_i \overline{s}_i \in k \text{ e } \sum_{1 \leq i \leq f} \overline{\lambda}_i \overline{s}_i \notin \mathcal{M}_{\mathbb{K}}.$$

Portanto, $\upsilon_p\big(\sum_{1 \leq i \leq f} \overline{\lambda}_i \overline{s}_i \big) = 0$ e $\upsilon_p(x_j) = \upsilon_p(c_{lj}) \in \mathbb{Z}$, para todo $i = 1, \cdots, f$, uma vez que c_{lj} é um elemento de $\mathbb{Q}_p$.

Assim,

$$\sum_{\substack{1 \leq i \leq f \\ 0 \leq j < e}} c_{ij} s_i \pi^j = \sum_{0 \leq j \leq e} x_j \pi^j \neq 0,$$

já que $\upsilon_p(x_j\pi^j) \in \mathbb{Z}^* + \frac{j}{e}$. Logo, para $i = 1, \cdots, f$ e $j = 0, \cdots, e-1$, vale que $\{s_i\pi^j\}$ são linearmente independentes sobre $\mathbb{Q}_p$.

Seja

$$S := \Big\{ \sum_{\substack{1\le i\le f\\ 0\le j<e}} c_{ij}s_i\pi^j \mid 0 \le c_{ij} \le p-1 \Big\} \subseteq \mathcal{O}_{\mathbb{K}}.$$

Se $d_1 \in \mathcal{O}_{\mathbb{K}}$, então $\overline{d}_1 = \sum_{1\le i\le f} b_{i1}\overline{s}_i$, com $b_{i1} \in \mathbb{F}_p$. Ou seja, $(d_1 - \sum_{1\le i\le f} b_{i1}s_i) \in \mathcal{M}_{\mathbb{K}}$ e, consequentemente, $d_1 - \sum_{1\le i\le f} b_{i1}s_i = \pi d_2$, para algum $d_2 \in \mathcal{O}_{\mathbb{K}}$. Indutivamente, construímos uma sequência tal que $d_{j-1} - \sum_{1\le i\le f} b_{i(j-1)}s_i = \pi d_j$. Portanto, temos que

$$d_1 = \sum_{1\le i\le f} b_{i1}s_i + \pi \sum_{1\le i\le f} b_{i2}s_i + \cdots + \pi^{j-1} \sum_{1\le i\le f} b_{ij}s_i + \cdots .$$

Logo, como $\pi^e = p$, segue que

$$\begin{aligned} d_1 &= \sum_{l=0}^{\infty} c_l p^l, \text{ com } c_l \in S \\ &= \sum_{l=1}^{\infty} \Big(\sum_{\substack{1\le i\le f\\ 0\le j<e}} c_{ijl}s_i\pi^j \Big) p^l \\ &= \sum_{\substack{1\le i\le f\\ 0\le j<e}} \Big(\sum_{l=0}^{\infty} c_{ijl}p^l \Big) s_i\pi^j. \end{aligned}$$

Reparemos que $\sum_{l=0}^{\infty} c_{ijl}p^l \in \mathbb{Z}_p$, logo $\mathcal{O}_{\mathbb{K}} \subseteq \langle s_i\pi^j\rangle_{\mathbb{Z}_p}$.

Se $a \in k$, então existe $u \in \mathbb{Z}$ tal que $p^u a \in \mathcal{O}_{\mathbb{K}}$. Ou seja,

$$p^u a = \sum_{\substack{1\le i\le f\\ 0\le j<e}} m_{ij}s_i\pi^j,$$

com $m_{ij} \in \mathbb{Z}_p$. Logo

$$a = \sum_{\substack{1\le i\le f\\ 0\le j<e}} (m_{ij}p^{-u})s_i\pi^j,$$

onde $m_{ij}p^{-u} \in \mathbb{Q}_p$. Portanto $k \subseteq \langle s_i\pi^j\rangle_{\mathbb{Q}_p} \subseteq k$, concluindo a prova. □

Definição 8.11. *Dada uma extensão finita $\mathbb{K}$ de $\mathbb{Q}_p$, dizemos que:*

a) $\mathbb{K}$ é não ramificada quando $e = 1$;

b) $\mathbb{K}$ é completamente ramificada quando $f = 1$.

Observação 8.12. *Se $\mathbb{K}$ é não ramificado, então $\mathcal{M}_{\mathbb{K}} = p\mathcal{O}_{\mathbb{K}}$.*

A partir deste momento assumiremos que $\mathbb{K}$ é uma extensão não ramificada de grau f sobre $\mathcal{O}_{\mathbb{K}}$. Portanto o corpo residual $k = \frac{\mathcal{O}_{\mathbb{K}}}{p\mathcal{O}_{\mathbb{K}}}$ é isomorfo a $\mathbb{F}_q$.

Lema 8.13. *Sejam $x, y \in \mathcal{O}_{\mathbb{K}}$ e $n \in \mathbb{Z}_{>0}$. Se $\upsilon_p(x-y) > 0$ então $\upsilon_p(x^{p^n} - y^{p^n}) \ge n + \upsilon_p(x-y)$.*

Demonstração. Se $\upsilon_p(y) > 0$, então $\upsilon_p(y^{p^n}) \geq p^n \upsilon_p(y) \geq n + \upsilon_p(y)$ e o lema é válido.

Para $\upsilon_p(y) = 0$, faremos a prova por indução sobre o expoente n. Primeiramente tomaremos $n = 1$. Se $\upsilon_p(x - y) > 0$, então $x = y + \alpha$, com $\upsilon_p(\alpha) > 0$, portanto, vale que

$$\begin{aligned}
\upsilon_p(x^p - y^p) =& \upsilon_p((y+\alpha)^p - y^p) \\
=& \upsilon_p(\binom{p}{1}\alpha y^{p-1} + \binom{p}{2}\alpha^2 y^{p-2} + \cdots + \alpha^p) \\
\geq& \min_{1 \leq j \leq p}\{\upsilon_p(\binom{p}{j}\alpha^j y^{p-j})\} \\
=& \min\{1 + \upsilon_p(\alpha), p\upsilon_p(\alpha)\} \\
=& 1 + \upsilon_p(\alpha).
\end{aligned}$$

Suponhamos agora que o lema seja válido para todo natural menor ou igual a n. Para $n + 1$, temos

$$\upsilon_p(x^{p^{n+1}} - y^{p^{n+1}}) = \upsilon_p((x^{p^n})^p - (y^{p^n})^p),$$

pelo caso $n = 1$,

$$\upsilon_p(x^{p^{n+1}} - y^{p^{n+1}}) \geq 1 + \upsilon_p(x^{p^n} - y^{p^n})$$

e pela hipótese de indução,

$$\upsilon_p(x^{p^{n+1}} - y^{p^{n+1}}) \geq 1 + n + \upsilon_p(x - y).$$

□

Lema 8.14. *Seja $x \in \mathcal{O}_{\mathbb{K}}$ e $q = p^f$. Se $\upsilon_p(x) > 0$, então $\upsilon_p(x^{q^n(q-1)}) \geq fn$. Se $\upsilon_p(x) = 0$, então $\upsilon_p(x^{q^n(q-1)} - 1) \geq fn$.*

Demonstração. Se $\upsilon_p(x) > 0$, então $\upsilon_p(x^{q^n(q-1)}) \geq p^{fn}(p^f - 1) \geq fn$.

Se $\upsilon_p(x) = 0$, então $\overline{x} \in \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}}\right)^*$ e, como $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}}$ é um corpo com q elementos, segue que $\overline{x}^{q-1} = \overline{1}$. Ou seja, $x^{q-1} - 1 \in \mathcal{M}_{\mathbb{K}}$.

Com isso, temos que $\upsilon_p(x^{q-1} - 1) \geq 1$, logo, pelo lema anterior, segue que

$$\upsilon_p(x^{p^{fn}(q-1)} - 1^{p^{fn}}) \geq fn + \upsilon_p(x^{q-1} - 1) \geq fn.$$

□

Definição 8.15. *Seja $T_q := \{b \in \mathbb{K} \mid b^q = b\}$. Denominamos T_q como o levantamento de Teichmuller de $\mathbb{F}_q$ em $\mathbb{K}$.*

Proposição 8.16. $|T_q| = q$.

Demonstração. Seja $a \in \mathbb{F}_q^* \cong \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}}\right)^*$. Então existe $a_0 \in \mathcal{O}_{\mathbb{K}}$ tal que $\overline{a}_0 = a$. Consequentemente, $a_0^q - a_0 = m_0 \in \mathcal{M}_{\mathbb{K}}$ com $\upsilon_p(m_0) = l_0 > 0$.

Seja $a_1 = a_0 + m_0$. Notemos que

$$\begin{aligned} \upsilon_p(a_1^q - a_1) =& \upsilon_p((a_0 + m_0)^q - (a_0 + m_0)) \\ =& \upsilon_p(a_0^q + \binom{q}{1} a^{q-1} m_0 + m_0^2 r - a_0 - m_0), \end{aligned}$$

onde $m_0^2 r = (a_0 + m_0)^q - a_0^q - \binom{q}{1} a^{q-1} m_0$. Assim,

$$\begin{aligned} \upsilon_p(a_1^q - a_1) =& \upsilon_p\big(m_0(\binom{q}{1} a^{q-1} + m_0 r)\big) \\ \geq& l_0 + \min\{\upsilon_p(q), \upsilon_p(m_0)\} \geq l_0 + 1. \end{aligned}$$

Construindo indutivamente a sequência $\{a_j\}_{j=0}^{\infty}$ tal que $\upsilon_p(a_j^q - a_j) \geq m_0 + \frac{j}{f}$, $\overline{a}_j = a$ e $\upsilon_p(a_{j+1} - a_j) = \upsilon_p(m_j) \geq m_0 + j$, temos que $\{a_j\}$ é uma sequência de Cauchy, logo converge para um $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $\alpha^q - \alpha = 0$. Como podemos encontrar uma sequência distinta para cada $a \in \mathbb{F}_q^*$ e o elemento 0 é trivial, temos que $|T_q| = |\mathbb{F}_q| = q$. □

Observação 8.17. *Cada elemento do levantamento de Teichmuller, T_q, representa uma classe distinta em $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}}$. Mais ainda, como $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}} \cong \mathbb{F}_q \cong \frac{D_{q-1}}{\mathcal{P}}$, é possível obter uma equivalência entre os elementos de T_q e o conjunto de resíduos módulo $\mathcal{P}$. Assim, os resultados obtidos no Capítulo 6 podem ser utilizados de forma similar para os números p-ádicos através dessa equivalência. Em particular, utilizaremos a Congruência de Stickelberger (Teorema 6.18) para os números p-ádicos no capítulo seguinte.*

9 Teoremas de Ax e Katz

Com as propriedades dos números p-ádicos e a congruência de Stickelberger vistas nos capítulos anteriores, temos o necessário para demonstrar o Teorema de Ax [Ax64] e, com isso, o Teorema de Ax-Katz [Ka71], seguindo a demonstração de [DHX05].

