

TEOREMA DE DAVENPORT E HASSE

por

JOSÉ HENRIQUE MENDES TARCIA

Dissertação apresentada
como exigência parcial
para a obtenção do título de MESTRE em
MATEMÁTICA

À Comissão Julgadora

Pontifícia Universidade Católica de São Paulo

1979

TEOREMA DE DAVENPORT E HASSE

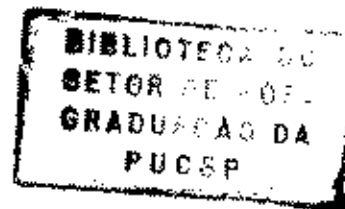
por

JOSÉ HENRIQUE MENDES TARCIA

Biblioteca MA - PUCSP



100077559



Dissertação apresentada
como exigência parcial
para a obtenção do título de MESTRE em
MATEMÁTICA

A Comissão Julgadora



Pontifícia Universidade Católica de São Paulo

1979

AGRADECIMENTOS

Ao Professor Doutor Fernando Furquim de Almeida, idealizador do curso de Pós Graduação em Matemática da Pontifícia Universidade Católica de São Paulo, sob cuja orientação foi realizado este trabalho, os mais sinceros agradecimentos.

A minha saudosa mãe, minha homenagem.

A minha esposa e filhos ofereço este trabalho.

O Autor.

COMISSÃO JULGADORA

Sebastião Figueiredo Almeida

João da Costa Faria

Alfredo

ÍNDICE

	pág.
INTRODUÇÃO -----	v
CAPÍTULO I	
Corpos Finitos -----	1
CAPÍTULO II	
Traço e Norma sobre um corpo finito -----	15
CAPÍTULO III	
Caracteres e Soma de Gauss -----	28
CAPÍTULO IV	
Teorema de Davenport e Hasse -----	44
BIBLIOGRAFIA -----	65

INTRODUÇÃO

Esta dissertação tem como objetivo estabelecer uma relação entre as somas de Gauss de um corpo finito F_q e de uma sua extensão F_{q^m} .

Para desenvolvê-la foi preciso a partir do corpo primo F_p , construir corpos finitos com $q = p^r$ elementos. Em seguida passou-se ao estudo do grupo de automorfismo das extensões de grau finito do corpo F_q e da decomposição de um polinômio.

$$f = X^n + a_1 X^{n-1} + \dots + a_n.$$

unitário e irredutível sobre F_q numa extensão F_{q^m} . Este estudo é importante, pois através dele podemos tirar conclusões sobre as extensões algébricas de F_q formadas pelas adjunções de cada uma das raízes de f à F_q e a F_{q^m} .

Houve necessidade de definir e verificar as propriedades do Traço e da Norma de um elemento pertencente a uma extensão de um corpo finito. A utilização da Norma e do Traço em nosso trabalho liga a soma de Gauss de um corpo com a de sua extensão de grau finito.

Foi preciso desenvolver também os caracteres de grupos finitos. Para os de um grupo aditivo ele foi estudado detalhadamente.

Seguindo a orientação de André Weil que demonstrou esse teorema muito consisamente de modo elementar, chegamos en tão ao objetivo estabelecido: o Teorema de Davenport e Hasse - "Seja $g'(x')$ a soma de Gauss do corpo F_q^m , então

$$-g'(x') = (-1)^m g(x)^m ,$$

onde $g(x)$ é a soma de Gauss do corpo F_q ."

CAPÍTULO I

CORPOS FINITOS

É nosso objetivo neste capítulo relembrar algumas propriedades dos corpos finitos e de suas extensões algébricas de grau finito.

1. Seja K um corpo finito. Pelo teorema de Wedderburn K é um corpo comutativo.

O corpo primo de K é o corpo F_p , pois este é o menor subcorpo contido num corpo finito, e portanto a característica de K é p . Isto significa que

$$px = 0, \quad \forall x \in K$$

Da definição de característica, segue imediatamente as seguintes propriedades:

(a) Para todo $x, y \in K$,

$$(x + y)^p = x^p + y^p + \sum_{n=1}^{p-1} \binom{p}{n} x^n y^{p-n}$$

Se $1 \leq n \leq p-1$, o coeficiente binomial $\binom{p}{n}$ é múltiplo inteiro de p , donde todos os termos do somatório são nulos e

$$(x + y)^p = x^p + y^p$$

b) Para todo $x, y \in K$, $(x \cdot y)^p = x^p \cdot y^p$

O corpo K é espaço vetorial sobre F_p de dimensão finita r . Esse número r é, por definição, o grau de K sobre F_p .

TEOREMA 1. K tem $q = p^r$ elementos.

Seja $\omega_1, \omega_2, \dots, \omega_r$ uma base de K sobre F_p . Então todo elemento $x \in K$ pode ser escrito de uma única maneira como combinação linear dos elementos da base.

$$x = \sum_{i=1}^r a_i \omega_i, \quad a_i \in F_p \quad (1 \leq i \leq r)$$

Cada a_i pode tomar todos os p valores de F_p . Como a combinação linear $\sum_{i=1}^r a_i \omega_i$ tem r coeficientes a_i , teremos p^r combinações lineares e portanto existe $q = p^r$ elementos em K .

2. Façamos algumas considerações sobre o grupo multiplicativo $K^* = K - \{0\}$ do corpo finito K .

Antes vamos recordar a definição de $\phi(n)$: a função de Euler-Gauss, e demonstraremos um lema que nos será útil em seguida.

Seja n um inteiro positivo maior ou igual a 1. Indiquemos por $\phi(n)$ a função de Euler-Gauss, ou seja, a função

aritmética que dá para cada n o número de inteiros m menores ou iguais a n e que são primos com n .

LEMA 1. Se $n \geq 1$, então $n = \sum_{d|n} \phi(d)$.

Seja d um divisor de n e consideremos o conjunto

$$A = \{1, 2, 3, \dots, n\}.$$

Seja C_d o subconjunto de A formado pelos números de A que têm com n o máximo divisor comum d .

$$C_d = \{j \in A \text{ tal que } (j, n) = d\}.$$

Como cada j de C_d é divisível por d , existe m tal que

$$j = md.$$

No entanto, nem todo número md tem com n o máximo divisor comum d . Vejamos em que condição isto acontece. Se

$$d = (j, n) = (md, \frac{n}{d} \cdot d) = d(m, \frac{n}{d})$$

$$(m, \frac{n}{d}) = 1$$

Por outro lado $j = md \leq n$, donde $m \leq \frac{n}{d}$.

Então cada j de C_d é da forma md com $1 \leq m \leq \frac{n}{d}$ e $(m, \frac{n}{d}) = 1$. O número deles é, pois, $\phi(\frac{n}{d})$.

Portanto o $\text{card}(C_d) = \phi(\frac{n}{d})$ (número de inteiros m ($1 \leq m \leq \frac{n}{d}$) primos com $\frac{n}{d}$).

Sejam $d_1, d_2, \dots, d_r$ todos os divisores de n , então temos

$$\text{card}(C_{d_1}) = \phi\left(\frac{n}{d_1}\right)$$

$$\text{card}(C_{d_2}) = \phi\left(\frac{n}{d_2}\right)$$

.....

$$\text{card}(C_{d_r}) = \phi\left(\frac{n}{d_r}\right)$$

Sendo $d_i \neq d_k$, como o máximo divisor comum de dois números é único,

$$C_{d_i} \cap C_{d_k} = \emptyset.$$

Como todo número de C_{d_i} pertence a A , e todo número de A tem com n o máximo divisor comum d_i , é claro que

$$A = \bigcup_{i=1}^k C_{d_i}.$$

Se $A = \bigcup_{i=1}^r C_{d_i}$ e os C_{d_i} são dois a dois disjuntos, então

$$\text{card}(A) = \sum_{i=1}^r \text{card}(C_{d_i})$$

donde

$$n = \sum_{i=1}^r \phi\left(\frac{n}{d_i}\right) = \sum_{d|n} \phi(n).$$

O lema 1 nos permitirá agora demonstrar o seguinte teorema.

TEOREMA 2. K^* é cíclico e de ordem $(q-1)$.

Sendo K^* um grupo finito, a ordem d de cada elemento de K^* divide $q-1$. Mas, se $d|q-1$, será que existe um elemento $x \in K^*$ de ordem $q-1$?

Supondo que sim, o subgrupo

$$S = \{1, x, x^2, \dots, x^{d-1}\}$$

gerado por x é cíclico e de ordem d .

Procuremos em S os elementos x^h que tenham ordem d .

Seja y a ordem de x^h . Então y é o menor número natural tal que

$$x^{hy} = 1. \quad (1)$$

Mas a ordem de x é d . Donde, de (1) segue

$$hy \equiv 0 \pmod{d}.$$

Dividindo a congruência por h ,

$$y \equiv 0 \pmod{\frac{d}{\delta}}$$

onde $\delta = (d, h)$. Como y é o menor número natural da classe $0 \pmod{\frac{d}{\delta}}$, segue

$$y = \frac{d}{\delta}.$$

Para que x^h tenha ordem d é necessário e suficiente que $\delta = 1$.

Então o número de elementos de S que tem ordem d é igual ao número de expoentes das potências de x em S que são primos com d , ou seja, $\phi(d)$.

Consideremos a equação

$$x^d = 1 \quad (2)$$

Como $x^d = 1$ é um polinômio do corpo K , sabemos que ela tem no máximo d soluções. Ora, os elementos de S que são todos distintos, são raízes da equação (2). Como $\text{card}[S] = d$, essas são todas as soluções de (2).

Resumindo o que foi dito de K^* até agora: dado - um $d|q-1$, ou não existe nenhum elemento de K^* com ordem d , ou existe $\phi(d)$.

Vamos introduzir uma nova função $\psi(d)$, definida no conjunto dos divisores de n do seguinte modo:

$$\psi(d) = \begin{cases} 0, & \text{se não existir nenhum elemento de } K^* \\ & \text{com ordem } d \\ \phi(d), & \text{se existir um elemento com ordem } d. \end{cases}$$

Suponhamos que $\psi(d) = 0$ para algum d . Como $\phi(d)$ é sempre diferente de zero,

$$(q-1) = \sum_{d|(q-1)} \psi(d) < \sum_{d|(q-1)} \phi(d) = (q-1),$$

o que é absurdo. Consequentemente, para todo divisor d de $(q-1)$, $\psi(d) = \phi(d)$. Logo, existe sempre um elemento de ordem d , isto é, dado $d|(q-1)$ em K^* há um elemento de ordem d .

Como $(q-1)|(q-1)$, e $\phi(q-1) > 0$, existe pelo menos um elemento de ordem $(q-1)$ em K^* . Logo, K^* é cíclico.

3. Seja Ω um fecho algébrico de F_p .

TEOREMA 3. Dado o número natural $r > 1$, existe um sub-corpo F_q de Ω e somente um, que tem $q = p^r$ elementos.

Consideremos o conjunto das raízes do polinômio

$$f = X^q - X.$$

Para todo $x, y \in \Omega$ e x, y raízes de f , temos

a) $(x + y)^q = x^q + y^q$, isto porque os coeficientes binomiais $\binom{q}{k} = 0$ para $1 \leq k \leq q-1$.

