

GRUPOS CARACTERIZADOS POR SUAS TÁBUAS  
DE CARACTERES

*Eduardo do Nascimento Marcos*

DISSERTAÇÃO APRESENTADA AO  
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA  
DA UNIVERSIDADE DE SÃO PAULO  
PARA OBTENÇÃO DO GRAU DE MESTRE  
EM MATEMÁTICA

ORIENTADOR: PROF. DR. HÉCTOR ALFREDO MERKLEN GOLDSCHMIDT

- Durante a elaboração deste trabalho o autor recebeu apoio financeiro do CNPq e FINEP.

São Paulo, outubro de 1980.

Ao Nini e ao João Piracaia,  
que andam comigo. ã Carmem,  
com muito amor e ao Heitor,  
que vai brilhar.

## ÍNDICE

1. Introdução .. .. .	1
I) Os grupos simpléticos .. .. .	1
II) Os grupos ortogonais ${}^{\mu}O^{\pi}(n,3)$ .. .. .	12
III) Os grupos unitários $PSU(n,2)$ .. .. .	18
IV) Os grupos ortogonais $O^{\mu}(2n,2)$ .. .. .	20
V) Grupos finitos gerados por 3-transposições .. .. .	21
VI) Tabela - Sumário .. .. .	23
2. Capítulo 1 - Teorema de Nagao .. .. .	25
A) Teoremas Gerais .. .. .	25
B) Grupos Gerados por 3-transposições Conjugadas .. .. .	27
C) $\Sigma_n$ .. .. .	31
Um Contra Exemplo .. .. .	40
3. Capítulo 2 - Teorema de Pahlings .. .. .	43
4. Apêndice .. .. .	54
5. Referências .. .. .	63

## PREFÁCIO

Um problema que surge na teoria de representações de grupos finitos é saber quando os caracteres, sobre  $C$ , de um grupo o determinam.

Resolver esse problema, completamente, parece uma tarefa difícil; facilmente encontramos exemplos de grupos que não são isomorfos, mas têm a mesma tábua de caracteres, como  $Q_4$  e  $D_8$ .

O que se tem conseguido até agora, é determinar classes de grupos que satisfazem essa propriedade.

Abaixo enumeramos alguns exemplos:

- 1) Os grupos comutativos finitos. Via o teorema de estrutura se demonstra facilmente que eles satisfazem essa propriedade.
- 2) O grupo de permutações  $\Sigma_n$ . Ver Nagao [9]. É o primeiro resultado nessa linha, e por isso alguns autores chamam os grupos caracterizados por tábuas de caracteres de grupos de Nagao.
- 3) Os grupos alternados. Existem duas demonstrações deste fato, uma de G. Higman [6] e outra de Tuyosi Oyama [10]; a primeira é bastante breve e simples.
- 4)  $\zeta(n,p)$  os grupos simétricos generalizados. A demonstração é de Yokonuma Takeo [14].
- 5) P. J. Lambert demonstra que os grupos  $PSL(2,q)$ ;  $PSL(3,q)$ ;  $PSU(3,q)$ ;  $SZ(q)$  e os grupos de tipo Ree satisfazem essa propriedade [7], [8].
- 6) H. Pahlings mostrou em [13] que os grupos  $Sp(2n, 2^k)$ ;

$PSU(n, 2^k)$ ;  $O^\mu(2n, 2^k)$ ;  $E_0^\mu(n, 5)$ , os grupos excepcionais  $W(E_6)$ ;  $W(E_7)$ ;  $W(E_8)$ ; e ainda os grupos  $H_3$  e  $H_4$  são caracterizados por suas respectivas tábua.

O objetivo principal dessa dissertação é expor um trabalho de H. Pahlings [11] que diz que os grupos descritos por Fischer, em seu famoso trabalho [3], são todos caracterizados por suas tábua de caracteres.

Em [13] H. Pahlings usa uma técnica parecida com a usada aqui que consiste em estudar uma equação de classes, como nós faremos no capítulo 2.

Na introdução damos uma descrição informal de alguns grupos lineares clássicos que nos interessam. Damos, no fim da introdução, uma tabela que funciona como sumário dos fatos mais importantes para nós.

No capítulo 1, damos uma demonstração do resultado de Nagao que afirma que  $\Sigma_n$  é caracterizado por sua tábua.

No capítulo 2, expomos o trabalho de Pahlings, que em linhas gerais, pode ser descrito como segue.

Fischer dá a lista dos grupos gerados por uma classe  $D$  de 3-transposições (vide def. 1, pág. 27) que satisfazem as propriedades  $G' = G''$ ;  $Z(G) = \{1\}$ . Desse trabalho se deduz que a classe  $D$  satisfaz a seguinte equação de classes  $\hat{D}^2 = |D| 1 + 2 \hat{T} + 3 \hat{W}$ .

Pahlings mostra que se um grupo é gerado por uma classe  $D$ , que satisfaz a equação acima, ele satisfaz as hipóteses do teorema de Fischer.

Depois Pahlings divide os grupos em três classes distintas. Os solúveis, os simples e os restantes.

Os solúveis são analisados caso por caso.

Para os simples, a solução é dada pelo teorema 1, do apêndice que é uma adaptação do trabalho de Artin [2], que afirma que dois desses grupos nunca têm a mesma ordem, logo não podem ter a mesma tábua de caracteres.

Para os grupos restantes, excluindo o grupo  $\Sigma_n$ , que é estudado no capítulo 1, o teorema 2 mostra que também, dois desses grupos nunca têm a mesma ordem.

#### AGRADECIMENTOS

Gostaria de deixar clara minha gratidão a meu orientador Prof. Hector A. Merklen Goldsmidt pelo seu trabalho de orientação e por sua amizade sincera.

Agradeço a A. Márcia de Toledo pela sua ajuda na datilografia.

Agradeço ao Rogério pela revisão de alguns erros de Português.

Quero deixar escrito que meu trabalho só foi possível graças aos grandes amigos, meus companheiros nessas andanças. Citar alguns nomes aqui seria esquecer outros essenciais.

Entre os amigos, no entanto, minha especial gratidão.

- ao Prof. Galdino, responsável que é pelo meu sentir prazer em estudar Matemática.

- ao Prof. César Polcino por sua contribuição ao meu inte  
resse pela Álgebra.

## INTRODUÇÃO

I) Os grupos simpléticos e em particular  $Sp(2n, 2)$ .

1. Uma forma bilinear  $f$  sobre um espaço vetorial  $V$  de dimensão  $n$  é dita alternada se  $f(x, x) = 0$  para todo  $x$  em  $V$ .

Observações: Temos que se  $f$  é alternada,  $f(x, y) = -f(y, x)$  e ainda se característica  $K \neq 2$ ,  $f(x, x) = 0 \forall x \in V \iff f(x, y) = -f(y, x) \forall x, y \in V$ .

Mostra-se ainda que posto  $f = 2m \leq n$  e existe uma base  $(e_i)_{i=1, \dots, 2m, \dots, n}$  tal que

$$f(x, y) = \sum_{i=1}^m \xi_i \eta_{m+i} - \eta_i \xi_{m+i} \quad \text{onde}$$

$$x = \sum_{i=1}^n \xi_i e_i \quad y = \sum_{i=1}^n \eta_i e_i.$$

Se  $\dim V = n$  então  $f$  será chamada fundamental, se posto  $f = n$ ; nesse caso teremos que  $n$  é par,  $n = 2m$ .

Uma base nas condições acima, para uma forma fundamental, será chamada simplética.

É também fácil mostrar que duas formas alternadas fundamentais definidas no mesmo espaço são equivalentes. (isto é existe  $u : V \rightarrow V$  inversível tal que  $f(x, y) = f'(u(x), u(y))$ ). Por isso quando estivermos tratando de uma forma alternada fundamental denotaremos  $f(x, y)$  por  $(x, y)$ .

2. Seja  $V$  um espaço de dimensão  $n$  no qual está definida uma forma bilinear alternada fundamental.

Denotaremos por  $Sp(n, K)$  o grupo constituído de todas as transformações lineares  $\mu$  tais que  $(\mu(x), \mu(y)) = (x, y) \forall x, y \in V$ .

Uma tal transformação será chamada transformação simplética, e o grupo de grupo simplético a  $n$  variáveis sobre o corpo  $K$ .

De agora em diante  $V$  denotará sempre um espaço vetorial, de dimensão finita  $n = 2m$  sobre um corpo  $K$ , no qual foi definida uma forma bilinear alternada fundamental,

Tem-se facilmente que uma transformação linear  $T : V \rightarrow V$  é simplética se e só se ela leva uma base simplética em base simplética. (Nesse caso ela leva todas)

### 3. Subespaços Isótopos.

I) Dado um subespaço  $W$  de  $V$  denotaremos por  $W^*$  o subespaço de  $V$  constituído dos  $y$  de  $V$  tais que  $(y, x) = 0$  para todo  $x$  em  $W$ .

$$(y \in W^* \iff (x, y) = 0 \forall x \in W).$$

II) Como  $(x, y) = -(y, x)$  temos que  $(W^*)^* = W$ .

III) Diremos que  $W$  é isótopo se  $W \cap W^* \neq \phi$  e que  $W$  é totalmente isótopo se  $W \subset W^*$ .

IV) Temos facilmente que se  $W$  não é isótopo  $V = W \oplus W^*$ .

V) Se  $W$  é totalmente isótopo. Se escrevemos

$p = \dim W$  e  $n = \dim V$  então  $p \leq n - p \implies 2p \leq n$ , de modo que concluimos que  $m = \frac{n}{2}$  é a dimensão máxima possível de um subespaço totalmente isótopo maximal. Um desses subespaços é dado pelo espaço gerado pelos primeiros  $m$  vetores de uma base simplética.

#### Proposição 1: 1º Teorema de Witt.

Seja  $V$  um espaço vetorial de dimensão  $n = 2m$  no qual foi definida, como acima, uma forma alternada fundamental. Então todo subespaço totalmente isótopo de dimensão  $p < m$  es-

tã contido num subespaço totalmente isôtro de dimensão  $m$ ; e mais; se dois subespaços  $W_1$  e  $W_2$  são totalmente isôtro e têm a mesma dimensão existe então uma transformação simplética que leva  $W_1$  em  $W_2$ .

Demonstração: Seja  $W_1$  um subespaço totalmente isôtro de  $\dim p \leq m$ ; seja  $e_1 \neq 0$  um vetor de  $W_1$  e  $e_{m+1}$  um vetor de  $V$  tal que  $(e_1, e_{m+1}) = 1$ , temos que  $e_1$  não pertence ao hiperplano conjugado de  $e_{m+1}$ ,  $H = \langle e_{m+1} \rangle^*$ .

Donde temos que

$$\dim (W_1 \cap H) = p + (n-1) - n = p-1$$

$$\dim (W_1 \cap H) = \dim (W_1 \cap \langle e_1, e_{m+1} \rangle^*).$$

Pode-se recomeçar o raciocínio para o subespaço  $\langle e_1, e_{m+1} \rangle^*$  de dimensão  $n-2$  e o subespaço totalmente isôtro  $W_1 \cap H$  de dimensão  $p-1$ . Assim, por recorrência, podemos conseguir  $2p$  vetores  $(e_1, \dots, e_p, e_{m+1}, \dots, e_{m+p})$  com  $(e_1, \dots, e_p)$  formando uma base de  $W$  e  $(e_{m+j}, e_k) = \delta_{jk}$ ,  $j, k = 1, \dots, p$ .

Seja  $P_p$  o espaço gerado por  $(e_1, \dots, e_p, e_{m+1}, \dots, e_{m+p})$ . Se tomarmos uma base simplética de  $P_p^*$   $(e_{p+1}, \dots, e_m, e_{m+1}, \dots, e_{2m})$  então teremos que a base  $(e_i)_{i=1 \dots m}$  é uma base simplética de  $V$  com os primeiros  $p$  vetores sendo base de  $W_1$ . Podemos fazer o mesmo raciocínio para  $W_2$  e os dois subespaços resultam equivalentes. (Isto é: existe a transformação citada.)

Proposição 2: 2º Teorema de Witt.

Com as hipóteses da proposição 1. Sejam  $W_1$  e  $W_2$  dois subespaços de  $V$ , de mesma dimensão para que exista uma transformação simplética levando  $W_1$  em  $W_2$  é necessário e suficiente que posto  $f|_{W_1} = \text{posto } f|_{W_2}$ .

Demonstração: É claro que a condição é necessária. É fácil ver que é suficiente quando  $W_1$  não for isótopo, ou quando totalmente isótopo. (cf proposição 1.)

De modo que podemos supor  $\dim(W_1 \cap W_1^*) = \dim(W_2 \cap W_2^*) = r \leq p$ ,  $r \neq 0$ .

Sejam  $E_1$  e  $E_2$  suplementares de  $W_1 \cap W_1^*$  e  $W_2 \cap W_2^*$ , com relação a  $W_1$  e  $W_2$  respectivamente.

$E_1$  e  $E_2$  são não isótopos e têm a mesma dimensão, existe portanto uma transformação simplética  $u$  levando  $E_1$  em  $E_2$  e podemos nos restringir ao caso  $E_1 = E_2$ .

Então no subespaço não isótopo  $E_1^*$  temos  $W_1 \cap W_1^*$  e  $W_2 \cap W_2^*$  são totalmente isótopos e portanto existe uma transformação simplética levando  $W_1 \cap W_1^*$  em  $W_2 \cap W_2^*$  e essa transformação leva  $W_1$  em  $W_2$ .

4. Queremos ver agora como é a matriz de uma transformação simplética que deixa os pontos de um subespaço totalmente isótopo maximal invariante. Seja então  $W$  tal subespaço,  $u$  uma tal transformação e ainda  $(e_i)_{i=1 \dots 2m}$  uma base simplética em que os primeiros  $n$  vetores formem uma base de  $W$ .

Seja  $u(x) = x + v(x)$ .

$$(x, y) = (u(x), u(y)) = (x + v(x), y + v(y)) =$$

$$(x, y) + (x, v(y)) + (v(x), y) + (v(x), v(y)) \quad \text{portanto}$$

$$(v(x), y) + (x, v(y)) + (v(x), v(y)) = 0 \quad \text{para todo } y, x.$$

Se tomarmos  $x$  em  $W$  então  $v(x) = 0$  e temos  $(x, v(y)) = 0$  para todo  $y$ , isto significa que  $v(y) \in W^* = W$ . Temos então que  $v$  é uma aplicação linear de  $V$  em  $W$  nula em  $W$ ,  $v: V \rightarrow W$ .

Então  $(v(x), v(y)) = 0$  e portanto  $(v(x), y) = -(x, v(y))$  e pode-se ver que  $M(u, (e_i)_{i=1, \dots, 2n}) = \begin{bmatrix} I & S \\ 0 & I \end{bmatrix}$  onde  $S$  é simétrica.

Uma transformação simplética que deixa invariante todos os pontos de um subespaço totalmente isótropo maximal será denominada singular.

Proposição 3: Seja  $u$  uma transformação simplética involutiva ( $u^2 = I$ ).

1) Se característica de  $K \neq 2$  então existe um subespaço  $W$  não isótropo (ou reduzido a  $\{0\}$ ) tal que

$$u|_W = \text{Id} \quad \text{e} \quad u|_{W^*} = -\text{Id}.$$

2) Se característica  $K = 2$  então  $u$  é singular.

Demonstração: Sejam  $v(x) = x - u(x)$  e  $w(x) = x + u(x)$   
 $v(w(x)) = w(v(x)) = 0$  isto significa que  $v(V) \subset \text{Ker } w$  e  $w(V) \subset \text{Ker } v$ .

Sejam ainda  $p, q$  posto de  $v$  e  $w$  respectivamente  $p \leq n - q$  pois  $p + q \leq n$ .

Se  $p < m$  então  $\text{Ker } v$  não é totalmente isótropo e teremos que  $\text{Ker } v$  contém um plano não isótropo  $P$ . Como  $u$  deixa invariante o subespaço  $P^*$ , e sua restrição a  $P^*$  é uma transformação simplética involutiva de dimensão  $n - 2$  e a demonstração se reduz ao subespaço de dimensão  $n - 2$ ,  $P^*$ .

Se  $q < m$  a demonstração é análoga. Resta o caso  $p = q = m$ , onde  $\text{Ker } v$  é totalmente isótropo e  $u$  é singular e involutiva. Temos então que para alguma base  $e_i$

$$M(u, (e_i)_{i=1, \dots, 2n}) = \begin{bmatrix} I & S \\ 0 & I \end{bmatrix} \text{ e portanto}$$

$$M(u^2, (e_i)_{i=1, \dots, 2m}) = \begin{bmatrix} I & 2S \\ 0 & I \end{bmatrix} = Id \text{ e temos que } 2S = 0.$$

Se característica  $K \neq 2$  temos  $2S = 0 \implies S = 0$  e portanto  $u = Id$ . (O caso  $\dim V = 2$  é deixado ao leitor.)

5: Chamaremos de transvecção simplética a uma transformação simplética involutiva da forma  $u(x) = x + \sigma(x)a$  onde  $\sigma$  é uma forma linear não nula, tal que  $\sigma \equiv 0$  em  $\langle a \rangle^*$ .  $\langle a \rangle^*$  será chamado o hiperplano da transvecção  $u$ .