Teorema 9.1 (Ax-1964). *Seja $f \in \mathbb{F}_q[x_1, \cdots, x_n]$, com $\deg(f) = d$, e $s := \lceil \frac{n-d}{d} \rceil$. Então o número de soluções de $f(x_1, \cdots, x_n) = 0$ em $\mathbb{F}_q^n$ é divisível por q^s.*

Demonstração. Sejam $\mathbb{Q}_p$ o corpo dos números p-ádicos com anel de inteiros $\mathbb{Z}_p$, $\mathbb{K}$ uma extensão de $\mathbb{Q}_p$ não ramificada, de grau f e com anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Como $\mathbb{K}$ é não ramificada, tomando $\mathcal{M}_{\mathbb{K}} = p\mathcal{O}_{\mathbb{K}}$, o ideal maximal de $\mathcal{O}_{\mathbb{K}}$, temos que o corpo residual de $\mathbb{K}$, definido como $k = \frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}}$, é uma extensão de grau f de $\mathbb{F}_p$, assim, $k \cong \mathbb{F}_q$, com $q = p^f$. Sejam T_q o levantamento de Teichmuller de k em $\mathbb{K}$ e $T_q^* = T_q \setminus \{0\}$. Reparemos que T_q^* é composto pelas raízes $(q-1)$-ésimas da unidade.

Se ζ_p é uma raiz p-ésima da unidade e $\alpha \in \mathbb{Z}_p$, definimos $\zeta_p^\alpha = \zeta_p^a$, onde $\alpha \equiv a \pmod p$, ou seja, $v_p(\alpha - a) \geq 1$. Definimos também $Tr : \mathbb{K} \to \mathbb{Q}_p$ a função traço.

Seja $C(x) = \sum_{m=0}^{q-1} c_m x^m$ o único polinômio de grau $q-1$ com coeficientes em $\mathbb{K}(\zeta_p)$ tal que $C(t) = \zeta_p^{Tr(t)}$ para todo $t \in T_q$. Podemos assumir a unicidade pela Interpolação de Lagrange. Reparemos que $C(t)$ é um caracter aditivo em T_q e, para $0 \leq j < q-1$, t^{-j} é um caracter multiplicativo em T_q^*. Portanto, podemos definir a soma de Gauss

$$g(j) = \sum_{t \in T_q^*} C(t)t^{-j} = \sum_{t \in T_q^*} t^{-j} \zeta^{Tr(t)}.$$

Assim, para todo $j \neq 0$, temos que

$$\begin{aligned} g(j) &= \sum_{t \in T_q^*} C(t)t^{-j} = \sum_{t \in T_q^*} t^{-j} \sum_{m=0}^{q-1} c_m t^m \\ &= \sum_{m=0}^{q-1} c_m \Big(\sum_{t \in T_q^*} t^{m-j} \Big) = (q-1)c_j. \end{aligned} \tag{9.1}$$

Analogamente, para $j = 0$, temos $-1 = g(0) = (q-1)(c_0 + c_{q-1})$. Como $c_0 = 1$, segue que $(q-1)c_{q-1} = -q$.

Dado $0 \leq j \leq q-1$, seja $j = (j_{f-1} \cdots j_1 j_0)_p$ a representação de j na base p. Definindo as funções $\sigma_p(j) = \sum_{i=0}^{f-1} j_i$, $\rho_p(j) = \prod_{i=0}^{f-1} j_i!$ e $\lambda = -\lambda_p = \zeta_p - 1$, pela Congruência de Stickelberger (Teorema 6.18), segue que

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

para todo $0 \leq j < q-1$. Com (9.1), temos que

$$c_j \equiv 0 \pmod{\lambda^{\sigma_p(j)}}, \tag{9.2}$$

para todo $0 \leq j \leq q-1$. Observemos que o caso $j = 0$ é trivial e o caso $j = q-1$ segue do fato de que $q = p^f = (\lambda_p)^{(p-1)f}$.

Definamos agora a função $\beta : \mathbb{F}_q \to \mathbb{C}$ tal que $\beta(x) = C(t) = \zeta_p^{Tr(t)}$, onde $t \in T_q$ e $\bar{t} = x$. Notemos que a função β é bem definida, pois cada elemento de T_q possui uma classe distinta em $\mathbb{F}_q = \frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}}$, e representa um caracter não trivial do grupo aditivo $\mathbb{F}_q$. Portanto, segue que

$$\sum_{x \in \mathbb{F}_q} \beta(xu) = \begin{cases} q, & \text{se } u = 0 \\ 0, & \text{se } u \neq 0. \end{cases}$$

Assim, temos

$$qN(f=0) = \sum_{x_0 \in \mathbb{F}_q} \sum_{x_1, \cdots, x_n \in \mathbb{F}_q} \beta(x_0 f(x_1, \cdots, x_n)),$$

onde $N(f=0)$ representa o número de soluções de $f = 0$ em $\mathbb{F}_q^n$. Tomemos $f(x_1, \cdots, x_n) = \sum_{w' \in W'} a_{w'} X^{w'}$, onde $W' = \{(w_1, \cdots, w_n) \in \mathbb{N}^n \mid w_1 + \cdots + w_n \leq d)\}$ e $X^{w'} = x_1^{w_1} \cdots x_n^{w_n}$. Para facilitar a notação, associaremos a cada $w' \in W'$ um elemento $w \in W = \{(1, w_1, \cdots, w_n) \in \mathbb{N}^{n+1} \mid w_1 + \cdots + w_n \leq d\}$, de modo que $x_0 f(x_1, \cdots, x_n) = \sum_{w \in W} a_w X^w$ e, por um abuso de notação, $a_w = a_{w'}$. Com isso, se A_w é o representante de Teichmuller de a_w, temos que

$$\begin{aligned} qN(f=0) &= \sum_{X \in \mathbb{F}_q^{n+1}} \prod_{w \in W} \beta(a_w X^w) \\ &= \sum_{t \in T_q^{n+1}} \prod_{w \in W} C(A_w t^w) \\ &= \sum_{t \in T_q^{n+1}} \prod_{w \in W} \sum_{i=0}^{q-1} c_i (A_w t^w)^i \\ &= \sum_{m \in M} \sum_{t \in T_q^{n+1}} \prod_{w \in W} c_{m(w)} A_w^{m(w)} t^{m(w)w}, \end{aligned}$$

onde $M := \{m : W \to \{0, 1, \cdots, q-1\}\}$. Escrevendo $\alpha(m) = \prod_{w \in W} A_w^{m(w)}$ e $e(m) = \sum_{w \in W} m(w)w$, para todo $m \in M$, obtemos

$$qN(f=0) = \sum_{m \in M} \alpha(m) \prod_{w \in W} c_{m(w)} \sum_{t \in T_q^{n+1}} t^{e(m)} \tag{9.3}$$

Vamos limitar inferiormente a potência máxima de q que divide cada uma das parcelas da equação anterior. Para isso, fixando uma função $m : W \to \{0, 1, \cdots, q-1\}$, observemos que

$$\sum_{t \in T_q^{n+1}} t^{e(m)} = \sum_{t_0 \in T_q} \cdots \sum_{t_n \in T_q} t_0^{e_1(m)} \cdots t_n^{e_n(m)},$$

onde $e(m) = (e_0(m), \cdots, e_n(m))$. Analogamente à Proposição 3.1, vale que

$$\sum_{t \in T_q} t^u = \begin{cases} q, & \text{se } u = 0 \\ 0, & \text{se } (q-1) \nmid u \\ q-1, & \text{se } (q-1) | u \text{ e } u \neq 0. \end{cases}$$

Assim, concluímos que $\sum_{t \in T_q^{n+1}} t^{e(m)} = 0$, se existe j tal que $(q-1) \nmid e_j(m)$ ou $\sum_{t \in T_q^{n+1}} t^{e(m)} = q^{n+1}$, se $e(m) = (0, \cdots, 0)$ ou

$$\sum_{t \in T_q^{n+1}} t^{e(m)} = (q-1)^{s+1} q^{n-s}, \tag{9.4}$$

se $(q-1)|e_j(m)$ para todo j e existem exatamente $s+1$ entradas não nulas em $e(m)$, com $s \geq 0$.

Como desejamos encontrar a maior potência de q que divide $N(f=0)$, nos interessa apenas o terceiro caso, já que nos outros ela já está determinada. Portanto, assumiremos que $(q-1)|e_j(m)$, para todo j, e que $e(m)$ possui $s+1$ entradas não nulas. Observemos que a primeira entrada de $e(m)$ é $\sum_{w \in W} m(w)$, ou seja, $\sum_{w \in W} m(w)$ é um múltiplo não nulo de $q-1$.

Para cada $m(w)$, definimos $m(w) = \sum_{i=0}^{q-1} m_i(w) p^i$ a sua representação na base p. Mais ainda, para todo r inteiro, definimos $m_{rf+i}(w) = m_i(w)$. Desta forma, denotaremos por $m^{(j)}(w) = \sum_{i=0}^{q-1} m_{i-j}(w) p^i$ a rotação dos algarismos de $m(w)$ na base p. Reparemos que $\sum_{t \in T_q^{n+1}} t^{e(m)} = \sum_{t \in T_q^{n+1}} t^{e(m^{(j)})}$, já que $\prod_{t \in T_q} t^p = \prod_{t \in T_q} t$. Ou seja, $(q-1)|e(m^{(j)})$, para todo j, e o número de entradas não nulas de $e(m^{(j)})$ também é $s+1$. Em particular, $(q-1)$ divide $\sum_{w \in W} m^{(j)}(w) \neq 0$, a primeira entrada de $e(m^{(j)})$.