Como x, y são raízes de f temos que $(x+y)^q = x+y$.

b) $(x \cdot y)^q = x^q \cdot y^q = x \cdot y$.

c) Dado x raiz de f , $x \neq 0$, então temos que $x = x^q$. Como $x \in \Omega$,

$$\frac{1}{x} = \frac{1}{x^q} = \left(\frac{1}{x}\right)^q$$

d) Se a característica de Ω é $p \neq 2$, $q = p^r$ é ímpar. Portanto, se $x \in \Omega$ é raiz de f ,

$$(-x)^q = (-1)^q x^q = -x.$$

Se $p = 2$,

$$x + x = (1+1)x = 2x = 0, \quad \forall x \in \Omega.$$

Logo, sempre existe o oposto de um elemento $x \in \Omega$.

O conjunto das raízes de f , é um subcorpo de Ω .

Como a derivada de f é diferente de zero, as raízes de $f = X^q - X$ são todas distintas. Portanto o conjunto

das raízes como vimos, é um corpo, com q elementos, o qual será indicado por F_q .

Qualquer outro corpo finito K com $q = p^r$ elementos é isomorfo a F_q . Como, K^* é cíclico, segue que, K^* é isomorfo a F_q^* . Colocando zero em ambos, temos, $K \cong F_q$.

4. Consideremos F_{q^m} a extensão finita de F_q de grau m . Seja $\phi: F_{q^m} \rightarrow F_{q^m}$ uma aplicação definida por $\phi(x) = x^q, \forall x \in F_{q^m}$. Mostremos que ϕ é um automorfismo de F_{q^m} .

De fato,

$$\text{a) } \forall x, y \in F_{q^m}, \quad \phi(x + y) = (x + y)^q = x^q + y^q = \phi(x) + \phi(y).$$

$$\text{b) } \forall x, y \in F_{q^m}, \quad \phi(x \cdot y) = (x \cdot y)^q = x^q \cdot y^q = \phi(x) \cdot \phi(y).$$

c) Suponhamos que dado $x, y \in F_{q^m}$, tenhamos $\phi(x) = \phi(y)$. Então,

$$\phi(x - y) = 0,$$

isto é,

$$(x - y)^p = 0,$$

como F_{q^m} é um corpo,

$$x - y = 0 \implies x = y,$$

donde ϕ é injetora.

d) é uma aplicação injetora de um conjunto finito em si próprio. Logo, ϕ é sobrejetora.

ϕ é um automorfismo de " F_{q^m} sobre F_{q^m} " que

deixa fixo F_q , porque

$$\phi(x) = x^q = x, \quad \forall x \in F_q.$$

Portanto ϕ pertence ao grupo de Galois de F_{q^m} sobre F_q .

A aplicação ϕ é denominada "automorfismo de Frobenius".

Para todo $x \in F_{q^m}$ e para $0 \leq i, j \leq m-1$

$$\phi^i \circ \phi^j(x) = \phi^i(\phi^j(x))$$

donde

$$\phi^i \circ \phi^j(x) = \phi^i(x^{q^j}) = (x^{q^j})^{q^i} = x^{q^j \cdot q^i}$$

segue que

$$\phi^i \circ \phi^j(x) = x^{q^{j+i}} = \phi^{i+j}(x).$$

$$\text{Logo, } \phi^i \circ \phi^j = \phi^{i+j}.$$

Os automorfismos $1, \phi, \phi^2, \dots, \phi^{m-1}$, são distintos, porque se

$$\phi^i = \phi^j \quad 0 \leq i, j < m$$

então,

$$\phi^i(x) = \phi^j(x) \quad \forall x \in F_{q^m}$$

$$x^{q^i} = x^{q^j} \quad \forall x \in F_{q^m}$$

Daí

$$x^{q^i} - x^{q^j} = 0 \quad \forall x \in F_{q^m}.$$

Suponhamos que $i > j$. Neste caso, o polinômio $x^{q^i} - x^{q^j} \in F_{q^m}[X]$ de grau $q^i (q^i > q^j)$ tem como raízes os q^m elementos do corpo F_{q^m} , o que é absurdo, pois, em F_{q^m}

o polinômio $X^{q^i} - X^{q^j}$ pode ter no máximo q^i raízes distintas. Logo, $i = j$.

Se os automorfismos $\phi^i (0 \leq i < m)$ são distintos, eles formam um grupo cíclico. Como a ordem do grupo de Galois de F_{q^m} sobre F_q é m , então $\phi^i (0 \leq i < m)$ são os m automorfismos de F_{q^m} em relação a F_q .

5. Sejam F_{q_1} e F_{q_2} duas extensões finitas do corpo F_p com $q_1 = p^{r_1}$ e $q_2 = p^{r_2}$ elementos, respectivamente.

TEOREMA 4. $F_{q_1} \subset F_{q_2}$ se, e somente se $r_1 | r_2$.

Se $F_{q_1} \subset F_{q_2}$,

$$[F_{q_2} : F_p] = [F_{q_1} : F_p] \cdot [F_{q_2} : F_{q_1}],$$

donde

$$r_2 = r_1 \cdot [F_{q_2} : F_{q_1}].$$

Portanto, $r_1 | r_2$.

Se $r_1 | r_2$, então $p^{r_1-1} | p^{r_2-1}$. Daí segue que

$$x^{p^{r_1-1}-1} | x^{p^{r_2-1}-1},$$

donde $x^{p^{r_1}-1} | x^{p^{r_2}-1}$. Consequentemente $F_{q_1} \subset F_{q_2}$.

$F_{q_1} \cap F_{q_2}$ é um corpo com $q_3 = p^{r_3}$ elementos.

TEOREMA 5. $F_{q_1} \cap F_{q_2}$ é uma extensão de F_p com grau $r_3 = (r_1, r_2)$.

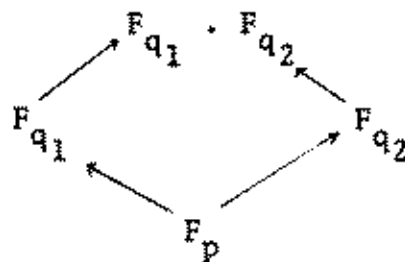
$$F_{q_1} \cap F_{q_2} \subset F_{q_1} \implies r_3 | r_1$$

$$F_{q_1} \cap F_{q_2} \subset F_{q_2} \implies r_3 | r_2$$

Qualquer corpo F_{q_r} com $q_r = p^r$ elementos contido em F_{q_1} e F_{q_2} vai estar contido em $F_{q_1} \cap F_{q_2}$. Portanto $r | r_3$. Logo $r_3 = (r_1, r_2)$.

Dadas as extensões F_{q_1} e F_{q_2} de F_p , consideremos $s = r_1 \cdot r_2$. Portanto o corpo F_{q_s} com p^s elementos contém F_{q_1} e F_{q_2} pois $r_1 | s$ e $r_2 | s$.

Definição: Sejam F_{q_1} e F_{q_2} extensões de F_p contidas num mesmo corpo F_{q_s} . Denotaremos então, por $F_{q_1} \cdot F_{q_2}$ o menor subcorpo de F_{q_s} que contém F_{q_1} e F_{q_2} , e denominaremos $F_{q_1} \cdot F_{q_2}$ composto de F_{q_1} e F_{q_2} em F_{q_s} .



$F_{q_1} \cdot F_{q_2}$ é um corpo com $q = p^{r_4}$ elementos.

TEOREMA 6. $F_{q_1} \cdot F_{q_2}$ é uma extensão de F_p de grau r_4 , onde r_4 é o mínimo múltiplo comum entre

$$r_1 = [F_{q_1} : F_p] \quad \text{e} \quad r_2 = [F_{q_2} : F_p].$$

$$F_{q_1} \subset F_{q_1} \cdot F_{q_2} \implies r_1 | r_4$$

(3)

$$F_{q_2} \subset F_{q_1} \cdot F_{q_2} \implies r_2 | r_4$$

Seja F_{q_r} um subcorpo de F_{q_s} de grau r sobre F_p , que contenha F_{q_1} e F_{q_2} . Logo, $r_1 | r$ e $r_2 | r$.

Como $F_{q_1} \cdot F_{q_2}$ é o menor subcorpo de F_{q_s} que contém F_{q_1} e F_{q_2} , então

$$r_4 | r. \quad (4)$$

De (3) e (4) temos que r_4 é o mínimo múltiplo comum de r_1 e r_2 .

TEOREMA 7. Seja $F_p \subset F_q$, então existe um elemento g de F_q , tal que $F_q = F_p(g)$.

Como já vimos o grupo multiplicativo F_q^* do corpo finito F_q é cíclico e de ordem $(q-1)$.

Seja g um gerador de F_q^* . Então

$$F_q^* = \{1, g, g^2, g^3, \dots, g^{q-2}\}.$$

Estes elementos formam um subconjunto de F_q com $(q-1)$ elementos. Acrescentando o zero a F_q^* temos o corpo F_q .

Logo,

$$F_q = F_p(g).$$

6. Decomposição de um polinômio irreduzível sobre F_q numa extensão F_{q^m} .

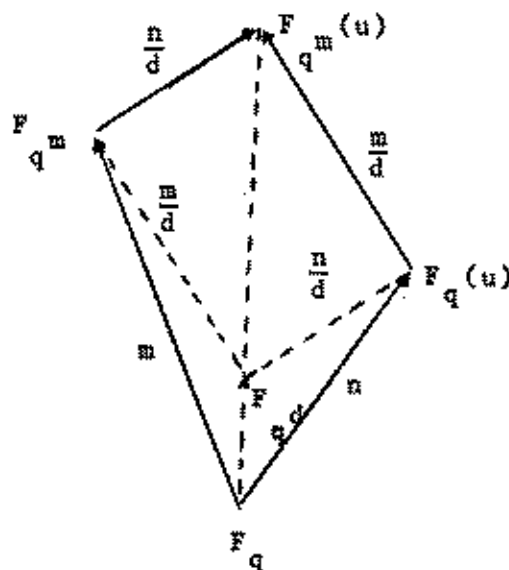
Seja $f = X^n + a_1 X^{n-1} + \dots + a_n$ um polinômio unitário e irredutível de $F_q[X]$. Tomando a extensão F_{q^m} de F_q , esse polinômio pode se decompor no anel $F_{q^m}[X]$. De fato, vale o seguinte teorema:

TEOREMA 8. Em $F_{q^m}[X]$, f se decompõe em $d=(m,n)$ fatores irredutíveis de grau $\frac{n}{d}$.

Seja u uma raiz de um polinômio irredutível de $F_{q^m}[X]$ que divide f o qual chamaremos de g . Como u é também raiz de f e $F_q[X]$, a adjunção de u a F_q dará o corpo $F_q(u)$, extensão de F_q de grau n .

Façamos a adjunção de u ao corpo F_{q^m} . O corpo $F_{q^m}(u)$ será então o menor corpo extensão de F_{q^m} que contém F_{q^m} e u . Desse modo ele é o composto de F_{q^m} e de $F_q(u)$. Portanto, se $d = (m,n)$, o grau de $F_{q^m}(u)$ sobre F_q é o mínimo múltiplo comum de m e n , ou seja, $m \cdot n / d$.