Observação: Dessa definição temos que uma transvecção simplética é qualquer transformação da forma  $u(x) = x + \lambda(x, a)a$   $\lambda \neq 0$  e se tomarmos  $b = \mu a$  temos que

$$u(x) = x + \lambda(x, a)a = x + \frac{\lambda}{\mu} (x, b)b.$$

Temos a seguinte proposição

Proposição 4: Sejam  $u(x) = x + \lambda_1(x, a)a$  e  $v(x) = x + \lambda_2(x, b)b$  duas transformações simpléticas de  $V$ . Para que elas sejam conjugadas é necessário e suficiente que  $\frac{\lambda_1}{\lambda_2}$  seja um quadrado em  $K$ .

Demonstração: Se  $w$  é uma transformação simplética qualquer  $w(u(w^{-1}(x))) = x + \lambda_1(w^{-1}(x), a)w(a) = x + \lambda_1(x, w(a))w(a)$ .

Temos então que se  $v(x)$  é conjugada a  $u$  por  $w$ ,  $x + \lambda_1(x, w(a))w(a) = x + \lambda_2(x, b)b$  e então  $b = k w(a)$ . Pela

observação anterior  $\lambda_1 = \frac{\lambda_2}{k^2}$ .

Agora se  $\frac{\lambda_1}{\lambda_2}$  é um quadrado, digamos  $k^2$ , temos que existe  $w$  que leva  $a$  em  $\frac{b}{k}$ . Verifica-se facilmente que

$$w(u(w^{-1}(x))) = x + \lambda_2(x, b)b$$

Observações: Se  $K \text{ GF}[2]$  o quociente citado é sempre um quadrado e temos que o conjunto  $D$  das transvecções simpléticas de  $Sp(2n, K)$  é uma classe de conjugação de elementos de ordem 2. O produto de duas destas transvecções tem neste caso ordem 2 ou 3.

Proposição 5: Toda transformação simplética em  $V$  é um produto de transvecções simpléticas.

Demonstração: Faremos a demonstração por recorrência em  $m = \frac{\dim V}{2}$ , e necessitamos antes de um lema.

Lema: Seja  $u$  uma transformação simplética de  $V$ . Então existem  $h$ , um produto de transvecções simpléticas, e  $x \neq 0$  em  $V$  tal que  $u_1 = hu$  deixa  $x$  invariante.

Demonstração:

Caso 1. Existe  $x$  tal que  $(u(x), x) \neq 0$ . Então seja  $a = u(x) - x$  e  $H = \langle a \rangle^*$ .  $H$  não contém  $x$  nem  $u(x)$  pois  $(a, x) = (a, u(x)) \neq 0$  e existe uma forma linear  $\sigma$  nula em  $H$  e igual a  $-1$  em  $u(x)$ .

Seja  $v$  a transvecção :  $v(y) = y + \sigma(y)a$  e  $u_1 = vu$  temos  $u_1(x) = v(u(x)) = u(x) + \sigma(u(x))a = u(x) - a = x$ .

Tomemos  $h = v$  e temos o que queremos.

Caso 2.  $(x, u(x)) = 0$  para todo  $x$  em  $V$ . Então seja  $x \neq 0$ . Ou  $u(x)$  é colinear a  $x$  ou  $\langle x, u(x) \rangle$  é um plano totalmente isotropo; em qualquer das hipóteses (se  $m > 1$ ) temos que existe  $y \neq 0$  tal que  $(x, y) \neq 0$  e  $(u(x), y) \neq 0$ .

"No caso  $u(x)$  colinear a  $x$  a afirmação é evidente e caso contrário basta tomar uma base simplética  $e_i$  com  $x = e_1$   $u(x) = e_2$  e  $y = e_{m+1} + e_{m+2}$ ."

Seja então  $a = y - u(x)$ . Resulta que  $u(x)$  e  $y$  não pertencem ao hiperplano  $H = \langle a \rangle^*$  e existe então uma transvecção simplética  $w$  tal que  $w(u(x)) = y$  e portanto pelo 1º caso existe  $v$  tal que  $u_1 = vw$  deixa  $x$  invariante. Tome  $h = uw$ , temos que  $u_1 = hu$  satisfaz a tese.

Passamos agora a demonstração da proposição. Sejam  $u_1, x$  como no lema .

Dividiremos a demonstração em 2 casos:

Caso 1.

Suponhamos que existe  $y$  tal que  $(x, y) \neq 0$  e  $(y, u_1(y)) \neq 0$ .

Temos  $(x, u_1(y)) = (x, y)$  donde  $(x, u_1(y) - y) = 0$  e temos que  $x$  pertence a  $\langle u_1(y) - y \rangle^* = \langle b \rangle^*$ .

Seja  $v'$  uma transvecção que deixa os pontos de  $\langle b \rangle^*$  invariantes e leva  $u_1(y)$  em  $y$ .

Temos que  $u_2 = v'u_1$  deixa invariante todos os pontos do plano não isótropo  $P_1 = \langle x, y \rangle$  e portanto deixa o subespaço  $P_1^*$  invariante.

Caso 2.

Suponhamos que  $(y, u_1(y)) = 0$  toda vez que  $(x, y) \neq 0$ . Seja  $y$  tal que  $(y, x + y) \neq 0$ . (A existência de tal  $y$  é fácil de se inferir.)

$$(u_1(y), x + y) = (u_1(y), x) = (y, x) \neq 0 \text{ e } (x, x + y) = (x, y) \neq 0.$$

Façamos  $b = x + y - u_1(y)$ ; temos que  $u_1(y)$  e  $x + y$  não pertencem ao hiperplano  $\langle b \rangle^*$  ao qual  $x$  pertence. Novamente existe  $v'$  levando  $x + y$  em  $u_1(y)$  e deixando fixos os pontos de  $\langle b \rangle^*$ .

Nos dois casos concluímos que, dada uma transformação simplética  $u$ , existe  $h$ , um produto de transvecções sim

pléticas, tal que  $v = h$  deixa invariante os elementos de um plano não isotrópico  $P = \langle x, y \rangle$ , "portanto deixa  $P^*$  invariante" e temos  $V = P \oplus P^*$ ,  $\dim P^* = n - 2$ . Por indução  $v|_{P^*} = \pi h_i$  onde  $h_i$  são transvecções simpléticas de  $P^*$  que podem ser estendidas a  $V$  agindo como a identidade em  $P$ .

Se  $h_i'$  é a extensão de  $h_i$  temos  $u = h^{-1} \pi h_i'$  e como  $h$  era um produto de transvecções o mesmo acontece com  $h^{-1}$ . Isso completa a demonstração.

Para o caso  $m = l = \frac{n}{2}$ . Temos que se existe  $x$  tal que  $(x, u(x)) \neq 0$  então como acima  $u_1 = v u_1$  deixa  $x$  invariante e é portanto uma transvecção.

Se por outro lado  $(x, u(x)) = 0$  para toda  $x$  então  $u$  já é uma transvecção ■

Se  $K$  é um corpo finito com  $k$  elementos algumas vezes denotaremos  $K$  por  $k$ .

Teorema 1: Com exceção de  $Sp(2, 2) \cong \Sigma_3$  e  $Sp(4, 2)$ ,  $Sp(2, 3)$ , o grupo  $Sp(n, k)$  não contém nenhum subgrupo próprio normal não contido no seu centro. (que em geral é igual a  $\{I, -I\}$  e que no caso  $K = GF[2^n]$  é igual a  $\{I\}$ ).

Demonstração: Faremos só a demonstração no caso  $K = GF[2]$ . No caso geral, supondo que  $H_1 \triangleleft Sp(2n, k)$  contém algum elemento que não está no centro, mostra-se que  $H_1$  contém as transformações  $u_\lambda(x) = x + \lambda(x, a)$  a ( $a \neq 0$ , fixo, e  $\lambda$  arbitrário) e daí usando-se a proposição 5 resulta que  $H_1 = Sp(2n, k)$ .

Vejamos com mais detalhe o caso  $K = GF[2]$ .

Seja  $H_1 \triangleleft Sp(2n, 2)$ ,  $n \geq 3$  e  $\{I\} \subsetneq H_1$ . Existe  $u$  em  $H_1$  tal que  $u \neq I$  e temos que existe  $x$  tal que  $u(x) \neq x$ .

Caso 1.  $(x, u(x)) \neq 0$  para todo  $x$ . Dado  $x$  arbitrariamente, existe  $y \notin \langle x, u(x) \rangle$  tal que  $(x, y) = 0$ ,  $(u(x), y) = (x, u(x)) \neq 0$ . Existe uma transformação simplética  $v$  tal que  $v(x) = u(x)$ ;  $v(u(x)) = y$ . A transformação simplética  $u_1 = v u v^{-1}$  pertence a  $H_1$  e  $u_1(x) = y$ .

Podemos nos restringir ao caso 2.

Caso 2. Existe  $x$  tal que  $(x, u(x)) = 0$ .

Seja  $H = \langle x \rangle^*$  e  $w$  uma transvecção de hiperplano  $H$ .  $u_1 = w^{-1} u w u^{-1}$  está em  $H_1$  e deixa fixos os pontos de  $H \cap u(H)$  pois se  $z \in H \cap u(H)$ ;  $z = u(h)$  e

$$u_1(z) = w^{-1} u w u^{-1}(u(h)) = w^{-1} u w(h) = w^{-1} u(h) = u(h) = z.$$

Seja  $P = \langle x, u(x) \rangle$ ;  $P \subset P^* = H \cap u(H)$  e  $u_1$  é uma transformação que pertence ao subgrupo normal  $H_1$ .

Seja  $W \subset H \cap u(H)$  e  $\dim W = n - 6$  com  $W$  não isótropo. Temos que  $u$  deixa invariante o subespaço não isótropo  $W^*$  de dimensão 6, e além disso podemos considerar toda função linear de  $W^*$  em  $W^*$  como restrição de uma função de  $v$ . Se mostrarmos que o teorema vale para  $n = 6$ , teremos que o grupo  $H$  contém alguma transvecção  $T : v \rightarrow v$  que satisfaz  $T(W^*) = W^*$ ,  $T(W) = W$  e  $T|_W = \text{id}$ . Como  $H_1$  contém uma transvecção e é normal e todas as transvecções são conjugadas  $H_1 = \text{Sp}(n, k)$ . Agora só nos resta demonstrar o seguinte fato se  $H_1 \triangleleft \text{Sp}(6, 2)$  e  $H_1 \neq \{1\}$  então  $H_1 = \text{Sp}(6, 2)$ .

Podemos supor que  $H_1$  contém uma transformação singular  $u : x \rightarrow x + v(x)$  (cf pág. 4) para a qual  $v(x)$  tem posto 1 ou 2.

Temos que  $M(u, e_i) = \begin{bmatrix} I & S \\ 0 & I \end{bmatrix}$   $S$  é simétrica e tem posto 1 ou 2.

Se  $S$  tem posto 2 então ela é equivalente a uma das matrizes.

$$S_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{ou} \quad S_2 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

No primeiro caso sejam  $w_1$  e  $w_2$  as transformações simpléticas que deixam os vetores  $(e_i)$   $i \neq 2$  e  $i \neq 4$  invariantes e

$$w_1(e_2) = e_2 + e_4 \quad w_1(e_4) = e_2$$

$$w_2(e_2) = e_4 \quad w_2(e_4) = e_2 .$$

Sejam  $u_1 = w_1 u w_1^{-1}$  e  $u_2 = w_2 u w_2^{-1}$  então  $u_2 u_1$  pertence a  $H_1$  e tem matriz simétrica associada semelhante à segunda. Logo  $H_1$  contém um elemento singular cuja matriz simétrica é igual à  $S_1 + S_2$  que tem posto 1 e  $H_1$  contém uma transvecção. Portanto  $H_1 = Sp(6,2)$ .

Agora se  $S$  é semelhante à  $S_2$  então  $S$  é semelhante à matriz

$$S' = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{donde } H_1 \text{ contém a transformação sim-}$$

plética singular correspondente a  $S + S' = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ , mas

essa matriz é semelhante a  $S_1$  e voltamos ao caso anterior.

No caso em que  $S$  tem posto 1 temos que  $u$  é uma transvecção.

No livro de Dickson [16], pág. 118, há uma demonstração de que  $Sp(4,2) \cong \Sigma_6$  por uma abordagem completamente di-

ferente. Lã os grupos  $Sp(2m, p^n)$  sã denotados por  $SA(2m, p^n)$ .

## II) Grupos Ortogonais $U_0^\pi(n, 3)$

Havendo descrito com algum detalhe os grupos simplé-  
ticos e, em especial, o grupo  $Sp(2n, 2)$ , faremos agora uma  
descrição sumãria dos outros grupos que nos interessam.

No que segue,  $E$  denotarã um espaço vetorial de  
dimensã  $m$  sobre um corpo  $K$ , cuja característca é diferen-  
te de 2, no qual estã definida uma forma bilinear simétrica  
 $f$  nã degenerada. As definições sã anãlogas as do caso an-  
terior.

Uma transformaço que deixa  $f$  invariante é chamada  
ortogonal e o grupo de todas as transformaço ortogo-  
nais serã chamado de grupo ortogonal e denotado por  $O(n, K, f)$ .  
Se  $W$  é um subespaço chamaremos de ortogonal a  $W$  ao subespaço denota-  
do por  $W^\perp$  constituído de todos os elementos  $y$  de  $E$  tais que  
 $f(x, y) = 0$  para todo  $x$  em  $W$ .

Aqui acontece algo bem diferente do caso simpléti-  
co; lã a forma alternada é essencialmente única, mas aqui  
nã acontece o mesmo. Porém, como veremos no Teorema 1, pode-  
mos no caso em que  $K = GF[p^n]$ ,  $p \neq 2$  chegar a algo parecido.

Dada a forma  $f$  podemos associar a ela uma forma  
quadrática definindo  $g(x) = f(x, x)$  e temos uma fórmula de pola-  
rizaço  $f(x, y) = \frac{1}{2}(g(x + y) - g(x) - g(y))$  que nos permite

recuperar  $f$ . A matriz de  $f$  numa base fixada  $(e_i)_{i=1, \dots, m}$  é a matriz  $(f(e_i, e_j))_{\substack{i=1, \dots, m \\ j=1, \dots, m}}$ .

Proposição 1: Seja  $f$  uma forma bilinear simétrica não degenerada,

$g \equiv \sum_{i,j=1, \dots, m} \alpha_{ij} \xi_i \xi_j$  a forma quadrática associada, então existe uma base com relação à qual

$$g \equiv \sum_{i=1}^m \alpha_i \xi_i^2 \text{ com } \alpha_i \neq 0.$$

Demonstração: Se  $m=1$  o fato é evidente.

Se  $m > 1$  seja  $v$  tal que  $g(v) \neq 0$ . Se  $W = \langle v \rangle$ , temos  $E = W \oplus W^\perp$ . Agora  $f|_{W^\perp}$  é bilinear simétrica não degenerada e  $\dim W^\perp = n - 1$ . Por indução,  $f|_{W^\perp}$  é diagonalizável.

Proposição 2: Seja  $f$  uma forma bilinear simétrica não degenerada sobre  $GF[p^n]$  ( $p > 2$ ). então existe uma base  $(\beta_i)_{i=1, \dots, m}$  tal que em relação a essa base a forma  $g$  se escreve assim:

$$g \equiv \sum_{i=1}^s \xi_i^2 + v \sum_{i=s+1}^m \xi_i^2 \text{ onde } v \text{ é um não quadrado qualquer.}$$

"Isto significa que  $M(f, \beta_i) = \begin{bmatrix} I & 0 \\ 0 & vI \end{bmatrix}$ ."

Demonstração: Seja  $K^{\#2}$  o subgrupo multiplicativo de  $K^{\#} = K - \{0\}$ , formado pelos quadrados de seus elementos.

$\frac{K^{\#}}{K^{\#2}}$  tem ordem 2, logo as classes laterais são  $\{K^{\#2}, vK^{\#2}\}$

onde  $v$  é um não quadrado qualquer.

Agora suponhamos que temos  $g$  na forma diagonal.  $Is$

é:  $(\beta_i)_{i=1, \dots, m}$   $g \equiv \sum_{i=1}^m \alpha_i \xi_i^2$  onde apenas os  $s$  primeiros

$\alpha_i$ 's são quadrados então:  $g \equiv \sum_{i=1}^s a_i^2 \xi_i^2 + v \sum_{i=s+1}^m a_i^2 \xi_i^2$ . To

mando-se  $\beta_i = \frac{\beta_i'}{a_i}$  temos  $g$  na forma procurada.

Esse resultado pode ser melhorado aproveitando-se o seguinte fato.

Seja  $v$  um quadrado então existem  $a$  e  $b$  tais que  $a^2 + b^2 = \frac{1}{v}$  (ver Dickson [16], pág. 64).

Seja  $g \equiv v \xi_1^2 + v \xi_2^2$  onde  $v$  é um não quadrado.

Seja  $(\gamma_1, \gamma_2)$  a seguinte base:  $\gamma_1 = a\beta_1 - b\beta_2$ ;  $\gamma_2 = b\beta_1 + a\beta_2$ .

Temos que  $f(\gamma_i, \gamma_j) = \delta_{ij}$  e então  $g \equiv \sum \xi_i^2$  na base  $(\gamma_1, \gamma_2)$ .

Teorema 1: Seja  $f$  uma forma bilinear simétrica não degenerada, num espaço de dimensão  $m$ , sobre  $GF[p^n]$ , e  $g$  a forma quadrática associada a  $f$ , então:

1) Se  $m$  é ímpar,  $g$  é equivalente a uma das seguintes formas:

$$g \equiv \sum_{i=1}^m \xi_i^2 \quad \text{ou} \quad g \equiv v \sum_{i=1}^m \xi_i^2 \quad \text{onde } v \text{ é um não quadrado, e}$$

seus grupos ortogonais associados são isomorfos (de modo que podemos considerar só uma delas).