Seja $\pi : W' \to W$ tal que $\pi(w_1, \cdots, w_n) = (1, w_1, \cdots, w_n)$. Notemos que, para cada função $m : W \to \{0, 1, \cdots, q-1\}$, podemos definir uma função correspondente $m' : W' \to \{0, 1, \cdots, q-1\}$, dada por $m'(w') = m \circ \pi(w')$. Assim, definindo $e'(m'^{(j)}) = \sum_{w' \in W'} m'(w') w'$, temos que $(q-1)|e'_i(m'^{(j)})$, para todo i, e $e'(m'^{(j)})$ possui s entradas não nulas. Com isso, temos que

$$s(q-1) \leq \sum_{i=1}^{n} e'_i(m'^{(j)}) = \sum_{i=1}^{n} \sum_{w' \in W'} m'^{(j)}(w') w_i \leq d \sum_{w' \in W'} m'^{(j)}(w').$$

Como $\sum_{w' \in W'} m'^{(j)}(w') = \sum_{w \in W} m^{(j)}(w)$ é um múltiplo de $q-1$, segue que

$$\left\lceil \frac{s}{d} \right\rceil (q-1) \leq \sum_{w' \in W'} m'^{(j)}(w').$$

Somando sobre $j = 0, 1, \cdots, f-1$, temos

$$\begin{aligned}\left\lceil \frac{s}{d} \right\rceil (q-1)f &\leq \sum_{j=0}^{f-1} \sum_{w' \in W'} m'^{(j)}(w') \\ &\leq \sum_{w' \in W'} \sum_{j=0}^{f-1} \sum_{i=0}^{f-1} p^i m'_{i-j}(w') \\ &\leq \sum_{w' \in W'} \sum_{i=0}^{f-1} p^i \sigma_p(m'(w')) \leq \frac{q-1}{p-1} \sum_{w' \in W'} \sigma_p(m'(w')),\end{aligned}$$

logo

$$\left\lceil \frac{s}{d} \right\rceil (p-1)f \leq \sum_{w' \in W'} \sigma_p(m'(w')).$$

Como p^f divide $\lambda^{(p-1)f}$, com (9.2), concluímos que a maior potência de q que divide $\prod_{w' \in W'} c_{m'(w')}$ é $\lceil \frac{s}{d} \rceil$. Logo, com (9.4), para cada $m \in M$ tal que $(q-1)|e(m)$, a potência máxima de q que divide $\prod_{w' \in W'} c_{m'(w')} \sum_{t \in T_q^{n+1}} e^{e(m)}$ é maior ou igual a $\lceil \frac{s}{d} \rceil + n - s$, onde s é o número de entradas não nulas de $e(m)$. Assim, usando a equação (9.3), obtemos que q^{r-1} divide $N(f=0)$, onde $r = \min_{0 \leq s \leq n} \left\lceil \frac{s}{d} \right\rceil + n - s$. Mas $\lceil \frac{s}{d} \rceil + n - s$ é decrescente com s variando nos inteiros entre 0 e n, logo $N(f=0)$ é divisível por $q^{\lceil \frac{n}{d} \rceil - 1} = q^{\lceil \frac{n-d}{d} \rceil}$. □

Corolário 9.2. *Sejam $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$, com $\deg(f_j) = d_j$, e $s := \lceil \frac{n - d_1 - \cdots - d_r}{d_1 + \cdots + d_r} \rceil$. Então o número de soluções do sistema $f_j(x_1, \cdots, x_n) = 0$, com $j = 1, \cdots, r$, é divisível por q^s.*

Teorema 9.3 (Ax 1964 - Katz 1971)**.** *a) Sejam $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ polinômios tais que $d_j := \deg(f_j)$, para todo $1 \leq j \leq r$, $d_1 \geq \cdots \geq d_r \geq 1$ e $\sum_{j=1}^r d_j < n$. Se*

$$\mu = \frac{n - \sum_{j=1}^r d_j}{\max_{1 \leq j \leq r} d_j},$$

então $q^{\lceil \mu \rceil}$ divide $\#\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid f_j(x_1, \cdots, x_n) = 0 \ \forall 1 \leq j \leq r\}$.

b) Para todo $n, r, d_1, \cdots, d_r \in \mathbb{Z}_{\geq 0}$, existem $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$, com $\deg(f_j) = d_j$, para $1 \leq j \leq r$, tais que a maior potência de q que divide $\#\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid f_j(x_1, \cdots, x_n) = 0 \ \forall 1 \leq j \leq r\}$ é $\left\lceil \frac{n - \sum_{j=1}^r d_j}{\max_{1 \leq j \leq r} d_j} \right\rceil$.

Neste trabalho apresentaremos apenas a prova da parte a) deste teorema, seguindo a demonstração de [DHX05]. A prova da parte b) pode ser encontrada em [Ka71].

Demonstração. Para todo $f \in \mathbb{F}_q[x_1, \cdots, x_n]$, denotamos por

$$Z(f) = \{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid f(x_1, \cdots, x_n) = 0\}.$$

Assim,

$$\begin{aligned}
\sum_{a_1,\cdots,a_r\in\mathbb{F}_q} |Z(a_1f_1+\cdots+a_rf_r)| = & \sum_{X\in\mathbb{F}_q^n} \sum_{\substack{a_1,\cdots,a_r\in\mathbb{F}_q \\ a_1f_1(X)+\cdots+a_rf_r(X)=0}} 1 \\
= & \sum_{a_1,\cdots,a_r\in\mathbb{F}_q} \sum_{X\in(Z(f_1)\cap\cdots\cap Z(f_r))} 1 \\
& + \sum_{a_1,\cdots,a_r\in\mathbb{F}_q} \sum_{\substack{X\in\mathbb{F}_q^n\setminus Z(f_1)\cap\cdots\cap Z(f_r) \\ a_1f_1(X)+\cdots+a_rf_r(X)=0}} 1 \\
= & q^r\mathcal{Z}_r + q^{r-1}(q^n-\mathcal{Z}_r),
\end{aligned}$$

onde $\mathcal{Z}_i = |Z(f_1)\cap\cdots\cap Z(f_i)|$, para todo $i\in\mathbb{Z}_{\geq 0}$. Ou seja,

$$\begin{aligned}
\mathcal{Z}_r = & \frac{1}{q^r-q^{r-1}}\Big(\sum_{a_1,\cdots,a_r\in\mathbb{F}_q} |Z(a_1f_1+\cdots+a_rf_r)| - q^{r-1+n}\Big) \\
= & \frac{1}{q-1}\Big(\frac{1}{q^{r-1}}\cdot\sum_{a_1,\cdots,a_r\in\mathbb{F}_q} |Z(a_1f_1+\cdots+a_rf_r)| - q^n\Big) \\
\equiv & \frac{q^{1-r}}{q-1}\sum_{a_1,\cdots,a_r\in\mathbb{F}_q} |Z(a_1f_1+\cdots+a_rf_r)| \pmod{q^n}.
\end{aligned}$$

A prova segue por indução sobre r. O caso $r=1$ corresponde ao Teorema de Ax (Teorema 9.1), pois $|Z(f_1)|$ é divisível por q^s, onde $s := \lceil\frac{n-d_1}{d_1}\rceil$.

Suponhamos que o teorema é valido para $r-1$. Se temos r polinômios, seja

$$L := \sum_{i=1}^{r}(d_1-d_i).$$

Fazendo uma segunda indução, agora sobre L, se $L=0$, como $d_1\geq d_j$, para todo $j=2,\cdots,r$, então $d_1=d_2=\cdots=d_r$ e

$$\begin{aligned}
\mathcal{Z}_r \equiv & \frac{q^{1-r}}{q-1}\sum_{a_1,\cdots,a_r\in\mathbb{F}_q} |Z(a_1f_1+\cdots+a_rf_r)| \pmod{q^n} \\
\overset{Ax}{\equiv} & \frac{q^{1-r}}{q-1}\sum_{a_1,\cdots,a_r\in\mathbb{F}_q} q^{\lceil\frac{n-d_1}{d_1}\rceil}\alpha_{a_1,\cdots,a_r} \pmod{q^n} \\
\equiv & \frac{q^{1-r}}{q-1}q^{\lceil\frac{n-d_1}{d_1}\rceil}\alpha \pmod{q^n} \\
\equiv & q^{\lceil\frac{n-d_1}{d_1}-(r-1)\rceil}\frac{\alpha}{q-1} \pmod{q^n} \\
\equiv & q^{\lceil\frac{n-d_1-\cdots-d_r}{d_1}\rceil}\frac{\alpha}{q-1} \pmod{q^n}.
\end{aligned}$$

Portanto $q^{\lceil\frac{n-d_1-\cdots-d_r}{d_1}\rceil}$ divide $\mathcal{Z}_r$.