Temos, então, o seguinte diagrama



de onde, o grau do polinômio irredutível g é $\frac{n}{d}$. Ora, como m , n e d são constantes, qualquer que seja a raiz u de f que tomarmos, como cada raiz de f será também a raiz de um polinômio g de $F_{q^m}[X]$ irredutível e de grau $\frac{n}{d}$, o polinômio f terá em $F_{q^m}[X]$ a seguinte decomposição

$$f = f_1 \cdot f_2 \cdot \dots \cdot f_d,$$

cada um deles de grau $\frac{n}{d}$.

CAPÍTULO II

TRAÇO E NORMA SOBRE UM CORPO FINITO

Seja F_{q^m} uma extensão de F_q , então o grupo de Galois G de F_{q^m} sobre F_q é cíclico e de ordem m , gerado pelo automorfismo $\phi(x) = x^q$.

Definição. Chamamos de traço de um elemento $x \in F_{q^m}$ a soma dos $\phi^j(x)$ para $0 \leq j \leq m-1$, isto é,

$$\text{Tr}(x) = \sum_{j=0}^{m-1} \phi^j(x) = x + x^q + x^{q^2} + \dots + x^{q^{m-1}}$$

Para todo $\phi^j \in G$ com $0 \leq j \leq m-1$,

$$\phi^j(\text{Tr}(x)) = \phi^j(x + x^q + x^{q^2} + \dots + x^{q^{m-1}}),$$

de onde segue

$$\phi^j(\text{Tr}(x)) = \phi^j(x) + \phi^j(x^q) + \phi^j(x^{q^2}) + \dots + \phi^j(x^{q^{m-1}}),$$

e

$$\phi^j(\text{Tr}(x)) = x^{q^j} + (x^q)^{q^j} + (x^{q^2})^{q^j} + \dots + (x^{q^{m-1}})^{q^j},$$

$$\phi^j(\text{Tr}(x)) = x^{q^j} + x^{q \cdot q^j} + x^{q^2 \cdot q^j} + \dots + x^{q^{m-1} \cdot q^j}.$$

Daí

$$\phi^j(\text{Tr}(x)) = x^{q^j} + x^{q^{j+1}} + x^{q^{j+2}} + \dots + x^{q^{j+(m-1)}}, \forall x \in F_{q^m}.$$

Portanto,

$$\phi^j(\text{Tr}(x)) = \phi^j(x) + \phi^{j+1}(x) + \dots + \phi^{j+(m-1)}(x), \quad \forall x \in F_{q^m}. \quad (1)$$

Sendo G um grupo cíclico de ordem m ,

$$\phi^m(x) = x, \quad \forall x \in F_{q^m}.$$

Então em (1) teremos que

$$\phi^{j+(m-j)}(x) = x$$

$$\phi^{j+(m-j+1)}(x) = \phi(x)$$

$$\dots\dots\dots$$

$$\phi^{j+(m-j+m-1)}(x) = \phi^{m-1}(x).$$

Portanto $\phi^j(\text{Tr}(x)) = \text{Tr}(x)$. Assim concluímos que o $\text{Tr}(x)$ é invariante sobre F_q . Logo, ele pertence a F_q .

Indicaremos por

$$\text{Tr}_{F_q}^{F_{q^m}}(x)$$

quando houver dúvida em relação a quais corpos está definido o traço.

O traço de um elemento x de F_q tem as seguintes propriedades:

a) Se $x \in F_q$, então $\text{Tr}(x) = mx$.

$$\text{Tr}(x) = x + x^q + x^{q^2} + \dots + x^{q^{m-1}}.$$

Como $x \in F_q$ isto implica que $x^q = x$. Portanto,

$$\begin{aligned} \text{Tr}(x) &= x + x + (x^q)^q + \dots + (x^q)^{q^{m-2}} = \\ &= x + x + x + \dots + x = mx. \end{aligned}$$

b) O traço é uma aplicação linear de F_m em F_q .

Para todo $x, y \in F_m$,

$$\text{Tr}(x+y) = (x+y) + \phi(x+y) + \phi^2(x+y) + \dots + \phi^{m-1}(x+y).$$

Como os ϕ^i , $1 \leq i \leq m-1$ são automorfismos de F_m ,

$$\begin{aligned} \text{Tr}(x+y) &= x + \phi(x) + \phi^2(x) + \dots + \phi^{m-1}(x) + \\ &+ y + \phi(y) + \phi^2(y) + \dots + \phi^{m-1}(y) = \\ &= \text{Tr}(x) + \text{Tr}(y). \end{aligned}$$

Para todo $x \in F_m$ e para todo $\lambda \in F_q$,

$$\text{Tr}(\lambda x) = \lambda x + (\lambda x)^q + (\lambda x)^{q^2} + \dots + (\lambda x)^{q^{m-1}}.$$

Daí

$$\text{Tr}(\lambda x) = \lambda x + \lambda^q x^q + \lambda^{q^2} x^{q^2} + \dots + \lambda^{q^{m-1}} x^{q^{m-1}}.$$

Como $\lambda \in F_q$

$$\begin{aligned} \text{Tr}(\lambda x) &= \lambda x + \lambda x^q + \lambda x^{q^2} + \dots + \lambda x^{q^{m-1}} = \lambda (x + x^q + x^{q^2} + \dots + x^{q^{m-1}}) = \\ &= \lambda \text{Tr}(x). \end{aligned}$$

c) A aplicação traço $\text{tr}: F_m \rightarrow F_q$ é sobrejetora.

F_m é um espaço vetorial de dimensão m sobre F_q . Como já vimos, o traço é uma aplicação linear de F_m em F_q .

Esta aplicação linear é não nula, pois se ela fos-

se nula o polinômio de grau q^{m-1} definido pela aplicação traço.

$$\text{tr}(x) = x + x^q + x^{q^2} + \dots + x^{q^{m-1}},$$

teria como raízes os q^m elementos de F_{q^m} . Mas isto não é possível, porque num corpo um polinômio de grau q^{m-1} tem no máximo q^{m-1} raízes distintas.

Portanto existe x pertencente a F_{q^m} tal que $\text{tr}(x) \neq 0$.

Seja B o núcleo da aplicação traço de F_{q^m} em F_q . O conjunto B é sub-grupo de F_{q^m} . Consequentemente, F_{q^m} é a reunião de classes laterais relativamente ao sub-grupo B , sendo que estas classes são duas a duas disjuntas.

$$F_{q^m} = B \cup (a_1+B) \cup (a_2+B) \cup \dots \cup (a_r+B)$$

com $a_j \in F_{q^m}$, para $1 \leq j \leq r$ e $a_1 = 0$.

Dado x pertencente a F_{q^m} , existe j tal que x seja um elemento da classe lateral a_j+B . Por conseguinte, existe $b \in B$ de modo que

$$x = a_j + b.$$

Portanto

$$\text{tr}(x) = \text{tr}(a_j+b) = \text{tr}(a_j) + \text{tr}(b) = \text{tr}(a_j),$$

pois sendo b pertencente ao núcleo da aplicação traço, $\text{tr}(b) = 0$.

Sejam a_j+B e a_k+B duas classes laterais de F_{q^m}

$(1 \leq j, k \leq r)$. Tomemos $x \in a_j + B$ e $y \in a_k + B$.

Suponhamos que

$$\text{tr}(x) = \text{tr}(y).$$

Como vimos anteriormente,

$$\text{tr}(a_j) = \text{tr}(a_k).$$

Como o traço é linear,

$$\text{tr}(a_j) - \text{tr}(a_k) = \text{tr}(a_j - a_k) = 0$$

e portanto, $a_j - a_k \in B$. Logo,

$$a_j \in a_k + B.$$

Isto significa que x e y fazem parte da mesma classe lateral.

Consequentemente, elementos de classes distintas - têm traços distintos.

Se o sub-conjunto B de F_{q^m} tem q^j elementos $(0 \leq j \leq m)$, então o conjunto das imagens de F_{q^m} através da aplicação traço, que indicaremos por $\text{Im}(F_{q^m})$, tem q^m/q^j elementos. Como $\text{Im}(F_{q^m}) \subset F_q$, então

$$q^{m-j} \leq q.$$

Sabemos que existe x pertencente a F_{q^m} tal que $\text{tr}(x) \neq 0$. Forçosamente $m-j = 1$, de onde

$$j = m - 1.$$

Assim sendo, o índice do sub-grupo $B \subset F_{q^m}$ relativamente ao grupo F_{q^m} é q , o que significa que

$$F_{q^m} = B \cup (a_2 + B) \cup \dots \cup (a_q + B)$$

com $a_j \in F_{q^m}$ para $1 \leq j \leq q$ e $a_1 = 0$.

F_{q^m} possui q classes laterais distintas em relação ao sub-grupo B .

Como elementos de uma mesma classe lateral $a_j + B$ de F_{q^m} tem o mesmo traço em F_q e, se aos elementos de classes laterais de F_{q^m} relativamente a B distintas, correspondem traços diferentes em F_q , então, $\text{Im}(F_{q^m})$ tem q elementos distintos.

Logo,

$$\text{Im}(F_{q^m}) = F_q.$$

$$d) \text{ Se } F_q \subset F_{q^r} \subset F_{q^m}, \text{ então } \text{Tr}_{F_q}^{F_{q^m}}(x) =$$

$$= \text{Tr}_{F_q}^{F_{q^r}}(\text{Tr}_{F_{q^r}}^{F_{q^m}}(x)) \text{ para todo } x \in F_{q^m}.$$

Seja G o grupo de Galois de F_{q^m} sobre F_q .

$$G = \{\phi^j, 0 \leq j \leq m-1\}.$$

O grupo de Galois de F_{q^r} sobre F_q , que indicaremos por H tem ordem r .

Determinemos a condição para que um elemento de G seja gerador de H .

Dado $\phi^j \in G$ ($0 \leq j \leq m-1$) a condição para que ϕ^j pertença a H é que

$$(\phi^j)^r = \phi^0;$$



Como ϕ tem ordem m , então

$$j \cdot r \not\equiv 0 \pmod{m}$$

$$j \not\equiv 0 \pmod{\frac{m}{r}},$$

pois $r = (m, r)$.

