Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Dois Teoremas de Brauer: Demonstração e Aplicações

Eliana Carla Rodrigues

Brasília
2013

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Dois Teoremas de Brauer: Demonstração e Aplicações

Eliana Carla Rodrigues

Dissertação apresentada como requisito parcial para
a obtenção do título de Mestre em Matemática.

Orientador
Prof. Dr. Marco Antonio Pellegrini

Brasília
2013

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Dois Teoremas de Brauer: Demonstração e Aplicações

Eliana Carla Rodrigues*

Dissertação apresentada como requisito parcial para
a obtenção do título de Mestre em Matemática.

Comissão examinadora:

Marco Antonio Pellegrini
___
Prof. Dr. Marco Antonio Pellegrini (Orientador)
MAT/UnB

Aline Gomes S. Pinto
___
Profa. Dr. Aline Pinto
MAT/UnB

SdM
___
Prof. Dr. Csaba Schneider MAT/UFMG

Brasília, 16 de Dezembro de 2013.

*A autora foi bolsista da Capes durante a elaboração desta dissertação.

Aos meus pais, Eva e Paulo,
e ao meu irmão Carlos.

Agradecimentos

À minha mãe, pelo amor incondicional, pela amizade, por sempre me apoiar e acreditar nas minhas decisões. Ao meu pai, por me ensinar a fazer minhas próprias escolhas. Ao meu irmão, agradeço o apoio e exemplo.

Aos meus tios e tias, à minha avó Aparecida, aos meus primos e primas. Agradeço por todos os momentos especiais que passamos juntos.

À Leila, que se fez minha irmã e devolveu a alegria da minha mãe por meio dos carinhos da Maria Júlia e da Ana Lara.

Ao professor Marco Pellegrini, por sua dedicação na realização deste trabalho, pela experiência adquirida com seus ensinamentos, pela paciência e principalmente pela amizade.

Aos professores da banca examinadora, Aline Pinto e Csaba Schneider, agradeço pelas sugestões.

Ao professor Jhone Caldeira do IME-UFG, por sempre acreditar em mim com palavras estimulantes de confiança.

À minha amiga Lais, por ser sempre a minha companheira dos bons e maus momentos. Por todas as vezes que não me deixou desistir e me ajudou a ser forte.

À minha "amiga-irmã" Nadya, pela amizade que conseguimos manter mesmo com a distância. Agradeço pelas conversas e orações.

Aos meus amigos Valdiego, Éder e Wildes. Por serem mais que amigos e sempre me apoiarem nos momentos de dificuldade e se alegrarem comigo nos momentos felizes.

Aos colegas da Pós-Graduação do Departamento de Matemática-UnB. Em especial, Otto, Leo, Ilana, Valter, Saieny, José Carlos, Bruno, Daiane, Hiuri, Juliana, Lucimeire, Alex (Teló), Keidna, Camila, Alexandre, Fábio, Joab, Silvio, Jamer, Javier, Josimar, Julian, Jhoel e Jaime.

Aos funcionários do Departamento de Matemática-UnB, em especial, Bruna, Irene, Claudia, Tiago e Fabiana.

À Capes pelo apoio financeiro.

Resumo

Sejam G um grupo finito e R um subanel de $\mathbb{C}$ que contém $\mathbb{Z}$. Richard Brauer demonstrou que uma função de classe de G é um R-caráter generalizado se, e somente se, sua restrição a qualquer subgrupo elementar de G é uma R-combinação linear de caracteres irredutíveis desse subgrupo. Ele também demonstrou que todo caráter irredutível de G pode ser escrito como uma $\mathbb{Z}$-combinação linear de caracteres obtidos por indução sobre caracteres lineares de subgrupos elementares de G. Nesta dissertação, apresentamos as demonstrações destes dois fundamentais teoremas seguindo o livro de Isaacs.

Em seguida, demonstramos dois resultados que aprimoram o segundo Teorema de Brauer. O primeiro, devido a Wilde, considera a hipótese adicional que o grupo é solúvel e o segundo, demonstrado por van der Waall, considera o caso de caracteres não principais.

Para finalizar, apresentamos algumas aplicações desses importantes Teoremas de Brauer. Vamos definir uma particular função de classe e mostrar que um múltiplo apropriado dessa função é um caráter generalizado. Esta função de classe aparece em vários problemas computacionais e apresentamos um deles. Em particular, vamos mostrar que os grupos $PSp(4,3)$ e $Sp(4,3)$ não são $(2,3)$-gerados.

Abstract

Let G be a finite group and R be a subring of $\mathbb{C}$ such that $\mathbb{Z} \subseteq R$. Richard Brauer showed that a class function of G is a R-generalized character if, and only if, its restriction to any elementary subgroup of G is a R-linear combination of irreducible characters of this subgroup. Moreover, he showed that every irreducible character of G can be written as a $\mathbb{Z}$-linear combination of characters obtained by induction from linear characters of elementary subgroups of G. In this dissertation, we will present the proof of these fundamental theorems following Isaacs' book.

Afterwards, we will prove two results that improve the second Brauer's Theorem. The first one is a result of Wilde, obtained adding the hypothesis that the group is solvable. The second result, estabilished by van der Waall, considers characters that are not principal.

To conclude, we will present some applications of these important theorems due to Brauer. We will define a particular class function and show that an appropriate multiple of this function is a generalized character. This class function appears in many computational problems and we will present one of them. In particular, we will show that the groups $PSp(4,3)$ and $Sp(4,3)$ are both not $(2,3)$-generated.

Sumário

Introdução

O objetivo desta dissertação é estudar dois importantes teoremas de R. Brauer sobre os caracteres de um grupo finito. A demonstração desses teoremas será dada seguindo o livro de Isaacs [8] e difere da demonstração original do próprio Brauer.

Iniciamos apresentando o conceito de representação complexa de um grupo finito e observamos que essa representação é determinada, a menos de equivalência, por seu caráter. Assim, no decorrer do primeiro capítulo apresentamos alguns resultados sobre a teoria dos caracteres de grupos finitos, em particular, sobre a teoria de Clifford para indução de caracteres de subgrupos normais de um grupo finito. Estudaremos também as propriedades dos grupos elementares e quase-elementares.

No segundo capítulo, vamos demonstrar os Teoremas de Brauer. No Teorema de Brauer sobre caracterização dos caracteres, obtemos que uma dada função de classe é um caráter generalizado se, e somente se, sua restrição a qualquer subgrupo elementar é um caráter generalizado. No Teorema de Brauer sobre caracteres induzidos, vamos demonstrar que qualquer caráter irredutível de um grupo finito G pode ser escrito como uma $\mathbb{Z}$-combinação linear de caracteres induzidos de subgrupos elementares de G. Na seção 2.2, vamos apresentar um resultado de van der Waall [18] em que consideramos uma hipótese adicional ao caráter, exigindo que ele seja não principal. Mostramos que podemos escrevê-lo como uma $\mathbb{Z}$-combinação linear de caracteres monomiais de G, onde cada caráter monomial não contém 1_G como componente irredutível. Na seção 2.3, apresentamos um resultado de Wilde [19] em que consideramos G um grupo solúvel. Neste caso, vamos demonstrar que o grau de qualquer caráter irredutível de G divide $|G : E|$, onde E é um subgrupo elementar de G que contribui para escrevermos o caráter como soma de caracteres induzidos.

No terceiro capítulo, apresentamos algumas aplicações dos Teoremas de Brauer. Para as seções 3.1 e 3.2, temos como referência um artigo de Isaacs [9], no qual uma particular função de classe será de extrema importância. Vamos mostrar que um múltiplo adequado desta função é um caráter generalizado. Na seção 3.3, apresentamos uma aplicação computacional, onde utilizamos a função de classe definida na seção 3.1 para demonstrar que os grupos $PSp(4,3)$ e $Sp(4,3)$ não são $(2,3)$-gerados.

Capítulo 1

Preliminares sobre a teoria dos caracteres

Neste capítulo iremos apresentar alguns conceitos básicos da teoria ordinária dos caracteres de grupos finitos, conceitos que iremos usar em capítulos sucessivos. Nossa referência principal é o livro de Isaacs [8]. O leitor pode também consultar [3] e [7].

1.1 - Representações de Grupos e Caracteres

Definição 1.1. Sejam G um grupo finito, V um $\mathbb{C}$-espaço vetorial de dimensão finita e $GL(V)$ o grupo dos automorfismos de V. Uma $\mathbb{C}$-*representação* de G é um homomorfismo $\Phi : G \to GL(V)$.

Definição 1.2. Sejam V e W espaços vetoriais sobre $\mathbb{C}$ de dimensão finita e sejam $\Phi_1 : G \to GL(V)$ e $\Phi_2 : G \to GL(W)$ duas $\mathbb{C}$-representações de G. Dizemos que Φ_1 e Φ_2 são *equivalentes* se existe um isomorfismo $\tau : V \to W$ tal que para todo $g \in G$ e todo $v \in V$ temos

$$\Phi_1(g) \cdot v = (\tau^{-1}\Phi_2(g)\tau) \cdot v.$$

Se V tem dimensão n, então escolhendo uma base de V obtemos uma representação matricial

$$\Phi : G \to GL(n, \mathbb{C}),$$

em que $GL(n, \mathbb{C})$ denota o grupo das matrizes inversíveis $n \times n$ com entradas em $\mathbb{C}$. Observamos que se mudamos a base de V obtemos representações equivalentes.

Em geral, não é simples descrever a matriz de uma representação. Por outo lado, considerando apenas os traços dessas matrizes conseguimos informações necessárias para obter resultados sobre um dado grupo finito.

Definição 1.3. Seja Φ uma $\mathbb{C}$-representação de G. O $\mathbb{C}$-*caráter* de G determinado por Φ é a função $\chi : G \to \mathbb{C}$ dada por $\chi(g) = Tr(\Phi(g))$.

O caráter determinado por uma representação não depende da escolha da base de V, pois representações equivalentes determinam o mesmo caráter.

Como a característica de $\mathbb{C}$ é zero, observamos que a função constante zero não é um $\mathbb{C}$-caráter pois $\chi(1) = Tr(\Phi(1)) = Tr(Id) = n$, onde Φ é uma $\mathbb{C}$-representação de G que determina o caráter χ. Neste caso, dizemos que $\chi(1)$ é o grau de χ.

Definição 1.4.

(i) Um caráter é dito *linear* se tem grau 1.

(ii) A função $1_G : G \to \mathbb{C}$ definida por $1_G(g) = 1$, para todo $g \in G$ é um caráter de G, pois é o traço do homomorfismo $\Phi : G \to \mathbb{C}$ definido por $\Phi(g) = 1$. O caráter 1_G é chamado de $\mathbb{C}$-*caráter principal.*

Denotaremos por $Lin(G)$ o conjunto formado pelos caracteres lineares de G.

Lema 1.5. *Se Φ é uma $\mathbb{C}$-representação de G e χ é o caráter associado, então χ é constante sobre as classes de conjugação de G.*

Demonstração. Primeiramente notamos que se P é não singular, então $Tr(P^{-1}AP) = Tr(PP^{-1}A) = Tr(A)$.

Sejam $g, h \in G$,

$$\begin{aligned} \chi(h^{-1}gh) = &\ Tr(\Phi(h^{-1}gh)) = Tr(\Phi(h^{-1})\Phi(g)\Phi(h)) \\ = &\ Tr(\Phi(h)^{-1}\Phi(g)\Phi(h)) = Tr(\Phi(g)) \\ = &\ \chi(g). \end{aligned}$$

Portanto, para todo $g \in G$, a função χ é constante sobre a classe de conjugação $Cl(g)$ de G que contém g.

■

Observamos que se Φ_1 e Φ_2 são $\mathbb{C}$-representações de G de grau n_1 e n_2 respectivamente, então a função Φ defininda por

$$\Phi(g) = \begin{bmatrix} \Phi_1(g) & 0 \\ 0 & \Phi_2(g) \end{bmatrix}$$

é também uma $\mathbb{C}$-representação de G de grau $n_1 + n_2$. Isso prova que o conjunto dos $\mathbb{C}$-caracteres de G é fechado por adição pois,

$$Tr(\Phi(g)) = Tr(\Phi_1(g)) + Tr(\Phi_2(g)).$$

De agora em diante, usaremos a palavra caráter em vez de $\mathbb{C}$-caráter e a palavra representação em vez de $\mathbb{C}$-representação.

Agora vamos associar uma álgebra ao grupo finito G e mostrar como podemos identificar representações dessa álgebra com representações de G.

Definição 1.6. Seja G um grupo finito. O conjunto

$$\mathbb{C}[G] = \left\{ \sum_{g \in G} a_g g; a_g \in \mathbb{C} \right\}$$

é chamado de *álgebra de grupo* associada a G. As operações em $\mathbb{C}[G]$ são definidas da seguinte forma

$$\begin{aligned} \sum_{g\in G} a_g g + \sum_{g\in G} b_g g &= \sum_{g\in G} (a_g + b_g) g \\ \left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) &= \sum_{g\in G} c_g g, \qquad \text{onde } c_g = \sum_{\substack{h,k\in G \\ hk=g}} a_h b_k \\ \lambda \left(\sum_{g\in G} a_g g\right) &= \sum_{g\in G} (\lambda a_g) g, \qquad \lambda \in \mathbb{C}. \end{aligned}$$

Se identificarmos cada $g \in G$ com o elemento $\sum_{x\in G} a_x x \in \mathbb{C}[G]$, onde $a_x = \begin{cases} 1, & \text{se } x = g \\ 0, & \text{se } x \neq g \end{cases}$, podemos assumir que $G \subseteq \mathbb{C}[G]$.

Se $\Phi : G \to GL(V)$ é uma representação de G, podemos estender Φ a $\mathbb{C}[G]$ definindo o homomorfismo $\tilde{\Phi} : \mathbb{C}[G] \to End_{\mathbb{C}}(V)$ por

$$\tilde{\Phi}(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \Phi(g),$$

então $\tilde{\Phi}$ é uma representação de $\mathbb{C}[G]$. Reciprocamente, se

$$\tilde{\Phi} : \mathbb{C}[G] \to End_{\mathbb{C}}(V)$$

é uma representação de $\mathbb{C}[G]$, podemos restringir $\tilde{\Phi}$ a uma representação $\Phi : G \to GL(V)$. Dessa forma, podemos identificar $\tilde{\Phi}$ com Φ.