Suponhamos agora que a hipótese vale quando $\sum_{i=1}^{r}(d_1 - d_i)$ é igual a $L - 1 \geq 0$. Se $\sum_{i=1}^{r}(d_1 - d_i) = L \geq 1$, consequentemente, $d_r < d_1$. Portanto,

$$\begin{aligned}\mathcal{Z}_r \equiv & \frac{q^{1-r}}{q-1} \sum_{a_1,\cdots,a_r \in \mathbb{F}_q} |Z(a_1 f_1 + \cdots + a_r f_r)| \pmod{q^n} \\ \equiv & \frac{q^{1-r}}{q-1} \sum_{a_1,\cdots,a_{r-1} \in \mathbb{F}_q} |Z(a_1 g_1 + \cdots + a_{r-1} g_{r-1} + g_r)| \pmod{q^n},\end{aligned}$$

onde $g_i(x_1, \cdots, x_{n+1}) = f_i(x_1, \cdots, x_n)$ para $1 \leq i \leq r-1$ e $g_r(x_1, \cdots, x_{n+1}) = x_{n+1} f_r(x_1, \cdots, x_n)$. Assim,

$$\begin{aligned}\mathcal{Z}_r \equiv & \frac{q^{1-r}}{(q-1)^2} \sum_{\substack{a_1,\cdots,a_r \in \mathbb{F}_q \\ a_r \neq 0}} |Z(a_1 g_1 + \cdots + a_r g_r)| \pmod{q^n} \\ \equiv & \frac{q^{1-r}}{(q-1)^2} \Big[\sum_{a_1,\cdots,a_r \in \mathbb{F}_q} |Z(a_1 g_1 + \cdots + a_r g_r)| \\ & - \sum_{a_1,\cdots,a_{r-1} \in \mathbb{F}_q} |Z(a_1 g_1 + \cdots + a_{r-1} g_{r-1})| \Big] \pmod{q^n} \\ \equiv & \frac{q^{1-r}}{(q-1)^2} \Big[\frac{q-1}{q^{1-r}} |Z(g_1) \cap \cdots \cap Z(g_r)| - \frac{(q-1)q}{q^{1-(r-1)}} \mathcal{Z}_{r-1} \Big] \pmod{q^n} \\ \equiv & \frac{1}{q-1} \big(|Z(g_1) \cap \cdots \cap Z(g_r)| - \mathcal{Z}_{r-1} \big) \pmod{q^n}.\end{aligned}$$

Pela hipótese de indução sobre r, $\mathcal{Z}_{r-1}$ é divisível por $q^{\lceil \frac{n-d_1-\cdots-d_{r-1}}{d_1} \rceil}$. Por outro lado, $g_1, \cdots, g_r$ são r polinômios de $n+1$ variáveis, com $\tilde{d}_j = \deg(g_j) = d_j$ para $1 \leq j \leq r-1$ e $\tilde{d}_r = \deg(g_r) = d_j + 1$. Assim,

$$\tilde{L} = \sum_{j=1}^{r} (\tilde{d}_1 - \tilde{d}_j) = L - 1.$$

Portanto, pela hipótese de indução sobre L, $|Z(g_1) \cap \cdots \cap Z(g_r)|$ é divisível por $q^{\lceil \frac{n+1-d_1-\cdots-d_{r-1}-(d_r+1)}{d_1} \rceil} = q^{\lceil \frac{n-d_1-\cdots-d_{r-1}-d_r}{d_1} \rceil}$.

Logo, $\mathcal{Z}_r$ é divisível por $q^{\lceil \frac{n-d_1-\cdots-d_{r-1}-d_r}{d_1} \rceil}$. □

Corolário 9.4. *Sejam $f_1, \cdots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$, com $\deg(f_j) = d_j$ e $d_1 \geq \cdots \geq d_r$ e $s := \lceil \frac{n-d_1-\cdots-d_r}{d_1} \rceil$. Se $g_1, \cdots, g_n \in \mathbb{F}_q[x]$ são polinômios de permutação, então o número de soluções do sistema $f_j(g_1(x_1), \cdots, g_n(x_n)) = 0$, para $j = 1, \cdots, r$, em $\mathbb{F}_q^n$ é divisível por q^s.*

Os Teoremas de Ax-Katz e Chevalley-Warning têm sido generalizados de várias formas e, ao longo deste trabalho, mostraremos algumas das generalizações presentes em [BBC19]. A seguir encontra-se a primeira delas, onde são considerados os graus parciais das funções f_i, $i = 1, \cdots, r$, com respeito a algumas variáveis e composição com funções g_j, $j = 1, \cdots, n$, não necessariamente de permutação. Para isso precisaremos das seguintes definições:

Definição 9.5. *Seja $f \in \mathbb{F}_q[x]$, definimos*

$$u(f) = \min\{\delta \in \mathbb{Z}_{>0} \mid \sum_{a \in \mathbb{F}_q} f(a)^\delta \neq 0\}.$$

Se não existe δ, definimos $u(f) = \infty$.

Definição 9.6. *Para cada $\mathcal{I} \subseteq \{1, \cdots, n\}$ não vazio, definimos o $\mathcal{I}$-grau de um monômio como $\deg_{\mathcal{I}}(at_1^{m_1} \cdots t_n^{m_n}) := \sum_{i \in \mathcal{I}} m_i$. Se $P \in \mathbb{F}_q[x_1, \cdots, x_n]$, então $\mathcal{I}$-grau de P é o máximo dos $\mathcal{I}$-graus de seus monômios.*

Lema 9.7. *Sejam $\mathcal{I} \subseteq \{1, \cdots, n\}$ não vazio e $f_1, \cdots, f_n \in \mathbb{F}_q[x]$. Se $P \in \mathbb{F}_q[x_1, \cdots, x_n]$ é um polinômio tal que $\deg_{\mathcal{I}}(P) < \sum_{i \in \mathcal{I}} u(f_i)$, então*

$$\sum_{(x_1, \cdots, x_n) \in \mathbb{F}_q^n} P(f_1(x_1), \cdots, f_n(x_n)) = 0.$$

Demonstração. Se $x_1^{m_1} \cdots x_n^{m_n}$ é um monômio de $P(x_1, \cdots, x_n)$, então $\sum_{i \in \mathcal{I}} m_i < \sum_{i \in \mathcal{I}} u(f_i)$, logo $m_j < u(f_j)$ para algum $j \in \mathcal{I}$. Portanto, pela definição de $u(f_i)$, temos $\sum_{x_j \in \mathbb{F}_q} f_j(x_j)^{m_j} = 0$. Assim, para todo monômio de $P(f_1(x_1), \cdots, f_n(x_n))$ temos:

$$\sum_{(x_1, \cdots, x_n) \in \mathbb{F}_q^n} f_1(x_1)^{m_1} \cdots f_n(x_n)^{m_n} = \prod_{i=1}^{n} \big(\sum_{x_i \in \mathbb{F}_q} f_i(x_i)^{m_i} \big) = 0,$$

concluindo a prova.

□

Teorema 9.8. *Sejam $P_1, \cdots, P_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ polinômios não constantes, $f_1, \cdots, f_n \in \mathbb{F}_q[x]$ polinômios quaisquer e $\mathcal{I} \subseteq \{1, \cdots, n\}$ não vazio. Se*

$$(q-1) \sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j) < \sum_{i \in \mathcal{I}} u(f_i)$$

e $\mathcal{S} := \{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid P_j(f_1(x_1), \cdots, f_n(x_n)) = 0 \ \forall 1 \leq j \leq r\}$, então p divide $|\mathcal{S}|$.

Demonstração. Sejam $P_1, \cdots, P_r \in \mathbb{F}_q[x_1, \cdots, x_n]$, $f_1, \cdots, f_n \in \mathbb{F}_q[x]$ e $\mathcal{I} \subseteq \{1, \cdots, n\}$ como no enunciado. Definimos o seguinte polinômio

$$\vartheta(x_1, \cdots, x_n) := \prod_{j=1}^{r} (1 - P_j(x_1, \cdots, x_n)^{q-1}).$$

Observemos que, se $P(x_1, \cdots, x_n) \neq 0$, então $P(x_1, \cdots, x_n)^{q-1} = 1$. Logo

$$\vartheta(c_1, \cdots, c_n) = \begin{cases} 1, & \text{se } P_j(c_1, \cdots, c_n) = 0, \forall 1 \leq j \leq r \\ 0, & \text{caso contrário.} \end{cases}$$

Assim,

$$\begin{aligned}
|\mathcal{S}| &\equiv \sum_{(x_1,\cdots,x_n)\in\mathbb{F}_q^n} \vartheta(f_1(x_1),\cdots,f_n(x_n)) \pmod p \\
&\equiv \sum_{(x_1,\cdots,x_n)\in\mathbb{F}_q^n} \prod_{j=1}^{r}(1-P_j(f_1(x_1),\cdots,f_n(x_n))^{q-1}) \pmod p \\
&\equiv \sum_{(i_1,\cdots,i_r)\in\{0,1\}^r} \sum_{(x_1,\cdots,x_n)\in\mathbb{F}_q^n} \prod_{j=1}^{r}(-P_j(f_1(x_1),\cdots,f_n(x_n))^{q-1})^{i_j} \pmod p.
\end{aligned}$$

Como para todo $(i_1,\cdots,i_r)\in\{0,1\}^r$ nos temos

$$\deg_{\mathcal{I}}\big(\prod_{j=1}^{r}(-P_j(x_1,\cdots,x_n)^{q-1})^{i_j}\big) \le (q-1)\sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j) < \sum_{i\in\mathcal{I}} u(f_i),$$

pelo Lema 9.7, $|\mathcal{S}|\equiv 0 \pmod p$, como queríamos provar.

□

Corolário 9.9. *Sejam $P_1,\cdots,P_r\in\mathbb{F}_q[x_1,\cdots,x_n]$, $f_1,\cdots,f_n\in\mathbb{F}_q[x]$ polinômios não constantes e $\mathcal{I}\subseteq\{1,\cdots,n\}$ não vazio. Se*

$$(q-1)\sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j) \le \sum_{i\in\mathcal{I}}\left\lceil \frac{q-1}{\deg(f_i)}\right\rceil,$$

então p divide

$$\#\{(x_1,\cdots,x_n)\in\mathbb{F}_q^n \mid P_j(f_1(x_1),\cdots,f_n(x_n))=0,\ \forall 1\le j\le r\}.$$

Demonstração. Basta mostrar que $u(f)\ge\frac{q-1}{\deg(f)}$ para todo polinômio não constante f. Suponhamos que existe $l<\frac{q-1}{\deg(f)}$ tal que $\sum_{c\in\mathbb{F}_q} f(c)^l\neq 0$. Nesse caso, $\deg(f^l)=l\deg(f)<q-1$. Escrevendo $f(x)^l=\sum_{j=0}^{q-2}a_jx^j$, temos que

$$\sum_{c\in\mathbb{F}_q}\sum_{j=0}^{q-2}a_jc^j=\sum_{j=0}^{q-2}a_j\big(\sum_{c\in\mathbb{F}_q}c^j\big)=0.$$

Absurdo! Logo $u(f)\ge\frac{q-1}{\deg(f)}$. □

Teorema 9.10. *Se $u(f)<\infty$, então $u(f)\le\#f(\mathbb{F}_q)-1$.*

Demonstração. Seja $g(c)=\#\{a\in\mathbb{F}_q\mid f(a)=c\}$ e $f(\mathbb{F}_q)=\{c_1,\cdots,c_{l+1}\}$. Suponhamos que $u(f)<\infty$ e $u(f)>\#f(\mathbb{F}_q)-1$. Então, $\sum_{a\in\mathbb{F}_q}f(a)^\delta=\sum_{j=1}^{l+1}g(c_j)c_j^\delta=0$ para todo $0\le\delta\le l$. Portanto

$$\begin{pmatrix}1&\cdots&1\\ c_1&\cdots&c_{l+1}\\ \vdots&\ddots&\vdots\\ c_1^l&\cdots&c_{l+1}^l\end{pmatrix}\begin{pmatrix}g(c_1)\\ g(c_2)\\ \vdots\\ g(c_{l+1})\end{pmatrix}=\begin{pmatrix}0\\0\\ \vdots\\0\end{pmatrix}.$$

Como a primeira matriz é a matriz de Vandermonde e, consequentemente, é invertível, temos que $g(c_1)=\cdots=g(c_{l+1})=0$. Absurdo! Logo $u(f)\le\#f(\mathbb{F}_q)-1$. □

Em [CSW93], Da Qing Wan, Peter Jau-Shyong Shiue e Ching Shyang Chen utilizam a função $u(f)$ para buscar cotas superiores e inferiores para $\#f(\mathbb{F}_q)$. A seguinte definição foi tomada de [BBC19], inspirada pelo trabalho de Wan, Shiue e Chen.