Logo,

$$j = \frac{m}{r},$$

e consequentemente

$$H = \{\phi^{i \cdot m/r}, 0 \leq i \leq r-1\}.$$

O grupo de Galois de F_{q^m} sobre F_{q^r} é G/H , que tem ordem $\frac{m}{r}$

$$G/H = \{H, \phi H, \phi^2 H, \dots, \phi^{\frac{m}{r}-1} H\}.$$

Descreveremos agora os elementos pertencentes a cada classe lateral $\phi^k H (0 \leq k \leq \frac{m}{r} - 1)$.

$$H = \{1, \phi^{\frac{m}{r}}, \phi^{2 \frac{m}{r}}, \dots, \phi^{(r-1) \frac{m}{r}}\}$$

$$\phi H = \{\phi, \phi^{\frac{m}{r}+1}, \phi^{2 \frac{m}{r}+1}, \dots, \phi^{(r-1) \frac{m}{r}+1}\}$$

$$\phi^2 H = \{\phi^2, \phi^{\frac{m}{r}+2}, \phi^{2 \frac{m}{r}+2}, \dots, \phi^{(r-1) \frac{m}{r}+2}\}$$

$$\dots \dots \dots \phi^{\frac{m}{r}-1} H = \{\phi^{\frac{m}{r}-1}, \phi^{2 \frac{m}{r}-1}, \phi^{3 \frac{m}{r}-1}, \dots, \phi^{m-1}\}$$

A intersecção das classes laterais é vazia, e

$$G = H \cup \phi H \cup \phi^2 H \cup \dots \cup \phi^{\frac{m}{r}-1} H.$$

$$= \phi^{(r-1)\frac{m}{r}} (\text{Tr}_{F_{q^r}}^F (x)).$$

Logo,

$$\begin{aligned} \text{Tr}_{F_q}^F (x) &= \text{Tr}_{F_{q^r}}^F (x) + \phi^{\frac{m}{r}} (\text{Tr}_{F_{q^r}}^F (x)) + \phi^{2\frac{m}{r}} (\text{Tr}_{F_{q^r}}^F (x)) + \dots + \\ &+ \phi^{(r-1)\frac{m}{r}} (\text{Tr}_{F_{q^r}}^F (x)). \end{aligned}$$

Como $\text{Tr}_{F_{q^r}}^F (x)$ pertence a F_{q^r} , então

$$\text{Tr}_{F_{q^r}}^F (x) = \text{Tr}_{F_q}^{F_{q^r}} (\text{Tr}_{F_{q^r}}^F (x)).$$

NORMA

Definição: Chamamos de norma de um elemento $x \in F_{q^m}$ ao produto dos $\phi^j(x)$ para $0 \leq j \leq m-1$, isto é,

$$N(x) = \prod_{j=0}^{m-1} \phi^j(x) = x \cdot x^q \cdot x^{q^2} \dots x^{q^{m-1}}.$$

Para todo $\phi^j \in G$ com $0 \leq j \leq m-1$ temos

$$\phi^j(N(x)) = \phi^j(x \cdot x^q \cdot x^{q^2} \dots x^{q^{m-1}}),$$

de onde segue

$$\phi^j(N(x)) = \phi^j(x) \cdot \phi^j(x^q) \cdot \phi^j(x^{q^2}) \dots \phi^j(x^{q^{m-1}}) =$$

$$= x^{q^j} \cdot x^{q^{2j}} \cdot x^{q^{3j}} \dots x^{q^{(m-1)+j}}.$$

Podemos concluir que:

$$\phi^j(N(x)) = \phi^j(x) \cdot \phi^{2j}(x) \cdot \phi^{3j}(x) \dots \phi^{(m-1)+j}(x),$$

para todo $x \in F_{q^m}$. Como já foi visto para o caso do traço, podemos concluir que $\phi^j(N(x)) = N(x)$, o que mostra que a norma é invariante sobre F_q . Logo, ela pertence a F_q .

Indicaremos por $N_{F_q^m}^q(x)$ quando houver dúvida em relação a quais corpos está definida a norma.

A norma de um elemento x de F_{q^m} tem as seguintes propriedades:

a) Se $x \in F_q$, então $N(x) = x^m$.

$$N(x) = x \cdot x^q \cdot x^{q^2} \dots x^{q^{m-1}},$$

como $x \in F_q$ isto implica que $x^q = x$. Portanto

$$N(x) = x \cdot x \cdot (x^q)^q \dots (x^q)^{q^{m-2}} = x \cdot x \cdot x \dots x = x^m$$

b) Para todo $x, y \in F_{q^m}$ e para todo $\lambda \in F_q$, temos que

$$N(x \cdot y) = N(x) \cdot N(y)$$

$$N(\lambda x) = \lambda^m \cdot N(x).$$

$$N(x \cdot y) = (x \cdot x^q \cdot x^{q^2} \dots x^{q^{m-1}}) \cdot (y \cdot y^q \cdot y^{q^2} \dots y^{q^{m-1}}) = N(x) \cdot N(y).$$

Sendo $\lambda \in F_q \subset F_{q^m}$ e $x \in F_{q^m}$,

$$N(\lambda x) = N(\lambda) \cdot N(x).$$

$$\text{Portanto, } N(\lambda x) = \lambda^m \cdot N(x).$$

c) A aplicação $N : F_{q^m}^* \rightarrow F_q^*$ é sobrejetora.

A aplicação $N : F_{q^m}^* \rightarrow F_q^*$ é um homomorfismo.

Indiquemos por B o núcleo de N . Se $x \in B$

$$N(x) = x^{\frac{q^m-1}{q-1}} = 1,$$

$B \neq \emptyset$ pois $N(1) = 1$.

O grupo multiplicativo $F_{q^m}^*$ é cíclico e de ordem (q^m-1) . Seja g um gerador de $F_{q^m}^*$. Então,

$$F_{q^m}^* = \{1, g, g^2, \dots, g^{q^m-2}\}.$$

Estudemos a condição para que um elemento de $F_{q^m}^*$ seja gerador do núcleo de N .

Dado $g^h \in F_{q^m}^*$, g^h pertence a B se

$$(g^h)^{\frac{q^m-1}{q-1}} = 1.$$

Como g^h tem ordem (q^m-1) ,

$$h \cdot \frac{q^m-1}{q-1} \equiv 0 \pmod{(q^m-1)},$$

donde

$$h \equiv 0 \pmod{(q-1)}.$$

pois

$$\frac{q^m-1}{q-1} = (q^{m-1}, \frac{q^m-1}{q-1}).$$

$$\text{Logo, } h = q - 1,$$

e consequentemente,

$$B = \{1, g^{(q-1)}, g^{2(q-1)}, \dots, g^{(\frac{q^m-1}{q-1} - 1) \cdot (q-1)}\}$$

Consideremos agora o grupo quociente $F_{q^m}^*/B$. Ele será formado pelas classes laterais.

$$F_{q^m}^*/B = \{B, gB, g^2B, \dots, g^{(q-2)}B\}.$$

Sendo N um homomorfismo do grupo $F_{q^m}^*$ no grupo F_q^* e B o núcleo de N , então pelo teorema do homomorfismo temos que $F_{q^m}^*/B$ é isomorfo ao conjunto das imagens de $F_{q^m}^*$ através de N , ou seja,

$$F_{q^m}^*/B \cong \text{Im}(F_{q^m}^*).$$

Portanto o conjunto $\text{Im}(F_{q^m}^*) \subset F_q^*$ tem exatamente $(q-1)$ elementos donde concluímos que

$$\text{Im}(F_{q^m}^*) = F_q^*.$$

d) Se $F_q \subset F_{q^r} \subset F_{q^m}$, então

$$N_{F_q^*}^{F_q^*}(x) = N_{F_q^*}^{F_q^*} (N_{F_q^*}^{F_q^*}(x))$$

para todo $x \in F_q^*$.

A demonstração desta propriedade é feita de maneira análoga à propriedade d do traço. Convém frisar que no traço levamos em consideração o grupo aditivo F_q^* e agora no caso - da norma temos o grupo multiplicativo F_q^* .

CAPÍTULO III

CARACTERES E SOMA DE GAUSS

1. Antes de estudarmos os caracteres de F_q^* , convém relembrar alguns resultados da teoria das raízes $(q-1)$ -ésimas da unidade no corpo complexo.

As raízes $(q-1)$ -ésimas da unidade formam um grupo multiplicativo G , cíclico, e de ordem $(q-1)$. Se ρ é uma raiz primitiva $(q-1)$ -ésima da unidade, o grupo G é dado por

$$G = \{1, \rho, \rho^2, \dots, \rho^{q-2}\}.$$

Sendo G de ordem $(q-1)$ e ρ o gerador, temos os dois resultados seguintes de fácil demonstração:

- a) $\rho^h = 1$, quando e somente quando $h \equiv 0 \pmod{q-1}$;
- b) $\rho^a = \rho^b$, quando e somente quando $a \equiv b \pmod{q-1}$.

Para representar G podemos, então, tomar como expoentes de ρ um qualquer sistema completo de restos $(\text{mod } q-1)$. Lembremos também que toda potência de ρ , ρ^h por exemplo, pode ser substituída por ρ^s , sendo s o resto mínimo positivo de $h \pmod{q-1}$.

2. Definição: Chama-se carácter do grupo multiplicativo F_q^* , um homomorfismo

$$\chi : F_q^* \rightarrow C^*$$

no grupo C^* do corpo dos números complexos.

Da definição decorrem os seguintes resultados imediatos.

$$a) \chi(1) = 1.$$

Para qualquer x de F_q^* , temos $\chi(x) = \chi(x.1)$ e como χ é homomorfismo, $\chi(x.1) = \chi(x).\chi(1)$. Portanto,

$$\chi(x) = \chi(x).\chi(1), \text{ de onde } \chi(1) = 1.$$

b) Se x é um qualquer elemento de F_q^* , como a ordem de F_q^* é $q-1$,

$$x^{q-1} = 1$$

daí,

$$\chi(x^{q-1}) = 1$$

e

$$\chi^{q-1}(x) = 1.$$

Concluindo, $\chi(x)$ é sempre uma raiz $(q-1)$ -ésima da unidade.

É fácil, então, determinar todas as imagens de um carácter.

De fato, sendo F_q^* um grupo cíclico, seja g o seu gerador.

$$F_q^* = \{1, g, g^2, \dots, g^{q-2}\}.$$

Por outro lado, o grupo G das raízes $(q-1)$ -ésima da unidade

será:

$$G = \{1, \rho, \rho^2, \dots, \rho^{q-2}\}$$

onde ρ é uma raiz $(q-1)$ -ésima primitiva da unidade.

Se fizermos $\chi(g) = \rho^j$, o carácter fica completamente determinado, pois,

$$\chi(g^i) = \rho^{ji}.$$

c) Podemos também determinar todos os caracteres do grupo F_q^* .

Realmente, cada carácter fica completamente conhecido se fizermos $\chi(g) = \rho^j$. Chamemos de χ_j o carácter determinado por

$$\chi_j(g) = \rho^j,$$

com $j = 0, 1, 2, \dots, q-2$. Teremos $q-1$ caracteres diferentes e são esses os únicos possíveis.

$$3. \text{ Seja } \hat{F}_q^* = \{\chi_0, \chi_1, \dots, \chi_{q-2}\}.$$

Vamos definir em $\hat{F}_q^*$ uma multiplicação de caracteres. Para isso façamos

$$\chi_r \cdot \chi_s(x) = \chi_r(x) \cdot \chi_s(x).$$

$\chi_r \cdot \chi_s$ é um carácter pois, $\chi_r \chi_s(g) = \chi_r(g) \cdot \chi_s(g)$, de onde,

$$\chi_r \cdot \chi_s(g) = \rho^r \cdot \rho^s = \rho^{r+s}.$$

Substituindo $r+s$ por seu resto mínimo positivo (mod $q-1$), di-

gamos k , temos:

$$\chi_r \cdot \chi_s(g) = \rho^k = \chi_k(g)$$

e podemos então definir a multiplicação de caracteres por

$$\chi_r \cdot \chi_s = \chi_k.$$

É claro que o produto é associativo e comutativo.