2) Se  $m$  é par,

$$g \equiv g_v \equiv \sum_{i=1}^{m-1} \xi_i^2 + v \xi_m^2 \quad \text{onde } v = 1 \text{ ou } v \text{ é um não quadrado.}$$

Demonstração: Pelo que fizemos, temos que podemos passar

da forma  $g_s \equiv \sum_{i=1}^s \xi_i^2 + v \sum_{i=s+1}^m \xi_i^2$  para a forma  $g_{s+2}$  mudan-

do a escolha de bases, de modo que podemos assumir que

$$M(f, \beta_i) = \begin{bmatrix} I_{m-1} & 0 \\ 0 & v \end{bmatrix}, \quad \text{se } m \text{ é par e } M(f, \beta_i) = [I] \quad \text{ou}$$

$M(f, \beta_i) = [vI]$ , se  $m$  é ímpar. Agora toda transformação deixando invariante uma forma do tipo  $[I]$ , deixa a forma do tipo  $[vI]$  invariante e vice-versa.

Temos então que existem dois tipos de grupos ortogonais que denotaremos por  ${}^{\mu}O(m, p^n)$ , onde  $\mu \in \{+, -\}$  e

$$\mu = + \text{ se } g \equiv \sum_{i=1}^m \xi_i^2 \quad \text{ou } g \equiv v \sum_{i=1}^m \xi_i^2$$

$$\mu = - \text{ se } g \equiv \sum_{i=1}^{m-1} \xi_i^2 + v \xi_m^2. \quad \text{onde } v \text{ é um não quadrado.}$$

Sabemos que  ${}^+O(m, p^n) \cong {}^-O(m, p^n)$ , se  $m$  é ímpar, e por isso denotaremos esse grupo simplesmente por  $O(2n+1, p^n)$ .

Os resultados seguintes se demonstram usando técnicas parecidas às do caso simplético. Para os detalhes ver [16], [17] e [18].

1) Se  $u$  é uma transformação ortogonal involutiva e existe um subespaço não isótropo  $V$ , tal que  $u|_V = \text{id}$  e  $u|_{V^\perp} = -\text{Id}$ .

No caso em que  $V$  é um hiperplano diremos que  $u$  é a simetria com respeito ao hiperplano  $V$ .

2) Toda transformação ortogonal a  $n$  variáveis sobre um corpo de característica  $\neq 2$  é um produto de no máximo  $n$  simetrias.

Denotamos por  ${}^{\mu}RO(n, p^m)$  o subgrupo normal de  ${}^{\mu}O(n, p^m)$  formado pelas transformações ortogonais de Determinante 1.

3)  $\Omega_n^{\mu}(p^m) = [{}^{\mu}O(n, p^m); {}^{\mu}RO(n, p^m)]$  é gerado pelos produtos de duas simetrias conjugadas e também pelos quadrados dos elementos de  ${}^{\mu}RO(n, p^m)$ .

4) Se  $n > 2$  o grupo  ${}^{\mu}RO(n, p^m) / \Omega_n^{\mu}(p^m)$  é isomorfo a um subgrupo do quociente  $\frac{k^{\#}}{k^{\#2}}$ .

5) O grupo  $P \Omega_n^\mu(p^m) = \frac{\Omega_n^\mu(p^m)}{Z(\Omega_n^\mu(p^m))}$  é simples para  $n \geq 5$ .

6) Se  $G \triangleleft \mu_0(n, p^m)$  então  $G \subset Z[\mu_0(n, p^m)]$  ou  $H \supset \Omega_n^\mu(p^m)$  para todo  $H \triangleleft G$ , tal que  $H \not\subset Z[\mu_0(n, p^m)]$ .

A seguir examinaremos um pouco melhor o caso especial  $K = GF[3]$ . Temos então os grupos  $\mu_0(2n, 3), \mu \in \{+, -\}$  e  $O(2n+1, 3)$ . Sabemos que os grupos ortogonais são gerados pelas simetrias que no caso considerado são todas do seguinte tipo:

$$\tau_a : x \longrightarrow x + \pi(x, a)a, \text{ onde } \pi = (a, a) \text{ e } (a, a) = \pm 1.$$

Seja  $D^\pi = \{\tau_a \mid (a, a) = \pi\}$ . Temos  $D^+$  e  $D^-$ , onde o sinal  $+$  é usado no caso  $(a, a) = 1$  e o sinal  $-$  no caso  $(a, a) = -1$ .  $D^+$  e  $D^-$  são duas classes de conjugação formadas por involuções que juntas geram  $\mu_0(m, p^n)$ . Denotaremos por  $\mu_0^\pi(m, p^n)$  o grupo  $\frac{\langle D^\pi \rangle}{Z\langle D^\pi \rangle}$ . É fácil verificar que  $Z\langle D^\pi \rangle \subset Z(\mu_0(m, p^n)) = \{I, -I\}$ .

O grupo  $\frac{\mu_0(n, 3)}{Z[\mu_0(n, 3)]}$ , se denota por  $P\Omega^\mu(n, 3)$  e pode-se demonstrar que é igual a  $\mu_0^+(n, 3) \cdot \mu_0^-(n, 3)$  e esses dois subgrupos são normais. Usando 6 pode-se ver que

$$P\Omega^\mu(n, 3) \subset \mu_0^\pi(n, 3).$$

Proposição 3:  $O^+(2n+1, 3) \cong P \Omega(2n+1, 3)$ .

Demonstração: Temos que  $O^+(2n+1, 3) \triangleleft P O(2n+1, 3)$  e

$P \Omega (2n+1, 3) \triangleleft O^+(2n+1, 3)$ . Observamos que se  $\{\tau_v, -\tau_v\} = \bar{\tau}_v$  é uma classe pertencente a  $O^+(2n+1, 3)$ , então existe uma base  $\beta$  tal que  $M[\tau_v, \beta] = \begin{bmatrix} -1 & & \\ & [I]_{2n} & \\ & & \end{bmatrix}$ . Vemos que  $-\tau_v$  é um comutador de  $O(2n+1, 3)$  pois é um produto de um número par de elementos de uma mesma classe de conjugação. Logo  $\tau_v$  está em  $P \Omega (2n+1, 3)$ .

Resulta, do já visto, que

$$P \Omega (2n+1, 3) \cong O^+(2n+1, 3) \triangleleft O^-(2n+1, 3) \cong PO(2n+1, 3).$$

Proposição 4:  $\frac{PO(2n+1, 3)}{P \Omega (2n+1, 3)} \cong Z_2$ .

Para demonstrarmos a proposição basta exibirmos um elemento de  $PO(2n+1, 3)$  que não pertença a  $P \Omega (2n+1, 3)$  ou equivalentemente exibir um elemento  $\tau_v$  de  $O(2n+1, 3)$  tal que  $\{\tau_v, -\tau_v\} \cap \Omega(2n+1, 3) = \emptyset$ .

Tomemos  $(e_i)_{i=1, \dots, n}$  a base na qual  $M[f, e_i] = I$ .

Seja  $v = e_1 + e_2$

$$\tau_v(x) = x - (x, v)v \quad \text{temos}$$

$$\tau_v(e_i) = e_i \quad \text{se } i > 2$$

$$\tau_v(e_2) = -e_1$$

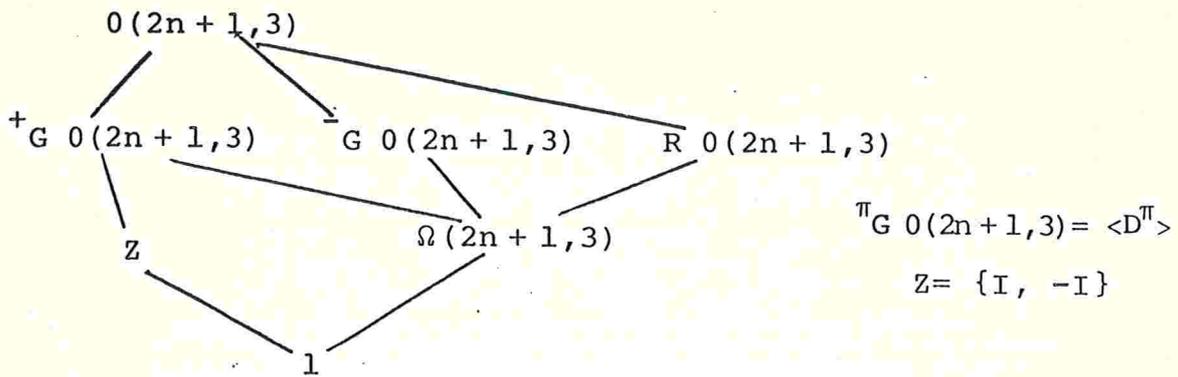
$$\tau_v(e_1) = -e_2$$

$$M_{\tau_v} = \begin{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} & \\ & I_{2n-1} \end{bmatrix}$$

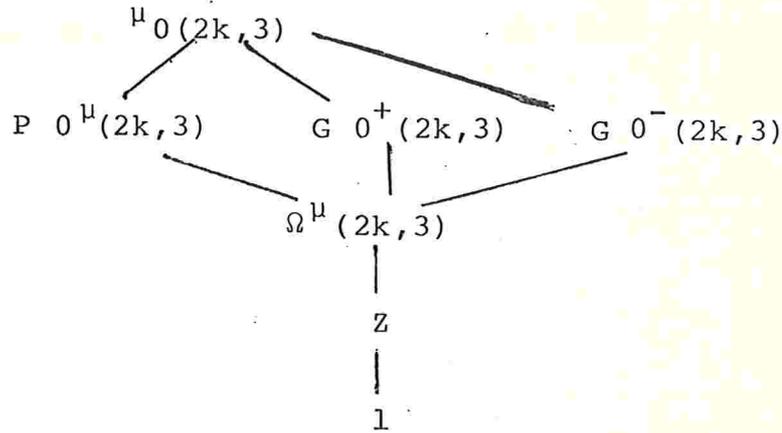
e então  $\tau_v \notin \Omega$  e  $-\tau_v \in \Omega$ .

Assim temos então mostrado que deveremos ter  $PO(2n+1, 3) \cong O^-(2n+1, 3)$  e que esse grupo contém  $O^+(2n+1, 3)$  como subgrupo de índice 2.

Temos para  $n \geq 2$  o seguinte reticulado de grupos.



Com técnicas análogas as do caso anterior pode-se demonstrar que para  $m = 2k, k \geq 3$ . Temos o seguinte reticulado de grupos.



Neste caso temos  $\mu_0^+(2k, 3) \cong \mu_0^-(2k, 3)$ , de modo que denotaremos esses grupos simplesmente por  $O^\mu(2k, 3)$  ( $k \geq 3$ ). Eles contêm como subgrupo simples o grupo dos comutadores  $P \Omega^\mu(2k, 3)$ .

### III) Grupos Unitários PSU(n, 2).

Novamente daremos apenas os enunciados dos resultados. Remetemos o leitor à bibliografia [16] capítulo 4 e 5, 2ª parte e [17], [18].

Seja  $K$  uma extensão separável de grau 2 de um corpo  $K_0$  e

$\xi \rightarrow \bar{\xi}$  o automorfismo não trivial de  $K|K_0$ . Seja  $E$  um espaço vetorial de dimensão  $n$  sobre  $K$ . Diz-se que  $f: E \times E \rightarrow K$  é bilinear hermitiana se satisfaz.

$$1) f(x + \lambda y, z) = f(x, z) + \bar{\lambda} f(y, z) \text{ e } 2) \overline{f(x, y)} = f(y, x).$$

Chamaremos de grupo unitário em  $n$  variáveis sobre  $K_0$  em relação a  $f$  (Notação  $U(n, K_0, f)$ ) ao conjunto de todas as transformações lineares de  $E$  em  $E$  que deixam  $f$  invariante.

Para cada  $x \in E$  temos  $\psi(x): E \rightarrow K$ , definida por  $\psi(x)(y) = f(x, y)$ ; o posto da aplicação semi-linear  $\psi: E \rightarrow E'$  é por definição o posto de  $f$ .

$f$  será dita fundamental se posto  $f = n$ . As noções de equivalência, ortogonalidade, etc., se transportam para esse caso.

Agora analisemos o caso em que  $K_0 = GF[2^n]$ , então toda forma hermitiana  $f$  admite uma base ortogonal e pode-se provar que duas formas fundamentais são sempre equivalentes e portanto os grupos associados são sempre isomorfos. Denotaremos esses grupos simplesmente por  $U(m, 2^n)$ .

O grupo  $U(n, K_0, f)$  contém um subgrupo normal que é o grupo das transformações unitárias de determinante 1 que denotaremos por  $U^+(n, K_0, f)$ . Este grupo é gerado pelas transvecções de det 1 relativas a vetores isotropos. (Exceto para  $k_0 = F_2$   $n \leq 3$ ).

O centro de  $U(n, K_0, f)$  consiste das transformações  $T(x) = \lambda x$  tais que  $\lambda \bar{\lambda} = 1$ . Ele é denotado por  $Z$ .

O grupo

$$\text{PSU}(n, K_0, f) = \frac{U^+(n, K_0, f)}{Z \cap U^+(n, K_0, f)} \text{ é simples, exceto para}$$

os casos  $K_0 = \text{GF}[3]$ ,  $n = 2$ , e  $K_0 = \text{GF}[2]$ ,  $n = 2$  ou  $n = 3$ . No caso  $K_0 = \text{GF}[2]$  existem geradores deste grupo que formam uma classe de conjugação tal que o produto de dois elementos têm sempre ordem 2 ou 3.

No livro de Dickson [16], os grupos  $\text{PSU}(m, p^n)$  são denotados por  $\text{HO}(m, p^{2n})$ .

#### IV) Os grupos ortogonais $O^\mu(2n, 2)$ .

Uma forma quadrática definida em um espaço  $E$  sobre  $\text{GF}[2^m]$  é qualquer função  $Q : E \longrightarrow \text{GF}[2^m]$  que satisfaz a seguinte propriedade:

$$Q(\lambda x + \eta y) = \lambda^2 Q(x) + \eta^2 Q(y) + \lambda \eta f(x, y), \text{ onde } f \text{ é uma forma bilinear alternada não degenerada.}$$

No caso em que  $m = 1$ , os escalares estão em  $\text{GF}[2]$  e  $\lambda^2$  é sempre igual a  $\lambda$ , de modo que a equação acima se escreve da seguinte forma:

$$Q(\lambda x + \eta y) = \lambda Q(x) + \eta Q(y) + \lambda \eta f(x, y).$$

Dizemos que duas formas quadráticas  $Q_1 : E \longrightarrow \text{GF}[2^m]$  e  $Q_2 : E \longrightarrow \text{GF}[2^m]$  são equivalentes se existe um isomorfismo  $u : E \longrightarrow E$  tal que  $Q_1(x) = Q_2(u(x))$ .

Dickson [16] mostra no capítulo VIII que toda forma quadrática  $Q : E \longrightarrow \text{GF}[2^m]$ , onde  $E$  tem dimensão par, é equivalente a uma forma do tipo

$$Q_\eta = \xi_1 \xi_{n+1} + \dots + \xi_{n-1} \xi_{2n-1} + (\mu \xi_n^2 + \xi_n \xi_{2n} + \mu \xi_{2n}^2), \text{ onde}$$

ou  $\mu x^2 + x + \mu$  é irredutível ou  $\mu = 0$ .

Denotaremos aqui por  $O^\mu(2n, 2^m)$  o grupo das transformações lineares que deixam  $Q_\mu$  invariante.

Esses grupos são gerados por involuções, que são as transvecções, cujo produto tem sempre ordem menor ou igual a 3.  $O^\mu(2n, 2^m)$  contém um subgrupo normal simples que é o grupo dos comutadores que denotaremos por  $PO^\mu(2n, 2)$ .

Gostaríamos ainda de avisar o leitor que no livro de Dickson esses grupos são denotados por  $G_\lambda$ .

#### V) Grupos finitos gerados por 3-transvecções.

Num trabalho famoso que suporemos conhecido [3], Bernd Fischer determina quais são os grupos finitos, com centro trivial, gerados por uma classe D de involuções conjugadas onde o produto de duas delas têm sempre ordem 2 ou 3 e  $G' = G''$ .

Fischer segue aproximadamente a seguinte seqüência de passos.

Seja E um conjunto maximal de involuções que comutam entre elas e seja n a cardinalidade de E. Fischer

prova que:

- 1)  $N_G(E)$  age de modo duplamente transitivo em E.
- 2)  $N_G(E)$  contém um 2-Sylow de G.
- 3)  $N_G(E) / C_G(E)$  é isomorfo a um dos seguintes grupos:

$\Sigma_n, A_n, GL(n, 2), L_m(4)$  onde  $m = \left\lfloor \frac{n}{2} \right\rfloor, \Sigma_{2^n} \cdot GL(n, 2)$  ou  $M_{22}, M_{23}, M_{24}$ .

Os primeiros casos vão dar origem a grupos conhecidos, mas os 3 últimos casos não eram esperados e eles vão dar origem a exatamente 3 grupos que denotaremos por  $F_{i22}$ ,  $F_{i23}$ ,  $F_{i24}$ .