Definição 9.11. *Se $f \in \mathbb{F}_q[x]$ é um polinômio tal que $u(f) = \#f(\mathbb{F}_q) - 1$, dizemos que f é um WSC-polinômio. Dizemos também que f é WSC-fraco se $u(f) < \infty$.*

Corolário 9.12. *Sejam $P_1, \cdots, P_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ polinômios não constantes e seja $\mathcal{I} \subseteq \{1, \cdots, n\}$ não vazio. Sejam $f_1, \cdots, f_n \in \mathbb{F}_q[x]$ tais que f_i é WSC-polinômio para todo $i \in \mathcal{I}$. Se*

$$(q-1)\sum_{j=1}^{r} \deg_{\mathcal{I}}(P_i) < \sum_{i \in \mathcal{I}} (\#f_i(\mathbb{F}_q) - 1),$$

então p divide

$$\#\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid P_j(f_1(x_1), \cdots, f_n(x_n)) = 0 \ \forall 1 \leq j \leq r\}.$$

Demonstração. Como f_i é WSC-polinômio para todo $i \in \mathcal{I}$, então $u(f_i) = \#f_i(\mathbb{F}_q) - 1$. Portanto $(q-1)\sum_{j=1}^{r} \deg_{\mathcal{I}}(P_i) < \sum_{i \in \mathcal{I}} u(f_i)$ e vale o Teorema 9.8. $\square$

10 Generalização dos teoremas de Ax-Katz e Chevalley-Warning

A próxima generalização dos teoremas de Ax-Katz e Chevalley-Warning foi realizada por Baoulina, Bishnoi e Clarck em [BBC19]. Supondo uma condição similar à usada no Teorema 9.8, utilizaremos composição com funções $f_i \in \mathbb{F}_q[x]$, com $i = 1, \cdots, n$ e tomaremos graus parciais dos polinômios P_j, com $j = 1, \cdots, r$. Para isso, precisaremos do seguinte lema e de algumas propriedades da soma dos algarismos de um natural na base p.

Lema 10.1. *Seja $f \in \mathbb{F}_q[t]$ não constante e seja $\tilde{f} \in T_q[t]$ o levantamento de Teichmuller de f. Escrevendo $\tilde{f}(t) = \sum_{l=1}^{R} b_l t^{m_l}$ onde $b_l \in \mathcal{O}_{\mathbb{K}}^*$, $m_l \in \mathbb{Z}_{\geq 0}$ e $m_1 < m_2 < \cdots < m_R$, então para $\delta \in \mathbb{Z}_{\geq 0}$ se satisfaz a relação*

$$\sum_{x \in T_q} \tilde{f}(x)^\delta = q\tilde{f}(0)^\delta + (q-1) \sum_{\substack{\sum_{l=1}^R \delta_l = \delta \\ \sum_{l=1}^R m_l\delta_l \in (q-1)\mathbb{Z}_{>0}}} \binom{\delta}{\delta_1, \cdots, \delta_R} b_1^{\delta_1} \cdots b_R^{\delta_R}.$$

Demonstração. Observemos que

$$\begin{aligned}
\sum_{x \in T_q} \tilde{f}(x)^\delta &= \sum_{x \in T_q} \Big(\sum_{l=1}^{R} b_l x^{m_l}\Big)^\delta \\
&= \sum_{x \in T_q} \sum_{u=0}^{m_R\delta} \Big(\sum_{\substack{\sum_{l=1}^R \delta_l = \delta \\ \sum_{l=1}^R m_R\delta_l = u}} \binom{\delta}{\delta_1, \cdots, \delta_R} b_1^{\delta_1} \cdots b_R^{\delta_R} \Big) x^u \\
&= \sum_{u=0}^{m_R\delta} \Big(\sum_{\substack{\sum_{l=1}^R \delta_l = \delta \\ \sum_{l=1}^R m_l\delta_l = u}} \binom{\delta}{\delta_1, \cdots, \delta_R} b_1^{\delta_1} \cdots b_R^{\delta_R} \Big) \sum_{x \in T_q} x^u.
\end{aligned}$$

Analogamente à Proposição 3.1,

$$\sum_{x \in T_q} x^u = \begin{cases} q, & \text{se } u = 0 \\ q-1, & \text{se } (q-1) | u \text{ e } u > 0 \\ 0, & se\ (q-1) \nmid u. \end{cases}$$

Assim, basta tomar $u \in (q-1)\mathbb{Z}_{\geq 0}$.

Se $m_1 \neq 0$, então $u = \sum_{l=1}^R m_l \delta_l > 0$, uma vez que $\sum_{l=1}^R \delta_l = \delta > 0$. Desta forma,

$$\sum_{x \in T_q} \tilde{f}(x)^\delta = (q-1) \sum_{\substack{\sum_{l=1}^R \delta_l = \delta \\ \sum_{l=1}^R m_l\delta_l \in (q-1)\mathbb{Z}_{>0}}} \binom{\delta}{\delta_1, \cdots, \delta_R} b_1^{\delta_1} \cdots b_R^{\delta_R}.$$

Por outro lado, se $m_1 = 0$ então $u \geq 0$ e

$$\sum_{x \in T_q} \tilde{f}(x)^\delta = b_1^\delta q + (q-1) \sum_{\substack{\sum_{l=1}^R \delta_l = \delta \\ \sum_{l=1}^R m_l \delta_l \in (q-1)\mathbb{Z}_{>0}}} \binom{\delta}{\delta_1, \cdots, \delta_R} b_1^{\delta_1} \cdots b_R^{\delta_R}.$$

Como $\tilde{f}(0) = \begin{cases} 0, & se\ m_1 = 0 \\ b_1, & se\ m_1 \neq 0 \end{cases}$ então

$$\sum_{x \in T_q} \tilde{f}(x)^\delta = \tilde{f}(0)^\delta q + (q-1) \sum_{\substack{\sum_{l=1}^R \delta_l = \delta \\ \sum_{l=1}^R m_l \delta_l \in (q-1)\mathbb{Z}_{>0}}} \binom{\delta}{\delta_1, \cdots, \delta_R} b_1^{\delta_1} \cdots b_R^{\delta_R}.$$

□

No Capítulo 6, havíamos definido a função σ_p como a soma dos algarismos na base p para inteiros módulo q. Aqui definiremos esta mesma função, porém, para inteiros de maneira geral. Cometeremos um abuso de notação e também denotaremos esta função por σ_p.

Definição 10.2. *Seja $N \geq 2$ um número natural e $a \in \mathbb{Z}_{\geq 0}$, então denotaremos por $\sigma_N(a)$ a soma dos algarismos de a na base N.*

Lema 10.3. *Seja $N \geq 2$ um número natural, $a, b \in \mathbb{Z}_{\geq 0}$ e $q = p^f$. Então:*

a) $\sigma_N(a) + \sigma_N(b) \geq \sigma_N(a+b)$;

b) $\sigma_N(a)\sigma_N(b) \geq \sigma_N(ab)$;

c) Se $a \in (q-1)\mathbb{Z}_{>0}$ então $\sigma_p(a) \geq \sigma_p(q-1) = f(p-1)$.

Demonstração. Sejam $a = (a_m a_{m-1} \cdots a_0)_N$ e $b = (b_m b_{m-1} \cdots b_0)_N$ representações de a e b na base N, com $0 \leq a_i, b_j \leq N-1$.

a) Temos $a+b = \sum_{j=0}^m (a_j+b_j)N^j = \sum_{j=0}^{m+1} c_j N^j$, onde $0 \leq a_j+b_j \leq 2N-2$ e $0 \leq c_j \leq N-1$. Observemos que

$$c_0 = \begin{cases} a_0 + b_0, & \text{se } a_0 + b_0 \leq N-1 \\ a_0 + b_0 - N, & \text{se } a_0 + b_0 \geq N. \end{cases}$$

Alem disso, definimos $\epsilon_1 = \begin{cases} 0, & \text{se } a_0 + b_0 \leq N-1 \\ 1, & \text{se } a_0 + b_0 \geq N. \end{cases}$. Portanto, indutivamente, temos

$$c_j = \begin{cases} a_j + b_j + \epsilon_j, & \text{se } a_j + b_j + \epsilon_j \leq N-1 \\ a_j + b_j + \epsilon_j - N, & \text{se } a_j + b_j + \epsilon_j \geq N \end{cases}$$

e $\epsilon_{j+1} = \begin{cases} 0, & \text{se } a_j + b_j + \epsilon_j \leq N-1 \\ 1, & \text{se } a_j + b_j + \epsilon_j \geq N. \end{cases}$, para $1 \leq j \leq m$. Para $j = m+1$, definimos $a_{m+1} = b_{m+1} = 0$ e segue que $c_{m+1} = \epsilon_{m+1}$. Assim,

$$\begin{aligned} \sigma_N(a+b) &= \sum_{j=0}^{m+1} c_j = \sum_{j=0}^{m+1} a_j + b_j + \epsilon_j(1-N) \\ &\leq \sum_{j=0}^{m} (a_j + b_j) = \sigma_N(a) + \sigma_N(b). \end{aligned}$$

b) Primeiramente vamos supor $0 \leq a \leq N-1$. Nesse caso $ab = \sum_{j=0}^m ab_j N^j$ e, pelo item a),

$$\sigma_N(ab) = \sigma_N(\sum_{j=0}^m ab_j N^j) \leq \sum_{j=0}^m \sigma_N(ab_j N^j) = \sum_{j=0}^m \sigma_N(ab_j).$$

Agora, escrevendo $ab_j = (u_s \cdots u_1 u_0)_N$, temos que $ab_j = u_0 + u_1 N + \cdots + u_s N^s \geq u_0 + u_1 + \cdots + u_s = \sigma_N(ab_j)$. Assim, concluímos que

$$\sigma_N(ab) \leq \sum_{j=0}^m \sigma_N(ab_j) \leq \sum_{j=0}^m ab_j = a\sigma_N(b).$$

De maneira geral, se $a = \sum_{j=0}^m a_j N^j$, pelo item a) e o caso anterior,

$$\sigma_N(ab) = \sigma_N(\sum_{j=0}^m a_j N^j b) \leq \sum_{j=0}^m \sigma_N(a_j b) \leq \sum_{j=0}^m a_j \sigma_N(b) = \sigma_N(a)\sigma_N(b).$$

c) Observemos que $(q-1) = (p-1)(p^{f-1} + p^{f-2} + \cdots + p + 1) = ((p-1), (p-1), \cdots, (p-1))_p$. Portanto $\sigma_p(q-1) = f(p-1)$.