O carácter χ_0 dado por $\chi_0(g) = \rho^0 = 1$, tem para qualquer x de F_q^* , $\chi_0(x) = 1$. Esse carácter, que é sempre igual a 1 chama-se carácter principal ou trivial, e temos

$$\chi_r \cdot \chi_0(x) = \chi_0(x) \cdot \chi_r(x) = \chi_r(x).$$

Portanto

$$\chi_r \cdot \chi_0 = \chi_r$$

ou seja, χ_0 é a unidade de F_q^* .

Para demonstrar a existência do inverso de um dado carácter, χ_r , procuraremos um número inteiro y tal que,

$$\chi_r \cdot \chi_y = \chi_0$$

o que é o mesmo que:

$$\chi_r(x) \cdot \chi_y(x) = \chi_0(x). \quad (1)$$

Ora, de (1) segue:

$$\chi_r(g) \cdot \chi_y(g) = \chi_0(g).$$

Portanto,

$$\rho^r \cdot \rho^y = \rho^0$$

o que resulta em

$$\rho^{r+y} = \rho^0$$

e

$$r + y \equiv 0 \pmod{q-1}$$

$$y \equiv -r \pmod{q-1}.$$

Logo, o carácter inverso é χ_{-r} . Como $-r \equiv s \pmod{q-1}$, sendo s resto mínimo positivo $\pmod{q-1}$,

$$\chi_r^{-1} = \chi_s \quad 0 \leq s < q-1$$

Concluindo, vimos que o produto de dois caracteres é um carácter, que esse produto é associativo e comutativo, que existe a unidade, que é o carácter principal χ_0 , e que todo carácter χ_r , tem um inverso $\chi_r^{-1} = \chi_s$. Assim sendo $\hat{F}_q^*$ é um grupo, chamado grupo dual de F_q^* .

4. É imediato mostrar que F_q^* e $\hat{F}_q$ são isomorfos.

De fato, o carácter χ_r fica completamente determinado se colocarmos $\chi_r(g) = \rho^r$. Ora, como $\chi_1(g) = \rho$ e sendo $\rho \neq 1$ e uma raiz $(q-1)$ -ésima da unidade, pela multiplicação de caracteres,

$$\begin{aligned} \chi_0 &= \chi_1^0 \\ \chi_1 &= \chi_1^1 \\ \chi_2 &= \chi_1^2 \\ &\vdots \\ \chi_j &= \chi_1^j \\ &\vdots \\ \chi_{q-2} &= \chi_1^{q-2} \end{aligned}$$

são todos distintos. Então,

$$\hat{F}_q^* = \{x_0, x_1, \dots, x_{q-2}\}$$

é um grupo cíclico com gerador x_1 e com o mesmo número de elementos que tem o grupo $F_{q^m}^*$. O isomorfismo desejado será:

$$\phi : g^r \rightarrow x_r.$$

5. Relações de Ortogonalidade

a) Se χ é um carácter de F_q^* ,

$$\sum_{x \in F_q^*} \chi(x) = \begin{cases} q-1 & \text{se } \chi = \chi_0 \\ 0 & \text{se } \chi \neq \chi_0 \end{cases}$$

1º caso: $\chi = \chi_0$, então para todo $x \in F_q^*$, $\chi(x) = 1$.

Portanto,

$$\sum_{x \in F_q^*} \chi(x) = \text{card}(F_q^*) = q-1$$

2º caso: $\chi \neq \chi_0$, então existe $y \in F_q^*$ tal que $\chi(y) \neq 1$.

Logo,

$$\sum_{x \in F_q^*} \chi(x) = \sum_{x \in F_q^*} \chi(x \cdot y) = \sum_{x \in F_q^*} \chi(x) \cdot \chi(y),$$

de onde chegamos a

$$(1 - \chi(y)) \cdot \sum_{x \in F_q^*} \chi(x) = 0.$$

Como $\chi(y) \neq 1$, então $\sum_{x \in F_q^*} \chi(x) = 0$.

b) Se x é um elemento de F_q^* ,

$$\sum_{x \in F_q^*} \chi(x) = \begin{cases} (q-1) & \text{se } x = 1 \\ 0 & \text{se } x \neq 1 \end{cases}$$

1º caso: $x = 1$, então para todo $x \in \hat{F}_q^*$, temos que $\chi(1) = 1$.

Portanto,

$$\sum_{x \in \hat{F}_q^*} \chi(1) = \text{card}(\hat{F}_q^*) = q-1$$

2º caso: $x \neq 1$. Seja g um gerador de F_q^* . Então $x = g^r$ ($1 \leq r < (q-1)$).

Consideremos ρ uma raiz $(q-1)$ -ésima primitiva da unidade. Existe $\chi_1 \in \hat{F}_q^*$ tal que $\chi_1(g) = \rho$. Consequentemente,

$$\chi_1(x) = \chi_1(g^r) = \rho^r \neq 1.$$

Logo,

$$\sum_{x \in \hat{F}_q^*} \chi(x) = \sum_{x \in \hat{F}_q^*} \chi_1(x) \chi(x) = \sum_{x \in \hat{F}_q^*} \chi_1(x) \cdot \chi(x) = \chi_1(x) \sum_{x \in \hat{F}_q^*} \chi(x).$$

Temos, a seguir:

$$(1 - \chi_1(x)) \sum_{x \in \hat{F}_q^*} \chi(x) = 0.$$

Como $\chi_1(x) \neq 1$, então $\sum_{x \in \hat{F}_q^*} \chi(x) = 0$.

Convenientemente, podemos definir os valores dos ca

racteres no ponto zero de F_q da seguinte forma:

$$\chi(0) = \begin{cases} 1 & \text{se } x = x_0 \\ 0 & \text{se } x \neq x_0 \end{cases} \quad \text{e} \quad \chi_r(0) = \begin{cases} 1 & \text{se } r = 0 \\ 0 & \text{se } r \neq 0 \end{cases}$$

6. Definição: Chama-se carácter do grupo aditivo F_q^+ , um homomorfismo

$$\psi : F_q^+ \rightarrow C^*$$

no grupo multiplicativo C^* do corpo dos números complexos.

Da definição decorrem os seguintes resultados:

a) $\psi(0) = 1$

Para qualquer $x \in F_q^+$, temos $\psi(x) = \psi(x+0)$ e como ψ é um homomorfismo, $\psi(x+0) = \psi(x) \cdot \psi(0)$ e, portanto, $\psi(x) = \psi(x) \cdot \psi(0)$, donde $\psi(0) = 1$

b) $\psi(x)$ é uma raiz p-ésima da unidade.

Seja x um elemento qualquer de F_q^+ . Como a característica de F_q é um número primo p ,

$$px = 0.$$

Daí vem,

$$\psi(px) = \psi(0) = 1.$$

Sendo ψ um homomorfismo,

$$\psi(px) = \psi(x+x+\dots+x) = \psi(x) \cdot \psi(x) \cdot \dots \cdot \psi(x)$$

e, portanto,

$$\psi^p(x) = \psi(px) = 1$$

Logo $\psi(x)$ é uma raiz p -ésima da unidade.

c) Carácter Principal

Se $\psi(x) = 1$, qualquer que seja x de F_q^+ , ψ é um carácter.

$$\text{Realmente, } \psi(x+y) = 1 = 1 \cdot 1 = \psi(x) \cdot \psi(y)$$

Este carácter denomina-se principal e indicaremos sempre por ψ_0 .

7. Valores de um Carácter $\psi(x)$

Inicialmente, lembremos que o corpo F_p é isomorfo ao anel $\mathbb{Z}/p\mathbb{Z}$ das classes de restos (mod p) e que podemos, portanto, tomar como elementos de F_p um qualquer sistema completo de restos (mod p). Por exemplo, o sistema completo de restos - mínimos positivos

$$0, 1, 2, \dots, (p-1). \quad (1)$$

O grupo aditivo F_p^+ é sub-grupo de F_q^+ . Consequentemente, F_q^+ é a união de suas classes laterais relativamente ao sub-grupo F_p^+ , sendo estas classes duas a duas disjuntas.

$$F_q^+ = F_p^+ \cup (a_2 + F_p^+) \cup (a_3 + F_p^+) \cup \dots \cup (a_{p^{r-1}} + F_p^+),$$

com $a_j \in F_q^+$ para $1 \leq j \leq p^{r-1}$ e $a_1 = 0$.

Um qualquer elemento x de F_q^+ pertence só a uma

das classes $a_j + F_p^+$ e, portanto, existe k pertencente ao sistema (1), tal que

$$x = a_j + k.$$

Como já vimos, os valores de um carácter ψ para x pertencente ao corpo F_q são raízes p -ésimas da unidade.

Consideremos $\psi(1) = \rho_1$, onde ρ_1 é uma qualquer raiz p -ésima da unidade. Sendo ψ um homomorfismo,

$$\begin{aligned}\psi(2) &= \psi(1+1) = \rho_1^2 \\ \psi(3) &= \psi(2+1) = \rho_1^3 \\ &\dots\dots\dots \\ \psi(p-1) &= \psi(p-2+1) = \rho_1^{p-1} \\ \psi(p) &= \psi(p-1+1) = \rho_1^p = 1\end{aligned}$$

Façamos agora $\psi(a_j) = \rho_j$ para $2 \leq j \leq p^{r-1}$, onde ρ_j é uma qualquer raiz p -ésima da unidade. Pelo fato de ψ ser um homomorfismo, então para x percorrendo a classe lateral $a_j + F_p^+$, temos:

$$\begin{aligned}\psi(a_j+1) &= \rho_j \rho_1 \\ \psi(a_j+2) &= \rho_j \rho_1^2 \\ &\dots\dots\dots \\ \psi(a_j+p-1) &= \rho_j \rho_1^{p-1} \\ \psi(a_j+p) &= \rho_j \rho_1^p = \rho_j\end{aligned}$$

Vimos que dado arbitrariamente o valor de $\psi(a_j)$ os valores de todos os elementos da classe $a_j + F_p^+$ estão determinada

dos. Então, para obtermos um carácter, basta darmos arbitrariamente os valores de $\psi(a_j)$, que o carácter será determinado. Como existe p_{r-1} classes laterais, então temos $p \cdot p^{r-1}$ caracteres aditivos de F_q^+ .

8. Podemos dar uma forma cômoda aos caracteres aditivos. De fato, seja $\psi(x)$ um carácter qualquer. Vamos mostrar que ele pode ser escrito

$$\psi(x) = \rho^{\text{tr}(x)}, \quad (2)$$

onde ρ é uma qualquer raiz p -ésima da unidade.

Para o nosso objetivo basta mostrar que (2) é um carácter de F_q^+ .