Notamos que podemos definir o caráter $\tilde{\chi} : \mathbb{C}[G] \to \mathbb{C}$ da seguinte forma,

$$\tilde{\chi}(\sum_{g\in G} a_g g) = Tr(\tilde{\Phi}(\sum_{g\in G} a_g g)).$$

Descreveremos agora como associar a uma representação um $\mathbb{C}[G]$-módulo e vice-versa.

Se $\Phi : G \to GL(V)$ é uma representação de G, para $v \in V$, defina $(\sum_{g\in G} a_g g)v = \sum_{g\in G} a_g \Phi(g)v$, então V é um $\mathbb{C}[G]$-módulo. De forma análoga, se V é um $\mathbb{C}[G]$-módulo de dimensão finita (como $\mathbb{C}$-espaço), para cada $g \in G$ defina $g_L : V \to V$ por $g_L(v) = gv$, então $\Phi : G \to GL(V)$ definida por $\Phi(g) = g_L$ é uma representação de G.

Pelo Lemma 1.2 em [3], observamos que módulos isomorfos correspondem a representações equivalentes e vice-versa.

Pelo Teorema de Maschke, [8, Theorem 1.9], a álgebra $\mathbb{C}[G]$ é semisimples, ou seja, cada $\mathbb{C}[G]$-módulo pode ser escrito como soma direta finita de módulos irredutíveis, onde um módulo é dito irredutível se não contém submódulos próprios. Podemos então considerar um conjunto representativo dos $\mathbb{C}[G]$-módulos irredutíveis $\mathscr{M}(\mathbb{C}[G]) = \{M_1, \ldots, M_n\}$ e para cada M_i consideramos a representação Φ_i associada como foi descrito anteriormente. O caráter χ_i associado a Φ_i (ou seja, a M_i) é dito irredutível e denotamos por $Irr(G) = \{\chi_1, \ldots, \chi_n\}$ o conjunto dos caracteres irredutíveis de G. Claramente $Lin(G)$ é contido em $Irr(G)$.

Observação 1.7. Como a soma de caracteres é um caráter, que corresponde à soma dos $\mathbb{C}[G]$-módulos associados, segue que $\chi = \sum_{i=1}^{k} n_i \chi_i$ é um caráter, onde os n_i's são inteiros não negativos e nem todos nulos. Reciprocamente, se Φ é uma representação que corresponde a um módulo V e χ é o caráter associado, podemos decompor V como soma direta de módulos irredutíveis e portanto χ é a soma dos correspondentes caracteres irredutíveis.

O centro da álgebra $\mathbb{C}[G]$ se ralaciona com o grupo G da seguinte forma.

Teorema 1.8. *Se G é um grupo finito, $Cl_1, \ldots, Cl_r$ são suas classes de conjugação e $C_i = \sum_{x \in Cl_i} x \in \mathbb{C}[G]$, então $\{C_1, \ldots, C_r\}$ é uma base para $Z(\mathbb{C}[G])$ e se $C_iC_j = \sum a_{ijv}C_v$, então as constantes multiplicativas a_{ijv} são inteiros não negativos.*

Demonstração. Ver [8, Theorem 2.4]. ∎

Vamos descrever algumas das propriedades do conjunto $Irr(G)$.

Teorema 1.9. *Seja G um grupo finito.*

(i) *$|Irr(G)|$ é igual ao número de classes de conjugação de G e*

$$\sum_{\chi \in Irr(G)} \chi(1)^2 = |G|.$$

(ii) *G é abeliano se, e somente se, todo caráter irredutível de G é linear.*

Demonstração. Ver [8, Corollary 2.6, 2.7]. ∎

Definição 1.10. Uma *função de classe* de um grupo G é uma função $\varphi : G \to \mathbb{C}$ que é constante sobre as classes de conjugação de G.

O conjunto das funções de classe de G será denotado por $CF(G)$. Observamos que $CF(G)$ é um espaço vetorial sobre $\mathbb{C}$, cuja dimensão é igual ao número de classes de conjugação de G.

Teorema 1.11. *Toda função de classe φ de G pode ser expressa na forma*

$$\varphi = \sum_{\chi \in Irr(G)} a_\chi \chi,$$

onde os a_χ são números complexos. Em particular, se φ é um caráter de G, então os a_χ são inteiros não negativos e não todos nulos.

Demonstração. Ver [8, Theorem 2.8]. ∎

Definição 1.12. Uma $\mathbb{Z}$-combinação linear dos elementos de $Irr(G)$ é dita *caráter generalizado* de G.

Claramente o conjunto dos caracteres generalizados de G é um anel que contém o conjunto dos caracteres de G.

Teorema 1.13 (Relação de Ortogonalidade Generalizada)**.** *Seja G um grupo finito. Se $Irr(G) = \{\chi_1, \ldots, \chi_n\}$, então para todo $h \in G$ temos que*

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(gh)\chi_j(g^{-1}) = \delta_{ij}\frac{\chi_i(h)}{\chi_j(1)}.$$

Demonstração. Ver [8, Theorem 2.13]. ∎

Quando $h = 1$ obtemos o seguinte resultado.

Corolário 1.14 (Primeira Relação de Ortogonalidade)**.**

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g^{-1}) = \delta_{ij}.$$

Lema 1.15. *Seja Φ uma representação de G que determina o caráter χ. Para todo $g \in G$ temos:*

(a) *$\Phi(g)$ é semelhante à matriz $diag(\epsilon_1, \ldots, \epsilon_t)$, onde $t = \chi(1)$;*

(b) *Se a ordem de g é $|g| = n$, então $\epsilon_i^n = 1$, para todo $i = 1, \ldots, t$;*

(c) *$\chi(g) = \sum_{i=1}^{t}\epsilon_i$ e $|\chi(g)| \leq \chi(1)$;*

(d) *$\chi(g^{-1}) = \overline{\chi(g)}$.*

Demonstração. Ver [8, Lemma 2.15]. ∎

Combinando a primeira Relação de Ortogonalidade e o Lema 1.15(d) obtemos que

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} = \delta_{ij}.$$

Isto sugere a seguinte definição.

Definição 1.16. Sejam φ e ψ funções de classe de G, definimos $[\cdot,\cdot]_G : CF(G) \times CF(G) \to \mathbb{C}$ por

$$[\varphi,\psi]_G = \frac{1}{|G|}\sum_{g\in G}\varphi(g)\overline{\psi(g)}.$$

Quando ficar claro pelo contexto, escreveremos apenas $[\varphi,\psi]$.

Segue da Primeira Relação de Ortogonalidade que o conjunto dos caracteres irredutíveis forma uma base ortonormal para o espaço das funções de classe.

Na proposição seguinte listaremos algumas propriedades das funções de classe.

Proposição 1.17. *Sejam $\varphi, \varphi_1, \varphi_2, \psi, \psi_1, \psi_2 \in CF(G)$ e $c_1, c_2 \in \mathbb{C}$.*

(a) $[\varphi,\psi]_G = \overline{[\psi,\varphi]_G}$;

(b) $[\varphi,\varphi]_G \geq 0$ *e* $[\varphi,\varphi]_G = 0$ *se, e somente se,* $\varphi = 0$;

(c) $[c_1\varphi_1 + c_2\varphi_2,\psi]_G = c_1[\varphi_1,\psi]_G + c_2[\varphi_2,\psi]_G$;

(d) $[\varphi, c_1\psi_1 + c_2\psi_2]_G = \overline{c_1}[\varphi,\psi_1]_G + \overline{c_2}[\varphi,\psi_2]_G$.

Segue da Proposição 1.17 que o produto $[\,,]$ é um produto interno hermitiano sobre $CF(G)$.

Corolário 1.18. *Sejam χ e ψ caracteres (não necessariamente irredutíveis) de G. Temos que $[\chi,\psi] = [\psi,\chi]$ é um inteiro não negativo e χ é irredutível se, e somente se, $[\chi,\chi] = 1$.*

Demonstração. Ver [8, Corollary 2.17]. ∎

Teorema 1.19 (Segunda Relação de Ortogonalidade)**.** *Sejam $g, h \in G$, temos que*

$$\sum_{\chi\in Irr(G)}\chi(g)\overline{\chi(h)} = \begin{cases} |C_G(g)| & \textit{se } g \textit{ é conjugado a } h \textit{ em } G \\ 0 & \textit{caso contrário} \end{cases}$$

Demonstração. Ver [8, Theorem 2.18]. ∎

Definição 1.20. Seja χ um caráter de G. O *núcleo* de χ é o conjunto

$$Ker(\chi) = \{g \in G;\ \chi(g) = \chi(1)\}.$$

Vejamos algumas propriedades do núcleo de um caráter.

Lema 1.21. *Seja χ um caráter de G tal que $\chi = \sum_{\chi_i \in Irr(G)} n_i\chi_i$. Então*

$$Ker(\chi) = \bigcap\{Ker(\chi_i); n_i > 0\}.$$

Demonstração. Se $g \in Ker(\chi)$, então $\chi(g) = \chi(1)$. Por outro lado, pelo Lema 1.15 temos que $|\chi_i(g)| \leq \chi_i(1)$. Assim, devemos ter $\chi_i(g) = \chi_i(1)$, sempre que $n_i \neq 0$. Logo $Ker(\chi) \subseteq \bigcap\{Ker(\chi_i); n_i > 0\}$.

Se $g \in \bigcap\{Ker(\chi_i); n_i > 0\}$, então $g \in Ker(\chi)$, pois

$$\chi(g) = \sum_{\chi_i \in Irr(G)} n_i\chi_i(g) = \sum_{\chi_i \in Irr(G)} n_i\chi_i(1) = \chi(1).$$

Portanto, $Ker(\chi) = \bigcap\{Ker(\chi_i); n_i > 0\}$.

■

Lema 1.22. *Seja Φ uma representação de G que determina o caráter χ. Então $Ker(\chi) = Ker(\Phi)$ e portanto, $Ker(\chi)$ é um subgrupo normal de G.*

Demonstração. Se $g \in Ker(\Phi)$, então $\Phi(g) = Id$ e portanto, $\chi(g) = \chi(1)$. Reciprocamente, se $g \in Ker(\chi)$, pelo Lema 1.15 temos que

$$\chi(1) = \chi(g) = \sum_{i=1}^{\chi(1)} \epsilon_i = |\sum_{i=1}^{\chi(1)} \epsilon_i| \leq \sum_{i=1}^{\chi(1)} |\epsilon_i| = \chi(1).$$

Donde $\epsilon_i = 1$, para todo $i = 1, \ldots, \chi(1)$. Como $\Phi(g)$ é semelhante à matriz $diag(\epsilon_1, \ldots, \epsilon_{\chi(1)}) = Id$, segue que $\Phi(g) = Id$ e portanto, $g \in Ker(\Phi)$.

■

Proposição 1.23. *Seja G um grupo finito e $N \trianglelefteq G$.*

(a) *Se χ é um caráter de G e $N \subseteq Ker(\chi)$, então χ é constante sobre as classes laterais de N em G e a função $\hat{\chi} : \frac{G}{N} \to \mathbb{C}$ definida por $\hat{\chi}(Ng) = \chi(g)$ é um caráter de $\frac{G}{N}$.*

(b) *Se $\hat{\chi}$ é um caráter de $\frac{G}{N}$, então a função $\chi : G \to \mathbb{C}$ definida por $\chi(g) = \hat{\chi}(Ng)$ é um caráter de G tal que $N \subseteq Ker(\chi)$.*

(c) *$\chi \in Irr(G)$ se, e somente se, $\hat{\chi} \in Irr(\frac{G}{N})$.*

Observação 1.24. Como χ é constante sobre as classes laterais de N em G, temos que $\chi(ng) = \chi(g)$, para todo $n \in N$.

Corolário 1.25. *Seja G um grupo finito com subgrupo comutador G'. O número de caracteres lineares de G é igual a $|G : G'|$.*

Demonstração. Seja $\psi \in Lin(G)$, então ψ define um homomorfismo de G em um subgrupo de $\mathbb{C}^*$. Dessa forma, $\frac{G}{Ker(\psi)} \lesssim \mathbb{C}^*$ e então $\frac{G}{Ker(\psi)}$ é cíclico, donde segue que $G' \subseteq Ker(\psi)$. Observamos que se $\psi_1 \neq \psi_2$, então $\hat{\psi_1} \neq \hat{\psi_2}$, onde $\hat{\psi_1}, \hat{\psi_2} \in Irr\left(\frac{G}{G'}\right)$. De fato,

$$\hat{\psi_1}(G'g) = \psi_1(g) \neq \psi_2(g) = \hat{\psi_2}(G'g),$$

para algum $g \in G$. Assim, pela Proposição 1.23, temos que

$$Irr\left(\frac{G}{G'}\right) = \{\hat{\psi};\, \psi \in Lin(G)\}.$$

Portanto, pelo Teorema 1.9, $|Lin(G)| = |Irr\left(\frac{G}{G'}\right)| = |G : G'|$.

■

Proposição 1.26. *Sejam χ e ψ caracteres de G. O produto*

$$(\chi\psi)(g) = \chi(g)\psi(g)$$

é também um caráter de G.

Demonstração. Ver [8, Corollary 4.2].

■

Corolário 1.27. *O conjunto dos caracteres lineares de G é um grupo que age sobre $Irr(G)$ por multiplicação.*

Demonstração. Sejam ψ_1, ψ_2 e $\psi \in Lin(G)$,

$$(\psi_1\psi_2)(1) = \psi_1(1)\psi_2(1) = 1,$$

então $\psi_1\psi_2 \in Lin(G)$ e $(\psi_1\psi_2)\psi(g) = \psi_1(\psi_2\psi)(g)$. Note que $1_G \in Lin(G)$ e $1_G\psi = \psi 1_G = \psi$, para qualquer $\psi \in Lin(G)$.