Por indução, suponhamos que $\sigma_p(c(q-1)) \geq \sigma_p(q-1)$ para todo $1 \leq c < k$. Seja $a = k(q-1) = dq + r$, com $0 \leq r \leq q-1$. Assim $\sigma_p(a) = \sigma_p(dq+r) = \sigma_p(d) + \sigma_p(r) \geq \sigma_p(d+r)$.

Notemos que $k(q-1) = dq + r$ implica que $(k-d)(q-1) = d + r$. Logo, $\sigma_p(a) \geq \sigma_p((k-d)(q-1))$ e, como $k - d < k$, pela hipótese de indução, $\sigma_p(a) \geq \sigma_p(q-1)$.

□

Proposição 10.4. *Se $q = p^f$, então para todo $n \in \mathbb{Z}_{\geq 0}$, se tem a relação $\sum_{v=0}^{f-1} \sigma_q(np^v) = \frac{q-1}{p-1}\sigma_p(n)$.*

Demonstração. Seja $n = n_0 + n_1 q + \cdots + n_r q^r$, com $0 \leq n_j \leq q-1$ para $0 \leq j \leq r$. Como $0 \leq n_j \leq q-1$, podemos escrever $n_j = \sum_{i=0}^{f-1} n_{j,i} p^i$, com $0 \leq n_{j,i} \leq p-1$. Dessa forma, temos $\sigma_q(n) = n_1 + n_2 + \cdots + n_r$ e $\sigma_p(n) = n_{0,0} + n_{0,1} + \cdots + n_{r,f-1}$. Assim, se

$0 \leq v \leq f-1$,

$$\begin{aligned}
np^v =& n_0p^v + n_1p^vq + \cdots + n_rp^vq^r \\
=& (\sum_{i=0}^{f-1} n_{0,i}p^i)p^v + (\sum_{i=0}^{f-1} n_{1,i}p^i)p^vq + \cdots + (\sum_{i=0}^{f-1} n_{r,i}p^i)p^vq^r \\
=& (\sum_{i=0}^{f-1} n_{0,i}p^{i+v}) + (\sum_{i=0}^{f-1} n_{1,i}p^{i+v})q + \cdots + (\sum_{i=0}^{f-1} n_{r,i}p^{i+v})q^r \\
=& (\sum_{i=v}^{f-1} n_{0,i-v}p^i) + (\sum_{j=0}^{v-1} n_{0,f-v+j}p^j + \sum_{i=v}^{f-1} n_{1,i}p^i)q \\
& + \cdots + (\sum_{j=0}^{v-1} n_{r-1,f-v+j}p^j + \sum_{i=v}^{f-1} n_{r,i}p^{i+v})q^r + (\sum_{j=0}^{v-1} n_{r,f-v+j}p^j)q^{r+1}.
\end{aligned}$$

Como cada coeficiente de q^i está entre 0 e $q-1$, para todo $0 \leq i \leq r+1$, temos

$$\begin{aligned}
\sigma_q(np^v) =& (\sum_{i=v}^{f-1} n_{0,i}p^i) + (\sum_{j=0}^{v-1} n_{0,f-v+j}p^j + \sum_{i=v}^{f-1} n_{1,i}p^i) \\
& + \cdots + (\sum_{j=0}^{v-1} n_{r-1,f-v+j}p^j + \sum_{i=v}^{f-1} n_{r,i}p^{i+v}) + (\sum_{j=0}^{v-1} n_{r,f-v+j}p^j)
\end{aligned}$$

$$\begin{aligned}
\sigma_q(np^v) =& (\sum_{j=0}^{v-1} n_{r,f-v+j}p^j + \sum_{i=v}^{f-1} n_{0,i}p^i) + (\sum_{j=0}^{v-1} n_{0,f-v+j}p^j + \sum_{i=v}^{f-1} n_{1,i}p^i) \\
& + \cdots + (\sum_{j=0}^{v-1} n_{r-1,f-v+j}p^j + \sum_{i=v}^{f-1} n_{r,i}p^{i+v}) \\
=& (\sum_{k=0}^{r} n_{k,f-v}) + (\sum_{k=0}^{r} n_{k,f-v+1})p + \cdots + (\sum_{k=0}^{r} n_{k,f-v-1})p^{f-1}.
\end{aligned}$$

Somando sobre v,

$$\begin{aligned}
\sum_{v=0}^{f-1} \sigma_q(np^v) =& \sum_{v=0}^{f-1}(\sum_{k=0}^{r} n_{k,f-v}) + \sum_{v=0}^{f-1}(\sum_{k=0}^{r} n_{k,f-v+1})p \\
& + \cdots + \sum_{v=0}^{f-1}(\sum_{k=0}^{r} n_{k,f-v-1})p^{f-1} \\
=& \sigma_p(n) + \sigma_p(n)p + \cdots + \sigma_p(n)p^{f-1} \\
=& \frac{q-1}{p-1}\sigma_p(n).
\end{aligned}$$

□

Lema 10.5 (Fórmula de Legendre)**.** *Seja $n \in \mathbb{N}$, então* $\upsilon_p(n!) = \displaystyle\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - \sigma_p(n)}{p-1}$.

Demonstração. Como $n!$ é o produto de todos os naturais menores ou iguais a n, temos que cada múltiplo de p^i entre 1 e n contribui em i fatores p em $n!$, logo incrementa em i o valor de $\sigma_p(n!)$. Por outro lado, temos que cada múltiplo de p^i é também um múltiplo de $p, p^2, \cdots, p^{i-1}$. Portanto somando o número de múltiplos, entre 1 e n, de p, p^2, p^3, e assim sucessivamente, obtemos $\upsilon_p(n!)$.

Assim, temos $\left\lfloor \frac{n}{p^i} \right\rfloor$ múltiplos de p^i entre 1 e n e, portanto, $\upsilon_p(n!) = \displaystyle\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$.

Agora, seja $n = p^k n_k + p^{k-1} n_{k-1} + \cdots + n_0$ a representação de n na base p. Então $\left\lfloor \frac{n}{p^i} \right\rfloor = p^{k-i} n_k + p^{k-i-1} n_{k-1} + \cdots + n_i$ e, portanto

$$
\begin{aligned}
\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor &= \sum_{i=1}^{k} (p^{k-i} n_k + p^{k-i-1} n_{k-1} + \cdots + n_i) \\
&= \sum_{i=1}^{k} \sum_{j=i}^{k} n_j p^{j-i} = \sum_{j=1}^{k} \sum_{i=1}^{j} n_j p^{j-i} \\
&= \sum_{j=1}^{k} n_j \frac{p^j - 1}{p-1} = \sum_{j=0}^{k} n_j \frac{p^j - 1}{p-1} \\
&= \frac{1}{p-1} \sum_{j=0}^{k} \left(n_j p^j - n_j \right) = \frac{1}{p-1} \left(n - \sigma_p(n) \right)
\end{aligned}
$$

□

Definição 10.6. *Seja $f \in \mathbb{F}_q[t]$ tal que $f = \sum_{l=1}^{R} b_l t^{m_l}$ com $b_l \in \mathbb{F}_q^*$, $m_l \in \mathbb{Z}_{\geq 0}$ e $m_1 < m_2 < \cdots < m_R$. Então*

$$\omega_q(f) := \min \left\{ \sum_{l=1}^{R} \gamma_l \mid 0 \leq \gamma_1, \cdots, \gamma_R \leq q-1 \ e \ \sum_{l=1}^{R} m_l \gamma_l \in (q-1)\mathbb{Z}_{>0} \right\}.$$

Teorema 10.7 (Generalização de Chevalley-Warning e Ax-Katz [BBC19])**.**

Sejam $P_1, \cdots, P_r \in \mathbb{F}_q[x_1, \cdots, x_n]$ polinômios não nulos e $\mathcal{I} \subseteq \{1, \cdots, n\}$, um subconjunto não vazio, tais que $\max_{1 \leq j \leq r} \deg_{\mathcal{I}}(P_j) > 0$. Sejam $f_1, \cdots, f_n \in \mathbb{F}_q[t]$ tais que f_i é não constante para todo $i \in \mathcal{I}$ e $\mathcal{S} = \{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid P_j(f_1(x_1), \cdots, f_n(x_n)) = 0, \ \forall\ 1 \leq j \leq r\}$. Se

$$(q-1) \sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j) < \sum_{i \in \mathcal{I}} \omega_q(f_i),$$

então $q^{\lceil \mu \rceil}$ divide $|\mathcal{S}|$, onde $\mu = \dfrac{\left(\sum_{i \in \mathcal{I}} (\frac{\omega_q(f_i)}{(q-1)}) - \sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j) \right)}{\max_{1 \leq j \leq r} \deg_{\mathcal{I}}(P_j)}$.

Demonstração. Primeiramente, interpretaremos o problema no corpo dos números p-ádicos. Por um abuso de notação, denotaremos por P_j e f_i o levantamento de Teichmuller para $\mathcal{O}_{\mathbb{K}}$ dos polinômios P_j e f_i do enunciado para todo $1 \leq j \leq r$ e $1 \leq i \leq n$.