Como o $\text{tr}(x)$ é um elemento do sistema (1), consequentemente, $\rho^{\text{tr}(x)}$ é uma raiz p -ésima da unidade. A aplicação definida em (2) é um homomorfismo do grupo aditivo F_q^+ no grupo multiplicativo C^* do corpo dos números complexos, pois, para todo x, y de F_q^+

$$\psi(x+y) = \rho^{\text{tr}(x+y)}.$$

Como tr é linear,

$$\rho^{\text{tr}(x+y)} = \rho^{\text{tr}(x) + \text{tr}(y)} = \rho^{\text{tr}(x)} \cdot \rho^{\text{tr}(y)}.$$

Daí,

$$\psi(x+y) = \psi(x) \cdot \psi(y)$$

9. Grupo Dual de F_q^+ .

Consideremos o conjunto dos caracteres aditivos de F_q^+ , que indicaremos por $\hat{F}_q^+$. Podemos tomar como multiplicação de caracteres, a multiplicação habitual de aplicação, isto é, se ψ e ψ' pertencem a $\hat{F}_q^+$, definiremos

$$\psi \cdot \psi'(x) = \psi(x) \cdot \psi'(x)$$

É claro que $\psi \cdot \psi'$ é um carácter. De fato, qualquer que seja x de F_q^+ , temos, $\psi(x) = \rho^{\text{tr}(x)}$ e $\psi'(x) = \rho_1^{\text{tr}(x)}$ e como ρ e ρ_1 são raízes p -ésimas da unidade $\rho \cdot \rho_1$ também será e vem,

$$\psi \cdot \psi'(x) = \psi(x) \cdot \psi'(x) = \rho^{\text{tr}(x)} \cdot \rho_1^{\text{tr}(x)}$$

de onde,

$$\rho^{\text{tr}(x)} \cdot \rho_1^{\text{tr}(x)} = (\rho \cdot \rho_1)^{\text{tr}(x)}.$$

Fazendo $\rho \cdot \rho_1 = \rho_2$,

$$\psi \cdot \psi'(x) = \rho_2^{\text{tr}(x)}.$$

Como ρ_2 é uma raiz p -ésima da unidade, $\psi \cdot \psi'$ é um carácter aditivo de F_q^+ .

A multiplicação que definimos é, portanto, estável em $\hat{F}_q^+$. Como a multiplicação em C^* é associativa e comutativa, segue as propriedades associativa e comutativa dos caracteres.

Também se verifica facilmente que a unidade de $\hat{F}_q^+$ é o carácter principal.

Finalmente, dado o caráter $\psi(x) = \rho^{\text{tr}(x)}$, observe-mos que $\overline{\psi(x)} = \overline{\rho^{\text{tr}(x)}} = \overline{\rho}^{\text{tr}(x)}$, onde $\overline{\rho}$ é também raiz p-ésima da unidade. $\overline{\psi(x)}$ é um caráter, pois

$$\psi \cdot \overline{\psi}(x) = \psi(x) \cdot \overline{\psi}(x) = \rho^{\text{tr}(x)} \cdot \overline{\rho}^{\text{tr}(x)} = (\rho \cdot \overline{\rho})^{\text{tr}(x)}.$$

Como $\rho \overline{\rho} = 1$,

$$\psi \cdot \overline{\psi}(x) = 1, \text{ para todo } x \in F_q^+$$

$$\psi \cdot \overline{\psi} = \psi_0.$$

$\overline{\psi}$ é o caráter inverso de ψ .

Concluindo, vimos que o produto de dois caracteres aditivos é um caráter aditivo; que esse produto é associativo e comutativo, que existe a unidade, que é o caráter principal ψ_0 e que todo caráter $\psi \in \hat{F}_q^+$ tem um inverso $\psi^{-1} = \overline{\psi}$. Assim sendo $\hat{F}_q^+$ é um grupo que se chama grupo dual de F_q^+ .

10. Outra notação para um caráter do grupo aditivo F_q^+ .

Seja ψ um caráter não principal do grupo aditivo F_q^+ .

Observemos que a aplicação $x \rightarrow ax$, sendo $a \neq 0$, é um automorfismo do grupo aditivo F_q^+ . Por conseguinte, se substituirmos em (2) x por ax , teremos:

$$\psi(ax) = \rho^{\text{tr}(ax)}$$



que também é um carácter de F_q^+ .

Mostramos em cada elemento a pertencente a F_q^+ , define um e só um carácter de F_q^+ , que indicamos por ψ_a .

Dados a e b pertencentes a F_q^+ , suponhamos

$$\psi(ax) = \psi(bx), \quad \forall x \in F_q^+.$$

Consequentemente,

$${}_p \text{tr}(ax) = {}_p \text{tr}(bx).$$

Dai,

$${}_p \text{tr}(ax) - {}_p \text{tr}(bx) = 1.$$

Como o traço é linear

$${}_p \text{tr}(ax) - \text{tr}(bx) = {}_p \text{tr}(a-b)x = 1, \quad \forall x \in F_q^+$$

Portanto para todo x pertencente a F_q^+ , vem que:

$$\text{tr}(a-b)x = 0.$$

Como o traço é uma aplicação não nula de F_q^+ ,

$$(a-b)x = 0, \quad \forall x \in F_q^+$$

de onde,

$$a = b$$

F_q^+ tem p^r elementos e cada um desses elementos define um único elemento no grupo dual $\hat{F}_q^+$, que também tem p^r elementos. Então, dado um carácter ψ do grupo aditivo F_q^+ , existe um único a pertencente a F_q^+ de modo que,

$$\psi = \psi_a$$

11 - Relação de Ortogonalidade

Seja ψ um carácter não principal de F_q^+ e x um qualquer elemento de F_q^+ .

$$\sum_{a \in F_q^+} \psi(ax) = \begin{cases} q & \text{se } x = 0 \\ 0 & \text{se } x \neq 0 \end{cases}$$

1º caso: $x = 0$, como para todo $a \in F_q^+$, $\psi(ax) = \psi(0) = 1$,

$$\sum_{a \in F_q^+} \psi(ax) = \sum_{a \in F_q^+} 1 = q$$

2º caso: $x \neq 0$

$$\sum_{a \in F_q^+} \psi(ax) = \sum_{a \in F_q^+} \psi_x(a) = \sum_{a \in U(a_j + F_q^+)} \psi_x(a) \quad (3)$$

ψ é um carácter não principal. Como $x \neq 0$,

$$\psi_x(a) = \psi(ax) \neq 1$$

para algum a de F_q^+ e, portanto, ψ_x é um carácter não principal.

Enquanto a percorre uma das classes laterais $a_j + F_q^+$ o valor de $\psi_x(a)$ percorre o conjunto das raízes p -ésimas da unidade. Como a soma das p raízes p -ésimas da unidade é zero, então a soma indicada em (3) será o resultado da adição de p^{r-1} parcelas iguais a zero, onde cada uma delas representa a soma dos $\psi_x(a)$ quando a percorre uma determinada clas-

se lateral $a_j \in F_p^+$.

12. Soma de Gauss.

Por definição, chamamos de soma de Gauss do corpo F_q ao número:

$$g(\chi) = \sum_{x \in F_q} \chi(x) \cdot \psi(x)$$

onde ψ é um carácter aditivo do grupo F_q fixo, e diferente de ψ_0 , e χ é qualquer um dos caracteres multiplicativos de F_q^* diferente de χ_0 .

CAPÍTULO IV

TEOREMA DE DAVENPORT E HASSE

O objetivo deste trabalho é demonstrar o teorema de Davenport e Hasse que permite relacionar a soma de Gauss num corpo finito e em suas extensões finitas.

Sejam $F_p \subset F_q \subset F_{q^m}$ corpos finitos, onde F_{q^m} é uma extensão finita de grau m de F_q , e F_q é uma extensão finita de grau r de F_p .

1- Para $y \in F_{q^m}$ seja $T(y)$ e $T_m(y)$, respectivamente, o traço de y em relação a F_p e F_q e ainda sejam $N(y)$ e $N_m(y)$, respectivamente, a norma de y em relação a F_p e F_q . Para $x \in F_q$ indiquemos por $t(x)$ e $n(x)$, respectivamente, o traço e a norma de x em relação ao corpo F_p .

Lema 1 - Se g é um gerador do grupo multiplicativo $F_{q^m}^*$, então, existe um gerador w do grupo multiplicativo F_q^* , tal que,

$$N_m(g) = w. \quad (1)$$

O grupo multiplicativo $F_{q^m}^*$ do corpo finito F_{q^m} é cíclico e de ordem $q^m - 1$.

Seja g um gerador de $F_{q^m}^*$, então

$$F_{q^m}^* = \{1, g, g^2, \dots, g^{q^m-2}\}$$

O grupo multiplicativo F_q^* do corpo finito F_q é sub-grupo de $F_{q^m}^*$.

Determinemos a condição para que um elemento g^h ($0 \leq h \leq q^m - 2$) de $F_{q^m}^*$ seja um gerador do sub-grupo F_q^* .

Sendo F_q^* um grupo cíclico de ordem $(q-1)$, então a condição para que um elemento g^h de $F_{q^m}^*$ pertença a F_q^* é que:

$$(g^h)^{q-1} = 1,$$

de onde temos

$$g^{h(q-1)} = 1$$

Como g é um gerador do grupo multiplicativo $F_{q^m}^*$, o qual tem ordem $q^m - 1$.

$$h \equiv 0 \pmod{\frac{q^m-1}{\delta}},$$

onde $\delta = (q^m - 1, q - 1)$. Sendo $\delta = q - 1$, então segue

$$h = \frac{q^m - 1}{q - 1}$$

Portanto, se g é um gerador de $F_{q^m}^*$, então existe

$$\omega = g^{\frac{q^m - 1}{q - 1}} \quad (2)$$

gerador do sub-grupo F_q^* .

Calculemos a norma do gerador g de $F_{q^m}^*$ em relação a F_q^* .

$$N_m(g) = g \cdot g^q \dots g^{q^{m-1}} = g^{\frac{q^m-1}{q-1}}$$

Logo, dado um gerador g de $F_{q^m}^*$, existe um gerador ω do grupo multiplicativo F_q^* , tal que

$$N_m(g) = \omega \quad (1)$$

Consideremos $\rho^* \neq 1$ uma raiz $(q-1)$ -ésima da unidade, ρ^* é também uma raiz (q^m-1) -ésima da unidade. Então:

$$\chi_r'(g) = \rho^{*r} \quad \text{para } 0 \leq r < q-1,$$

determina um carácter multiplicativo do grupo $F_{q^m}^*$, onde g é um gerador de $F_{q^m}^*$.

TEOREMA 1 - Dado y pertencente a $F_{q^m}^*$, então

$$\chi_r'(y) = \chi_r(N_m(y)),$$

onde χ_r é um carácter multiplicativo de F_q^* definido por $\chi_r(\omega) = \rho^{*r}$.

Para um y qualquer de $F_{q^m}^*$ calculemos o valor de $\chi_r'(y)$.

Sendo g gerador de $F_{q^m}^*$,

$$y = g^s \quad \text{para} \quad 0 \leq s \leq q-2$$

Portanto,

$$\chi'_r(y) = \chi'_r(g^s)$$

Sendo χ'_r um carácter,

$$\chi'_r(g^s) = (\chi'_r(g))^s = (\rho^{*r})^s = \rho^{*r \cdot s} \quad (3)$$

Agora, calculemos $\chi_r(N_m(y))$.

$$\chi_r(N_m(y)) = \chi_r(N_m(g^s)).$$

Pela propriedade da norma

$$\chi_r(N_m(g^s)) = \chi_r(N_m(g))^s.$$

Pelo lema 1, sabemos que existe w gerador de F_q^* , tal que $N(g) = w$. Então

$$\chi_r(N_m(y)) = \chi_r(w^s) = (\rho^{*r})^s = \rho^{*rs} \quad (4)$$

De (3) e (4),

$$\chi'_r(y) = \chi_r(N_m(y)).$$

Seja ρ' uma raiz p -ésima primitiva da unidade.