Agora defina $\overline{\psi} : G \to \mathbb{C}$ por $\overline{\psi}(g) = \overline{\psi(g)}$. Temos que $\overline{\psi}$ é o caráter associado à representação $\overline{\Phi} : G \to \mathbb{C}$ definida por $\overline{\Phi}(g) = (\Phi(g)^T)^{-1}$, onde Φ é uma representação que determina o caráter ψ. Então

$$(\psi\overline{\psi})(g) = (\overline{\psi}\psi)(g) = |\psi(g)|^2 = 1, \text{para todo } g \in G,$$

logo $\psi\overline{\psi} = 1_G$. Portanto, $Lin(G)$ é um grupo.

Vejamos que $Lin(G)$ age sobre $Irr(G)$ por multiplicação. De fato, se $\psi \in Lin(G)$ e $\chi \in Irr(G)$,

$$\begin{aligned} [\chi\psi, \chi\psi] &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\psi(g)\overline{\chi(g)\psi(g)} \\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\chi(g)}|\psi(g)|^2 \\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\chi(g)} \\ &= [\chi, \chi] = 1. \end{aligned}$$

Portanto, $\chi\psi \in Irr(G)$.

∎

Considerando G um grupo abeliano finito, vamos demonstrar uma importante relação entre G e o grupo $Lin(G)$.

Teorema 1.28. *Se G é um grupo abeliano finito, então G é isomorfo a $Lin(G)$.*

Demonstração. Pelo Corolary 10.22 em [15], temos que G é produto direto de grupos cíclicos, então podemos supor sem perda de generalidade que G é cíclico, pois $Lin(H \times K) = Lin(H) \times Lin(K)$, pelo Theorem 4.22 em [8].

Seja g um gerador de G. Como um caráter de G é determinado por seu valor em g e este valor deve ser uma raiz $|g|$-ésima da unidade, temos que existem no máximo $|g|$ caracteres de G.

Seja ζ uma raiz $|g|$-ésima primitiva da unidade. Definindo $\chi_1(g^i) = \zeta^i$, temos que χ_1 é um homomorfismo e portanto um caráter linear. Vejamos que χ_1 tem a mesma ordem de g.

Primeiramente observamos que

$${\chi_1}^{|g|}(g^i) = (\zeta^i)^{|g|} = (\zeta^{|g|})^i = 1.$$

Agora se k é tal que ${\chi_1}^k(g^i) = 1$, para todo $i = 1, \ldots, |g|$, então $(\zeta^i)^k = 1$, para todo $i = 1, \ldots, |g|$. Em particular, $\zeta^k = 1$ e portanto $|g|$ divide k. Assim, como $|Lin(G)| = |G|$, temos que $Lin(G)$ é um grupo cíclico. Portanto G é isomorfo a $Lin(G)$.

∎

1.2 - Inteiros Algébricos

Nesta seção, vamos demonstrar que se χ é um caráter de um grupo finito G, então $\chi(g)$ é um inteiro algébrico para todo $g \in G$. Esse resultado vai ser utilizado para mostrar que o grau de qualquer caráter irredutível de G divide a ordem de G.

Definição 1.29. Um número complexo diz-se *inteiro algébrico* se é raiz de um polinômio mônico com coeficientes inteiros.

Lema 1.30. *Um número racional é inteiro algébrico se, e somente se, é um número inteiro.*

Demonstração. Se $a \in \mathbb{Z}$, então a é raiz do polinômio $x - a$ e portanto a é um inteiro algébrico. Reciprocamente, suponha que $\frac{r}{s}$ com $r, s \in \mathbb{Z}$ e $mdc(r, s) = 1$ é raiz do polinômio com coeficientes inteiros

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0, \ n \geq 2.$$

Temos

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0$$

que implica

$$r^n = -s(a_{n-1}r^{n-1} + a_{n-2}sr^{n-2} + \cdots + a_0s^{n-1}).$$

Logo, $s \mid r^n$ e assim $s = \pm 1$, pois $mdc(r, s) = 1$. Portanto, $\frac{r}{s} \in \mathbb{Z}$.

■

Teorema 1.31. *Seja S um anel tal que $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$. Se S é um $\mathbb{Z}$-módulo finitamente gerado, então todo elemento de S é um inteiro algébrico.*

Demonstração. Ver [8, Theorem 3.4].

■

Corolário 1.32. *Os inteiros algébricos formam um subanel de $\mathbb{C}$.*

Demonstração. Ver [8, Corollary 3.5].

■

Corolário 1.33. *Se χ um caráter de G, então $\chi(g)$ é um inteiro algébrico, para todo $g \in G$.*

Demonstração. Seja $|g| = n$. Pelo Lema 1.15 $\chi(g) = \sum_{i=1}^{\chi(1)} \epsilon_i$, onde ϵ_i é raiz do polinômio $x^n - 1 \in \mathbb{Z}[x]$. Logo $\chi(g)$ é soma de inteiros algébricos e portanto, pelo Corolário 1.32, $\chi(g)$ é um inteiro algébrico.

■

Observação 1.34. Seja $\chi \in Irr(G)$ e Φ uma representação que determina o caráter χ. Se $z \in Z(\mathbb{C}[G])$, pelo Lemma 2.25 em [8] temos que $\Phi(z) = \epsilon_z I_n$, para algum $\epsilon_z \in \mathbb{C}$. Definimos a função

$$\begin{aligned} \omega_\chi : Z(\mathbb{C}[G]) &\to \mathbb{C} \\ z &\mapsto \epsilon_z \end{aligned}.$$

Observamos que a escolha de ϵ_z não depende da representação que determina o caráter χ, pois a única matriz semelhante a $\epsilon_z I_n$ é ela mesma. Além disso, como Φ é um homomorfismo, temos que ω_χ também é um homomorfismo e, em particular, é uma função $\mathbb{C}$-linear. Portanto, é suficiente definir ω_χ sobre uma base de $Z(\mathbb{C}[G])$.

Pelo Teorema 1.8, temos que $C_1, \ldots, C_r$ é uma base para $Z(\mathbb{C}[G])$, onde $C_i = \sum_{x \in Cl_i} x$. Então $\Phi(C_i) = \epsilon_{C_i} I_n = \omega_\chi(C_i) I_n$ e $\chi(C_i) = \omega_\chi(C_i)\chi(1)$.

Por outro lado, $\Phi(C_i) = \Phi(\sum_{x \in Cl_i} x) = \sum_{x \in Cl_i} \Phi(x)$. Dessa forma temos que $\chi(C_i) = |Cl_i|\chi(x_i)$, onde x_i é um representante da classe Cl_i. Portanto,

$$\omega_\chi(C_i) = |Cl_i| \frac{\chi(x_i)}{\chi(1)}.$$

Teorema 1.35. *Sejam $\chi \in Irr(G)$ e C a soma de uma classe de $\mathbb{C}[G]$. Então $\omega_\chi(C)$ é um inteiro algébrico.*

Demonstração. Sejam $Cl_1, \ldots, Cl_k$ as classes de conjugação de G e $C_1, \ldots, C_k$ as correspondentes somas de classe. Pelo Teorema 1.8, temos que $C_i C_j = \sum_v a_{ijv} C_v$, onde $a_{ijv} \in \mathbb{Z}$. Como ω_χ é um homomorfismo, segue que

$$\omega_\chi(C_i)\omega_\chi(C_j) = \sum_v a_{ijv}\omega_\chi(C_v).$$

Assim, o conjunto S de todas as $\mathbb{Z}$-combinações lineares de $\omega_\chi(C_i)$ é fechado por multiplicação. Além disso, $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$, pois $\omega_\chi(1) = 1$. Portanto, pelo Teorema 1.31, todos os elementos de S são inteiros algébricos.

■

Teorema 1.36. *Se χ é um caráter irredutível de G, então $\chi(1)$ divide $|G|$.*

Demonstração. Pela Primeira Relação de Ortogonalidade, temos que

$$|G| = \sum_{g \in G} \chi(g)\overline{\chi(g)}.$$

Agora vamos escrever esta equação em termos de ω_χ. Usando a mesma notação do teorema anterior, temos

$$|G| = \sum_{i=1}^{k} |Cl_i|\chi(g_i)\chi({g_i}^{-1}) = \sum_{i=1}^{k} \chi(1)\omega_\chi(C_i)\chi({g_i}^{-1}),$$

onde g_i um representante da classe Cl_i, assim

$$\frac{|G|}{\chi(1)} = \sum_{i=1}^{k} \omega_\chi(C_i)\chi({g_i}^{-1}).$$

O Teorema 1.35 e o Corolário 1.33 implicam que $\omega_\chi(C_i)$ e $\chi({g_i}^{-1})$ são inteiros algébricos e, pelo Corolário 1.32, $\frac{|G|}{\chi(1)}$ é também um inteiro algébrico. Logo, segue do Lema 1.30 que $\frac{|G|}{\chi(1)} \in \mathbb{Z}$ e portanto $\chi(1)$ divide $|G|$.

■

1.3 - Caracteres Induzidos

Se H é um subgrupo de G, então para todo caráter χ de G podemos obter um caráter $\chi_{|_H}$ de H, por restrição. O que faremos nessa seção é obter caracteres de G a partir de caracteres de H.

Definição 1.37. Sejam H um subgrupo de G e φ uma função de classe de H. A *função de classe induzida de H a G* é definida por $\varphi^G : G \to \mathbb{C}$

$$\varphi^G(g) = \frac{1}{|H|} \sum_{x \in G} \varphi^\circ(xgx^{-1}),$$

onde $\varphi^\circ(h) = \begin{cases} \varphi(h), & \text{se } h \in H \\ 0, & \text{se } h \notin H \end{cases}.$

Observamos que φ^G é uma função de classe de G e

$$\varphi^G(1) = |G : H|\varphi(1).$$

Lema 1.38 (Reciprocidade de Frobenius)**.** *Sejam H um subgrupo de G, φ uma função de classe de H e θ uma função de classe de G. Então*

$$[\varphi, \theta_{|_H}]_H = [\varphi^G, \theta]_G.$$

Demonstração. Por definição,

$$[\varphi^G, \theta]_G = \frac{1}{|G|} \sum_{g \in G} \varphi^G(g)\overline{\theta(g)} = \frac{1}{|G|}\frac{1}{|H|} \sum_{g \in G} \sum_{x \in G} \varphi^\circ(xgx^{-1})\overline{\theta(g)}.$$

Considerando $y = xgx^{-1}$, temos que $\theta(g) = \theta(y)$. Assim,

$$[\varphi^G, \theta]_G = \frac{1}{|G|}\frac{1}{|H|} \sum_{y \in G} \sum_{x \in G} \varphi^\circ(y)\overline{\theta(y)} = \frac{1}{|H|} \sum_{y \in H} \varphi(y)\overline{\theta(y)} = [\varphi, \theta_{|_H}]_H.$$

■

Corolário 1.39. *Se H é um subgrupo de G e φ um caráter de H, então φ^G é um caráter de G.*

Demonstração. Seja $\chi \in Irr(G)$. A restrição $\chi_{|_H}$ é um caráter de H, logo pelo Lema 1.38 e pelo Corolário 1.18, temos que $[\varphi^G, \chi] = [\varphi, \chi_{|_H}]$ é um inteiro não negativo. Por outro lado, $\varphi(1) \neq 0$ implica que $\varphi^G(1) = |G : H|\varphi(1) \neq 0$ e então $\varphi^G \neq 0$. Portanto φ^G é um caráter de G.

■

Corolário 1.40. *Se H é um subgrupo de G e φ um caráter irredutível de H, então existe um caráter irredutível χ de G tal que φ é componente da restrição $\chi_{|_H}$.*

Demonstração. Seja $\chi \in Irr(G)$ uma componente de φ^G. Temos que

$$0 \neq [\varphi^G, \chi] = [\varphi, \chi_{|_H}].$$

Portanto, φ é componente de $\chi_{|_H}$.

■

Corolário 1.41. *Sejam G um grupo abeliano e H um subgrupo de G. Então todo $\lambda \in Irr(H)$ é a restrição de algum $\mu \in Irr(G)$.*

Demonstração. Pelo Corolário 1.40, existe um caráter irredutível μ de G tal que λ é componente da restrição $\mu_{|_H}$. Como G é abeliano, $\lambda(1) = 1 = \mu(1)$ e portanto, $\lambda = \mu_{|_H}$.

■

Teorema 1.42. *Se $H \leqslant G$, então temos as seguintes propriedades.*

(a) *Se ψ_1, ψ_2 são caracteres de H, então*

$$(\psi_1 + \psi_2)^G = {\psi_1}^G + {\psi_2}^G.$$

(b) *Se ψ é um caráter de H e χ é um caráter de G, então*

$$\chi\psi^G = (\chi_{|_H}\psi)^G.$$

(c) *Se $K \leqslant H \leqslant G$ e ψ é um caráter de K, então*

$$\psi^G = (\psi^H)^G.$$

Demonstração.

(a) Para todo $g \in G$,

$$\begin{aligned}(\psi_1 + \psi_2)^G(g) = & \frac{1}{|H|}\sum_{x \in G}(\psi_1 + \psi_2)^\circ(xgx^{-1}) \\ = & \frac{1}{|H|}\sum_{x \in G}\psi_1^\circ(xgx^{-1}) + \frac{1}{|H|}\sum_{x \in G}\psi_2^\circ(xgx^{-1}) \\ = & \psi_1^G(g) + \psi_2^G(g).\end{aligned}$$

(b) Para todo $g \in G$,

$$\begin{aligned}(\chi_{|_H}\psi)^G(g) &= \frac{1}{|H|}\sum_{x \in G}\chi(xgx^{-1})\psi^\circ(xgx^{-1}) \\ &= \chi(g)\frac{1}{|H|}\sum_{x \in G}\psi^\circ(xgx^{-1}) \\ &= \chi(g)\psi^G(g).\end{aligned}$$

(c) Pela reciprocidade de Frobenius, para qualquer $\chi \in Irr(G)$ temos

$$[(\psi^H)^G, \chi]_G = [\psi^H, \chi_{|_H}]_H = [\psi, (\chi_{|_H})_{|_K}]_K = [\psi, (\chi_{|_K})]_K = [\psi^G, \chi]_G.$$

Portanto, $\psi^G = (\psi^H)^G$.