Afirmação: Se $X = \{(x_1, \cdots, x_n) \in T_q^n \mid P_j(f_1(x_1), \cdots, f_n(x_n)) \equiv 0 \pmod{p},\ \forall 1 \leq j \leq n\}$, então $|\mathcal{S}| = |X|$.

Para obter essa relação, consideremos a aplicação natural

$$\mathcal{O}_{\mathbb{K}}^n \to \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}_{\mathbb{K}}}\right)^n \cong \mathbb{F}_q^n$$

definida por $(x_1, \cdots, x_n) \mapsto (\bar{x}_1, \cdots, \bar{x}_n)$. Portanto, se $(y_1, \cdots, y_n) \in \mathcal{S}$, então para cada j existe um único $x_j \in T_q$ tal que $\overline{x}_j = y_j$. Assim, temos que

$$\begin{aligned}\overline{P_j(f_1(x_1), \cdots, f_n(x_n))} =& P_j(\overline{f_1(x_1)}, \cdots, \overline{f_n(x_n)}) \\ =& P_j(f_1(\overline{x}_1), \cdots, f_n(\overline{x}_n)) = 0,\end{aligned}$$

logo $P_j(f_1(x_1), \cdots, f_n(x_n)) \in \mathcal{M}_{\mathbb{K}}$, ou seja, $\upsilon_p(P_j(f_1(x_1), \cdots, f_n(x_n))) > 0$.

Com isso, usando o Lema 8.14 obtemos que

$$\upsilon_p\big(|\mathcal{S}| - \sum_{(x_1,\cdots,x_n)\in T_q^n} \prod_{j=1}^{r} \big(1 - P_j(f_1(x_1), \cdots, f_n(x_n))^{(q-1)q^n}\big)\big) \geq fn,$$

equivalentemente

$$\upsilon_p\big(|\mathcal{S}| - \sum_{i\in I} \sum_{(x_1,\cdots,x_n)\in T_q^n} \prod_{j=1}^{r} \big(-P_j(f_1(x_1), \cdots, f_n(x_n))^{(q-1)q^n}\big)^{i_j}\big) \geq fn,$$

onde $I = \{0,1\}^r$ e $i = (i_1, \cdots, i_r)$.

Assim, basta mostrar que $q^{\lceil \mu \rceil}$ divide

$$A := \sum_{(x_1,\cdots,x_n)\in T_q^n} \prod_{j=1}^{r} (P_j(f_1(x_1), \cdots, f_n(x_n)))^{(q-1)q^n},$$

já que a valoração nas outras parcelas é maior.

Escrevendo $P_j(t_1, \cdots, t_n) = \sum_{k=1}^{L_j} a_{jk} t_1^{h_{1jk}} \cdots t_n^{h_{njk}}$ com $a_{jk} \in \mathcal{O}_{\mathbb{K}}$ e $h_{ijk} \in \mathbb{Z}_{\geq 0}$, temos que

$$\begin{aligned}A = \sum_{\substack{\beta_{j1}+\cdots+\beta_{jL_j}=(q-1)q^n \\ 1\leq j\leq r}} & \Big[\Big(\prod_{j=1}^{r} \binom{(q-1)q^n}{\beta_{j1}, \cdots, \beta_{jL_j}} a_{j1}^{\beta_{j1}} \cdots a_{jL_j}^{\beta_{jL_j}}\Big) \\ & \times\Big(\prod_{i=1}^{n} \sum_{x_i\in T_q} f_i(x_i)^{\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}}\Big)\Big].\end{aligned}$$

No primeiro produtório, utilizando os Lemas 10.3 e 10.5, concluímos que

$$\upsilon_p\left(\binom{(q-1)q^n}{\beta_{j1}, \cdots, \beta_{jL_j}}\right) = \frac{1}{p-1} \sum_{k=1}^{L_j} \sigma_p(\beta_{jk}) - f. \tag{10.1}$$

No segundo produtório, escrevendo $f_i(t) = \sum_{l=1}^{R_i} b_{il} t^{m_{il}}$, onde $b_{il} \in \mathcal{O}_{\mathbb{K}}$ e $m_{il} \in \mathbb{Z}_{\geq 0}$ para todo $i \in \mathcal{I}$ e usando o Lema 10.1, temos que

$$\sum_{x_i\in T_q} f_i(x_i)^{\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}} = q f_i(0)^{\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}} + (q-1)B_i,$$

onde

$$B_i = \sum_{\substack{\sum_{l=1}^{R_i} \gamma_{il} = \sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk} \\ \sum_{l=1}^{R_i} m_{il}\gamma_{il} \in (q-1)\mathbb{Z}_{\geq 0}}} \binom{\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}}{\gamma_{i1}, \cdots, \gamma_{iR_i}} b_{i1}^{\gamma_{i1}} \cdots b_{iR_i}^{\gamma_{iR_i}}.$$

Sem perda de generalidade, podemos assumir que $\mathcal{I} = \{1, \cdots, N\}$ e que $\upsilon_p(B_i) < f$ para $i \in \{1, \cdots, M\}$ com $0 \leq M \leq N \leq n$. Nesse caso, usando o Lema 10.5 novamente, para $i \in \{1, \cdots, M\}$ temos

$$\upsilon_p(B_i) \geq \min \upsilon_p\left(\binom{\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}}{\gamma_{i1}, \cdots, \gamma_{iR_i}}\right) = \frac{\min \sum_{l=1}^{R_i} \sigma_p(\gamma_{il}) - \sigma_p\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}\big)}{p-1}, \quad (10.2)$$

onde o min é sobre todos os γ_{il} tais que $\sum_{l=1}^{R_i} \gamma_{il} = \sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}$ e $\sum_{l=1}^{R_i} m_{il}\gamma_{il} \in (q-1)\mathbb{Z}_{\geq 0}$.

Agora, somando (10.1) sobre j e (10.2) sobre i, basta mostrar que

$$\begin{aligned}\frac{1}{p-1}\Big[\sum_{i=1}^{M}\Big(\sum_{l=1}^{R_i}\sigma_p(\gamma_{il}) - \sigma_p\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}\big)\Big) + \sum_{j=1}^{r}\sum_{k=1}^{L_j}\sigma_p(\beta_{jk})\Big] - rf \\ \geq f\left\lceil \frac{\left(\sum_{i=1}^{M}\left(\frac{\omega_q(f_i)}{(q-1)}\right) - \sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j)\right)}{\max_{1\leq j\leq r}\deg_{\mathcal{I}}(P_j)}\right\rceil,\end{aligned}$$

para qualquer conjunto de γ_{il} tais que $\sum_{l=1}^{R_i} \gamma_{il} = \sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}$ e $\sum_{l=1}^{R_i} m_{il}\gamma_{il} \in (q-1)\mathbb{Z}_{\geq 0}$.

Como $\sum_{i=1}^{M} h_{ijk} \leq \deg_{\mathcal{I}}(P_j)$, para todo $0 \leq v \leq f-1$ segue que

$$\begin{aligned}\sum_{i=1}^{M}\sigma_q\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}p^v\big) &\leq \sum_{j=1}^{r}\sum_{k=1}^{L_j}\sigma_q(\beta_{jk}p^v)\sum_{i=1}^{M} h_{ijk} \\ &\leq \sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j)\sum_{k=1}^{L_j}\sigma_q(\beta_{jk}p^v) \\ &=(q-1)\sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j) \\ &\quad + \sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j)\big(\sum_{k=1}^{L_j}\sigma_q(\beta_{jk}p^v) - (q-1)\big).\end{aligned}$$

Logo

$$\begin{aligned}(q-1)\sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j) \geq& \sum_{i=1}^{M}\sigma_q\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}p^v\big) \\ &- \big(\max_{1\leq j\leq r}\deg_{\mathcal{I}}(P_j)\big)\sum_{j=1}^{r}\big(\sum_{k=1}^{L_j}\sigma_q(\beta_{jk}p^v) - (q-1)\big).\end{aligned} \quad (10.3)$$

Com a relação direta $\gamma \equiv \sigma_q(\gamma) \pmod{q-1}$ e o fato de que $\sum_{l=1}^{R_i} m_{il}\gamma_{il}p^v \in (q-1)\mathbb{Z}_{\geq 0}$ para todo $0 \leq v \leq f-1$ e $1 \leq i \leq M$, temos que $\sum_{l=1}^{R_i} m_{il}\sigma_q(\gamma_{il}p^v) \in (q-1)\mathbb{Z}_{\geq 0}$, logo, pela definição de $\omega(f_i)$, segue que $\sum_{l=1}^{R_i} \sigma_q(\gamma_{il}p^v) \geq \omega_q(f_i)$ e, mais ainda,

$$\sum_{i=1}^{M} \omega_q(f_i) \leq \sum_{i=1}^{M}\sum_{l=1}^{R_i} \sigma_q(\gamma_{il}p^v).$$

Portanto, subtraindo da desigualdade (10.3) , obtemos

$$\begin{aligned}
&\sum_{i=1}^{M} \omega_q(f_i) - (q-1)\sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j) \\
&\qquad \leq \sum_{i=1}^{M}\Big(\sum_{l=1}^{R_i} \sigma_q(\gamma_{il}p^v) - \sigma_q\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}p^v\big)\Big) \\
&\qquad\qquad + \big(\max_{1\leq j\leq r} \deg_{\mathcal{I}}(P_j)\big)\sum_{j=1}^{r}\Big(\sum_{k=1}^{L_j}\sigma_q(\beta_{jk}p^v) - (q-1)\Big).
\end{aligned}$$

Já que $\max_{1\leq j\leq r}\deg_{\mathcal{I}}(P_j) > 0$, segue que

$$\begin{aligned}
&\frac{\sum_{i=1}^{M}\Big(\sum_{l=1}^{R_i} \sigma_q(\gamma_{il}p^v) - \sigma_q\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}p^v\big)\Big)}{\max_{1\leq j\leq r}\deg_{\mathcal{I}}(P_j)} + \sum_{j=1}^{r}\sum_{k=1}^{L_j}\sigma_q(\beta_{jk}p^v) - r(q-1) \\
&\qquad \geq (q-1)\frac{\sum_{i=1}^{M}\frac{\omega_q(f_i)}{q-1} - \sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j)}{\max_{1\leq j\leq r}\deg_{\mathcal{I}}(P_j)}.
\end{aligned}$$