Sabemos que os três grupos  $F_{i22}$ ,  $F_{i23}$ ,  $F_{i24}$  tem um subgrupo próprio simples normal, que é o grupo dos comutadores e que é igual ao próprio grupo nos dois primeiros casos e tem índice 2 no terceiro caso.

Para se obter mais informações a respeito desses grupos, veja-se [14].

GRUPOS CLÁSSICOS

G	$ G /z(G)$	Casos considerados	Cerados por 3-transp conj	Grupos Simples	Observações
$S_p(2n, q)$	$\frac{1}{q} q^{n^2} \prod_{i=1}^n (q^{2i} - 1)$ $\delta = (2, q-1)$	$Sp(n, 2)$	$Sp(2n, 2)$ $n \geq 2$	$Sp(2n, q)$ $q \geq 3$	$Sp(2, 2) \cong PSU(2, 2) \cong \Sigma_3$ $\cong O^-(2, 2)$
$O^m(2n, q)$	$ PG^m(2n, q) $ $\frac{1}{q} q^{n(n-1)} (q^n - \epsilon) \prod_{i=1}^{n-1} (q^{2i} - 1)$	$O^m(2n, 2)$ Exceto $O^+(4, 3)$	$O^m(2n, 2)$ $n \geq 2$		$O^+(4, 2) \cong \Sigma_3 \wr \Sigma_2$ $O^+(2, 2) \cong \Sigma_2$
$PSU(n, q)$	$\frac{1}{q} q^{n(n+1)/2} \prod_{i=2}^n (q^i - (-1)^i)$ $\delta = (n, q+1)$	$PSU(n, 2)$	$PSU(n, 2)$ $n \geq 4$	$PSU(n, 2)$ $n \geq 4$	
$P\Omega(2n+1, 3)$ ou $+0(2n+1, 3)$	$ Sp(2n, 3) $	$P\Omega(2n+1, 3)$ todos	$n \geq 2$	$n \geq 2$	
$-0(2n+1, 3)$	$ Sp(2n, 3) $	todos	$n \geq 2$		$G \cong P\Omega(2n+1, 3)$

GRUPOS DE FISCHER

$Fi_{22}$	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23 \longrightarrow$	simples
$Fi_{23}$	$2^{18} \cdot 3^{23} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \longrightarrow$	simples
$Fi_{24}$	$2^{22} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	tem comutador $C'$ de índice 2 simples



## CAPÍTULO 1

Provaremos nesse capítulo o resultado de Nagao [9], já citado na Introdução, que é o seguinte:

Teorema: O grupo de permutação  $\Sigma_n$  é caracterizado pela sua tábua de caracteres.

### A. Teoremas Gerais:

Definições e Notações: Sejam  $G$  e  $G'$  dois grupos; diremos que eles tem a mesma tábua de caracteres se existem duas permutações  $(\alpha, \beta)$  tais que  $\chi_\eta(C_\theta) = \chi_{\alpha(\eta)}(C_{\beta(\theta)})$ , onde  $\chi_\eta$  denota um caracter sobre  $C$ ,  $C_\theta$  uma classe de conjugação.

Para simplificar denotaremos:

$\chi_{\alpha(\mu)}$  por  $\chi'_\mu$  e  $C_{\beta(\theta)}$  por  $C'_\theta$ . A classe  $\{1\}$  será denotada por  $C_1$ .

As provas, a seguir, são baseadas em resultados conhecidos da teoria dos caracteres que podem ser encontrados em [19], [20], [22].

Proposição 1: Se  $G$  e  $G'$  têm a mesma tábua de caracteres então:

- 1)  $|G| = |G'|$
- 2)  $\text{gr } \chi_u = \text{gr } \chi'_u$

$$3) |C_\alpha| = |C'_\alpha|$$

4)  $C_{\alpha\beta\gamma} = C'_{\alpha\beta\gamma}$  (onde  $C_{\alpha\beta\gamma}$  são as constantes de multiplicação, determinadas como segue).

Cada elemento da classe  $C_\gamma$  pode ser obtido de  $C_{\alpha\beta\gamma}$  maneiras, como produto  $x \cdot y$  com  $x$  em  $C_\alpha$  e  $y$  em  $C_\beta$ .

Demonstração:  $\chi'_u(C'_1) = \chi_u(C_1) = \text{gr } \chi_u$ .

Temos  $\sum_{u=1}^k \chi'_u(C'_1) \overline{\chi'_u(C'_1)} > 0$  e pelas relações de ortogonalidade,  $C'_1$  é a classe do elemento unidade de  $G'$ , conseqüentemente  $\text{gr } \chi_u = \text{gr } \chi'_u$  e isso demonstra 2. Então temos que

$$|G| = \sum_{u=1}^k (\text{gr } \chi_u)^2 = \sum_{u=1}^k (\text{gr } \chi'_u)^2 = |G'| \text{ e demonstramos 1}$$

$$\frac{|G|}{|C_\alpha|} = \sum_{u=1}^k \chi_u(C_\alpha) \overline{\chi(C_\alpha)} = \sum_{u=1}^k \chi_{u'}(C_{\alpha'}) \overline{\chi_{u'}(C_{\alpha'})} = \frac{|G'|}{|C_{\alpha'}|} \text{ e como}$$

$$|G| = |G'| \text{ temos que } |C_\alpha| = |C_{\alpha'}|.$$

Pela definição temos

$$C_\alpha C_\beta = \sum_{\gamma} C_{\alpha\beta\gamma} C_\gamma \text{ e concluímos:}$$

$$\frac{|C_\alpha| \chi_u(C_\alpha)}{\text{gr } \chi_u} \cdot \frac{|C_\beta| \chi_u(C_\beta)}{\text{gr } \chi_u} = \sum_{\gamma} \frac{C_{\alpha\beta\gamma} |C_\sigma| \chi_u(C_\sigma)}{\text{gr } \chi_u} \quad (1)$$

Assim:

$$\sum_u \frac{\overline{\chi_u(C_\gamma)}}{\text{gr } \chi_u} \left[ |C_\alpha| \chi_u(C_\alpha) |C_\beta| \chi_u(C_\beta) \right] =$$

$$= \sum_u \overline{\chi_u(C_\gamma)} \cdot \sum_{\sigma} C_{\alpha\beta\gamma} |C_\sigma| \chi_u(C_\sigma) = \sum_{u,\sigma} C_{\alpha\beta\gamma} |C_\sigma| \chi_u(C_\sigma) \overline{\chi_u(C_\gamma)} =$$

$$= C_{\alpha\beta\gamma} |G|. \text{ e deduzimos que}$$

$$C_{\alpha\beta\gamma} = \frac{1}{|G|} \sum_{u\sigma} C_{\alpha\beta\gamma} |C_{\sigma}| \chi_u(C_{\sigma}) \overline{\chi_u(C_{\gamma})} \text{ analogamente temos que}$$

$$C_{\alpha'\beta'\gamma'} = \frac{1}{|G|} \sum_{u'\sigma'} C_{\alpha'\beta'\gamma'} |C_{\sigma'}| \chi_{u'}(C_{\sigma'}) \overline{\chi_{u'}(C_{\gamma'})}.$$

Pela observação, temos que na expressão acima cada parcela  $\sum_{\sigma'} C_{\alpha'\beta'\gamma'} |C_{\sigma'}| \chi_{u'}(C_{\sigma'})$  pode ser substituída por  $|C_{\alpha'}| \chi_{u'}(C_{\alpha'}) \cdot |C_{\beta'}| \chi_{u'}(C_{\beta'}) / \text{gr} \chi_{u'}$ , e pelos 3 primeiros fatos temos 4.

### B. Grupos Gerados por 3-transposições conjugadas

Definição 1. Diremos que um grupo finito G é gerado por uma classe de 3-transposições conjugadas se existe uma classe de conjugação D tal que

$$1) \langle D \rangle = G$$

$$2) x, y \in D \implies x^2 = 1 \neq x \text{ e } |xy| \leq 3.$$

#### Notações e Observações Gerais:

I) Denotaremos por  $\hat{A}$  a soma dos elementos de uma classe A de G, soma essa tomada no anel de grupo  $C(G)$ .

II)  $C_D(x)$  denota o subconjunto formada pelos elementos de D que comutam com x.

III) Seja G um grupo gerado por uma classe de conjugação D que satisfaz uma equação da forma.

$$\hat{D}^2 = |D|1 + 2 \hat{T} + 3 \hat{W} \text{ onde T e W são classes distintas de G.}$$

Sejam:

$$B_v = \{(x, y) | x, y \in D \text{ e } x \cdot y = v\} \text{ então}$$

$$|B_v| = 2 \iff v \in T \text{ e } |B_v| = 3 \iff v \in W.$$

Dado x em D sejam:

$$D_x = \{y \in D \mid xy \in T\}$$

$$A_x = \{y \in D \mid xy \in W\}$$

Temos trivialmente que  $D = \{x^{-1}\} \cup D_x \cup A_x$ .

Lema 1. Com as notações anteriores temos

1)  $C_D(x) = \{x^{-1}\} \cup D_x$

2)  $x^2 \in T \cup \{1\}$ .

Demonstração: a) Mostraremos que  $\{x^{-1}\} \cup D \subset C_D(x)$ . Com efeito:  $y \in D_x \Rightarrow xy = yx^y = x^y y^{xy}$  e então  $x^y \in \{x, y\}$  que implica  $y \in C_D(x)$ .

b) Demonstração de 2.

Suponhamos que  $x^2 \in W$ , então  $W = \{u^2 \mid u \in D\}$  pois  $y \in W \Leftrightarrow y = a^{-1}x^2a = a^{-1}xa a^{-1}xa = (a^{-1}xa)^2$ .

Se tivéssemos  $A_x = \{x\}$  então  $C_D(x) = D$  e  $G$  seria comutativo; e então  $G$  não satisfaria a equação inicial.

Seja então  $z \in A_x - \{x\}$  temos  $xz = zx^z = x^z z^{xz} = u^2$ , para algum  $u$  em  $D$ , e teremos então  $x^z \in \{x, z, u\}$ .

Se  $x^z = u$  vem  $u = z^{xz}$  e teremos

$$z^{-1}xz = z^{-1}x^{-1}z x z \text{ e então } x = z \text{ contradição.}$$

Se  $x^z = z$  então  $x = z$  contradição. Então para todo  $z \in A_x$ , temos  $x^z = x$  que implica  $z \in C_D(x)$  e portanto teríamos  $G$  comutativo. Contradição.

c) agora mostraremos que  $C_D(x) \subset \{x^{-1}\} \cup D_x$ .

Pelo observado acima basta mostrar que  $C_D(x) \cap A_x = \emptyset$ .

Seja  $z \in C_D(x) \cap A_x$ , temos:

$xz = zx = uu' = u'u$  e  $u \notin \{x, z\}$ .

Então  $u = u'$  e temos que ter  $xz$  em  $T \cup \{1\}$

e isso vai contra o fato de que  $z$  está em  $A_x$  ■.

Proposição 2: Com as mesmas notações do lema 1 temos:

Ou  $D$  é uma classe de 3-transposições ou  $G \cong \Sigma_4$  e  $D$  é a classe de elementos de ordem 4 deste grupo; (classe associada aos 4-ciclos).

Demonstração: Se  $w \in W$  então  $|B_w| = 3$ .

$C_G(w)$  opera por conjugação em  $B_w$ .

Afirmo que  $w$  opera transitivamente em  $B_w$  pois suponha que  $(x, y)^w = (w^{-1}xw, w^{-1}yw) = (x, y)$  então  $w^{-1}xw = x$ , mas  $w = xy \Rightarrow y^{-1}x^{-1}xxy = x \Rightarrow y^{-1}xy = x \Rightarrow y \in C_D(x) = \{x^{-1}\} \cup D_x$  (contra a hipótese) logo  $w$  opera transitivamente em  $B_w$  e temos que  $3 \mid |w|$ .

Além disso temos:  $xy = yx^y = x^y y^{xy} = y^{xy} x^{yxy}$  e  $w$  de onde segue que  $y^{xy} \in \{x, y, x^y\}$ . Mas  $y^{xy} = y \Rightarrow y^x = y \Rightarrow y \in C_D(x)$  (contra a hipótese), e  $y^{xy} = x^y$  implica  $x = y$ .

Portanto temos que ter  $y^{xy} = x$  que implica  $xyx = yxy$  (1).

Como  $D$  é uma classe de conjugação, seus elementos têm todos a mesma ordem. Temos então duas possibilidades:

A)  $D$  consiste de involuções.

Nesse caso temos:  $C_D(x) = \{x^{-1}\} \cup D_x = \{x\} \cup D_x$  e portanto  $T$  consiste de involuções.

Como  $3 \mid |\langle w \rangle|$  e como, por (1).

$w^3 = (xy)^3 = xyxyxy = xyxxyx = 1$   $w$  consiste de elementos de ordem 3.

E nesse caso,  $D$  é uma classe de 3-transposições.

B) Os elementos de  $D$  não são involuções.

Então pelo lema 1:  $T = \{y^2 \mid y \in D\}$ .

Temos que  $D_x = \{x\}$ , pois se  $y \in D_x - \{x\}$  então:  
 $xy = yx = u^2 \Rightarrow u \in \{x, y\} \Rightarrow x = u = y$  absurdo.

Então para cada  $x$  em  $D$  existe exatamente um  $x'$  em  $D$  tal que  $x'^2 = x^2$  ( $x \neq x'$ ).

Agora se  $g \in C_G(x)$ , então  $x'^g, x'^g = x'^2 = x^2$ .

Ora  $x'^g = x \Rightarrow x' = x$  absurdo.

$x'^g = x' \Rightarrow g \in C_G(x')$  segue que  $C_G(x) = C_G(x')$ .

Em particular  $x' \in C_G(x) \cap D$  isto é

$x' \in C_D(x) = \{x, x^{-1}\}$  (Lema) o que implica  $x' = x^{-1}$ . Então  
 $x^4 = x^2 x'^2 = x^2 x'^2 = x^2 (x^{-1})^2 = 1$  e deduzimos que  $|x| \mid 4$ .

Como  $x$  não é uma involução temos que  $|x| = 4$ .

Temos provado que neste caso  $D$  é constituído de elementos de ordem 4 e portanto  $T$  é constituído de elementos de ordem 2.

Mostremos a seguir que os elementos de  $W$  têm todos ordem 3.

Sejam  $x, y \in D$  tais que  $(x, y) \in W$ ; então por (1):

$$(xy)^2 = xyxy = xxyx = y^2 x^{-1} \in D^2.$$

$y \in A_x$ ; ora o elemento  $(xy)^2 \notin T \cup \{1\}$  pois  $3 \mid |x \cdot y|$ .

Logo  $(x, y)^2 \in W$  e temos então  $|xy| = |xy|^2$  e vem que  $2 \nmid |xy|$ .

Agora observamos que

$$(xy)^3 = x(yxy)xy = xxyxxy = y^2 y \in D^2 \text{ e como } 2 \nmid |xy| \text{ deduzimos que } (xy)^3 \in W \cup \{1\}.$$

Finalmente como  $3 \mid |xy|$  temos

$$(xy)^3 = 1 \text{ e portanto } |xy| = 3 \text{ e } yx^2 = y^{-1}.$$

Então se  $y \in D - \{x, x^{-1}\}$ , temos que  $y^2 x^2 = x^2 y^2$  pois

$$x^2 y^2 x^2 = x^2 yx^2 x^2 yx^2 = y^{-2} = y^2.$$

Isto implica que:

$$y^2 x^2 = x^2 y^2 = (x^2 yx^2) x^2 y = y^{-1} x^2 y \in T.$$

Portanto  $\langle T \rangle = T \cup \{1\}$  é um 2-grupo que age por conjugação em  $\{y, y^{-1}\}$ , o núcleo dessa ação é pelo visto acima  $\{1, y^2\}$  logo  $|\langle T \rangle| = 4 \implies |T| = 3$ .

Conseqüentemente  $|D| = 6$ .

Pelo visto acima  $D$  é da forma

$$D = \{x, x^{-1}, y, y^{-1}, z, z^{-1}\}.$$

Seja  $a = xy^2$ ,  $b = y^2z$  e  $c = y^2x$

temos trivialmente que

$$a^2 = b^2 = c^2 = (ab)^3 = (bc)^3 = (ac)^2 = 1 \quad (2).$$

Mostremos que  $\langle a, b, c \rangle = \langle x, y, z \rangle$ .

1)  $y \in \langle a, b, c \rangle$  pois ou  $abc = y$  ou  $abc = y^{-1}$  pois temos  $abc = xy^2 y^2 zy^2 x = xzy^2 x = xzxx^{-1} y^2 x = xzxx^2 y^2 = xzx^{-1} y^2$  e  $xzx^{-1} \in \{y, y^{-1}\}$ .

Como  $ay^2 = x$  e  $y^2 b = z$ , resulta o que afirmamos. Então segue de (2) que  $G \cong \Sigma_4$ . (Veja Dickson [16], pág. 287).

### C) O caso $\Sigma_n$ .

#### Definições e Comentários:

Agora vamos demonstrar o teorema enunciado no começo do capítulo: O grupo  $\Sigma_n$  é caracterizado por sua tábua de caracteres.

Podemos supor  $n \geq 4$  pois  $\Sigma_2 \cong Z_2$  e  $\Sigma_3$  é o único

grupo não comutativo com ordem 6.

Observemos que  $\Sigma_n$  satisfaz a equação  $\hat{D}^2 = |D|1 + 2\hat{T} + 3\hat{w}$  onde D a classe das transposições.