∎

Agora vamos enunciar algumas definições e resultados que serão utilizados no próximo capítulo.

Definição 1.43. Um caráter de G é dito *homogêneo* se é múltiplo de algum caráter irredutível de G.

Definição 1.44. Seja Φ uma representação que determina o caráter χ. Definimos $det\,\chi : G \to \mathbb{C}$ por

$$(det\,\chi)(g) = det\,\Phi(g).$$

Temos que $det\,\chi$ está bem definido e é um caráter linear de G. Assim podemos definir $o(\chi) = |det\,\chi|$, onde $det\,\chi$ é visto como um elemento do grupo dos caracteres lineares de G.

Vamos considerar π um conjunto de números primos e π' o seu complemento no conjunto dos números primos.

Definição 1.45. Dizemos que um número inteiro é um *π-número*, se todos os seus fatores primos pertencem ao conjunto π.

Definição 1.46. Dizemos que $\chi \in Irr(G)$ é *π-especial* se

(i) $\chi(1)$ é um π-número;

(ii) Para todo subgrupo subnormal S de G e toda componente irredutível θ de $\chi_{|S}$, $o(\theta)$ é um π-número.

Escreveremos $X_\pi(G)$ para denotar o conjunto dos caracteres π-especiais de G.

Definição 1.47. Um grupo G é dito um *π-grupo*, se a ordem de todo elemento de G é um π-número.

Teorema 1.48. *Seja $\chi \in Irr(G)$. Suponha que existe uma série normal*

$$1 = G_0 < G_1 < \ldots < G_n = G,$$

tal que $\frac{G_i}{G_{i-1}}$ é um π-grupo ou um π'-grupo e $\chi_{|G_i}$ é homogêneo, para todo $i = 0, 1, \ldots, n$. Então χ fatora unicamente como $\chi = \alpha \cdot \beta$, onde $\alpha \in X_\pi(G)$ e $\beta \in X_{\pi'}(G)$.

Demonstração. Ver [13, Theorem 21.7].

■

Definição 1.49. Um grupo G é dito *π-separável* se possui uma série normal tal que cada fator é um π-grupo ou um π'-grupo.

Teorema 1.50. *Sejam G um grupo π-separável e $H \leqslant G$ tal que o índice de H em G é um π'-número. Então a função $f : X_\pi(G) \to X_\pi(H)$, definida por $f(\chi) = \chi_{|H}$ é injetiva.*

Demonstração. Ver [13, Theorem 21.10].

■

1.3.1 Grupos elementares e quase elementares

Agora vamos definir um importante tipo de grupo e estudar algumas de suas propriedades.

Definição 1.51. Sejam G um grupo finito e p um número primo.

(a) Seja $|G| = ap^n$, onde a é tal que $p \nmid a$. Um *p-complemento* de G é um subgrupo de G cuja ordem é a;

(b) Dizemos que G é *p-elementar*, se é produto direto de um grupo cíclico e um p-grupo. Dizemos que G é *elementar*, se é p-elementar para algum primo p;

(c) Dizemos que G é *p-quase elementar*, se G tem um p-complemento cíclico e normal. Dizemos que G é *quase elementar*, se é p-quase elementar para algum primo p.

Observamos que se G é p-elementar, então G é p-quase elementar.

Lema 1.52. *Sejam G um grupo finito e p um número primo que divide a ordem de G. Se G possui um p-complemento normal N, então N é único e é o produto de todos os q_i-subgrupos de Sylow de G, com $q_i \neq p$.*

Demonstração. Se $|G| = p^a$, então $N = \{1\}$ e portanto é único. Suponha que $|G| = p^a {q_1}^{a_1} {q_2}^{a_2} \dots {q_n}^{a_n}$ e $|N| = {q_1}^{a_1} {q_2}^{a_2} \dots {q_n}^{a_n}$, com q_i primo, para todo $i = 1, \dots, n$. Como N é normal em G e contém um q_i-subgrupo de Sylow Q de G, temos que $Q^g \leqslant N^g = N$, para todo $g \in G$. Logo

$$\left(\prod_{q_i \neq p} \prod_{Q \in Syl_{q_i}(G)} Q \right) \subseteq N.$$

Reciprocamente, se $x \in N$ é tal que $|x| = q_1^{d_1}$, temos que x pertence a um q_1-subgrupo de Sylow de G. Se $|x| = q_1^{d_1} q_2^{d_2}$, existem $\alpha, \beta \in \mathbb{Z}$ tais que $1 = \alpha q_1^{d_1} + \beta q_2^{d_2}$, então

$$x = x^{\alpha q_1^{d_1}} x^{\beta q_2^{d_2}} \in Q_{q_2} Q_{q_1},$$

onde Q_{q_i} é um q_i-subgrupo de Sylow de G. Procedendo por indução,

$$N \subseteq \left(\prod_{q_i \neq p} \prod_{Q \in Syl_{q_i}(G)} Q \right).$$

Portanto N é único, por ser o produto de todos os q_i-subgrupos de Sylow de G, com $q_i \neq p$.

■

Para demonstrarmos o próximo resultado sobre grupos elementares e quase elementares vamos precisar do seguinte resultado sobre p-grupos.

Lema 1.53. *Se G é um p-grupo finto, então G é nilpotente.*

Demonstração. Sejam $Z_0(G) = \{1\}$ e $Z_1 = Z(G)$. Para $i \geqslant 1$, defina $Z_{i+1}(G)$ por $\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right)$. Como $Z(G)$ é não trivial e $\frac{Z_{i+1}(G)}{Z_i(G)}$ é um p-grupo finito, temos que a série central superior de G é estritamente crescente e do fato de G ser finito segue que

$$1 < Z(G) < Z_2(G) < \cdots < Z_r(G) = G,$$

para algum $r \in \mathbb{N}$.

Observamos que esta é uma série normal de G, visto que $Z(G) \lhd G$ e para todo $i \geqslant 1$ temos $Z_{i+1}(G) \lhd G$, pois pelo Teorema da Correspondência,

$$\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right) \unlhd \frac{G}{Z_i(G)}.$$

Além disso, para todo $i \geqslant 1$ os quocientes $\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right)$ são abelianos. Portanto G é nilpotente.

■

Lema 1.54. *Sejam G um grupo finito e H um subgrupo de G.*

(a) *Se G é p-quase elementar, então H é p-quase elementar;*

(b) *Se G é elementar, então H é elementar.*

Demonstração.

(a) Se G é p-quase elementar, podemos escrever $G = C \rtimes P$, onde C é um grupo cíclico e P é um p-grupo. Sem perda de generalidade, podemos supor que P é um p-subgrupo de Sylow de G e que C é um p'-grupo. Observamos que $\frac{G}{C} \simeq P$, onde C e P são grupos solúveis, então G é solúvel. Daí, se H é um subgrupo de G, temos que H é solúvel.

Suponha que $|H| = bp^n$, com $mdc(b,p) = 1$. Pelo Teorema de Hall (Theorem 5.28 em [15]), existe um subgrupo K de H tal que $|K| = b$. Daí, como $H \cap P$ é um p-subgrupo de Sylow de H, temos

$$|H : K| = p^n, \quad |H : P \cap H| = b$$

e como $mdc(|K|, |H \cap P|) = 1$, segue que $H = K \cdot (H \cap P)$.

Observamos que K é cíclico e normal em H, pois pelo Lema 1.52,

$$K \subseteq \left(\prod_{q_i \neq p} \prod_{Q \in Sly(H)} Q \right) \subseteq \left(\prod_{q_i \neq p} \prod_{R \in Sly(G)} R \right) = C.$$

Portanto H é p-quase elementar.

(b) Se $G = C \times P$ é p-elementar, então G é p-quase elementar e todo subgrupo H de G é p-quase elementar, pelo item (a). Logo, seguindo a demonstração do item (a) podemos escrever

$$H = (C \cap H) \rtimes (P \cap H).$$

Por outro lado, observamos que $(P \cap H) \trianglelefteq H$. Portanto,

$$H = (C \cap H) \times (P \cap H),$$

ou seja, H é p-elementar.

■

Para demonstrar mais algumas propriedades dos grupos quase elementares precisamos da seguinte definição.

Definição 1.55. Seja χ um caráter de G. Dizemos que χ é *monomial* se $\chi = \lambda^G$, onde λ é um caráter linear de algum subgrupo de G, não necessariamente próprio. O grupo G é dito um *M-grupo* se todo caráter irredutível é monomial.

Queremos mostrar que todo grupo quase elementar é um M-grupo. Precisamos de algumas propriedades de grupos supersolúveis.

Definição 1.56. Um grupo G é dito *supersolúvel* se existe uma série normal

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n = \{1\},$$

tal que os quocientes $\frac{G_0}{G_1}$, $\frac{G_1}{G_2}, \ldots,$ $\frac{G_n}{G_{n-1}}$ são grupos cíclicos.

Proposição 1.57. *Se G é um p-grupo finito, então G é supersolúvel.*

Demonstração. Pelo Lema 1.53, temos que para algum $r \in \mathbb{N}$ a série

$$1 < Z(G) < Z_2(G) < \cdots < Z_r(G) = G$$

é uma série normal tal que $i \geqslant 1$ os quocientes $\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right)$ são abelianos.

Agora vamos refinar a série acima para obter uma série de composição de G. Pelo Teorema Fundamental dos Grupos Abelianos Finitos, podemos considerar

$$\frac{Z_{i+1}(G)}{Z_i(G)} = C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_n^{a_n}}, \text{ para todo } i \geqslant 1,$$

onde $C_{p_j^{a_j}}$ é um grupo cíclico de ordem $p_j^{a_j}$ e cada p_j é um número primo.

Para todo $i \geqslant 1$, podemos considerar a série

$$\begin{aligned} Z_i(G) &< Z_i(G)C_{p_1} < Z_i(G)C_{p_1^2} < \cdots < Z_i(G)C_{p_1^{a_1}} < \\ &< Z_i(G)C_{p_1^{a_1}} \times Z_i(G)C_{p_2} < \cdots < Z_i(G)C_{p_1^{a_1}} \times Z_i(G)C_{p_2^{a_2}} < \\ &< \cdots < Z_i(G)C_{p_1^{a_1}} \times Z_i(G)C_{p_2^{a_2}} \times \cdots \times Z_i(G)C_{p_n^{a_n}} = Z_{i+1}(G). \end{aligned}$$

Pelo Teorema da Correspondência, para todo $j = 1, \ldots, n$ temos que $Z_i(G)C_{p_1^{a_1}} \times Z_i(G)C_{p_2^{a_2}} \times \cdots \times Z_i(G)C_{p_j^{a_j}} \lhd G$, pois

$$\frac{Z_i(G)C_{p_1^{a_1}} \times Z_i(G)C_{p_2^{a_2}} \times \cdots \times Z_i(G)C_{p_j^{a_j}}}{Z_i(G)} \leqslant Z\left(\frac{G}{Z_i(G)}\right) \trianglelefteq \frac{G}{Z_i(G)}.$$

Logo, como qualquer subgrupo de $Z(G)$ é um subgrupo normal de G, temos que

$$\begin{aligned} \{1\} &< \cdots < Z(G) < \cdots < Z_i(G) < Z_i(G)C_{p_1} < \cdots < \\ &< Z_i(G)C_{p_1^{a_1}} \times Z_i(G)C_{p_2^{a_2}} \times \cdots \times Z_i(G)C_{p_n^{a_n}} = Z_{i+1}(G) < \cdots < G \end{aligned}$$

é uma série de composição de G em que cada chief factor é cíclico, pois

$$\frac{Z_i(G)C_{p_1^{a_1}} \times Z_i(G)C_{p_2^{a_2}} \times \cdots \times Z_i(G)C_{p_j^{a_j}}}{Z_i(G)C_{p_1^{a_1}} \times Z_i(G)C_{p_2^{a_2}} \times \cdots \times Z_i(G)C_{p_j^{a_j-1}}} \simeq \frac{C_{p_j{}^{a_j}}}{C_{p_j{}^{a_j-1}}} \simeq C_{p_j}.$$

Portanto G é supersolúvel.

■

Teorema 1.58. *Seja $N \trianglelefteq G$ tal que N é solúvel e todo subgrupo de Sylow de N é abeliano. Se $\frac{G}{N}$ é supersolúvel, então G é um M-grupo.*

Demonstração. Ver [7, Theorem 24.3].

■

Corolário 1.59. *Se G é quase elementar, então G é um M-grupo.*

Demonstração. Por hipótese $G = C \rtimes P$, onde P é um p-grupo e C é um grupo cíclico. Como C é cíclico, temos que C é solúvel e que todo subgrupo de Sylow de C é abeliano. Por outro lado, pela Proposição 1.57, o p-grupo $\frac{G}{C}$ é supersolúvel. Portanto, pelo Teorema 1.58 temos que G é um M-grupo.

■

1.4 - Os Teoremas de Clifford e Gallagher

Em geral, se N é um subgrupo de G e $\chi \in Irr(G)$ pouco pode ser dito a respeito de $\chi_{|_N}$. No entanto, se adicionarmos a hipótese de que N é um subgrupo normal de G, conseguimos obter resultados importantes.

Definição 1.60. Sejam N um subgrupo normal de G, φ uma função de classe de N e $g \in G$. Definimos $\varphi^g : N \to \mathbb{C}$ por $\varphi^g(h) = \varphi(ghg^{-1})$ e dizemos que φ^g é *conjugado* a φ em G.

No Lema seguinte listaremos algumas propriedades do conjugado de uma função de classe

Lema 1.61. *Sejam $N \trianglelefteq G$, φ, θ funções de classe de N e $x, y \in G$. Então*

(a) *φ^x é uma função de classe de N;*

(b) *$(\varphi^x)^y = \varphi^{xy}$;*

(c) $[\varphi^x, \theta^x] = [\varphi, \theta]$;

(d) $[\chi_{|_N}, \varphi^x] = [\chi_{|_N}, \varphi]$, *para toda função de classe* χ *de* G;

(e) *Se* φ *é um caráter de* N*, então* φ^x *também é um caráter de* N.