Dado y pertencente a $F_{q^m}^+$

$$\psi'(y) = \rho'^{T(y)},$$

que define um carácter aditivo de $F_{q^m}^+$. Assim como, dado x

pertencente a F_q^+

$$\psi(x) = \rho, t(x)$$

define um carácter aditivo de F_q^+ .

Para y pertencente a $F_{q^m}^+$,

$$\psi'(y) = \rho, T(y) = \rho, t(T_m(y))$$

e

$$\psi'(y) = \psi(T_m(y)). \quad (5)$$

2 - Seja χ um carácter multiplicativo de F_q e ψ um carácter aditivo de F_q ambos não principais e consideremos os polinômios unitários de $F_q[x]$. isto é, os polinômios

$$f = x^r + c_1 x^{r-1} + \dots + c_r$$

com coeficientes $1, c_1, c_2, \dots, c_r$ de F_q .

Chamemos de

$$\lambda(f) = \chi(c_r) \psi(c_1) \quad (6)$$

e de $n(f)$ o grau r do polinômio f .

$$n(f) = r \quad (7)$$

Esses dois números $\lambda(f)$ e $n(f)$ satisfazem as seguintes propriedades: $\lambda(f_1 \cdot f_2) = \lambda(f_1) \cdot \lambda(f_2)$ e $n(f_1 \cdot f_2) = n(f_1) + n(f_2)$

(8)
A segunda propriedade é conhecida. Quanto à primeira, basta fazer os cálculos. De fato, se

$$f_1 = x^r + c_1 x^{r-1} + \dots + c_r$$

$$f_2 = x^s + d_1 x^{s-1} + \dots + d_s$$

temos

$$\lambda(f_1) = x(c_r) \psi(c_1)$$

$$\lambda(f_2) = x(d_s) \psi(d_1)$$

Multiplicando f_1 por f_2 ,

$$f_1 \cdot f_2 = x^{r+s} + (c_1 + d_1) x^{r+s-1} + \dots + c_r d_s$$

e, portanto,

$$\lambda(f_1 \cdot f_2) = x(c_r \cdot d_s) \cdot \psi(c_1 + d_1)$$

donde

$$\lambda(f_1 \cdot f_2) = x(c_r) x(d_s) \cdot \psi(c_1) \psi(d_1).$$

Logo,

$$\lambda(f_1 \cdot f_2) = \lambda(f_1) \cdot \lambda(f_2).$$

De (8) segue imediatamente que

$$\lambda(f^a) = \lambda^a(f)$$

(9)

$$n(f^a) = an(f)$$

No anel $F_q[x]$, como sabemos todo polinômio se decompõe e de um só modo num produto de fatores irredutíveis. Então, se $f \in F_q[x]$, chamando de $p_1, p_2, \dots, p_k$ os seus fatores

irredutíveis diferentes, temos:

$$f = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \alpha_i > 0$$

e, portanto,

$$\lambda(f) = \lambda(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \lambda^{\alpha_1}(p_1) \cdot \lambda^{\alpha_2}(p_2) \cdots \lambda^{\alpha_k}(p_k)$$

$$n(f) = \alpha_1 n(p_1) + \alpha_2 n(p_2) + \cdots + \alpha_k n(p_k) \quad (10)$$

Convém notar que pela decomposição única de f em seus fatores irredutíveis e como estamos trabalhando com polinômios unitários, dado f , os polinômios irredutíveis

$p_1, p_2, \dots, p_k$ e os expoentes $\alpha_1, \alpha_2, \dots, \alpha_k$ estão univocamente determinados e, reciprocamente, dados os polinômios irredutíveis $p_1, p_2, \dots, p_k$ e os números naturais $\alpha_1, \alpha_2, \dots, \alpha_k$, o polinômio $f = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ também está univocamente determinado.

3 - Consideremos o anel das séries formais de potências $F_q[[x]]$. A série $1 - \lambda(p)x^{n(p)}$, onde p é um polinômio irredutível de $F_q[x]$, tem o primeiro termo diferente de zero, portanto tem inverso. Donde,

$$\frac{1}{1 - \lambda(p)x^{n(p)}} = 1 + \lambda(p)x^{n(p)} + \lambda^2(p)x^{2n(p)} + \dots \quad (11)$$

Consideremos o produto formal estendido a todos polinômios irredutíveis e unitários de $F_q[x]$.

$$\prod_p \frac{1}{1 - \lambda(p)x^{n(p)}} = 1 + \prod_p (1 + \lambda(p)x^{n(p)} + \lambda^2(p)x^{2n(p)} + \dots) \quad (12)$$

O produto do 2º membro de (12) tem o primeiro termo igual a 1. Um outro termo qualquer correspondente aos fatores primos $p_1, p_2, \dots, p_k$, será da forma

$$\lambda^{\alpha_1}(p_1)x^{\alpha_1 n(p_1)} \lambda^{\alpha_2}(p_2)x^{\alpha_2 n(p_2)} \dots \lambda^{\alpha_k}(p_k)x^{\alpha_k n(p_k)}$$

isto é,

$$\lambda^{\alpha_1}(p_1) \lambda^{\alpha_2}(p_2) \dots \lambda^{\alpha_k}(p_k) x^{\alpha_1 n(p_1) + \dots + \alpha_k n(p_k)}$$

donde, de acordo com (10)

$$\lambda(f) \cdot x^{n(f)}$$

onde

$$f = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

ou seja, $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$ é a decomposição única de f em seus fatores primos.

Pelo que já foi dito, como f está univocamente determinado pelos primos $p_1, p_2, \dots, p_k$ e os expoentes $\alpha_1, \alpha_2, \dots, \alpha_k$ o termo $\lambda(f) x^{n(f)}$ ocorre uma a uma só vez no segundo membro de (12) e ainda mais cada polinômio unitário

f aparecerá uma e uma só vez nesse desenvolvimento . Portanto,

$$\prod_p \frac{1}{1 - \lambda(p) x^{n(p)}} = \sum_f \lambda(f) x^{n(f)}$$

donde o seguinte teorema:

TEOREMA 2 - Seja χ e ψ dois caracteres não principais de F_q , respectivamente, multiplicativo e aditivo. Se considerarmos, para qualquer polinômio unitário irreduzível p de $F_q[x]$.

$$p = x^r + c_1 x^{r-1} + \dots + c_r$$

$$\lambda(p) = \chi(c_r) \psi(c_1)$$

e

$$n(p) = r$$

teremos a identidade formal

$$\prod_p \frac{1}{1 - \lambda(p) x^{n(p)}} = \sum_f \lambda(f) x^{n(f)} + 1 \quad (13)$$

onde, no 2º membro, f percorre todos os polinômios unitários de $F_q[x]$.

Chamemos de

$$e_n = \sum_f \lambda(f) ,$$

a soma estendida a todos os polinômios f pertencentes a $F_q[x]$, unitários e de grau n .

Calculemos os valores de e_n , para $n \geq 1$.

Para $n = 1$,

$$e_1 = \sum_{c \in F_q} \chi(c) \psi(c) = g(\chi)$$

Para $n \geq 2$,

$$e_n = q^{n-2} \sum_{c_n \in F_q} \chi_r(c_n) \sum_{c_1 \in F_q} \psi(c_1) = 0.$$

porque tanto $\sum_{c_n \in F_q} \chi(c_n) = 0$ como $\sum_{c_1 \in F_q} \psi(c_1) = 0$.

Substituindo em (13) esses resultados,

$$1 + g(\chi)x = \prod_p [1 - \lambda(p) x^{n(p)}]^{-1} \quad (14)$$

5 - Seja F_{q^m} uma extensão finita de F_q de grau m . Como foi feito inicialmente, consideremos χ' um caráter multiplicativo de F_{q^m} e ψ' um caráter aditivo de F_{q^m} , ambos não principais, e tomemos os polinômios unitários de $F_{q^m}[Y]$, ou seja,

$$f' = Y^s + d_1 Y^{s-1} + \dots + d_s \quad (15)$$

com coeficientes $1, d_1, \dots, d_s$ de F_{q^m} .

Chamemos de

$$\lambda'(f') = \chi'(d_s) \psi'(d_1) \quad (16)$$

e de $n'(f')$ o grau do polinômio f'

$$n'(f') = s$$

Repetindo os estudos feitos nos itens 2,3 e 4 deste capítulo, chegaremos ao seguinte resultado:

$$1 + g'(\chi')Y = \prod_{p'} [1 - \lambda'(p')Y^{n'(p')}]^{-1}, \quad (17)$$

onde, no segundo membro o produto é tomado sobre todos os polinômios unitários e irredutíveis no anel $F_{q^m}[Y]$.

7 - Recordemos o resultado obtido no capítulo I - item 6.

Seja p um polinômio irredutível unitário em $F_q[x]$ e de grau n . Numa extensão F_{q^m} de F_q , p se decompõe em $d = (m,n)$ polinômios irredutíveis de grau $\frac{n}{d}$ em $F_{q^m}[x]$.

$$p = p'_1 \cdot p'_2 \cdots p'_d, \quad p'_i \in F_{q^m}[x] \quad \text{para} \quad i = 1, 2, \dots, d$$

Consideremos um fator irredutível de p em $F_{q^m}[x]$.

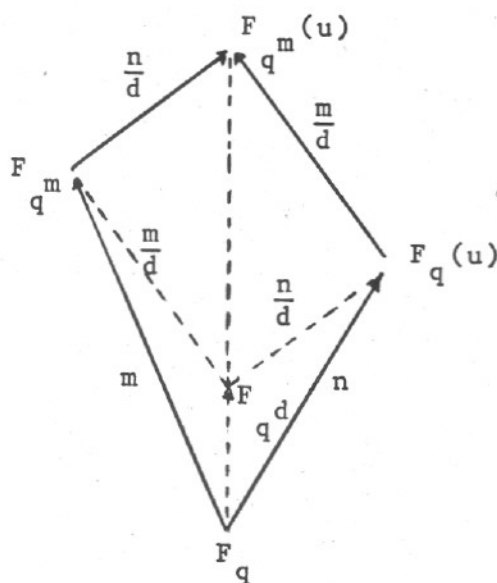
Indiquemos este fator por p' e seja u uma raiz de p' . A raiz u gera sobre F_q uma extensão $F_q(u)$ de grau $n = n(p)$ e sobre F_{q^m} uma extensão $F_{q^m}(u)$ de grau $n'(p') = \frac{n}{d}$.

A extensão $F_{q^m}(u)$ de F_{q^m} obtida pela adjunção da raiz u do polinômio p' pertencente a $F_{q^m}[x]$ a F_{q^m} é o menor sub-corpo que contém u e F_{q^m} . Como F_q é sub-corpo de F_{q^m} , $F_{q^m}(u)$ é o menor sub-corpo que contém $F_q(u)$ e F_{q^m} , o que significa que $F_{q^m}(u)$ é o composto de $F_q(u)$ e F_{q^m} .

$$\text{Sendo } (m, \frac{n}{d}) = 1,$$

$$[F_{q^m}(u) : F_q] = [F_{q^m} : F_q] [F_{q^m}(u) : F_{q^m}] = m \cdot \frac{n}{d}$$

Podemos daí formar o seguinte diagrama:



8 - Consideremos a e b , respectivamente, norma e traço de u tomados em $F_q(u)$ relativamente a F_q .