Assumimos que G é um grupo com a mesma tábua de caracteres que  $\Sigma_n$ . Denotaremos por  $C(i_1^{(\alpha_1)}, i_2^{(\alpha_2)}, \dots)$  a classe de G associada à classe de  $\Sigma_n$  cujos elementos são expressos como um produto de  $\alpha_1$  ciclos de comprimento  $i_1$  vezes  $\alpha_2$  ciclos de comprimento  $i_2$ , etc.. Por exemplo, se  $n \geq 7$  então  $C(2^{(2)}, 3)$  é a classe associada a do elemento  $(12)(34)(567)$  e  $C(4, 3)$  é a classe associada a do elemento  $(1234)(567)$ .

Vamos supor que  $C(2)$  é uma classe de 3-transposição, o que certamente acontece se  $n \neq 4$ .

Lema 2. Nas hipóteses e notações acima temos:

A ordem de um elemento de  $C(4)$  é 4.

Demonstração: Da tábua de multiplicação tiramos que qualquer elemento de  $C(4)$  pode ser escrito como um produto de um elemento de  $C(2)$  por um de  $C(3)$ .

Seja  $x \in C(4)$  com  $x = ay$   $a \in C(2)$  e  $y \in C(3)$ . Observamos primeiro que  $x^2 = 1 \Rightarrow aya = 1 \Rightarrow yay = a \Rightarrow yay^2 = ay = yay^{-1} = x$ ; e tiramos que  $x \in C(2)$  (contra a hipótese).

Novamente temos que (da tábua de multiplicação)

$$x = bz = b'z'; \quad (b, b' \in C(2); z', z \in C(2^{(2)}))$$

Se  $[x, b] = 1$  vem  $b = xbx^{-1}$  então  $b = bzbz^{-1}b^{-1} = bzbz^{-1}b^{-1} \Rightarrow bzbz = x^2 = 1$  o que já mostramos que é contradição.

Desde que  $x = bz = xbxz^{-1} = xbx^{-1}xz^{-1} = (x^2bx^{-2})(x^2zx^{-2})$  e  $b \neq xbx^{-1}$  temos que ter  $x^2bx^{-2} \in \{b, xbx^{-1}\}$  mas como

$x^2 b x^2 = x b x^{-1} \Leftrightarrow b = x b x^{-1}$ , o que não pode acontecer, temos que ter  $x^2 b x^{-2} = b$  isto é:

$(b z b z) b (z b z b) = b$  e então  $(b z)^4 = x^4 = 1$  e temos que  $|x| \mid 4$ . Como  $x^2 \neq 1$  vem que  $|x| = 4$ .

Lema 3:

Seja  $k \leq \left\lfloor \frac{n}{2} \right\rfloor$  e sejam  $a_i (i=1, \dots, k)$  elementos de

$C(2)$ .

- 1) Se  $a_1 x \dots x a_k \in C(2^{(k)})$  então todos os  $a_i$ 's comutam entre si.
- 2) Qualquer elemento de  $C(2^k)$  pode ser expresso de modo único (a menos da ordem), como produto de  $k$  elementos de  $C(2)$ .
- 3) Se os  $a_i$ 's  $i=1, \dots, k$  são todos distintos e comutam entre si, então  $\prod_{i=1}^k a_i \in C(2^{(k)})$ .

Demonstração: Façamos indução em  $k$ .

Se  $k=1$  ou  $k=2$ , a conclusão sai do lema 1.

Assumamos agora que o lema é verdadeiro para todo  $s \leq k-1$ .

1) Da tábua de multiplicação temos que qualquer elemento de  $C(2^{(k)})$  pode ser expresso de  $k!$  modos como produtos de  $k$  elementos de  $C(2)$  e exatamente de  $k$  modos como produto de elementos de  $C(2^{(k-1)})$  vezes um elemento de  $C(2)$ .

Se um produto de um elemento  $x$  de  $[C(2)]^{k-1}$  vezes  $a$  de  $C(2)$  é tal que  $x \cdot a \in C(2^{(k)})$  então  $x \in C(2^{(k-1)})$ . Caso contrário,  $x \cdot a$  poderia ser escrito de mais de  $k!$  maneiras como produto de  $k$  elementos de  $C(2)$ . Então temos:

Se  $a_1, \dots, a_k$  são elementos de  $C(2)$

$a_1 \dots a_k \in C(2^{(k)}) \Rightarrow a_1 \dots a_{k-1} \in C(2^{(k-1)})$  e, pela hipótese

de indução  $a_1, \dots, a_{k-1}$  comutam entre si. Como  $a_2, \dots, a_k a_1 = a_1(a_2, \dots, a_k) a_1 \in C(2^k)$  temos também que  $a_2, \dots, a_k$  comutam entre si. Analogamente  $a_3, \dots, a_k a_1 a_2 \in C(2^k)$  e portanto também  $a_1$  e  $a_k$  comutam.

2) Os arranjos dos  $a_i$ 's são  $k!$  e portanto eles dão todos os modos de escrever o elemento  $a_1, \dots, a_k$  de  $C(2^{(k)})$  como produto de  $k$  elementos de  $C(2)$ .

3) Consideremos o conjunto  $C(2^{(k-1)}) \cdot C(2)$ . Da tábua de multiplicação sai que esse conjunto tem elementos em  $C(2^{(k)})$ ;  $C(2^{(k-2)}, 3)$ ;  $C(2^{(k-3)}, 4)$  e  $C(2^{(k-2)})$ .

Todo elemento de  $C(2^{(k-2)}, 3)$  pode ser escrito de modo único como um produto  $x \cdot y$ ; com  $x \in C(2^{(k-2)})$  e  $y \in C(3)$ .

Portanto

$$xy = [(xy)] [x(xy)^{-1}] [(xy)y(xy)^{-1}] \Rightarrow xy y(xy)^{-1} = (xy)x^{-1} = y, \quad \text{pois}$$

$$y(xy)^{-1} \in C(3), \text{ e temos } xy = yx, \text{ o que implica } |xy| = \text{mmc}(|x|, |y|) = 6.$$

De um modo completamente análogo pode-se mostrar que a ordem de um elemento de  $C(2^{(k-3)}, 4)$  é 4.

Como todos os  $a_i$ 's comutam  $\prod_{i=1}^k a_i \notin C(2^{(k-3)}, 4) \cup C(2^{(k-2)}, 3)$  e só resta mostrar que  $\prod_{i=1}^k a_i \notin C(2^{(k-2)})$ .

Se  $\prod_{i=1}^k a_i \in C(2^{(k-2)})$  teríamos

$$a_1 \dots a_k = b_1 \dots b_{k-2}, \quad b_i \in C(2) \text{ e}$$

$$a_1 \dots a_{k-1} = b_1 \dots b_{k-2} a_k \text{ de onde por 2)}$$

$a_k$  seria igual a um dos  $a_i$   $1 \leq i \leq k-1$ , o que é uma contradição.

Lema 4: Se  $a_1, a_2$  são elementos de  $C(2)$  tais que  $a_1 \cdot a_2$  es-

tã em  $C(2^{(2)})$  então existe um elemento  $b$  de  $C(2)$  tal que  $a_1 a_2 b \in C(4)$  e isto implica que  $a_1 b \in C(3)$  e  $a_2 b \in C(3)$ .

Demonstração: Desde que  $C(2^{(2)}) \cdot C(2)$  contém  $C(4)$  existe  $b$  tal que  $a_1 a_2 b \in C(4)$  que implica  $b \notin \{a_1, a_2\}$ .

Precisamos mostrar que  $a_i b \in C(3)$ ;  $i=1,2$ .

Se  $a_i b \notin C(3)$  ( $i=1,2$ ),  $a_i b \in C(2^{(2)})$  e então  $a_1 a_2 b \in C(2^{(3)})$ ; contradição.

Se  $a_1 b \in C(2^{(2)})$  e  $a_2 b \in C(3)$  então  $a_1$  comuta com  $a_2 b$  e  $|a_1 a_2 b| = 6$ ; contradição.

Portanto  $a_1 b, a_2 b \in C(3)$ .

Lema 5: Sejam  $a_1, a_2, b$  elementos de  $C(2)$  tais que  $a_1 a_2 \in C(2^{(2)})$ .

Se  $a_i b \in C(3)$  ( $i=1,2$ ) então  $x = a_1 a_2 b \in C(4)$ .

Demonstração:  $C(2) \cdot C(3) = C(2,3) \cup C(4) \cup C(2)$ .

1) Se  $x$  pertence a  $C(2)$

$a_1 a_2 = xb$  implica  $x = a_1$  ou  $x = a_2$  então ou  $a_1 b$  ou  $a_2 b$  pertence a  $C(2^{(2)})$ , contra a hipótese.

2) Se  $x$  pertence a  $C(2,3)$  então  $x$  pode ser escrito de maneira única como um produto de um elemento de  $C(2)$  por um de  $C(3)$ . Como  $x = a_1(a_2 b) = a_2(a_1 b)$  temos que  $a_1 = a_2$  e portanto  $a_1 a_2 = 1$ ; contradição.

Só resta a possibilidade de  $x \in C(4)$ .

Lema 6. Se  $a_1 a_2 a_3$  são elementos de  $C(2)$  tais que  $a_1 a_2 a_3$  pertence a  $C(2^{(3)})$  e  $b$  um elemento de  $C(2)$  que não comuta com  $a_1 a_2$  então  $b$  comuta com  $a_3$ .

Demonstração: Suponhamos que  $b$  não comuta com  $a_3$ .

Então  $a_i b$  pertence a  $C(3)$  para  $i=1,2,3$  e, pelo

lema 4,  $a_2 a_3 b$  seria um elemento de  $C(4)$ . Então  $x = a_1 a_2 a_3 b$  pertence a  $C(2^{(3)}) \cdot C(2) \cap C(2) \cdot C(4)$  mas

$$C(2^{(3)}) \cdot C(2) = C(2^{(4)}) \cup C(2^{(2)}, 3) \cup C(2^{(2)}) \cup C(2, 4)$$

$C(2) \cdot C(4) = C(2, 4) \cup C(3) \cup C(3) \cup C(2^{(2)})$  de onde  $x$  pertence a  $C(2^{(2)})$  ou a  $C(2, 4)$ .

Se  $x$  pertence a  $C(2^{(2)})$  então

$$x = a_1 a_2 a_3 b = a'_1 a'_2 \text{ e temos que}$$

$a_1 a_2 a_3 b = a'_1 a'_2 b$  pertence a  $C(2^{(3)})$ . Então  $b$  comuta com  $a_i$  para  $i = 1, 2, 3$ , contra a hipótese.

Se  $a_1 a_2 a_3 b$  pertence a  $C(2, 4)$  então

$a_1 a_2 a_3 b = a_2 a_1 a_3 b$  que implica  $a_1 = a_2 = a_3$ , contra a hipótese, pois  $a_1 a_2 a_3$  pertence a  $C(2^{(3)})$ .

Lema 7: Sejam  $a_1, a_2, a_3$  elementos de  $C(2)$ .

Se  $a_1$  não comuta com  $a_2$  e  $a_3$  comuta com  $a_1$  e  $a_2$  então existe  $b$  pertencente a  $C(2)$  que comuta com  $a_1$  e não comuta com  $a_2$  nem com  $a_3$ .

Demonstração: Pelo lema 5 existe  $b$  tal que  $b$  pertence a  $C(2)$ ;  $a_3 a_2 b$  pertence a  $C(4)$  e  $b$  não comuta com  $a_2$  e  $a_3$ .

Se  $b$  comuta com  $a_1$  a demonstração termina aqui; assumamos que  $b$  não comuta com  $a_1$ .

$$\text{Então } x = a_1 a_2 b \text{ pertence a } C(3) \cdot C(2) = C(2) \cup C(3, 2) \cup C(4).$$

1) Se  $x$  pertence a  $C(3, 2)$

$$x = a_1 a_2 b = x^{-1} a_1 a_2 b x = x^{-1} a_1 a_2 x x^{-1} b x \in C(3) \cdot C(2) \text{ implica } a_1 a_2 = x^{-1} a_1 a_2 x \text{ ou seja } [x, a_1 a_2] = 1 \text{ que implica } [b, a_1 a_2] = 1.$$

Então  $x = a_1 a_2 b = b a_1 a_2$  implica  $b = a_2$ ; contradição.

2) Se  $x = a_1 a_2 b$  pertence a  $C(2)$  então

$xb = a_1 a_2 = a_2 (a_2^{-1} a_1 a_2) = (a_1 a_2 a_1^{-1}) a_1$  é um elemento de  $C(3)$  e portanto  $b = a_2$  ou  $b = a_2^{-1} a_1 a_2$  ou  $b = a_1$ . Em qualquer caso  $b$  comuta com  $a_3$ .

3) Se  $x$  pertence a  $C(4) \subset C(2^{(2)}) \subset C(2)$ .

Existem elementos  $c_i^1$  ( $i = 1, 2, 3$ ) com  $c_1^1 \cdot c_2^1$  em  $C(2^{(2)})$  e  $c_1^1 c_2^1 c_3^1 = x$  pertence a  $C(4)$ .

Pelo lema 4,  $c_1^1 c_3^1$  e  $c_2^1 c_3^1$  estão em  $C(3)$ . Como  $c_2^1 c_3^1 c_1^1 = c_1^1 (c_1^1 c_2^1 c_3^1) c_1^1$  está em  $C(4)$  existem elementos  $c_1 c_2 c_3$  de  $C(2)$  tais que  $x = c_1 c_2 c_3$  e  $c_1 c_3$  pertence a  $C(2^{(2)})$  e  $c_1 c_2$  e  $c_2 c_3$  estão em  $C(3)$ .

Como  $c_1$  comuta com  $c_3$  e  $(c_1 c_3)^3 = 1$  temos que  $xc_1 x^{-1} = c_1^{x^{-1}} = c_1 c_2 c_3 c_1 c_3 c_2 c_1 = c_1 c_2 c_1 c_2 c_1 = c_2$ .

Por outro lado, como  $(c_2 c_3)^3 = 1$   
 $c = c_1 (c_2 c_3 c_2 c_3 c_2) c_1 = c_1 c_3 c_1 = c_3$ .

Ora, qualquer elemento de  $C(4)$  pode ser expresso como produto de um elemento de  $C(2)$  vezes um elemento de  $C(3)$  de 4 modos distintos.

Mas  $x = c_1 c_1^{x^{-1}} c_1^{x^{-2}} = c_1^{x^{-2}} c_1^{x^{-3}} c_1 = c_1^{x^{-3}} (c_1 c_1^{x^{-1}}) = c_1^{x^{-1}} c_1^{x^{-2}} c_1^{x^{-3}}$  como  $c_1, c_1^{x^{-1}}, c_1^{x^{-2}}, c_1^{x^{-3}}$  são todos distintos,  $a_1$  deve ser igual a algum dos  $c_i^{x^{-1}}$   $i = 1, 2, 3$ .

Então existem dois elementos  $a_2', b'$  de  $C(2)$  tais que  $x = a_1 a_2' b'$  e  $a_1 b' \in C(2^{(2)})$ . Segue daí que  $a_2 b = a_2' b' = b (b a_2 b) = (a_2 b a_2) a_2$ , e  $b' \neq b$  e  $b' \neq a_2$  pois  $[a_1, b] \neq 1$  e  $[a_1, a_2'] = 1$ .

Como qualquer elemento de  $C(3)$  pode ser expresso como um produto de dois elementos de  $C(2)$  de 3 maneiras e como  $(ba_2)^3 = 1$  devemos ter

$$b' = ba_2b = a_2ba_2 \text{ e então } [b', a_2] \neq 1, [b', a_3] \neq 1 \text{ e } [b', a_1] = 1.$$

Assim  $b'$  é o elemento procurado e isso termina a demonstração.

---

Após apresentar essa série de lemas preliminares que demonstram bem o tipo de técnica para esse assunto vamos finalmente demonstrar o teorema.

Teorema: Se  $G$  tem a mesma tábua de caracteres que o grupo de permutações  $\Sigma_n$ , então  $G \cong \Sigma_n$ .

Demonstração:

1) Suponha  $n$  par  $n = 2m$ ,  $n \neq 4$  e  $D = C(2)$  uma classe de 3-transposições conjugadas de  $G$ .

Para  $n = 2$ ,  $G$  resulta comutativo e nada temos a demonstrar.

a)  $n = 2m$  ( $m > 2$  e  $D = C(2)$  uma classe de 3-transposições conjugadas de  $G$ ).

Sejam  $a_1, \dots, a_m$  elementos de  $C(2)$  com  $a_1, \dots, a_m$  em  $C(2^{(m)})$ .

Pelo lema 4 existe um elemento  $b_1$  em  $C(2)$  tal que  $a_1a_2b_1$  está em  $C(4)$ , ( $a_1b_1$  e  $a_2b_1$  estão em  $C(3)$ ) e  $b_1$  comuta com  $a_i$  se  $i=1,2$ .

Agora assumamos que construímos  $b_1, \dots, b_k$   $k < m - 1$  elementos de  $C(2)$  tais que todos os  $b_i$ 's comutam com todos os  $b_j$ 's e  $a_j$ 's exceto com  $a_i$  e  $a_{i+1}$ .

Existe  $b_{k+1}$  em  $C(2)$  que comuta com  $b_k$  e não comuta com  $a_{k+1}$  e  $a_{k+2}$  então pelo lema 6,  $b_{k+1}$  comuta com todos os  $b_j$ 's e  $a_j$ 's exceto  $a_{k+1}$  e  $a_{k+2}$ .