Demonstração. Ver [8, Lemma 6.1].

■

Teorema 1.62. *Suponha que* H *e* K *são subgrupos de* G *e*

$$G = \dot{\bigcup}_{i=1}^{m} Hr_iK.$$

Se ψ *é um caráter de* H*, então*

$$(\psi^G)_{|_K} = \sum_{i=1}^{m} ((\psi^{r_j})_{|_{H^{r_j} \cap K}})^K.$$

Demonstração. Ver [7, Theorem 17.4].

■

Teorema 1.63 (Teorema de Clifford)**.** *Sejam* $N \trianglelefteq G$*,* $\chi \in Irr(G)$ *e* θ *uma componente irredutível de* $\chi_{|_N}$*. Suponha que* $\theta_1 = \theta, \theta_2, \ldots, \theta_t$ *são os conjugados distintos de* θ *em* G*. Então*

$$\chi_{|_N} = e \sum_{i=1}^{t} \theta_i,$$

onde $e = [\chi_{|_N}, \theta]$.

Demonstração. Vamos calcular $(\theta^G)_{|_N}$. Para todo $n \in N$ e todo $g \in G$, temos que $gng^{-1} \in N$. Assim,

$$\theta^G(n) = \frac{1}{|N|} \sum_{g \in G} \theta^\circ(gng^{-1}) = \frac{1}{|N|} \sum_{g \in G} \theta^g(n),$$

ou seja, $|N|(\theta^G)_{|_N} = \sum_{g \in G} \theta^g$. Se $\varphi \in Irr(N)$ e $\varphi \notin \{\theta_1 = \theta, \theta_2, \ldots, \theta_t\}$, então

$$0 = [\sum_{g \in G} \theta^g, \varphi] = |N|[(\theta^G)_{|_N}, \varphi]$$

e portanto $[(\theta^G)_{|_N}, \varphi] = 0$. Pela hipótese de que θ é uma componente irredutível de $\chi_{|_N}$ e pela Reciprocidade de Frobenius, temos

$$0 < [\theta, \chi_{|_N}] = [\theta^G, \chi]$$

e assim χ é uma componente de θ^G, daí $[\chi_{|_N}, \varphi] = 0$. Então toda componente irredutível de $\chi_{|_N}$ deve pertencer à órbita de θ, logo $\chi_{|_N} = \sum_{i=1}^{t} e_i\theta_i$. Agora note que $e_i = [\chi_{|_N}, \theta_i] = [\chi_{|_N}, \theta^g] = [\chi_{|_N}, \theta]$, pelo Lema 1.61(d). Portanto, $\chi_{|_N} = e\sum_{i=1}^{t} \theta_i$.

■

Corolário 1.64. *Sejam $N \trianglelefteq G$, $\chi \in Irr(G)$ e suponha que $[\chi_{|_N}, 1_N] \neq 0$. Então $N \subseteq Ker(\chi)$.*

Demonstração. No Teorema de Clifford, pegamos $\theta = 1_N$. Dessa forma, a órbita de 1_N tem um único elemento pois $(1_N)^g = 1_N$, para todo $g \in G$. Assim, $\chi_{|_N} = e\sum_{i=1}^{t} \theta_i$ implica que $\chi_{|_N} = \chi(1) \cdot 1_N$ e portanto, $N = Ker(\chi_{|_N}) \subseteq Ker(\chi)$.

■

Corolário 1.65. *Sejam $N \trianglelefteq G$ e $\chi \in Irr(G)$. Se $\theta \in Irr(N)$ é tal que $[\chi_{|_N}, \theta] \neq 0$, então $\theta(1) \mid \chi(1)$.*

Demonstração. Considerando $\theta = \theta_1$ no Teorema de Clifford e o fato de que $\theta^g(1) = \theta(1)$, para todo $g \in G$, temos que

$$\chi(1) = \chi_{|_N}(1) = e\sum_{i=1}^{t} \theta_i(1) = et\theta(1).$$

Portanto $\theta(1) \mid \chi(1)$.

■

Definição 1.66. Seja $N \trianglelefteq G$ e $\theta \in Irr(N)$. O subgrupo

$$I_G(\theta) = \{g \in G; \theta^g = \theta\}$$

é chamado *grupo de inércia* de θ em G.

Como $I_G(\theta)$ é o estabilizador de θ quando consideramos a ação de G sobre $Irr(N)$, segue que $I_G(\theta)$ é um subgrupo de G e $N \subseteq I_G(\theta)$. Além disso, $|G : I_G(\theta)|$ é o tamanho da órbita de θ, então no Teorema de Clifford temos $\chi_{|_N} = e\sum_{i=1}^{t} \theta_i$, com $t = |G : I_G(\theta)|$. Em particular, t divide $|G : N|$.

Diremos que θ é *G-invariante* se $I_G(\theta) = G$.

O próximo teorema é de fundamental importância par a teoria de caracteres de subgrupos normais.

Teorema 1.67. *Sejam $N \trianglelefteq G$, $\theta \in Irr(N)$ e $T = I_G(\theta)$. Defina*

$$\mathscr{A} = \{\psi \in Irr(T); [\psi_{|_N}, \theta]_N \neq 0\}, \quad \mathscr{B} = \{\chi \in Irr(G); [\chi_{|_N}, \theta]_N \neq 0\}.$$

(a) *Se $\psi \in \mathscr{A}$, então $\psi^G \in Irr(G)$;*

(b) *A função $F : \mathscr{A} \to \{$caracteres de $G\}$ definida por $F(\psi) = \psi^G$ é uma bijeção entre $\mathscr{A}$ e $\mathscr{B}$;*

(c) *Se $\psi \in \mathscr{A}$ e $\chi = \psi^G$, então ψ é a única componente irredutível de $\chi_{|_T}$ que pertence a $\mathscr{A}$;*

(d) *Se $\psi \in \mathscr{A}$ e $\chi = \psi^G$, então $[\psi_{|_N}, \theta]_N = [\chi_{|_N}, \theta]_N$.*

Demonstração.

(a) Sejam $\psi \in \mathscr{A}$ e χ uma componente irredutível de ψ^G. Pela Reciprocidade de Frobenius temos que $[\psi, \chi_{|_T}]_T = [\psi^G, \chi]_G > 0$ e assim, ψ é uma componente de $\chi_{|_T}$ e como θ é uma componente de $\psi_{|_N}$, temos que $\chi \in \mathscr{B}$.

Sejam $\theta = \theta_1, \theta_2, \ldots, \theta_t$ os conjugados distintos de θ em G, onde $t = |G : T|$. Pelo Teorema de Clifford, $\chi_{|_N} = e\sum_{i=1}^{t} \theta_i$ e $\psi_{|_N} = f\theta$, pois θ é invariante em T. Como ψ é componente de $\chi_{|_T}$, temos que $f \leq e$. Daí,

$$et\theta(1) = \chi(1) \leq \psi^G(1) = t\psi(1) = ft\theta(1) \leq et\theta(1). \qquad (*)$$

Logo $e = f$ e em particular, $\chi(1) = \psi^G(1)$. Portanto $\chi = \psi^G \in \mathscr{B}$.

(d) Por $(*)$ temos que $[\chi_{|_N}, \theta]_N = e = f = [\psi_{|_N}, \theta]_N$.

(c) Seja $\psi_1 \in \mathscr{A}$ uma componente irredutível de $\chi_{|_T}$ tal que $\psi \neq \psi_1$, temos que $[\chi_{|_T}, \psi_1] > 0$ e pela Reciprocidade de Frobenius

$$[\chi_{|_N}, \theta]_N \geq [(\psi + \psi_1)_{|_N}, \theta]_N = [\psi_{|_N}, \theta]_N + [\psi_{1|_N}, \theta]_N > [\psi_{|_N}, \theta]_N,$$

pois $[\psi_{1|_N}, \theta]_N > 0$. Mas isto contradiz (d). Portanto, ψ é a única componente irredutível de $\chi_{|_T}$ que pertence a $\mathscr{A}$.

(b) Pelo item (a) temos que $Im(F) \subseteq Irr(G)$ e pelo item (d), temos que $Im(F) \subseteq \mathscr{B}$. Vejamos que F é injetora.

Se ψ_1 e $\psi_2 \in \mathscr{A}$ são tais que $F(\psi_1) = F(\psi_2)$, então $\psi_1^G = \psi_2^G = \chi$. Pela Reciprocidade de Frobenius,

$$[\chi_{|_T}, \psi_1]_T = [\chi, (\psi_1)^G]_G > 0 \quad \text{e} \quad [\chi_{|_T}, \psi_2]_T = [\chi, (\psi_2)^G]_G > 0$$

ou seja, ψ_1 e ψ_2 são componentes de $\chi_{|_T}$. Assim, pelo item (c) $\psi_1 = \psi_2$.

Agora vejamos que F é sobrejetora.

Se $\chi \in \mathscr{B}$, então $[\chi_{|_N}, \theta]_N \neq 0$ e θ é uma componente de $\chi_{|_N}$, donde segue que deve existir alguma componente irredutível ψ de $\chi_{|_T}$ tal que $[\psi_{|_N}, \theta]_N \neq 0$, logo $\psi \in \mathscr{A}$. Pelo Teorema de Frobenius, $[\psi^G, \chi]_G = [\psi, \chi_{|_T}]_T \neq 0$, ou seja, χ é uma componente irredutível de ψ^G. Portanto, $\chi = \psi^G$.

∎

Corolário 1.68. *Todo grupo nilpotente é um M-grupo.*

Demonstração. Ver [8, Corollary 6.14].

∎

Para o próximo corolário precisamos da definição seguinte.

Definição 1.69. Seja $\chi \in Irr(G)$. Dizemos que χ é *primitivo* se $\chi \neq \theta^G$, para todo caráter θ de qualquer subgrupo próprio de G.

Corolário 1.70. *Se $\chi \in Irr(G)$ é primitivo, então para todo $N \trianglelefteq G$, $\chi_{|_N}$ é um caráter homogêneo.*

Demonstração. Pelo Teorema de Clifford, $\chi_{|_N} = e\sum_{i=1}^{t} \theta_i$, onde $\theta = \theta_1, \ldots, \theta_t$ são os conjugados distintos de θ em G, $[\chi_{|_N}, \theta] \neq 0$ e $t = |G : I_G(\theta)|$. Então, pelo Teorema 1.67(b), $\chi = \psi^G$ para algum $\psi \in Irr(I_G(\theta))$. Assim, da hipótese de χ ser primitivo, segue que $I_G(\theta) = G$. Portanto $\chi_{|_N} = e\theta$.

∎

Vamos agora demonstrar o Teorema de Gallagher. Esse resultado é consequência de um teorema mais geral, para o qual precisamos da próxima definição.

Definição 1.71. Sejam $H \leqslant G$ e ψ um caráter de H. Dizemos que ψ é extensível a G, se existe um caráter χ de G tal que $\chi_{|_H} = \psi$.

Teorema 1.72. *Sejam $N \trianglelefteq G$ e $\varphi, \theta \in Irr(N)$ invariantes em G tais que $\varphi\theta$ é irredutível e θ é extensível a $\chi \in Irr(G)$. Se*

$$\mathscr{S} = \{\beta \in Irr(G); [\varphi^G, \beta] \neq 0\} \quad e \quad \mathscr{T} = \{\psi \in Irr(G); [(\varphi\theta)^G, \psi] \neq 0\}.$$

Então

$$\begin{aligned} F : \mathscr{S} &\to \mathscr{T} \\ \beta &\mapsto \beta\chi \end{aligned}$$

é uma bijeção.

Demonstração. Temos que $(\varphi^G)_{|_N}$ é múltiplo de φ e comparando os graus temos $(\varphi^G)_{|_N} = |G:N|\varphi$. Daí,

$$[\varphi^G, \varphi^G]_G = [\varphi, (\varphi^G)_{|_N}]_N = |G:N|[\varphi, \varphi]_G = |G:N|.$$

Analogamente, $[(\varphi\theta)^G, (\varphi\theta)^G] = |G:N|$.

Escrevendo $\varphi^G = \sum_{\beta \in \mathscr{S}} e_\beta \beta$, segue do Teorema 1.42(b) que

$$[\varphi^G, \varphi^G] = |G:N| = [\varphi^G\chi, \varphi^G\chi]$$

e assim,

$$\sum_{\beta \in \mathscr{S}} {e_\beta}^2 = \sum_{\beta, \gamma \in \mathscr{S}} e_\beta e_\gamma [\beta\chi, \gamma\chi].$$

Para todo $\beta \in \mathscr{S}$ temos que $e_\beta > 0$, $[\beta\chi, \gamma\chi] \geq 0$ e $[\beta\chi, \beta\chi] \geq 1$, logo $[\beta\chi, \gamma\chi] = 0$, se $\beta \neq \gamma$ e $[\beta\chi, \beta\chi] = 1$. Portanto os $\beta\chi$ são caracteres irredutíveis distintos, para distintos β e são todas as componentes de $(\varphi\theta)^G$.

∎

Um caso particular do Teorema 1.72 é quando $\psi = 1_N$. Este resultado é conhecido como Teorema de Gallagher.

Corolário 1.73 (Gallagher). *Sejam $N \trianglelefteq G$ e $\chi \in Irr(G)$ tais que $\chi_{|_N} = \theta \in Irr(N)$. Então os caracteres $\beta\chi$ com $\hat{\beta} \in Irr(\frac{G}{N})$ são irredutíveis, distintos para distintos $\hat{\beta}$ e são todas as componentes irredutíveis de θ^G.*

Agora vamos utilizar o Teorema de Clifford para demonstrar o próximo resultado.

Teorema 1.74. *Seja* $\frac{K}{L}$ *um chief factor abeliano, isto é,* $K, L \lhd G$ *e não existe* $M \lhd G$ *tal que* $L < M < K$*. Se* $\theta \in Irr(K)$ *é invariante em* G*, então*

(a) $\theta_{|_L} \in Irr(L)$*, ou*

(b) $\theta_{|_L} = e\psi$ *para algum* $\psi \in Irr(L)$ *e* $e^2 = |K : L|$*, ou*

(c) $\theta_{|_L} = \sum_{i=1}^{t} \psi_i$*, onde os* $\psi_i \in Irr(L)$ *são distintos e* $t = |K : L|$*.*

Demonstração. Sejam φ uma componente irredutível de $\theta_{|_L}$ e $T = I_G(\varphi)$. Como θ é invariante em G, todo G-conjugado de φ é uma componente de $\theta_{|_L}$ e portanto é K-conjugado a φ. Daí, $|G : T| = |K : K \cap T|$ e portanto $KT = G$.