Além disso, como $\sum_{l=1}^{R_i}\gamma_{il}p^v = \sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}p^v$ por definição, pelo Lema 10.3, vale que $\sum_{l=1}^{R_i}\sigma_q(\gamma_{il}p^v) - \sigma_q\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}p^v\big)$ é um múltiplo não negativo de $q-1$ para todo $1 \leq i \leq M$, logo

$$\begin{aligned}
&\sum_{i=1}^{M}\Big(\sum_{l=1}^{R_i} \sigma_q(\gamma_{il}p^v) - \sigma_q\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}p^v\big)\Big) + \sum_{j=1}^{r}\sum_{k=1}^{L_j}\sigma_q(\beta_{jk}p^v) - r(q-1) \\
&\qquad \geq (q-1)\left\lceil\frac{\sum_{i=1}^{M}\frac{\omega_q(f_i)}{q-1} - \sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j)}{\max_{1\leq j\leq r}\deg_{\mathcal{I}}(P_j)}\right\rceil.
\end{aligned}$$

Assim, somando sobre v e usando a Proposição 10.4, concluímos que

$$\begin{aligned}
&\frac{1}{p-1}\Big[\sum_{i=1}^{M}\Big(\sum_{l=1}^{R_i} \sigma_p(\gamma_{il}) - \sigma_p\big(\sum_{j=1}^{r}\sum_{k=1}^{L_j} h_{ijk}\beta_{jk}\big)\Big) + \sum_{j=1}^{r}\sum_{k=1}^{L_j}\sigma_p(\beta_{jk})\Big] - rf \\
&\qquad \geq f\left\lceil\frac{\sum_{i=1}^{M}\frac{\omega_q(f_i)}{(q-1)} - \sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j)}{\max_{1\leq j\leq r}\deg_{\mathcal{I}}(P_j)}\right\rceil.
\end{aligned}$$

Finalmente, como $\upsilon_p(B_i) \geq f$, para todo $M < i \leq N$, e $\omega_q(f_i) < q-1$, concluímos que

$$\begin{aligned}\upsilon_p(A) &\geq f \left\lceil \frac{\sum_{i=1}^{M} \frac{\omega_q(f_i)}{(q-1)} - \sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j)}{\max_{1\leq j\leq r} \deg_{\mathcal{I}}(P_j)} \right\rceil + f(N-M)\\ &\geq f \left\lceil \frac{\sum_{i=1}^{N} \frac{\omega_q(f_i)}{(q-1)} - \sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j)}{\max_{1\leq j\leq r} \deg_{\mathcal{I}}(P_j)} \right\rceil\end{aligned}$$

como queríamos provar.

□

Proposição 10.8. *Para todo $f \in \mathbb{F}_q[x]$, se $k < \omega_q(f)$, então $\sum_{x\in\mathbb{F}_q} f(x)^k = 0$.*

Demonstração. Escrevendo $f(x) = \sum_{l=1}^{R} b_l x^{m_l}$, temos que

$$f(x)^k = \sum_{k_1+\cdots+k_R=k} \binom{k}{k_1, \cdots, k_R} b_1^{k_1} \cdots b_R^{k_R} x^{k_1m_1+\cdots+k_Rm_R}.$$

Como $\omega_q(f)$ é mínimo e $k < \omega_q(f)$, para todo $k_1, \cdots, k_R$, temos que $k_1m_1+\cdots+k_Rm_R \notin (q-1)\mathbb{Z}_{>0}$. Logo, pela Proposição 3.2, $\sum_{x\in\mathbb{F}_q} f(x)^k = 0$. □

Da definição de $\omega_q(f)$ temos que $\sum_{l=1}^{R} m_l\gamma_l \in (q-1)\mathbb{Z}_{>0}$, logo $\sum_{l=1}^{R} \gamma_l \geq \frac{q-1}{deg(f)}$. Assim, pela proposição anterior, concluímos que $\frac{q-1}{deg(f)} \leq \omega_q(f) \leq u(f)$, onde $u(f)$ é como na Definição 9.7.

Mais ainda, quando $k\deg(f) < q-1$, temos $\sum_{x\in\mathbb{F}_q} f(x)^k = 0$, mas quando $k\deg(f) = q-1$, vale que $\sum_{x\in\mathbb{F}_q} f(x)^k \neq 0$. Portanto, segue que $\deg(f)|(q-1)$ se, e somente se, $u(f) = \omega_q(f) = \frac{q-1}{\deg(f)}$. A volta é obtida de maneira direta. Com isso, os seguintes corolários são imediatos.

Corolário 10.9. *Sejam $P_1, \cdots, P_r \in \mathbb{F}_q[t_1, \cdots, t_n]$ polinômios não nulos e $\mathcal{I} \subseteq \{1, \cdots, n\}$ um subconjunto não vazio. Sejam $f_1, \cdots, f_n \in \mathbb{F}_q[t]$ polinômios não constantes com $\deg(f_i)|(q-1)$ se $i \in \mathcal{I}$ e $\mathcal{S} = \#\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid P_j(f_1(x_1), \cdots, f_n(x_n)) = 0,\ \forall\ 1 \leq j \leq r\}$. Se*

$$(q-1)\sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j) < \sum_{i\in\mathcal{I}} u(f_i),$$

então q divide $\mathcal{S}$.

Corolário 10.10. *Sejam $P_1, \cdots, P_r \in \mathbb{F}_q[t_1, \cdots, t_n]$ polinômios não nulos e $\mathcal{I} \subseteq \{1, \cdots, n\}$ um subconjunto não vazio tais que $\max_{1\leq j\leq r} \deg_{\mathcal{I}}(P_j) > 0$. Sejam $f_1, \cdots, f_n \in \mathbb{F}_q[t]$ polinômios não constantes para todo $i \in \mathcal{I}$ e $\mathcal{S} = \#\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid P_j(f_1(x_1), \cdots, f_n(x_n)) = 0,\ \forall\ 1 \leq j \leq r\}$. Se*

$$\sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j) < \sum_{i\in\mathcal{I}} \frac{1}{\deg(f_i)},$$

então $q^{\lceil\mu\rceil}$ divide $\mathcal{S}$, onde $\mu = \frac{\left(\sum_{i\in\mathcal{I}}(\frac{1}{\deg(f_i)}) - \sum_{j=1}^{r}\deg_{\mathcal{I}}(P_j)\right)}{\max_{1\leq j\leq r}\deg_{\mathcal{I}}(P_j)}$.

Corolário 10.11. *Sejam* $P_1, \cdots, P_r \in \mathbb{F}_q[t_1, \cdots, t_n]$ *polinômios não nulos e* $\mathcal{I} \subseteq \{1, \cdots, n\}$ *um subconjunto não vazio tais que* $\max_{1 \le j \le r} \deg_{\mathcal{I}}(P_j) > 0$. *Sejam* $f_1, \cdots, f_n \in \mathbb{F}_q[t]$ *com* $f_i = t^{m_i}$ *e* $m_i \in \mathbb{Z}_{>0}$ *para todo* $i \in \mathcal{I}$ *e* $\mathcal{S} = \#\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid P_j(f_1(x_1), \cdots, f_n(x_n)) = 0,\ \forall\ 1 \le j \le r\}$. *Definindo* $d_i = (m_i, q-1)$, *se*

$$\sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j) < \sum_{i \in \mathcal{I}} \frac{1}{d_i},$$

então $q^{\lceil \mu \rceil}$ *divide* $\mathcal{S}$, *onde* $\mu = \frac{\left(\sum_{i \in \mathcal{I}}(\frac{1}{d_i}) - \sum_{j=1}^{r} \deg_{\mathcal{I}}(P_j)\right)}{\max_{1 \le j \le r} \deg_{\mathcal{I}}(P_j)}$.

Tomando $\mathcal{I} = \{1, \cdots, n\}$ e $m_1 = \cdots = m_n = 1$ no Corolário 10.11 retornamos ao Teorema de Ax-Katz (Teorema 9.3).

Referências

[Apo] Apostol, T. M., *Introduction to Analytic Number Theory*. Springer Verlag (1976)

[Ax64] Ax, J., *Zeroes of Polynomials over Finite Fields*. American Journal of Mathematics. **86** (1964), 255-261.

[BBC19] Baoulina, I. N., Bishnoi, A., Clarck, P. L., *A Generalization of the Theorems of Chevalley-Warning and Ax-Katz via Polynomial Substitutions*. Proceedings of the American Mathematical Society. **147** (2019), 4107-4122.

[CZ14] Cao, W., Zan, H., *Powers of Polynomials and Bounds of Value Sets*. Journal of Number Theory. **143** (2014), 286-292.

[CSW93] Chen, C. S., Jau-Shyong, P., Wan, D., *Value Sets of Polynomials over Finite Fields*. Proceedings of the American Mathematical Society. **119** (1993), 711-717.

[Chev35] Chevalley, C., *Démonstration d'une hypothèse de M. Artin*, Abhandlungen aus dem Mathematischen Seminar Universität Hamburg. **11** (1935), 73?75.

[DHX05] Hou, X., *A Note on the Proof of a Theorem of Katz*. Finite Fields and Their Applications. **11** (2005), 316-319.

[IR] Ireland, K., Rosen, M., *A Classical Introduction to Modern Number Theory*. Springer-Verlag (1998).

[Ka71] Katz, M. N., *On a Theorem of Ax*. American Journal of Mathematics. **93** (1971), 485-499.

[LN] Lidl, R., Niederreiter, H., *Finite Fields (2nd ed., Encyclopedia of Mathematics and its Applications)*. Cambridge University Press (1996).

[Rob] Robert, Alain M., *A Course in p-adic Analysis*. Springer-Verlag (2000).

[Wan95] Wan, D., *A Chevalley-Warning Approach to p-adic Estimates of Character Sums*. Proceedings of the American Mathematical Society. **123** (1995), 45-54.

[War35] Warning, E., *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abhandlungen aus dem Mathematischen Seminar Universität Hamburg. **11** (1935), 76?83.

[Wash] Washington, Lawrence C., *Introduction to Cyclotomic Fields*. Springer-Verlag (1997).