Existem assim  $(m-1)$  elementos  $b_1, \dots, b_{m-1}$  de  $C(2)$  tais que  $|a_i b_i| = |b_i a_{i+1}| = 3$ .

Seja  $c_{2k-1} = a_k$  e  $c_{2k} = b_k$ .

Os elementos  $c_1, \dots, c_{n-1}$  satisfazem as relações fundamentais seguintes

- 1)  $c_i^2 = 0$
- 2)  $(c_i c_j)^2 = 1$  se  $1 < j - i$
- 3)  $(c_i c_{i+1})^3 = 1$

e então  $G \cong \Sigma_n$ . (ver Dickson [16], cap. XIII).

b) Consideremos agora o caso  $n=4$ .

Se  $G$  tem a mesma tábua de caracteres que  $\Sigma_4$  então vale uma das hipóteses seguintes:

- a)  $C(2)$  é uma classe de involuções de  $G$  e pelo que fizemos até aqui  $G \cong \Sigma_4$  ou
- b)  $C(2)$  é uma classe de elementos de ordem 4 e então  $G \cong \Sigma_4$ .

2) Seja  $n=2m+1$ .

O teorema vale se  $m=0$ , de modo que podemos assumir que  $m > 1$ . (No caso  $m=1$ , se  $G$  tem a mesma tábua que  $\Sigma_3$  então  $|G|=6$  e  $G$  é não comutativo e tiramos que  $G \cong \Sigma_3$ .)

Pelo mesmo modo da parte 1, construímos  $(n-2)$  elementos  $c_1, \dots, c_{n-2}$  que satisfazem as relações fundamentais e esses elementos geram então um grupo  $G_1$  isomorfo a  $\Sigma_{n-1}$

e mais  $|G : G_1| = n$ .

Desde que  $G$  contém apenas um subgrupo normal próprio e seu índice é 2 temos  $\bigcap_{x \in G} G_1^x = 1$  e segue que  $G$  é isomorfo a algum subgrupo de  $\Sigma_n$  como  $|G| = n!$  segue que  $G \cong \Sigma_n$  (Teorema do "Core"). ■

Um contra-exemplo, para mostrar que existem grupos não caracterizados pela Tábua de Caracteres.

Agora mostraremos que os dois grupos não comutativos  $Q_8$  e  $D_4$  têm a mesma tábua de caracteres.

Seja  $G$  um desses grupos.

$$\{1, a\} = Z(G) = G'.$$

Temos que existem 4 caracteres lineares. Como  $G$  tem algum caracter irreduzível não linear e  $\sum_i x_i^2(1) = 8 = |G|$ , só resta a possibilidade de mais um caracter irreduzível de ordem 2, portanto  $G$  tem 5 caracteres irreduzíveis e  $G$  tem 5 classes de conjugação.

Sejam:  $1, a, b, c, d$  os representantes das classes de conjugação,  $\{1, a\} = Z(G)$ ;  $\frac{G}{Z(G)} \cong Z_2 \times Z_2$ .

Temos já a seguinte informação, usando a tábua de caracteres de  $G/Z(G)$ .

	1	a	b	c	d
1G	1	1	1	1	1
$\chi_2$	1	1	-1	1	-1
$\chi_3$	1	1	1	-1	-1
$\chi_4$	1	1	-1	-1	1
$\chi_5$	2	$\beta$	$\alpha_1$	$\alpha_2$	$\alpha_3$

Agora, usando as relações de ortogonalidade, tiramos que  $\beta = -2$ ,  $\alpha_1 = \alpha_2 = \alpha_3 = 0$ .

Temos assim construído a tábua da caracteres de qualquer grupo não comutativo de ordem 8. Algo bem análogo ao caso anterior poderia ser feito para dois grupos não comutativos quaisquer de ordem  $p^3$ ,  $p$  primo.

A menos de isomorfismos existem apenas 2 grupos não abelianos de ordem  $p^3$  e eles têm a mesma tábua de caracteres.

Observações: 1) O que fizemos nos dá um isomorfismo de tábua de caracteres  $(\psi, \tau)$  entre  $Q_8$  e  $D_4$ , mas nesse isomorfismo de tábua a ordem de um elemento  $x$  de  $Q_8$  nem sempre é igual a ordem de um elemento da classe correspondente em  $D_4$ . Essa é uma das razões mais fortes para não podermos concluir que eles são isomorfos.

2) O contra-exemplo também é importante, exatamente por corresponder a grupos relativamente "simples". Isso já evita que procuremos resultados do tipo: todo grupo solúvel é caracterizado por sua tábua de caracteres.



## CAPÍTULO 2

Neste Capítulo demonstramos que certos grupos gerados por 3-transposições são caracterizados por suas tábuas.

Assumiremos um resultado não trivial já enunciado na introdução, demonstrado por Bernd Fischer e que é o seguinte.

Seja  $D$  uma classe de 3-transposições conjugadas de um grupo finito  $G$  satisfazendo

$G' = G''$ ,  $O_3(G) \leq Z(G) \leq O_2(G)$  " $O_p(G)$  é definido como sendo o  $p$ -subgrupo normal maximal de  $G$ ."

Seja  $G^* = \frac{G}{Z(G)}$ , então  $G^*$  é um dos seguintes grupos:

- 1)  $\Sigma_n, n \geq 5$
- 2)  $S_p(2n, 2), n \geq 2$
- 3)  $O^\mu(2n, 2), \mu \in \{1, -1\}$  e  $n \geq 2$
- 4)  $PSU(n, 2), n \geq 4$
- 5)  ${}^\mu O^\pi(n, 3), \mu \in \{+1, -1\}; \pi \in \{-1, +1\}$   $n \geq 4$
- 6) Um dos grupos denotados por  $Fi_{22}, Fi_{23}, Fi_{24}$  e que Fischer denota por  $M(22), M(23), M(24)$  respectivamente.

Esses grupos foram descritos na introdução.

O tipo de técnica usado aqui, daria uma nova demonstração, um pouco mais rápida, do resultado do capítulo 1, mas assumiremos esse fato como demonstrado.

Teorema 1:

Os seguintes grupos são caracterizados por sua tabela de caracteres.

- 1) Os grupos simétricos  $\Sigma_n$
- 2) Os grupos simpléticos  $S_p(2n, 2)$
- 3) Os grupos ortogonais  $O^\mu(2n, 2)$   $\mu \in \{+1, -1\}$
- 4) Os grupos unitários  $PSU(n, 2)$
- 5) Os grupos ortogonais  $\pi O^\mu(n, 3)$   $\mu \in \{+1, -1\}$ ,  $\pi \in \{+1, -1\}$  com excessão de  $O^+(4, 3)$
- 6) Os grupos de Fischer que denotaremos por  $Fi_{22}$ ,  $Fi_{23}$ ,  $Fi_{24}$ .

Do resultado de Fischer temos que se  $D$  é uma classe de 3-transposições  $\langle D \rangle = G$  tal que  $G' = G''$ ;  $O_3(3) \leq Z(G) \leq O_2(G)$  então existem classes de conjugação  $T, W$  em  $G$  tais que  $\hat{D}^2 = |D| \cdot 1 + 2 \hat{T} + 3 \hat{W}$ .

Começamos mostrando uma espécie de recíproco desse fato.

Já sabemos da proposição 2 da introdução que, se  $G = \langle D \rangle$  e

$$\hat{D}^2 = |D| \cdot 1 + 2 \hat{T} + 3 \hat{W} \text{ então}$$

$G \cong \Sigma_4$  ou  $D$  é uma classe de 3-transposições de  $G$ .

Temos agora

Lema 1: Se  $G$  é um grupo gerado por uma classe de conjugação  $D$  tal que  $\hat{D}^2 = |D| \cdot 1 + 2\hat{T} + 3\hat{W}$ ,  $G \cong \Sigma_4$  ou  $D$  é uma classe de 3-transposições,  $G$  é não solúvel e para todo subgrupo normal  $N$  de  $G$  têm-se que  $N \leq Z(G)$  ou  $N \geq G'$ .

Em particular, temos que  $G'' = G'$  e que  $O_2(G) \leq Z(G) \geq O_3(G)$ .

Demonstração:

Seja  $G \not\cong \Sigma_4$ . Então  $D$  é uma classe de 3-transposições.

Seja  $N \triangleleft G$ .

Se  $N \cap D^2 = \{1\}$  então  $N \leq Z(G)$  pois  $d \in D$ ;  $n \in N \implies ndn^{-1}d^{-1} \in N \cap D^2 = \{1\}$  e  $nd = dn$ . Logo se  $N \not\leq Z(G)$  e  $N \triangleleft G$  então  $N \cap D^2 \neq \{1\}$  e vem que  $T \subset N$  ou  $W \subset N$ .

Para completar a demonstração, precisamos do lema seguinte:

Lema 2: Se  $G \not\cong \Sigma_4$  então  $\langle W \rangle = \langle T \rangle = G'$ .

Temos que

$D^2 \subset G'$  pois  $d_1 d_2 = d_1 d_1^a \in G \quad \forall d_1, d_1 \in D \cdot \frac{G}{\langle W \rangle} = \frac{\langle D, W \rangle}{\langle W \rangle}$  e então se  $d_1, d_2 \in D$  ou  $[d_1, d_2] = 1$  ou  $d_1 d_2 \in W$ . (Neste caso, passando ao quociente módulo  $\langle W \rangle$  temos  $\bar{d}_1 \bar{d}_2 = 1$  o que implica  $\bar{d}_1 = \bar{d}_2$ .)

Portanto

$[\bar{d}_1, \bar{d}] = 1 \quad \forall \bar{d}_1, \bar{d}_2 \in \frac{\langle D, W \rangle}{\langle W \rangle} \text{ e } \frac{G}{\langle W \rangle} \text{ é comutativo.}$

Para provar que  $\langle T \rangle = \langle W \rangle$ , raciocinamos pelo absurdo.

Suponhamos que  $H = \langle T \rangle \subsetneq \langle W \rangle = G'$ . Denotaremos por -

a operação de redução módulo H.

Temos que  $\bar{G} = \frac{G}{H} = \langle \bar{D} \rangle = \frac{\langle D \ H \rangle}{H}$  e o produto de dois elementos de  $\bar{D}$  tem sempre ordem 3.

Então pelo corolário 3 de GLAUBERMAN [5], temos que  $\bar{G}' = \frac{G'}{H}$  é um 3-grupo.

Como  $\bar{G} = \bar{G}' \langle \bar{d} \rangle$ ,  $d \in D$ , temos que  $Z(\bar{G}) \subsetneq \bar{G}'$ . Afirmo que  $\bar{G}'$  é minimal normal não central pois seja K tal que  $H \leq K \subsetneq G'$  e  $K \triangleleft G$ .

Então  $\bar{K} = \frac{K}{H} \subset \bar{Z} = Z(\frac{G}{H})$  pois se  $\bar{d} \in \bar{D}$   $\bar{k} \in \bar{K}$ ,  $dkd^{-1}k^{-1} \in D^2 \cap K$ .

Como  $dkd^{-1}k^{-1} \in W$  implica  $W \subset K$  deve-se ter  $dkd^{-1}k^{-1} \in H$  e então  $dk = kd$ .

Segue daqui que  $Z(\bar{G}') \subset Z(\bar{G})$  e como  $Z(\bar{G}) \subset G'$ , resulta  $Z(\bar{G}') = Z(\bar{G})$ .

Analogamente, temos que

$$\bar{G}'' \subset Z(\bar{G}) = Z(\bar{G}')$$

$\langle d \rangle$  age trivialmente em todo subgrupo normal próprio de  $\bar{G}'$ .

Mas  $d$  age não trivialmente em  $\bar{G}'$  pois, em caso contrário,  $\langle \bar{d} \rangle$  seria normal e  $\bar{G}$  seria comutativo.

Afirmo que  $\langle d \rangle$  opera não trivialmente em  $\frac{\bar{G}'}{\bar{G}''}$ . Pois sabemos que:

a)  $\langle d \rangle$  age não trivialmente em  $\bar{G}'$ .

b)  $\langle d \rangle$  age trivialmente em  $\bar{G}''$ .

Seja  $\bar{x}$  um elemento de  $\bar{G}'$

$$[\bar{x}, \bar{d}] \in \bar{G}'' \implies \bar{x}^{-1} \bar{x}^{\bar{d}} = \bar{z} \implies \bar{z} \in \bar{G}''.$$

Então  $\bar{x} = \bar{x}^{\bar{d}^2} = (\bar{x}\bar{z})^{\bar{d}} = \bar{x}^{\bar{d}} \bar{z}^{\bar{d}} = \bar{x}^{\bar{d}} \bar{z} = \bar{x} \bar{z}^2$  e resulta que  $\bar{z}^2 = 1$ ; mas  $\bar{z} \in \bar{G}$  que é um 3-grupo e portanto  $\bar{z} = 1$  ou

seja  $\bar{x}^{\bar{d}} = \bar{x}$ . Como  $\bar{x}$  é arbitrário em  $\bar{G}'$  isso contradiz a hipótese a).

Afirmo que  $\langle d \rangle$  age irreduzivelmente em  $\frac{\bar{G}'}{\bar{G}''}$ . Pois seja  $\bar{S} = \frac{\bar{G}'}{\bar{G}''}$ , um 3-grupo abeliano elementar, e suponhamos que  $\bar{S} = \bar{S}_1 \oplus \bar{S}_2$  onde  $S_i \neq 1$  e  $S_i$  é  $d$  invariante ( $i=1,2$ ). Então  $\bar{G}' = S_1 \cdot S_2$  onde, para  $i=1,2$ ,  $S_i$  é um subgrupo próprio  $\langle d \rangle$  invariante e normal em  $\bar{G}'$ .

Mas então  $\langle d \rangle$  age como identidade em cada  $S_i$  e o mesmo acontece com  $\bar{S}_i$  contra a primeira parte, logo temos que a ação de  $d$  sobre  $\frac{\bar{G}'}{\bar{G}''}$  é indecomponível logo irreduzível.

Mas as representações irreduzíveis de  $Z_2$  sobre  $GF(3)$  são de grau 1. Logo temos  $\frac{\bar{G}'}{\bar{G}''} \cong Z_3$  e portanto  $\frac{\bar{G}'}{Z(\bar{G}')}$  é cíclico, de onde  $\bar{G}'$  é comutativo. Então temos que  $\bar{G}' \cong Z_3$  e  $\bar{G} = \frac{G}{H} \cong \Sigma_3 = \bar{G}' \langle d \rangle$ .

Em resumo, temos que

$$G = \langle D \rangle; \quad \hat{D}^2 = |D| 1 + 2 \hat{T} + 3 \hat{W}.$$

$$\langle T \rangle = H, \quad \langle W \rangle = G', \quad H \subset \langle W \rangle \quad \text{e} \quad \frac{G}{H} \cong S_3.$$

Afirmo que então  $\langle x \rangle H \cap D = C_D(x) = C$  ( $\forall x \in D$ ) pois  $y \in xH \cap D \Rightarrow y = xh' \Rightarrow xy = h' \in T \Rightarrow y \in C_D(x)$ .

A inclusão oposta é imediata.

Então  $\langle x \rangle H \cap D = \langle y \rangle H \cap D$  pois  $a \in \langle x \rangle H \cap D \Rightarrow a = xh = xh' h'^{-1}h = yh' h'^{-1}h = yh'' \in \langle y \rangle H \cap D$ .

Analogamente  $\langle y \rangle H \cap D \subset \langle x \rangle H \cap D$ .

Temos então que  $C_D(x) = C_D(y)$ .

Vejamos que  $H$  normaliza  $C_D(x) = \{x\} \cup D_x$

$h \in H$ ,  $a \in C_D(x)$  e  $a = xh'$  então

$$h^{-1}xh'h = xx^{-1}h^{-1}x^{-1}h'h = xh'' \text{ portanto } h^{-1}ah \in C_D(x).$$

Seja agora

$$Q_x = \langle ab \mid a, b \in C_D(x) \rangle.$$

$Q_x$  é um 2 grupo abeliano elementar pois é gerado por elementos de ordem dois que comutam entre si. E  $Q_x \triangleleft H$  pois se  $ab \in Q_x$  e  $h \in H$  então  $h(ab)h^{-1} = hah^{-1}hbh^{-1} = cd$  onde  $c, d \in C_D(x)$ .

Então,  $H = \pi_{x \in D} Q_x$  e cada  $Q_x \triangleleft H$ , de onde  $H$  é um 2-grupo.

Afirmo que  $H$  é um subgrupo minimal normal não central de  $G$ . Pois se  $B \triangleleft_+ H$ ;  $B \triangleleft G$  então  $B \cap D^2 = \{1\}$  e  $B \subset Z(G)$ .

Então  $\frac{H}{H \cap Z(G)}$  não contém nenhum subgrupo característico próprio pois, pelo teorema da correspondência, esse grupo seria imagem de um subgrupo  $H$  normal em  $G$  que portanto deveria estar contido em  $Z(G)$ .

Portanto  $\frac{H}{H \cap Z(G)}$  tem expoente 2 isto é: é um 2-grupo abeliano elementar.