Como $L \trianglelefteq K \cap T$, fica bem definido o quociente $\frac{K \cap T}{L}$ e temos que $\frac{K \cap T}{L} \trianglelefteq \frac{K}{L}$, pois $\frac{K}{L}$ é abeliano. Assim, pelo Teorema da Correspondência, $K \cap T \trianglelefteq K$ e pelo Segundo Teorema do Isomorfismo $K \cap T \trianglelefteq T$, donde $K \cap T \trianglelefteq KT = G$. Logo, por hipótese temos $K \cap T = K$ ou $K \cap T = L$.

Se $K \cap T = L$, pelo Teorema de Clifford, $\theta_{|_L} = e \sum_{i=1}^{t} \varphi_i$, onde $t = |K : L|, \varphi_1 = \varphi$ e os $\varphi_i, 1 \leq i \leq t$ são distintos. Dessa forma, $\theta(1) = e|K : L|\varphi(1)$. Por outro lado, como θ é uma componente de φ^K, temos que $\theta(1) \leq |K : L|\varphi(1)$ e portanto $e = 1$. Concluímos assim a demonstração do item (c).

Agora se $K \cap T = K$, então φ é invariante em K e assim $\theta_{|_L} = e\varphi$, para algum e. Seja $\hat{\lambda} \in Irr\left(\frac{K}{L}\right)$, como $\frac{K}{L}$ é abeliano, λ é um caráter linear e $\lambda\theta \in Irr(K)$ é tal que $(\lambda\theta)_{|_L} = \theta_{|_L} = e\varphi$. Suponha que todos os caracteres $\lambda\theta$ são distintos quando $\hat{\lambda}$ percorre $Irr\left(\frac{K}{L}\right)$. Cada um desses $|K : L|$ caracteres é uma componente irredutível de φ^K, pois

$$[\varphi^K, \lambda\theta]_K = [\varphi, (\lambda\theta)_{|_L}]_L = [\varphi, e\varphi]_L = e,$$

assim temos

$$|K : L|e\varphi(1) \leq \varphi^K(1) = |K : L|\varphi(1).$$

Portanto $e = 1$, concluindo a demonstração do item (a).

Agora suponha que $\lambda\theta = \mu\theta$ para alguns $\hat{\lambda}, \hat{\mu} \in Irr\left(\frac{K}{L}\right)$ com $\hat{\lambda} \neq \hat{\mu}$. Seja $U = Ker(\lambda\mu^{-1})$, temos que $L \leqslant U < K$ e θ é zero em $K \setminus U$. Como

θ é invariante em G, segue que θ é zero em $K \setminus U^g$, para todo $g \in G$. Então θ é zero em

$$\bigcup_{g\in G}(K \setminus U^g) = K \setminus \bigcap_{g\in G} U^g = K \setminus L,$$

onde $\bigcap\limits_{g\in G} U^g = L$, pois $\bigcap\limits_{g\in G} U^g \trianglelefteq G$ e $\frac{K}{L}$ é um chief factor.

Dessa forma,

$$1 = [\theta, \theta]_K = \frac{1}{|K|}\sum_{x\in L}|\theta(x)|^2 = \frac{|L|}{|K|}[\theta_L, \theta_L] = \frac{1}{|K:L|}e^2,$$

concluindo a demonstração do item (b).

■

Corolário 1.75. *Seja $N \trianglelefteq G$ tal que $|G : N| = p$, com p primo. Se $\chi \in Irr(G)$, então*

(a) *$\chi_{|_N}$ é irredutível, ou*

(b) *$\chi_{|_N} = \sum\limits_{i=1}^{p}\theta_i$, onde os θ_i são irredutíveis e distintos.*

Demonstração. Considere $K = G$ e $L = N$ no Teorema 1.74. Note que (b) não pode ocorrer pois p não é um quadrado.

■

Corolário 1.76. *Seja $N \trianglelefteq G$ tal que $|G : N| = p$, com p primo. Se $\theta \in Irr(N)$ é invariante em G, então θ é extensível a G.*

Demonstração. Seja χ uma componente irredutível de θ^G. Temos que $\chi_{|_N} = e\theta$ para algum e. Comparando com o Corolário 1.75, temos $e = 1$ e portanto θ é extensível a G.

■

Definição 1.77. Sejam $N \trianglelefteq G$ e $\chi \in Irr(G)$. Dizemos que χ é um *M-caráter relativo* com respeito a N, se existirem um subgrupo H com $N \leqslant H \leqslant G$ e $\psi \in Irr(H)$ tais que $\psi^G = \chi$ e $\psi_{|_N} \in Irr(N)$.

Se todo caráter de G é um M-caráter relativo com respeito a N, então G é um *M-grupo relativo* com respeito a N.

Teorema 1.78. *Seja $N \trianglelefteq G$ tal que $\frac{G}{N}$ é solúvel. Se todo chief factor de todo subgrupo de $\frac{G}{N}$ tem ordem não quadrado, então G é um M-grupo relativo com respeito a N.*

Demonstração. Ver [8, Theorem 6.22].

■

Note que as hipóteses anteriores sobre $\frac{G}{N}$ são automaticamente satisfeitas quando $\frac{G}{N}$ é nilpotente, pois todos os chief factors de subgupos têm ordem prima.

Capítulo 2

Os Teoremas de Brauer

Nosso objetivo aqui é determinar uma condição necessária e suficiente para que uma dada função de classe seja um caráter generalizado, ou pelo menos uma R-combinação linear de caracteres irredutíveis, onde R é um anel tal que $\mathbb{Z} \subseteq R \subseteq \mathbb{C}$.

2.1 - Enunciados e demonstração dos Teoremas

Dada uma função de classe, nem sempre é fácil ver se ela é um caráter ou não. Observamos isso nos seguintes exemplos.

Exemplo 2.1. A função $\psi : G \to \mathbb{C}$ definida por $\psi(g) = |Cl(g)|$ é uma função de classe, mas não é um caráter nem um caráter generalizado de G.

Considere $G = S_4$ e sua tabela de caracteres dada por

g :	1	(12)	(12)(34)	(123)	(1234)
$\|C_G(g)\|$:	24	4	8	3	4
$\|Cl(g)\|$:	1	6	3	8	6
χ_1 :	1	1	1	1	1
χ_2 :	1	-1	1	1	-1
χ_3 :	2	0	2	-1	0
χ_4 :	3	1	-1	0	-1
χ_5 :	3	-1	-1	0	1

Vejamos que ψ não pode ser escrita como uma $\mathbb{Z}$-combinação linear de caracteres irredutíveis.

De fato, se $\psi = \sum_{\chi_i \in Irr(S_4)} a_i\chi_i$, então

$$a_i = [\psi, \chi_i] = \frac{1}{|S_4|}\sum_{g\in S_4} \psi(g)\overline{\chi_i(g)} = \frac{1}{24}\sum_{g_j} |Cl(g_j)|\psi(g_j)\chi_i(g_j),$$

onde g_j são os representantes das classes de conjugação de G. Assim, utilizando a tabela de caracteres de S_4 obtemos $a_1 = \frac{146}{24} \notin \mathbb{Z}$, logo ψ não é um caráter generalizado de G e portanto, pelo Teorema 1.11, temos que ψ não é um caráter de S_4.

Exemplo 2.2. A função $\theta : G \to \mathbb{C}$ definida por $\theta(g) = |C_G(g)|$ é um caráter de G.

Seja $V = \mathbb{C}[G]$ visto como $\mathbb{C}$-espaço vetorial. Defina $\Phi : G \to GL(V)$ por $\Phi(g) \cdot x = gxg^{-1}$, para todo $x \in \mathbb{C}[G]$. Esta função é uma representação de G pois, se $g_1, g_2 \in G$, então

$$\Phi(g_1g_2) \cdot x = g_1g_2x{g_2}^{-1}{g_1}^{-1} = \Phi(g_1) \cdot g_2x{g_2}^{-1} = \Phi(g_1)\Phi(g_2) \cdot x.$$

Para todo $x \in G$, temos que $gxg^{-1} \in G$. Assim, $\Phi(g)$ é uma matriz de permutação e portanto o seu traço é o número de elementos de G que são fixados por esse homomorfismo, ou seja,

$$\theta(g) = |\{x \in G; gxg^{-1} = x\}| = |C_G(g)|.$$

Seguindo o livro de Isaacs [8] vamos apresentar algumas definições e lemas necessários para enunciar e demonstrar o Teorema de Brauer. Outras demonstrações deste importante resultado podem ser encontradas em [1], [7], [10] e [17].

Definição 2.3. Seja R um anel tal que $\mathbb{Z} \subseteq R \subseteq \mathbb{C}$. Uma R-combinação linear de caracteres irredutíveis de G é dita um *R-caráter generalizado* de G.

Denotaremos por $R[Irr(G)]$ o conjunto dos R-caracteres generalizados de G.

O Teorema de Brauer caracteriza as funções de classe que são R-caracteres generalizados e também nos dá uma forma de como escrever os caracteres irredutiveis de um grupo finito.

Definição 2.4. Sejam $\mathscr{H}$ uma família de subgrupos de G e R um anel tal que $\mathbb{Z} \subseteq R \subseteq \mathbb{C}$.

(a) $\mathscr{R}_R(G, \mathscr{H})$ é o conjunto das funções de classe θ de G tais que $\theta_{|_H} \in R[Irr(H)]$, para todo $H \in \mathscr{H}$.

(b) $\mathscr{I}_R(G, \mathscr{H})$ é o conjunto das R-combinações lineares de caracteres ψ^G, para $\psi \in Irr(H)$ e $H \in \mathscr{H}$.

Se $R = \mathbb{Z}$ escreveremos simplesmente $\mathscr{R}(G, \mathscr{H})$ e $\mathscr{I}(G, \mathscr{H})$.

Lema 2.5. *Sejam $\mathscr{H}$ uma coleção de subgrupos de G e R um anel tal que $\mathbb{Z} \subseteq R \subseteq \mathbb{C}$. Então*

(a) $\mathscr{I}(G, \mathscr{H}) \subseteq \mathscr{I}_R(G, \mathscr{H}) \subseteq R[Irr(G)] \subseteq \mathscr{R}_R(G, \mathscr{H})$.

(b) $\mathscr{R}_R(G, \mathscr{H})$ *é um anel em que* $\mathscr{I}_R(G, \mathscr{H})$ *é um ideal.*

Demonstração.

(a) Segue da definição.

(b) Primeiramente observamos que $\mathbb{Z}[Irr(H)]$ é um anel comutativo com identidade 1_H, para todo $H \in \mathscr{H}$. Como $\mathbb{Z} \subseteq R$, segue que $R[Irr(H)]$ também é um anel.

Se $\varphi, \theta \in \mathscr{R}_R(G, \mathscr{H})$, então

$$(\varphi\theta)_{|_H} = \varphi_{|_H}\theta_{|_H} \in R[Irr(H)],$$

ou seja, $\varphi\theta \in \mathscr{R}_R(G, \mathscr{H})$ e portanto $\mathscr{R}_R(G, \mathscr{H})$ é um anel.

Agora sejam $\varphi \in \mathscr{I}_R(G, \mathscr{H})$ e $\theta \in \mathscr{R}_R(G, \mathscr{H})$. Podemos escrever

$$\varphi = \sum_{H \in \mathscr{H}} (\psi_{(H)})^G, \quad \text{com} \quad \psi_{(H)} \in R[Irr(H)]$$

e pelo Teorema 1.62(b) obtemos

$$\varphi\theta = \sum_{H \in \mathscr{H}} (\psi_{(H)})^G \, \theta = \sum_{H \in \mathscr{H}} (\psi_{(H)}\theta_{|_H})^G.$$

Daí $\varphi\theta \in \mathscr{I}_R(G, \mathscr{H})$, pois $\psi_{(H)}\theta_{|_H} \in R[\mathrm{Irr}(H)]$. Portanto $\mathscr{I}_R(G, \mathscr{H})$ é ideal de $\mathscr{R}_R(G, \mathscr{H})$.

■

Segue do Lema 2.5 que para provar que $\mathscr{I}_R(G, \mathscr{H}) = R[Irr(G)]$ é suficiente mostrarmos que $1_G \in \mathscr{I}(G, \mathscr{H})$. Além disso, se provarmos isso para alguma família $\mathscr{H}$ de subgrupos de G, obtemos

$$\mathscr{I}_R(G, \mathscr{H}) = R[Irr(G)] = \mathscr{R}_R(G, \mathscr{H}),$$

para todo anel R tal que $\mathbb{Z} \subseteq R \subseteq \mathbb{C}$.

Agora vamos enunciar o Teorema de Brauer.

Teorema 2.6 (Brauer). *Seja R um anel tal que $\mathbb{Z} \subseteq R \subseteq \mathbb{C}$.*

(a) *Uma função de classe θ de G é um R-caráter generalizado se, e somente se, $\theta_{|_E} \in R[Irr(E)]$ para todo subgrupo elementar $E \subseteq G$.*

(b) *Todo $\chi \in Irr(G)$ é uma $\mathbb{Z}$-combinação linear de caracteres da forma λ^G, para caracteres lineares λ de subgrupos elementares de G.*

Seja $\mathscr{E}$ o conjunto dos subgrupos elementares de G. O item (a) do Teorema 2.6 é exatamente a afirmação de que

$$R[Irr(G)] = \mathscr{R}_R(G, \mathscr{E}).$$

Esta parte do resultado é conhecida como "caracterização dos caracteres."