Sendo,

$$p = x^n + bx^{n-1} + \dots + a \in F_q[x].$$

o número

$$\lambda(p) = \chi(a) \psi(b). \quad (18)$$

Do mesmo modo, sejam a' e b' , respectivamente, norma e traço de u tomados em $F_{q^m}(u)$ relativamente a F_{q^m} .

Sendo

$$p' = Y^{\frac{n}{d}} + b'Y^{\frac{n}{d}-1} + \dots + a' \in F_{q^m}[Y],$$

o número

$$\lambda'(p') = \chi'(a') \psi'(b'). \quad (19)$$

Por (5) e pelo Teorema 1, temos que

$$\lambda'(p') = \chi(N_m(a')) \psi(T_m(b')), \quad (20)$$

onde

$$N_m(a') = N_{F_q}^{F_{q^m}}(a') = N_{F_q}^{F_{q^m}}(N_{F_q}^{F_{q^m}(u)}(u)) = N_{F_q}^{F_{q^m}(u)}(u)$$

e

$$T_m(b') = T_{F_q}^{F_q m}(b') = T_{F_q}^{F_q m} (T_{F_q}^{F_q m(u)}(u)) = T_{F_q}^{F_q m(u)}(u).$$

Considerando o diagrama podemos calcular $N_m(a')$ e $T_m(b')$ da seguinte forma:

$$N_m(a') = N_{F_q}^{F_q(u)} (N_{F_q}^{F_q m(u)}(u)) = N_{F_q}^{F_q(u)} ((u)^{\frac{m}{d}}) = (N_{F_q}^{F_q(u)}(u))^{\frac{m}{d}} = a^{\frac{m}{d}}$$

e

$$T_m(b') = T_{F_q}^{F_q(u)} (T_{F_q}^{F_q m(u)}(u)) = T_{F_q}^{F_q(u)} (\frac{m}{d} u) = \frac{m}{d} T_{F_q}^{F_q(u)}(u) = \frac{m}{d} \cdot b$$

Portanto, em (19)

$$\lambda'(p') = \chi(a^{\frac{m}{d}}) \psi(\frac{m}{d} b),$$

de onde vem

$$\lambda'(p') = [\chi(a) \psi(b)]^{\frac{m}{d}}.$$

Utilizando (18),

$$\lambda'(p') = [\lambda(p)]^{\frac{m}{d}}$$

9 - Agora, consideremos o lado esquerdo da igualdade (17). A ela juntemos os d fatores irredutíveis p_i' do polinômio p em $F_{q^m}[x]$ os quais tem grau $n'(p_i') = \frac{n}{d}$ e tem o mesmo valor para $\lambda'(p_i')$. Também troquemos a indeterminada Y por X^m . Assim procedendo obtemos a seguinte expressão.

$$\left[1 - \lambda(p)^{\frac{m}{d}} x^m \frac{n}{d} \right]^{-d}.$$

O número $\lambda(p)^{\frac{m}{d}}$ é um número complexo, porque

$$\lambda(p) = \chi(a) \psi(b)$$

onde $\chi(a)$ é uma raiz (q^m-1) -ésima da unidade e $\psi(b)$ é uma raiz p -ésima da unidade.

TEOREMA 3 - Mostremos que para um número complexo $\alpha \neq 0$ vale a seguinte identidade:

$$\left[1 - \alpha^{\frac{m}{d}} x^m \frac{n}{d} \right]^d = \prod_{j=0}^{m-1} \left[1 - \alpha (w^j x)^n \right], \quad (21)$$

onde w é uma raiz m -ésima primitiva da unidade.

Para mostrarmos esta identidade vamos colocar o segundo membro de (21) numa forma mais conveniente.

$$\prod_{j=0}^{m-1} [1 - \alpha(w^j x)^n] = (1 - \alpha x^n)(1 - \alpha w^n x^n)(1 - \alpha w^{2n} x^n) \dots (1 - \alpha w^{(m-1)n} x^n) \quad (22)$$

Sendo w uma raiz m -ésima primitiva da unidade, vamos verificar quais são os fatores distintos do produto (22).

Para isto vamos verificar quando

$$w^{jn} = 1.$$

Usando a hipótese de que w é uma raiz m -ésima primitiva da unidade, então

$$jn \equiv 0 \pmod{m}$$

donde segue imediatamente,

$$j \equiv 0 \pmod{\frac{m}{d}},$$

sendo $d = (m, n)$.

Logo,

$$1, w^{\frac{m}{d}n}, w^{2\frac{m}{d}n}, \dots, w^{(d-1)\frac{m}{d}n}$$

são todos iguais a um e w^n vem ser uma raiz $\frac{m}{d}$ -ésima primitiva da unidade.

O grupo das raízes $\frac{m}{d}$ -ésimas da unidade gerado por

$w^n \quad \bar{e}:$

$$G = \{1, w^n, w^{2n}, \dots, w^{(\frac{m}{d} - 1)n}\}.$$

Os fatores distintos de (22) serão:

$$(1 - \alpha x^n), (1 - \alpha w^n x^n), (1 - \alpha w^{2n} x^n), \dots, (1 - \alpha w^{(\frac{m}{d} - 1)n} x^n) \quad (23)$$

Como

$$w^{(i \frac{m}{d} + j)n} = w^{jn} \quad \text{para } i = 0, 1, 2, \dots, (d-1) \text{ e } j = 0, 1, 2, \dots, (\frac{m}{d}-1),$$

pois $w^{i(\frac{m}{d})n} = 1$, para $i = 0, 1, 2, \dots, (d-1)$, então, o produto

(22) pode ser agrupado da seguinte maneira:

[illegible]

Portanto,

$$\prod_{j=0}^{m-1} [1 - \alpha(w^j_x)^n] = \prod_{k=0}^{\frac{m}{d}-1} [1 - \alpha(w^k_x)^n]^d \quad (24)$$

Vamos agora, escrever o primeiro membro de (21) na

forma do segundo membro de (24).

Para isto, calculemos as raízes de $\left[1 - \alpha x^{\frac{m}{d}n} v^{\frac{m}{d}}\right]^d$,
onde $d = (m,n)$.

As raízes do polinômio acima tem multiplicidade d .
Chamemos,

$$\alpha x^n = v$$

e determinemos as raízes da equação:

$$1 - v^{\frac{m}{d}} = 0,$$

isto é,

$$v^{\frac{m}{d}} = 1 \quad (25)$$

Como já foi visto, se w é uma raiz m -ésima primitiva da unidade, então w^n é uma raiz $\frac{m}{d}$ -ésima primitiva da unidade, sendo $d = (m,n)$.

As soluções de (25) serão:

$$1, w^n, w^{2n}, \dots, w^{(\frac{m}{d} - 1)n},$$

ou seja,

$$v = w^{-kn} \quad \text{para } k = 0, 1, 2, \dots, (\frac{m}{d} - 1).$$

Substituindo v por seu valor,

$$\alpha x^n = w^{-kn},$$

isto é,

$$\alpha w^{kn} x^n = 1 \quad \text{para} \quad k = 0, 1, 2, \dots, \left(\frac{m}{d} - 1\right)$$

consequentemente,

$$\left[1 - \alpha^{\frac{m}{d}} x^{n \frac{m}{d}}\right]^d = \prod_{j=0}^{\left(\frac{m}{d}-1\right)} \left[1 - \alpha(w^j x)^n\right]^d. \quad (26)$$

Logo de (24) e (26)

$$\prod_{j=0}^{m-1} \left[1 - \alpha(w^j x)^n\right] = \left[1 - \alpha^{\frac{m}{d}} x^{n \frac{m}{d}}\right]^d$$

Sabendo que $\lambda(p)^{\frac{m}{d}}$ é um número complexo não nulo,

$$\left[1 - \lambda(p)^{\frac{m}{d}} x^{n \frac{m}{d}}\right]^{-d} = \prod_{j=0}^{m-1} \left[1 - \lambda(p)(w^j x)^n\right]^{-1}.$$

10 - Teorema de Davenport e Hasse.

Seja $g'(x')$ a soma de Gauss do corpo F_q^m ,

$$g'(x') = \sum_{y \in F_q^m} \chi'(y) \psi'(y).$$

então,

$$-g'(x') = (-1)^m g(x)^m,$$

onde $g(x)$ é a soma de Gauss do corpo F_q .

Consideremos o resultado obtido em (17),

$$1 + g'(x')Y = \prod_{p'} [1 - \lambda'(p')Y^{n'(p')}]^{-1}. \quad (17)$$

Lembremos que os d polinômios irredutíveis p'_i de p em $F_q[x]$ têm o mesmo grau $\frac{n}{d}$ e todos eles têm para $\lambda'(p'_i)$ o mesmo valor, isto é, $\lambda'(p') = \lambda^{m/d}(p)$. Levando em consideração estes fatos e substituindo Y por X^m , teremos em (17)

$$1 + g'(x')x^m = \prod_p [1 - \lambda(p)^{\frac{m}{d}} x^{m \frac{n}{d}}]^{-d}$$

Pelo resultado obtido em (27),

$$1 + g'(x')x^m = \prod_{j=0}^{m-1} \prod_p [1 - \lambda(p)(w^j x)^n]^{-1}.$$

Agora, pela igualdade (14)

$$1 + g'(x')x^m = \prod_{j=0}^{m-1} [1 + g(x)w^j x].$$

A soma das raízes m -ésimas da unidade é zero, assim como é zero a soma dos produtos de duas a duas raízes m -ésimas da unidade, até a soma dos produtos de $(m-1)$ a $(m-1)$ raízes m -ésimas da unidade, temos então:

$$1 + g'(x')x^m = 1 + (g(x))^m w^{\frac{m(m-1)}{2}} x^m,$$

donde

$$g'(x')x^m = (-1)^{(m+1)}(g(x))^mx^m$$

e,

$$-g'(x') = (-1)^m(g(x))^m$$

BIBLIOGRAFIA

- /1/ AZEVEDO, A. e PICCINI, R - Introdução à teoria dos grupos
Rio de Janeiro - Instituto de Matemática Pura e Aplicada,
1969.
- /2/ JOLY, J.R. - Équations et variétés algébriques sur un
corps fini - L'Enseignement mathém. 19, 1973, 5-9, 36-40,
106-109.
- /3/ KAPLANSKY, I. - Introdução à teoria de Galois. Notas de
Matemática nº 13. Rio de Janeiro - Instituto de Matemática
Pura e Aplicada, 1958.
- /4/ LANG, S. - Algebra. Addison - Wesley Publishing Company,
1972.
- /5/ SCHMIDT, WOLFGANG M. - Equations over finite fields an
elementary approach, Lectures. Notes in Mathematics, 536.
Berlin. Heidelberg - Springer Verlag, 1976.
- /6/ SERRE, J.P. - Cours d'arithmétique. Presses Universitaire
de France, 1970.
- /7/ WEIL, A. - Number of solutions of equations in finite
fields. Bull. Amer. Math. Soc. 55, nº 5, May 1949, 497-508.