Pelo que fizemos acima temos que  $G$  é o produto semi-direto de  $\langle d, e \rangle$  por  $H$  e  $\langle d, e \rangle \cong \Sigma_3 \cong \frac{G}{H}$  que tem centro trivial, donde tiramos que  $Z(G) \subset H$  e  $\frac{H}{Z(G)}$  é um 2-grupo abeliano elementar que não contém nenhum subgrupo próprio normal em  $\frac{G}{Z(G)}$ . Pois, pelo teorema da correspondência, esse grupo seria imagem de um subgrupo normal de  $G$  contido em  $H$  mas  $H$  é minimal normal não central.

$\langle d, e \rangle$  age em  $V = \frac{H}{Z(G)}$ . Afirimo que essa ação é irre-  
dutível e fiel pois seja

$$\bar{a} \in \frac{H}{Z(G)} \text{ e } \phi_x \text{ a imagem de } x \text{ pela ação citada,}$$

$$\phi_x(\bar{a}) = \bar{a} \quad \forall x \in \langle d, e \rangle,$$

$$\bar{a} \in Z\left(\frac{G}{Z(G)}\right) \text{ e } \langle \bar{a} \rangle < \frac{H}{Z(G)} \text{ e } \langle \bar{a} \rangle \triangleleft \frac{G}{Z(G)} \Rightarrow \bar{a} = 1$$

e se  $\ker \phi \neq \{1\}$ , então  $\ker \phi = A_3$  e teríamos uma representa-  
ção irreduzível não trivial de  $\frac{\Sigma_3}{A_3} \cong Z_2$  sobre  $GF[2] = F_2$ ,  
que não é possível.

Temos então que  $\frac{H}{Z(G)}$  é um módulo irreduzível de  $F_2 | \Sigma_3 |$ .

ou seja de  $\frac{F_2[\Sigma_3]}{\text{Rad } F_2[\Sigma_3]}$ .

$$\text{Ora } \text{Rad } F_2[\Sigma_3] = \langle \{1 + (12); 1 + (13); 1 + (23)\} \rangle.$$

Pois existem pelo menos duas representações irredu-  
zíveis de  $\Sigma_3$ ; a trivial e a ação de  $\Sigma_3$  no grupo de Klein  $V_4$   
como subgrupo normal de  $\Sigma_4$  e então

$$\text{Dim}_{GF[2]} \left[ \frac{F_2[\Sigma_3]}{\text{Rad } F_2[\Sigma_3]} \right] \geq 3.$$

$$\text{Como } \langle \{1 + (12); 1 + (13); 1 + (23)\} \rangle < \text{Rad } F_2 | \Sigma_3 |,$$

temos então que só existe uma representação irreduzível não  
trivial de  $\Sigma_3$  sobre  $GF(2)$  que é aquela de  $\Sigma_3$  no grupo  
de Klein e concluimos que  $\frac{G}{Z(G)}$  é isomorfo ao produto semi-di-  
reto de  $\Sigma_3$  por  $\frac{H}{Z(G)}$  que é o produto semi-direto de  $\Sigma_3$  por  
 $V_4$ , onde a ação de  $\Sigma_3$  sobre  $V_4$  é irreduzível logo  $\frac{G}{Z(G)} \cong \Sigma_4$ .

Agora vou demonstrar que  $G \cong \Sigma_4$ . Temos que existe  
um epimorfismo  $\psi : G \longrightarrow \Sigma_4$  tal que  $\text{Ker } \psi = Z(G)$ .

$$\text{Seja } \bar{D} = \psi(D) \dots$$

Temos que se  $d_1 d_2 \in D$ ;  $d_1 \neq d_2 \Rightarrow \psi(d_1) \psi(d_2) = \psi(d_1 d_2) \neq 1$ ,  
pois  $d_1 d_2 \in D^2$  e  $D^2 \cap Z(G) = \{1\}$ , isto é  $\psi(d_1) \neq \psi(d_2)$ .

$$\text{Se } |d_1 d_2| = 2 \Rightarrow |\psi(d_1 d_2)| = 2$$

$$|d_1 d_2| = 3 \Rightarrow |\psi(d_1 d_2)| = 3$$

temos que  $\psi(D)$  é um conjunto de elementos de ordem 2 de  $\Sigma_4$ .

$$\text{Seja } \bar{d}_1 = \psi(d_1) \in \psi(D) \text{ e } \bar{g}_1 = \psi(g_1) \in \Sigma_4$$

$$\bar{g}_1 \bar{d}_1 \bar{g}_1 = \psi(g_1) \psi(d_1) \psi(g_1) = \psi(g_1 d_1 g_1) \in \psi(D).$$

Ou seja  $\psi(D)$  é uma classe de 3 transposições conjugadas de  $\Sigma_4$ .

Temos que  $\psi(D) = C(12) = (12)^{\Sigma_4}$  e como  $\psi$  conserva a ordem dos produtos de elementos de  $D$  temos que  $G \cong \Sigma_4$ .

Fim da demonstração do lema 1.

Temos então provado que  $G' = \langle T \rangle = \langle W \rangle$ .

Afirmo que então  $G'' = G'$  (o que implica que  $G$  não é solúvel).

Com efeito:

$$G'' \neq G' \Rightarrow G'' \cap D^2 = \{1\} \Rightarrow G'' \subset Z(G).$$

Lembramos que  $\frac{G'}{Z(G)}$  é um subgrupo minimal normal de  $\frac{G}{Z(G)}$ .

Teríamos que  $\frac{G'}{Z(G)}$  seria comutativo e caracteristicamente simples logo sua ordem seria potência de um primo, mas como  $T \notin Z(G)$  e  $W \notin Z(G)$ ,  $\frac{G'}{Z(G)}$  tem elementos de ordens 2 e 3.

Então  $G' = G''$  não é um p-grupo e todo subgrupo de  $G$  normal que contém  $G'$  está contido no centro de  $G$ . Como  $O_2(G)$  e  $O_3(G)$  não contém  $G'$  temos que  $O_2(G) \leq Z(G) \leq O_3(G)$ .

Temos provado que todo grupo que satisfaz a equação de classes dada, verifica as hipóteses do teorema de Fischer.

Agora estamos em condições de demonstrar o teorema.

Seja  $G$  um dos grupos mencionados no teorema.

Suponhamos em primeiro lugar que  $G$  é solúvel. Então vale uma das possibilidades seguintes

- 1)  $G \cong \{1\} \cong {}^{\mu}0^{\circ}(2,3) \cong 0^-(3,3)$
- 2)  $G \cong \Sigma_2 \cong 0^+(2,2)$
- 3)  $G \cong \Sigma_3 \cong 0^-(2,2) \cong \text{Sp}(2,2) \cong \text{PSU}(2,2)$
- 4)  $G \cong \Sigma_4 \cong 0^+(3,3)$
- 5)  $G \cong 0^+(4,2) \cong L_2(2) \times L_2(2) \cong \Sigma_3 \times \Sigma_3$
- 6)  $G \cong \text{PSU}(3,2)$ .

Já sabemos que os 4 primeiros casos são grupos caracterizados por sua tábua de caracteres.

No 5º caso, temos que  $G \cong \Sigma_3 \times \Sigma_3$  e não é difícil mostrar que o produto direto de 2 grupos caracterizados por tábua de caracteres é um grupo caracterizado por tábua de caracteres [7].

Para o 6º caso existe uma demonstração curta e simples na referência [8] pág. 237.

Se  $G$  é não solúvel,  $G$  é gerado por uma classe  $D$  de 3-transposições conjugadas,  $Z(G) = \{1\}$  e  $\hat{D}^2 = |D| 1 + 2 \hat{T} + 3 \hat{W}$  logo se  $H$  é um grupo com a mesma tábua de caracteres de  $G$  teremos pela proposição 1 parte 3, do capítulo 1, que  $Z(H) = 1$  e ainda  $H$  será simples se e só se  $G$  o for.

Temos então que analisar 2 hipóteses distintas

I)  $G$  é simples. Então vale uma das seguintes afirmações:

- a)  $G \cong \text{Sp}(2n, 2) \quad n \geq 3$
- b)  $G \cong \text{PSU}(n, 2) \quad n \geq 4$
- c)  $G \cong 0^+(2n + 1, 3) \cong P \Omega^-(2n + 1, 3) \quad n \geq 2$
- d)  $G \cong \text{Fi}_{22}$
- e)  $G \cong \text{Fi}_{23}$ .

Mostraremos no apêndice que excetuando-se a coincidência ( $\text{PSU}(4, 2) \cong 0^+(5, 3)$ ) esses grupos têm todos ordens distintas. Então pela proposição 1; parte 1, do capítulo 1; temos que eles são todos caracterizados por suas tábuas de caracteres.

II)  $G$  não é simples.

Então temos que ter  $G'$  simples e  $|G : G'| = 2$  e acontece um dos casos abaixo:

- a)  $G \cong \Sigma_n \quad n \geq 5$  e  $G' \cong A_n$
  - b)  $G \cong 0^\mu(2n, 2)$  e  $G' \cong P \Omega^\mu(2n, 2) \quad n \geq 3$
  - c)  $G \cong 0^-(2n + 1, 3)$  e  $G' \cong P \Omega^-(2n + 1, 3) \quad n \geq 2$
  - d)  $G \cong {}^\mu 0(2n, 3)$  e  $G' \cong P \Omega^\mu(2n, 3) \quad n \geq 3$ .
- Se  $n = 2$  então  $G' \cong P \Omega^-(2n, 3)$ .
- e)  $G \cong \text{Fi}_{24}$ .

No caso a o teorema já foi demonstrado no capítulo 1. Para os outros casos mostraremos no apêndice que todos eles têm ordens distintas salvo coincidências devido aos isomorfismos.

$$\Sigma_5 \cong 0^-(4, 2), \quad \Sigma_6 \cong {}^+0(4, 3) \cong S_p(4, 2), \quad \Sigma_8 \cong 0^+(6, 2).$$

Então novamente pelo teorema 1, do capítulo 1, parte 1, dois desses grupos nunca têm a mesma tábua de caracteres, salvo nos isomorfismos citados ■.

## Apêndice

Neste apêndice nós provaremos os dois teoremas seguintes:

I) Teorema 1. Exceto o caso dos grupos  $PSU(4,2)$  e  ${}^+O(5,3)$  que são isomorfos, não existe nenhuma coincidência entre as ordens dos seguintes grupos:

$$1) G = Sp(2n,2) \quad n \geq 3; \quad |G| = 2^{n^2} \prod_{i=1}^n (2^{2i}-1) < 2^{n(2n+2)}.$$

$$2) G = PSU(n,2) \quad n \geq 4; \quad |G| = \frac{1}{d} 2^{\frac{n(n-1)}{2}} \prod_{i=1}^n (2^i - (-1)^i) < q^{n^2-1}, d=(n,3).$$

$$3) G = O^+(2n+1,3) \cong P\Omega^-(2n+1,3) \quad n \geq 2;$$

$$|G| = \frac{1}{2} 3^{n^2} \prod_{i=1}^n (3^{2i} - 1) < 3^{n(2n-1)}.$$

$$4) G \cong Fi_{22}; \quad |G| = 2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13.$$

$$5) G \cong Fi_{23}; \quad |G| = 2^{18} \cdot 3^{28} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23.$$

II) Teorema 2. Não existe nenhuma coincidência entre as ordens dos seguintes grupos:

$$1) G = P\Omega^{\mu}(2n,2) \quad n \geq 3; \quad |G| = 2^{n(n-1)} (2^{n-\mu}) \prod_{i=1}^{n-1} (2^{2i}-1) < 2^{n(2n-1)}.$$

$$2) G = P\Omega^-(2n+1,3) \quad n \geq 2; \quad |G| = \frac{1}{2} 3^{n^2} \prod_{i=1}^n (3^{2i}-1) < 3^{n(2n-1)}.$$

$$3) G = P\Omega^{\mu}(2n,3) \quad n \geq 3; \quad |G| = \frac{1}{d} 3^{n(n-1)} (3^{n-\mu}) \prod_{i=1}^{n-1} (3^{2i}-1) < 3^{n(2n-1)}; \quad d=(3,n).$$

O que faremos aqui é uma adaptação aos nossos casos dos dois belíssimos trabalhos de Emil Artin citados nas

referências [1], [2].

A) Preliminares: Sobre polinômios ciclotômicos

I) Notações, Definições e Comentários:

$\psi_n(x)$  denotará o n-ésimo polinômio ciclotômico e  $\phi_n(x; y) = y^{y(n)} \phi_n(x/y)$  a forma homogênea associada a ele.

Sejam a e b inteiros satisfazendo  $|a| \geq |b| + 1 \geq 2$  e seja p um número primo.

Se  $p \mid a^n - b^n$  então  $p \nmid a \iff p \nmid b$ .

Se  $p \mid a^n - b^n$ ,  $p \nmid a$  e  $p \nmid b$  então  $a^n - b^n \equiv 0 \pmod{p}$  e  $\frac{a^n}{b^n} \equiv 1 \pmod{p}$ .

Em toda a parte A, f denotará a ordem de  $\frac{a}{b}$  módulo p. Temos que  $p \mid a^n - b^n \iff f \mid n$ .

Temos então que vale o seguinte resultado  $p \mid \phi_n(a, b) \implies f \mid n$ .

Examinaremos no que se segue condições para a validade da recíproca desta implicação.

$\text{ord}_p m$  indicará o expoente da mais alta potência de p que divide m; assim  $p^{\text{ord}_p m} \mid m$  e  $p^{\text{ord}_p m + 1} \nmid m$ .

Temos que  $(\frac{a}{b})^{p-1} \equiv 1$  logo  $f \mid p-1$  e portanto  $\text{ord}_p f = 0$ .

Lema 1: Seja p ímpar e f definido acima então:

a) Se  $f \nmid n$  então  $\text{ord}_p(a^n - b^n) = 0$

b) Se  $f \mid n$  então  $\text{ord}_p(a^n - b^n) = \text{ord}_p(a^f - b^f) + \text{ord}_p n$

A parte a) foi mostrada implicitamente nas observações acima.

Seja agora  $f \mid n$  e escrevamos:  $n = f p^i m$ ,  $p \nmid m$  e seja  $r = f p^i$ .

Se  $m > 1$  temos:

$$\begin{aligned} \frac{a^n - b^n}{a^r - b^r} &= \frac{[(a^r - b^r) + b^r]^m - b^{rm}}{a^r - b^r} \\ &= \frac{\sum_{j=0}^m \binom{m}{j} (a^r - b^r)^{m-j} b^{rj} - b^{rm}}{a^r - b^r} \\ &= \sum_{j=0}^{m-1} \binom{m}{j} (a^r - b^r)^{m-(j+1)} b^{rj} \\ &= \sum_{j=0}^{m-2} \binom{m}{j} (a^r - b^r)^{m-(j+1)} \cdot b^{rj} + m b^{r(m-1)}. \end{aligned}$$

Temos que  $p$  divide a primeira parcela mas não a segunda, isto é  $p \nmid \frac{a^n - b^n}{a^r - b^r}$  e concluímos que  $\text{ord}_p(a^n - b^n) = \text{ord}_p(a^r - b^r)$ .

Suponhamos agora que  $m=1$  isto é:

$n = f p^i$  e seja  $s = f p^{i-1}$

$$\frac{a^n - b^n}{a^s - b^s} = \sum_{j=0}^{p-2} \binom{p}{j} (a^s - b^s)^{p-(j+1)} \cdot b^{sj} + p b^{s(p-1)}$$

Como  $p \geq 3$  temos que a 1ª parcela é divisível por  $p^2$  mas a segunda não é e temos que  $\text{ord}_p(a^n - b^n) = \text{ord}_p(a^s - b^s) + 1$ .

Por indução em  $i$  completamos a demonstração.

Lema 2: Seja  $p$  ímpar e  $f$  definido acima então:

$\text{ord}_p \phi_f(a, b) > 0$ ;  $\text{ord}_p \phi_{fp^i}(a, b) = 1$  se  $i > 0$  e em todos os outros casos  $\text{ord}_p \phi_n(a, b) = 0$ .

Demonstração: Seja  $n = f p^i m$ ;  $p \nmid m > 1$  e  $r = f p^i$  já vimos que

$$p \nmid \frac{a^n - b^n}{a^r - b^r}, \text{ mas } \phi_n(a, b) \mid \frac{a^n - b^n}{a^r - b^r} \text{ logo } \text{ord}_p \phi_n(a, b) = 0$$

nesse caso.

Se  $f \nmid n$ , como  $\phi_n(a, b) \mid a^n - b^n$  temos que  $\text{ord}_p \phi_n(a, b) = 0$ .

Seja agora  $n = f p^i$  ( $i \geq 1$ ) e seja  $s = f p^{i-1}$ .

Temos que

$$p \mid \frac{a^n - b^n}{a^s - b^s} = \prod_{\substack{d \mid n \\ d \nmid s}} \phi_d(a, b) \text{ e o \u00fanico fator } \phi_d(a, b) \text{ tal}$$

$$\text{que } f \mid d \text{ \u00e9 o fator } \phi_n(a, b) \text{ logo } \text{ord}_p \phi_n(a, b) = \text{ord}_p \frac{a^n - b^n}{a^s - b^s} = 1.$$

Finalmente, no caso  $n = f$  temos que

$$p \mid a^f - b^f = \prod_{t \mid f} \phi_t(a, b) \text{ mas } \phi_t(a, b) \mid a^t - b^t \text{ logo se } t < s$$

$$\text{ord}_p \phi_t(a, b) = 0 \text{ e temos que } \text{ord}_p \phi_f(a, b) > 0.$$

Precisamos agora analisar o caso  $p = 2$ .