Todo subgrupo elementar E em $\mathscr{E}$ é nilpotente e portanto é um M-grupo, pelo Corolário 1.68. Assim, para todo $\varphi \in Irr(E)$ temos que $\varphi = \lambda^E$, onde λ é um caráter linear de algum $E_0 \leqslant E$. Como $E_0 \in \mathscr{E}$ e $\varphi^G = (\lambda^E)^G = \lambda^G$, segue que $\mathscr{I}(G, \mathscr{E})$ é exatamente o conjunto das $\mathbb{Z}$-combinações lineares de λ^G, para algum caráter linear $\lambda \in Irr(E)$ com $E \in \mathscr{E}$. Portanto o item (b) do Teorema 2.6 se resume na afirmação de que

$$\mathbb{Z}[Irr(G)] = \mathscr{I}(G, \mathscr{E}).$$

Este resultado é conhecido como "Teorema sobre caracteres induzidos."

Pelo Lema 2.5, a demonstração do Teorema 2.6 segue do fato de 1_G pertencer a $\mathscr{I}(G, \mathscr{E})$. Para verificar isso, precisamos de alguns resultados preliminares.

Lema 2.7 (Banaschewski)**.** *Sejam S um conjunto finito não vazio e R o anel das funções definidas sobre S que tomam valores inteiros. Se a função 1_S não pertence a S, então existem $x \in S$ e um primo p tais que p divide $f(x)$, para toda função $f \in R$.*

Demonstração. Para cada $x \in S$, definimos $I_x = \{f(x); f \in R\}$ e observamos que I_x é um subgrupo aditivo de $\mathbb{Z}$.

Se $x \in S$ é tal que $I_x < \mathbb{Z}$, então $I_x \subseteq (p)$ para algum p primo e portanto p divide $f(x)$, para toda função $f \in R$.

Vamos assumir que $I_x = \mathbb{Z}$, para todo $x \in S$.

Para cada $x \in S$, podemos escolher $f_x \in R$ tal que $f_x(x) = 1$. Assim, $(f_x - 1_S)(x) = 0$, para todo $x \in S$. Logo $\prod_{x \in S}(f_x - 1_S) = 0$ e expandindo esse produto obtemos uma expressão para 1_S como combinação linear de produtos das funções f_x. Portanto $1_S \in R$.

∎

Lema 2.8. *Sejam $H, K \leqslant G$. Temos que*

$$(1_H)^G(1_K)^G = \sum a_U (1_U)^G,$$

para subgrupos $U \subseteq K$ e inteiros $a_U \geq 0$.

Demonstração. Escrevendo $\theta = (1_H)^G$ e utilizando o Teorema 1.42(b), obtemos

$$(1_H)^G(1_K)^G = \theta(1_K)^G = (\theta_{|K} 1_K)^G = (\theta_{|K})^G = ((1_H{}^G)_{|K})^G. \quad (*)$$

Agora $G = \dot{\bigcup}_{i=1}^{m} H r_i K$ e pelo Teorema 1.62,

$$(1_H{}^G)_{|K} = \sum_{j=1}^{m} ((1_H{}^{r_j})_{|_{H^{r_j} \cap K}})^K = \sum_{j=1}^{m} (1_{H^{r_j} \cap K})^K = \sum a_U (1_U)^K,$$

onde $U = H^{r_j} \cap K$. Portanto retornando em $(*)$ e utilizando o Teorema 1.42(c), temos

$$(1_H)^G(1_K)^G = \left(\sum a_U 1_U{}^K\right)^G = \sum a_U (1_U)^G.$$

∎

Corolário 2.9. *Temos as seguintes propriedades.*

(a) *O conjunto das $\mathbb{Z}$-combinações lineares dos caracteres de G da forma $(1_H)^G$ é um anel, o qual denotaremos por $P(G)$.*

(b) *Seja $\mathscr{H}$ uma coleção de subgrupos de G com a propriedade de que se $K \leqslant H \in \mathscr{H}$, então $K \in \mathscr{H}$. Denote por $P(G, \mathscr{H})$ o conjunto das $\mathbb{Z}$-combinações lineares dos caracteres da forma $(1_H)^G$, com $H \in \mathscr{H}$. Então $P(G, \mathscr{H})$ é um ideal de $P(G)$.*

Lema 2.10. *Se $x \in G$ e p é um número primo, então existe um subgrupo p-quase elementar $H \subseteq G$ tal que $(1_H)^G(x)$ não é divisível por p.*

Demonstração. Sejam C o p-complemento do grupo $\langle x \rangle$, único pelo Lema 1.52 pois $\langle x \rangle$ é cíclico, e $N = N_G(C)$. Como $C \trianglelefteq \langle x \rangle$, fica bem definido o quociente $\frac{\langle x \rangle}{C}$ que é um p-grupo abeliano. Dessa forma, podemos escolher $\frac{H}{C} \in Syl_p\left(\frac{N}{C}\right)$ tal que $\langle x \rangle \leqslant H$. Se $\left|\frac{H}{C}\right| = p^\alpha$, então $|H| = |C|p^\alpha$ e como $mdc(|C|, p) = 1$, temos que C é um p-complemento normal para H, ou seja, H é p-quase elementar.

Por outro lado,

$$\begin{aligned}(1_H)^G(x) = & \frac{1}{|H|} \sum_{g \in G} 1_H{}^{\circ}(gxg^{-1}) = \frac{1}{|H|} |\{g \in G; gxg^{-1} \in H\}| \\ = & \frac{1}{|H|} |\{g \in G; Hgx = Hg\}| = |\{Hy; Hyx = Hy, y \in G\}|.\end{aligned}$$

Se $Hyx = Hy$, então $x^{y^{-1}} \in H$ o que implica $C^{y^{-1}} \subseteq H$. Como $mdc(|C|, p) = 1$, podemos escrever $H = PC$, onde P é um p-grupo. Como $H \trianglelefteq G$, segue que $H = H^{y^{-1}} = P^{y^{-1}} C^{y^{-1}}$ e portanto $C^{y^{-1}}$ é um p-complemento normal de H. Pelo Lema 1.52, temos que C é o único p-complemento de H, logo $C^{y^{-1}} = C$ e então $y \in N$. Assim, para determinar $(1_H)^G(x)$, devemos contar o número de pontos fixados pela ação do grupo $\langle x \rangle$ sobre as classes de H em N.

Agora observamos que $C \trianglelefteq N$ e $C \leqslant H$. Dessa forma, para todo $c \in C$ e todo $y \in N$, temos $Hyc = Hy$ e portanto C está contido no núcleo da ação do grupo $\langle x \rangle$ sobre o conjunto $\{Hy;\ y \in N\}$.

Como $\frac{\langle x \rangle}{C}$ é um p-grupo, segue que o número de classes não fixadas é divisível por p e portanto, pela Equação de Classes,

$$(1_H)^G(x) \equiv |N : H| \pmod{p}.$$

Pela escolha de H, temos que $p \nmid |N : H|$ e portanto p não divide $(1_H)^G(x)$.

■

Teorema 2.11 (L. Solomon)**.** *Seja $\mathscr{H}$ o conjunto dos subgrupos quase elementares de G e $\mathscr{H}_p$ o conjunto dos subgrupos p-quase elementares de G, para algum primo p. Então*

(a) $1_G \in P(G, \mathscr{H})$;

(b) $m1_G \in P(G, \mathscr{H}_p)$ *para algum* $m \in \mathbb{Z}$ *tal que* $p \nmid m$.

Demonstração.

(a) Pelo Corolário 2.9, temos que $P(G, \mathscr{H})$ é um anel de $\mathbb{Z}$-funções sobre G. Suponha que $1_G \notin P(G, \mathscr{H})$. Pelo Lema 2.7, existe $x \in G$ e um número primo p tal que $p \mid \varphi(x)$, para toda função $\varphi \in P(G, \mathscr{H})$. Em particular $p \mid (1_H{}^G)(x)$, contradizendo o Lema 2.10. Portanto $1_G \in P(G, \mathscr{H})$.

(b) Definindo $R = \{\varphi + np1_G ; \varphi \in P(G, \mathscr{H}_p), n \in \mathbb{Z}\}$, observamos que R é um anel, não necessáriamente com unidade. Suponha que existem $x \in G$ e um primo q tais que $q \mid \varphi(x)$, para toda função $\varphi \in R$. Como $p1_G \in R$, temos que $q \mid p1_G(x)$, donde segue que $q = p$, contradizendo o Lema 2.10. Assim, pelo Lema 2.7, temos que $1_G \in R$ e portanto $(1 - np)1_G \in P(G, \mathscr{H})$, para algum $n \in \mathbb{Z}$.

■

Lema 2.12. *Suponha que $G = CP$ onde $C \trianglelefteq G$, P é um p-grupo e $p \nmid |C|$. Seja λ um caráter linear de C, invariante em G e suponha que $C_C(P) \subseteq Ker(\lambda)$. Então $\lambda = 1_C$.*

Demonstração. Seja $K = Ker(\lambda)$. Pela Observação 1.24, definimos o caráter $\hat{\lambda} : \frac{C}{K} \to \mathbb{C}$ por $\hat{\lambda}(Kx) = \lambda(kx)$, para qualquer $k \in K$.

Afirmação 1: $Kc_1 = Kc_2$ se, e somente se, $\hat{\lambda}(Kc_1) = \hat{\lambda}(Kc_2)$, para todos $c_1, c_2 \in C$.

Como λ é linear, em particular é um homomorfismo, temos

$$\begin{aligned} \lambda(k_1c_1) = \hat{\lambda}(Kc_1) = \hat{\lambda}(Kc_2) = \lambda(k_2c_2) &\iff \lambda(k_1c_1(k_2c_2)^{-1}) = 1 \\ &\iff k_1c_1(k_2c_2)^{-1} \in K \\ &\iff Kc_1 = Kc_2. \end{aligned}$$

Afirmação 2: O caráter $\hat{\lambda}$ é invariante sob a ação de P.

De fato, como $C \trianglelefteq G$ e $K \leqslant C$, temos que para cada $k \in K$ e cada $p \in P$, existe $c \in C$ tal que

$$pk = cp.$$

Pelo fato de K ser um subgrupo normal de C, temos que

$$cK = Kc \Rightarrow ck = k_1c \Rightarrow c = k_1ck^{-1}, \text{ para algum } k_1 \in K.$$

Escrevendo $y = ck^{-1}p$, obtemos $pk = k_1ck^{-1}p = k_1y$ e assim,

$$(kx)^p = pkxp^{-1} = k_1yxp^{-1}.$$

Por outro lado,

$$\begin{aligned} \hat{\lambda}^p(Kx) &= \hat{\lambda}(pKxp^{-1}) = \hat{\lambda}(Kyxp^{-1}) \\ &= \lambda(k_1yxp^{-1}) = \lambda(pkxp^{-1}) \\ &= \lambda^p(kx) = \lambda(kx), \text{ pois } \lambda \text{ é invariante sob a ação de } P \\ &= \hat{\lambda}(Kx). \end{aligned}$$

Pelas afirmações 1 e 2 temos que $(Kx)^p = Kx$, para todo $p \in P$ e todo $x \in C$. Portanto P normaliza cada classe Kx para $x \in C$.

Na ação de conjugação de P sobre o conjunto $Kx = \{kx; k \in K\}$, temos que o número de pontos não fixados por essa ação é divisível por p. Assim, pela Equação de Classes, $|Kx| \equiv |Fix_P(Kx)| \pmod p$, onde $Fix_P(Kx) = \{kx; pkxp^{-1} = kx, k \in K \ , \forall\ p \in P\}$. Mas $|Kx| = |K|$ não é divisível por p, logo $p \nmid |Fix_P(Kx)|$ e então $Kx \cap C_C(P) \neq \emptyset$. Por hipótese $C_C(P) \subseteq K$, donde concluimos que $Kx = K$, para qualquer $x \in C$, ou seja, $K = C$ e portanto $\lambda = 1_C$.

∎

Agora vamos demonstrar o Teorema de Brauer, utilizando o Teorema 2.11(a) para reduzir o problema a subgrupos quase elementares.

Demonstração. Queremos mostrar que $1_G \in \mathscr{I}(G, \mathscr{E})$. Para isso, vamos usar indução sobre $|G|$.

Se $|G| = 1$, então G é elementar e portanto $1_G \in \mathscr{I}(G, \mathscr{E})$.

Suponha que $|G| > 1$. Por hipótese de indução, $1_H \in \mathscr{I}(H, \mathscr{E}_H)$ para todo $H < G$, onde $\mathscr{E}_H$ é o conjunto dos subgrupos elementares de

H. Assim, pelo Lema 2.5, temos que $\mathbb{Z}[Irr(H)] = \mathscr{I}(H, \mathscr{E}_H)$, para todo $H < G$.

Para toda $\varphi \in \mathscr{I}(H, \mathscr{E}_H)$,

$$\varphi = \sum_{K \in \mathscr{E}_H} (\psi_{(K)})^H, \quad \text{onde } \psi_{(K)} \in \mathbb{Z}[Irr(K)]$$

e pelo Teorema 1.42(c)

$$\varphi^G = \sum_{K \in \mathscr{E}_H} ((\psi_{(K)})^H)^G = \sum_{K \in \mathscr{E}_H} (\psi_{(K)})^G,$$

donde segue que $\varphi^G \in \mathscr{I}(G, \mathscr{E}_H) \subseteq \mathscr{I}(G, \mathscr{E})$. Assim, para todo $H < G$ e $\varphi \in \mathscr{I}(H, \mathscr{E}_H)$ temos que $\varphi^G \in \mathscr{I}(G, \mathscr{E})$. Visto isso, é suficiente mostrar que 1_G é uma $\mathbb{Z}$-combinação linear de caracteres induzidos de subgrupos próprios de G.

Seja $\mathscr{H}$ o conjunto dos subgrupos quase elementares de G. Se G não é quase elementar, pelo Teorema 2.11(a) temos que $1_G \in P(G, \mathscr{H})$ e portanto é uma $\mathbb{Z}$-combinação linear de caracteres da forma $(1_H)^G$, onde $H \in \mathscr{H}$ é um subgrupo próprio de G.

Suponha que G é quase elementar e seja C um p-complemento cíclico e normal de G. Considere $P \in Syl_p(G)$ e $Z = C_C(P)$. Podemos supor que G não é elementar. De fato, se G é elementar, por definição $G \in \mathscr{E}$ e $1_G \in \mathscr{I}(G, \mathscr{E})$.