Os argumentos anteriores valem sem nenhuma modificação para provar o seguinte fato:

se  $n = m 2^i$ ,  $m > 1$  \u00edmpar  $i \geq 1$  ent\u00e3o:  $2 \nmid \frac{a^n - b^n}{a^{2^i} - b^{2^i}}$  e portanto

$\text{ord}_2 \phi_n(a, b) = 0$  e  $\text{ord}_2(a^n - b^n) = \text{ord}_2(a^{2^i} - b^{2^i})$ . Agora se

$$n = 2^i \quad i \geq 1 \text{ temos } \phi_n(a, b) = a^{2^{i-1}} + b^{2^{i-1}} = \frac{a^{2^i} - b^{2^i}}{a^{2^{i-1}} - b^{2^{i-1}}}.$$

Seja  $i > 1$  e escrevamos  $a = 2k + 1$   $b = 2s + 1$

$$\phi_n(a, b) = \sum_{j=0}^{2^{i-1}-1} 2^j \binom{2^{i-1}}{j} (k^j + s^j)$$

$$= 2 + \binom{2^{i-1}}{1} 2(k + s) + \sum_{j=2}^{2^{i-1}-1} 2^j \binom{2^{i-1}}{j} (k^j + s^j)$$

que é divisível por 2 mas não por 4 e portanto temos concluído que  $\text{ord}_2 \phi_n(a,b) = 1$  e ainda  $\text{ord}_2(a^{2^i} - b^{2^i}) = \text{ord}_2(a^{2^{i-1}} - b^{2^{i-1}}) + 1$ .

Por indução concluímos que

$$\text{ord}_2(a^{2^i} - b^{2^i}) = \text{ord}_2(a^2 - b^2) + (i - 1).$$

Agora temos que  $\phi_2(a,b) = a - b$  e  $\phi_1(a,b) = a + b$  e um e somente um desses números é congruo a 2 módulo 4 isto é tem ordem 1. (Isso vem do fato deles serem pares mas sua soma é o dobro de um ímpar.)

Reformulamos a seguir os resultados obtidos acima na forma de uma proposição.

Proposição 1:

A) Seja  $p$  ímpar e  $f$  definido acima então

1) Se  $f \mid n$ , então  $\text{ord}_p(a^n - b^n) = \text{ord}_p(a^f - b^f) + \text{ord}_p n$ . Em todos os outros casos  $\text{ord}_p(a^n - b^n) = 0$ .

2)  $\text{ord}_p(\phi_f(a,b)) = \text{ord}_p(a^f - b^f) > 0$ ,  $\text{ord}_p \phi_{fp^i}(a,b) = 1$  se  $i > 1$ . Em todos os outros casos  $\text{ord}_p(\phi_n(a,b)) = 0$ .

B) Seja  $p = 2$  se  $i > 1$ ,  $2 \nmid k$ .

$$1) \text{ord}_2(a^{2^i \cdot k} - b^{2^i \cdot k}) = \text{ord}_2(a^2 - b^2) + (i - 1)$$

$$= \max \{ \text{ord}_2(a + b), \text{ord}_2(a - b) \} + i.$$

$$2) \text{ord}_2 \phi_2(a,b) = 1 \iff \text{ord}_2 \phi_1(a,b) > 1.$$

$$3) \text{ord}_2 \phi_1(a,b) = 1 \iff \text{ord}_2 \phi_2(a,b) > 1.$$

$$4) \text{ord}_2 \phi_{2^i}(a,b) = 1 \text{ se } i > 1.$$

Em todos os outros casos temos  $\text{ord}_p \phi_n(a,b) = 0$ .

B) Demonstração do Teorema 1.

Exceto quando explícito o contrário, todos os lemas seguintes se referirão aos grupos lineares 1), 2), 3).

Definição 1: Se  $G$  é um grupo linear sobre um corpo finito  $K$  chamaremos de característica de  $G$  a característica de  $K$ .

Definição 2: Se  $p$  é um primo qualquer e  $N$  um número natural chamaremos de  $p$ -contribuição a  $N$  a maior potência de  $p$  que divide  $N$ . E denotaremos  $\gamma(p)$ .

Assim, dizer que a  $p$ -contribuição a  $N$  é um número  $b$  significa que  $p^{\text{ord}_p N} = b$ .

Lema 3: Para os grupos  $Sp(2n, 2)$  ( $n \geq 3$ ),  $PSU(n, 2)$  ( $n \geq 5$ ),  $O^+(2n + 1, 3)$  ( $n \geq 2$ ), a característica  $p$  é o primo cuja contribuição a ordem de  $G$  é maior.

Demonstração: Suponhamos que  $p_1 \mid |G|$  e  $p_1 \neq \text{carac } G$  e seja  $\gamma(p_1)$  a  $p_1$ -contribuição a  $|G|$ .

Temos que  $\gamma(p_1) \mid \Pi = (a^n - 1)(a^{n-1} - 1) \dots (a - 1)$  onde  $a = 4, -2, 9$  respectivamente.

Seja  $f = \text{ord } a \pmod{p_1}$ , as parcelas  $a^{if} - 1$  com  $0 \leq i \leq \left[ \frac{n}{f} \right]$  são as únicas que dão alguma  $p_1$ -contribuição a  $\text{ord } \Pi$ .

Temos que  $\text{ord}_{p_1}(a^{if} - 1) = \text{ord}_{p_1}(a^f - 1) + \text{ord } i$ , (se  $p_1$  é ímpar; o que certamente acontece no primeiro e segundo caso) e se  $p_1 = 2$   $\text{ord}_2(a^i - 1) \leq \max\{\text{ord}(a-1), \text{ord}_2(a+1)\} + \text{ord}_2 i$ . Os termos  $p_1^{\text{ord}_{p_1} i}$  dão uma contribuição menor ou igual a  $\text{ord} \left[ \frac{n}{f} \right]!$  e a ordem dessa contribuição é menor ou igual à soma.

$$\left[ \frac{n}{fp_1} \right] + \left[ \frac{n}{fp_1^2} \right] + \dots + \left[ \frac{n}{fp_1^k} \right] \leq \frac{n}{fp_1} + \frac{n}{fp_1^2} + \dots + \frac{n}{fp_1^k} = \frac{n}{f(p_1-1)} \leq \frac{n}{p_1-1}$$

e então temos que esse termos contribuem com um fator menor

ou igual a  $p_1^{\frac{n}{p_1-1}} = \left( p_1^{\frac{1}{p_1-1}} \right)^n$  (observe-se que esta é uma função decrescente de  $p_1$ .)

Agora analisemos a contribuição do termo  $\text{ord}_{p_1}(a^f - 1)$  em cada caso.

Comecemos com o 2º caso (i.e.  $G = \text{PSU}(n, 2)$   $n \geq 4$ ), onde  $a = -2 = -p$ .

Podemos supor  $p_1$  ímpar e então:

$$\text{ord}_{p_1}((-p)^f - 1) \leq \frac{\log(p^f + 1)}{\log p_1} \leq f \frac{\log(p + 1)}{\log p_1}$$

e esses termos contribuem para  $|\text{PSU}(n, 2)|$  com um fator menor ou igual a

$$\left[ \frac{n}{f} \right] f \frac{\log(p + 1)}{\log p_1} \leq \frac{\log(p + 1)^n}{\log p_1} \leq (p + 1)^n.$$

Nos casos  $G = \text{Sp}(2n, 2)$  ( $n \geq 3$ ) e  $G = \text{O}^+(2n+1, 3)$  ( $n \geq 2$ ),  $a = p^2$ .

Se  $p_1$  é ímpar então  $p_1$  divide apenas um dos fatores de  $(a^f - 1) = (p^f - 1)(p^f + 1)$  e vale a mesma estimativa.

Se  $p_1 = 2$  o que só pode acontecer quando  $G = \text{O}^+(2n+1, 3)$ , temos que  $\max\{\text{ord}_2(p^f + 1), \text{ord}_2(p^f - 1)\} = 3$  e portanto esses termos contribuem para a ordem de  $G$  com um fator menor ou igual a  $2^{3n}$ .

Em resumo temos:

Se  $p_1$  é ímpar (o que certamente acontece nos dois primeiros casos) então

$$\gamma(p_1) \leq p_1^{\frac{n}{p_1-1}} (p+1)^n \leq 3^{\frac{n}{2}} \cdot (p+1)^n$$

Se  $p_1 = 2$  temos que

$$\gamma(p_1) \leq 2^n \cdot 2^{3n} = 2^{4n} = 4^n \cdot 4^n.$$

Mostraremos o Teorema agora em cada caso.

Se  $\gamma(p_1) \geq \gamma(p)$  teríamos:

No caso  $G = \text{Sp}(2n, 2)$ :

$$2^{n^2} < 3^{n/2} \cdot 3^n \text{ e então } 2^n < 3^{1/2} \cdot 3 \text{ absurdo (pois } n \geq 3).$$

No caso  $G = \text{PSU}(n, 2)$ :

$$2^{\frac{n(n-1)}{2}} < 3^{\frac{n}{2}} \cdot 3^n \text{ e então } 2^{\frac{n-1}{2}} < 3^{\frac{1}{2}} \cdot 3 \implies$$

$$\implies \frac{n-1}{2} \leq 2 \implies n \leq 5.$$

Basta considerar separadamente o caso  $n = 5$ .

No caso  $G = O^+(2n+1, 3)$ :

Se  $p_1$  é ímpar:

$$3^{n^2} < 3^{n^2/2} \cdot 3^n \implies 3^n < 3^{1/2} \cdot 3 \implies n = 1.$$

Se  $p_1 = 2$ :

$$3^{n^2} < 4^n \cdot 4^n \implies 3^n < 16 \implies n = 1 \text{ ou } n = 2$$

e basta verificar diretamente o caso  $n = 2$ .

Este lema mostra que o Teorema 1 vale para grupos com características distintas.

Agora vamos mostrar que não há coincidência entre as ordens de dois grupos com a mesma característica ( $= 2$ ).

Temos que

$$|\text{Sp}(2n, 2)| = 2^{n^2} \prod_{i=1}^n (4^i - 1)$$

$$|\text{PSU}(n, 2)| = \frac{1}{d} 2^{\frac{n(n-1)}{2}} \prod_{i=1}^n (2^i - (-1)^i), \quad d = (n, 3) \quad \text{e}$$

sabemos que

$$2^i - 1 = \prod_{s|i} \phi_s(2)$$

$$2^i + 1 = \prod_{\substack{s|2i \\ s+i}} \phi_s(2)$$

Seja então  $\alpha$  o maior valor de  $s$  tal que  $\phi_s(2)$  divide o número  $|G|$  e  $\beta$  o segundo maior.

Para  $G = Sp(2n, 2)$  temos que  $\alpha = 2n$ ,  $\beta = 2(n-1)$ .

Para  $G = PSU(n, 2)$  temos:

- 1) Se  $n = 3$  então  $|G| = 2^3(2^3 + 1)$  e  $\alpha = 6$ ,  $\beta = 2$
- 2) Se  $n$  é ímpar e  $n \geq 5$  então  $\alpha = 2n$  e  $\beta = 2(n, 2)$  pois  $(n-1) > 2(n-2) \iff n-1 > 2n-4 \iff 3 > n$ .
- 3) Se  $n = 4$  então  $|G| = 2^6(2^4 - 1)(2^3 + 1) \cdot 3$  e  $\alpha = 6$ ,  $\beta = 4$ .
- 4) Se  $n$  é par  $n \geq 6$  então

$$|G| = 2^{\frac{n(n-1)}{2}} (2^n - 1)(2^{n-1} + 1)(2^{n-2} - 1) + \dots + \frac{3}{d} \quad \text{e} \quad \text{então}$$

$$\alpha = 2(n-1) \text{ e } \beta = 2(n-3).$$

Podemos construir a seguinte tabela:

G		$\alpha$	$\beta$	$\alpha - \beta$
$Sp(2n, 2)$		$2n$	$2(n-1)$	$2$
$PSU(n, 2)$	$n$ ímpar	$2n$	$2(n-2)$	$4$
$PSU(4, 2)$		$6$	$4$	$2$
$PSU(n, 2)$	$n$ par $n \geq 6$	$2(n-1)$	$2(n-3)$	$4$

Vemos que a única possibilidade de coincidência seria de  $|PSU(4, 2)|$  com algum  $|Sp(2n, 2)|$  e teríamos que ter  $\alpha = 2n = 6$  que implica  $n = 3$ . Mas nesse caso a 2 contribuição é distinta.

Assim fica demonstrado que os 3 tipos de grupos lineares citados têm sempre ordens distintas. Vamos demonstrar agora que eles têm ordens distintas de  $|Fi_{22}|$  e  $|Fi_{23}|$ .

Temos

$|Fi_{22}| = 2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$  e o número primo cuja contribuição é maior, é 2. Mas temos:

- a)  $|Fi_{22}| \neq |Sp(2n, 2)|$ , pois a 2-contribuição ã ordem de um

grupo do tipo  $Sp(2n, 2)$  tem expoente quadrado perfeito e 17 não o é.

b)  $|Fi_{22}| = |PSU(n, 2)| \Rightarrow \frac{n(n-1)}{2} = 17$  e essa equação não tem solução inteira.

$|Fi_{23}| = 2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \cdot 23$ . e a maior contribuição é a do primo 3. Mas  $|Fi_{23}| = |O^+(2n+1, 3)|$  implica  $n^2 = 18$  e novamente essa equação não tem solução inteira.

A demonstração do teorema 1 está completa.

### C) Demonstração do Teorema 2.

Tudo se passa como no caso do teorema 1. Omitiremos maiores detalhes, para os quais remetemos o leitor aos trabalhos de Artin ([1], [2]).

Pode-se fazer uma análise idêntica à anterior mostrando que agora também vale o lema 3, isto é: Para os 3 primeiros tipos de grupos, a contribuição do primo  $p$  é a maior das contribuições de todos os primos; elimina-se a possibilidade de coincidência do primeiro com qualquer dos outros dois.

Em seguida fazendo uma análise de  $\alpha$  e  $\beta$ , como anteriormente mostramos que esses 3 grupos primeiros têm todos ordens distintas.

E temos que a maior contribuição à  $|Fi_{24}|$  é a do primo 3. Como a equação  $n(n-1) = 16$  não tem solução inteira  $|Fi_{24}| \neq |P \Omega^u(2n, 3)|$ .

Se  $|P \Omega(2n+1, 3)| = |Fi_{24}|$  então  $n^2 = 16$  e  $n = 4$ . Como  $|P \Omega^4(9, 3)| \neq |Fi_{24}|$ , tampouco há coincidência neste caso.

Referências

- [1] E. Artin: The orders of the linear groups. Comm Pure Appl. Math 8, 355-366 (1955)
- [2] E. Artin: The orders of the classical simple groups. Comm. Pure Appl Math 8, 455-472 (1955)
- [3] B. Fischer: Finite groups generated by 3-transposition I. Inventiones Math 13, 232-244 (1971) MR 45 # 3557.
- [4] D. Gorenstein: The classifications of finite simple groups. Bulletin of the Am. Math Society 1, 43-199 (1979)
- [5] G. Glaubermann: Central Elements in core-free groups. Journal of Algebra 4, 403-420 (1966)
- [6] G. Higman: Construction of simple groups from character tables. Finite simple groups ed. M.B. Powell, Academic Press London, 1971
- [7] P. J. Lambert: Characterizing groups by their character table I. Quart J. Math Oxford (2) 23 427-433 (1972)
- [8] P. J. Lambert: Characterizing groups by their character table II. Quart J. Math Oxford (2) 24 223-240 (1973)
- [9] H. Nagao: On the groups with the same table of characters as symmetric groups J. Inst. Polytechnic. Osaka City Univ 8 1-8 (1957) MR 19-387
- [10] Toyama: On the groups with the same table of characters as alternating groups, Osaka J. Math 1 (1964) 91-101
- [11] H. Pahlings: On the character table of finite groups ge

nerated by 3-transposition, Communications in Algebra 2  
(2) 117-131 (1974)

- [12] H. Pahlings: Characterization of groups by their character table I. Commun. Algebra 4 (1976) 111-153
- [13] H. Pahlings: Characterization of groups by their character table II. Commun. Algebra 4 (2) 155-178 (1976)
- [14] T. Yokonuma: On a property of some generalized symmetric groups. J. Fac. Sci. Univ. Tokio Sec. I, 12 193-211 (1965)  
MR 32 =# 7650

Temos ainda a seguinte bibliografia:

- [15] E. Artin: Geometric Algebra, Interscience Tracts n<sup>o</sup> 3 New York. London Interscience Publ (1957)
- [16] L. E. Dickson: Linear groups with an exposition on the Galois field Theory. Dover Publication Inc 1958 N.Y.
- [17] J. Dieudonné: Sur les groupes classiques Publication de L'institut de Math de L'univ. de Strasbourg VI, Hermann Paris (1973)
- [18] J. Dieudonné: La Géométrie des groupes classiques Ercy der Math. New Folge Helms Berlin (Springer) (1955)
- [19] W. Feit: Characters of Finite groups. New York Yale University, W. A. Benjamin, Inc (1967)
- [20] A. Gonçalves: Tópicos em Representação de Grupos. 9<sup>o</sup> Colóquio Brasileiro de Matemática, IMPA (1973)
- [21] D. Gorenstein: Finite groups, Harper and Row, New York (1968)

[22] H. A. Merklen Goldschmidt: Notas do Curso de Representa  
ção de Grupos, ministrado no IME-USP, (1978)