Afirmamos que $Z < C$ e $E = PZ < G$.

De fato, se fosse $Z = C$, teríamos $P \lhd G$, contradizendo o fato de que G não é elementar, logo $Z < C$. Para demonstrar que $E = PZ \leq G$, observamos que para todo $g \in G$ existem $c \in C$ e $p \in P$ tais que $g = cp$ e assim, usando o fato de C ser abeliano,

$$gz = cpz = czp = zcp = zg,$$

para todo $z \in Z$, logo $Z \leqslant Z(G) \lhd G$ e portanto $E \leqslant G$. Agora

$$|E| = |P||Z| \neq |C||P| = |G|,$$

implicando que E é um subgrupo próprio de G.

Escrevendo $(1_E)^G = 1_G + \Xi$, onde Ξ é um caráter, possivelmente redutível, de G, devemos mostrar que toda componente irredutível de Ξ é obtida por indução de um subgrupo próprio de G, dessa forma teremos

$$1_G = (1_E)^G - \Xi \in \mathscr{I}(G, \mathscr{E}).$$

Note que $CE = C(ZP) = CP = G$ e $C \cap E = Z$. De fato, sendo $E = PZ$ temos que se $x \in C \cap E$ então podemos escrever $x = pz$, com $z \in Z$ e $p \in P$. Assim,

$$xz^{-1} = p \in C \cap P = \{1\} \Rightarrow xz^{-1} = 1 \Rightarrow x = z \in Z,$$

logo $C \cap E \subseteq Z$. Por outro lado, $Z \subseteq C$ e $Z \subseteq E$. Portanto temos $C \cap E = Z$.

Seja χ uma componente irredutível de Ξ. Como $G = CE$, pelo Teorema 1.62,

$$1_C + \Xi_{|_C} = ((1_E)^G)_{|_C} = ((1_E)_{|_{E\cap C}})^C = (1_Z)^C.$$

Daí, pela Reciprocidade de Frobenius,

$$[1_C + \Xi_{|_C}, 1_C] = [(1_Z)^C, 1_C] = [1_Z, 1_Z] = 1,$$

donde segue que $[\Xi_{|_C}, 1_C] = 0$ e portanto $[\chi_{|_C}, 1_C] = 0$.

Considere λ uma componente irredutível de $\chi_{|_C}$, então $\lambda \neq 1_C$. Como $Z \lhd G$, segue que $Z \subseteq Ker((1_E)^G)$. Além disso, para todo $z \in Z$,

$$\begin{aligned}(1_E)^G(z) = (1_E)^G(1) \quad &\Rightarrow 1_G(z) + \Xi(z) = 1_G(1) + \Xi(1)\\ &\Rightarrow \Xi(z) = \Xi(1)\\ &\Rightarrow Z \subseteq Ker(\Xi).\end{aligned}$$

Pelo Lema 1.21, segue que $Z \subseteq Ker(\chi)$, donde concluímos que $Z \subseteq Ker(\lambda)$ e pelo Lema 2.12, λ não é invariante em G. Portanto $T = I_G(\lambda)$ é subgrupo próprio de G e pelo Teorema 1.67(b), resulta que $\chi = \psi^G$, para algum $\psi \in Irr(T)$.

■

Veremos agora um caso especial do item (a) do Teorema de Brauer.

Corolário 2.13. *Seja χ uma função de classe de G. Suponha*

(a) $\chi_{|_E}$ *é um caráter generalizado para todo subgrupo elementar $E \subseteq G$;*

(b) $[\chi, \chi] = 1$*;*

(c) $\chi(1) \geq 0$.

Então $\chi \in Irr(G)$.

Demonstração. Pela hipótese (a) e Teorema 2.6(a), temos que $\chi = \sum a_\xi \xi$, onde $\xi \in Irr(G)$ e $a_\xi \in \mathbb{Z}$. Assim, da hipótese (b) temos no máximo um coeficiente $a_\xi \neq 0$ e este $a_\xi = \pm 1$. Assim $\chi = \pm\ \xi$, para algum caráter $\xi \in Irr(G)$. Como $\xi(1) > 0$, segue de (c) que $\chi \in Irr(G)$.

■

Corolário 2.14. *Sejam p um número primo e $\mathscr{E}_p$ o conjunto dos subgrupos p-elementares de G. Temos que*

$$m1_G \in \mathscr{I}(G, \mathscr{E}_p),$$

para algum $m \in \mathbb{Z}$ com $p \nmid m$.

Demonstração. Pelo Teorema 2.11(b), existe $m \in \mathbb{Z}$ com $p \nmid m$ tal que $m1_G$ é uma $\mathbb{Z}$-combinação linear de caracteres da forma $(1_H)^G$ para subgrupos p-quase elementares $H \subseteq G$.

Denote por $\mathscr{E}_H$ o conjunto dos subgrupos elementares de H. Se H é p-quase elementar, então $\mathscr{E}_H \subseteq \mathscr{E}_p$ e pelo Teorema 2.6(b) temos

$$1_H = \sum a_\lambda \lambda^H,$$

onde λ é um caráter linear de algum subgrupo elementar de H.

Logo, pelo Teorema 1.42(c),

$$(1_H)^G = \sum a_\lambda \lambda^G \in \mathscr{I}(G, \mathscr{E}_H) \subseteq \mathscr{I}(G, \mathscr{E}_p).$$

Portanto $m1_G \in \mathscr{I}(G, \mathscr{E}_p)$.

■

2.2 - Algumas Particularizações dos Teoremas

Vamos aprimorar o Teorema de Brauer sobre caracteres induzidos, o qual afirma que todo caráter irredutível de um grupo G é uma $\mathbb{Z}$-combinação linear de caracteres da forma λ^G, onde λ é um caráter linear de algum subgrupo elementar de G. Esse resultado é de van der Waall [18].

Teorema 2.15 (van der Waall). *Seja $\chi \in Irr(G)$ tal que $\chi \neq 1_G$. Então χ é uma $\mathbb{Z}$-combinação linear de caracteres monomiais de G, onde cada caráter monomial não contém 1_G como componente irredutível.*

Demonstração. Seja $\mathscr{H}$ o conjunto dos subgrupos p-quase elementares de G. Pelo Teorema 2.11,

$$1_G = \sum_{H \in \mathscr{H}} a_H (1_H)^G, \quad \text{onde } a_H \in \mathbb{Z}$$

e pelo Teorema 1.42(b), temos

$$\chi(1_H)^G = (1_H \chi_{|_H})^G = (\chi_{|_H})^G.$$

Assim,

$$\sum_{H \in \mathscr{H}} a_H \chi (1_H)^G = \sum_{H \in \mathscr{H}} a_H (\chi_{|_H})^G \Rightarrow \chi \sum_{H \in \mathscr{H}} a_H (1_H)^G = \sum_{H \in \mathscr{H}} a_H (\chi_{|_H})^G \Rightarrow$$

$$\chi = \sum_{H \in \mathscr{H}} a_H (\chi_{|_H})^G.$$

Escrevendo $\chi_{|_H} = b_H 1_H + T_{|_H}$, onde $b_H \in \mathbb{Z}_+$ e $T_{|_H}$ é zero ou $T_{|_H} = \sum_i \xi_i$, com $1_H \neq \xi_i \in Irr(H)$. Observamos que tais ξ_i são caracters monomiais, pelo Corolário 1.59. Daí,

$$\chi = \sum_{H \in \mathscr{H}} a_H b_H (1_H)^G + \sum_{H \in \mathscr{H}} a_H (T_{|_H})^G,$$

onde $(T_{|_H})^G$ é zero ou $(T_{|_H})^G = \sum_i {\xi_i}^G$, com ${\xi_i}^G$ caráter monomial de G que não tem 1_G como componente irredutível, pois pela Reciprocidade de Frobenius, $[1_G, {\xi_i}^G] = [1_H, \xi_i] = 0$.

Por outro lado, podemos escrever

$$\sum_{H \in \mathscr{H}} a_H b_H (1_H)^G = - \sum_{H \in \mathscr{H}} a_H b_H ((1_{\{1\}})^H - 1_H)^G + \sum_{H \in \mathscr{H}} a_H b_H ((1_{\{1\}})^H)^G.$$

Como cada subgrupo quase elementar H é um é um M-grupo, temos

$$(1_{\{1\}})^H - 1_H = \sum_i \gamma_i,$$

onde $\gamma_i \in Irr(H)$ é monomial e diferente de 1_H, pois pela Reciprocidade de Frobenius,

$$[(1_{\{1\}})^H - 1_H, 1_H] = [1_{\{1\}}, 1_{\{1\}}] - [1_H, 1_H] = 0,$$

ou seja, $[\sum_i \gamma_i, 1_H] = \sum_i [\gamma_i, 1_H] = 0$, logo $[\gamma_i, 1_H] = 0$.

De maneira análoga ao que fizemos anteriormente,

$$((1_{\{1\}})^H - 1_H)^G = \sum_i \gamma_i{}^G,$$

onde cada $\gamma_i{}^G$ é um caráter monomial de G que não contém 1_G como componente irredutível.

Afirmamos que $\sum_{H \in \mathscr{H}} a_H b_H = 0$ e $\sum_{H \in \mathscr{H}} a_H b_H ((1_{\{1\}})^H)^G = 0$.

De fato,

$$\begin{aligned} 0 = [\chi, 1_G] = [\sum_{H \in \mathscr{H}} a_H (\chi_{|H})^G, 1_G] &= \sum_{H \in \mathscr{H}} a_H [(\chi_{|H})^G, 1_G] \\ &= \sum_{H \in \mathscr{H}} a_H [\chi_{|H}, 1_H] \\ &= \sum_{H \in \mathscr{H}} a_H b_H. \end{aligned}$$

Daí, para todo $x \in G$

$$\begin{aligned} \sum_{H \in \mathscr{H}} a_H b_H ((1_{\{1\}})^H)^G(x) &= \sum_{H \in \mathscr{H}} a_H b_H (1_{\{1\}})^G(x) \\ &= \sum_{H \in \mathscr{H}} a_H b_H \sum_{g \in G} (1_{\{1\}})^\circ(gxg^{-1}) \\ &= \begin{cases} |G| \sum_{H \in \mathscr{H}} a_H b_H, & \text{se } x = 1 \\ 0, & \text{se } x \neq 1 \end{cases} \\ &= 0. \end{aligned}$$

Portanto,

$$\chi = -\sum_{H \in \mathscr{H}} a_H b_H ((1_{\{1\}})^H - 1_H)^G + \sum_{H \in \mathscr{H}} a_H (T_{|H})^G$$

é uma $\mathbb{Z}$-combinação linear de caracteres monomiais de G, onde cada caráter monomial não contém 1_G como componente irredutível.

■

Agora vamos considerar um grupo solúvel finito e particularizar o Teorema de Brauer sobre caracteres induzidos. Este é um resultado de Wilde [19].

Primeiramente vamos demonstrar o seguinte resultado.

Lema 2.16. *Sejam G um grupo solúvel finito e $\chi \in Irr(G)$. Suponha que χ permanece irredutível quando é restrito a um p-subgrupo de Sylow de G. Então*

$$\chi = \sum_F a_F (\gamma_{(F)})^G,$$

onde F é um subgrupo elementar de G e $\gamma_{(F)} \in Lin(F)$. Além disso, $\chi(1)$ divide cada índice $|G : F|$, para cada F tal que $a_F \neq 0$.

Demonstração. Pelo item (b) do Teorema de Brauer,

$$1_G = \sum_E a_E (\lambda_{(E)})^G,$$

onde E é um subgrupo elementar de G, o caráter $\lambda_{(E)} \in Irr(E)$ é linear e $a_E \in \mathbb{Z}^*$. Multiplicando por χ e utilizando o Teorema 1.42(b), obtemos

$$\chi = \sum_E a_E (\lambda_{(E)})^G \chi = \sum_E a_E (\lambda_{(E)} \chi_{|E})^G. \qquad (*)$$

Cada subgrupo E é nilpotente, portanto é um M-grupo, pelo Corolário 1.68. Assim,

$$\chi_{|E} = \sum_{F \subseteq E} b_F (\xi_{(F)})^E,$$

onde b_F é um inteiro positivo não nulo e $\xi_{(F)} \in Lin(F)$. Daí, em $(*)$ obtemos

$$\begin{aligned}
\chi &= \sum_E a_E \left(\lambda_{(E)} \sum_{F \subseteq E} b_F (\xi_{(F)})^E \right)^G \\
&= \sum_E a_E \sum_{F \subseteq E} b_F \left(\left((\lambda_{(E)})_{|F} \xi_{(F)} \right)^E \right)^G, \text{ pelo Teorema 1.42(b)} \\
&= \sum_E a_E \sum_{F \subseteq E} b_F ((\lambda_{(E)})_{|F} \xi_{(F)})^G, \text{ pelo Teorema 1.42(c)} \\
&= \sum_{F \subseteq E} c_F (\lambda_{(E)_{|F}} \xi_{(F)})^G,
\end{aligned}$$

onde $\lambda_{(E)_{|F}}, \xi_{(F)} \in Irr(F)$ são caracteres lineares tais que

$$[\lambda_{(E)_{|F}} \xi_{(F)}, \chi_{|F}]_F \neq 0$$

e F é um subgrupo elementar, pelo Lema 1.54(b). Escrevendo $F = Q \times H$, onde Q é um p-grupo e H é um p'-grupo, temos que

$$\lambda_{(E)_{|F}} \xi_{(F)} = \alpha \cdot \beta,$$

onde α é um caráter irredutível de Q e β é um caráter irredutível de H.

Seja P um p-subgrupo de Sylow de G que contém Q. Pela Reciprocidade de Frobenius,

$$[\alpha^P, \chi_{|_P}]_P = [\alpha, \chi_{|_Q}]_Q \neq 0.$$

Afirmação: $\chi(1)$ divide $\alpha^P(1) = |P : Q|\alpha(1)$.

Vamos dividir a demonstração em casos.

Caso 1: Suponha que $Q \subseteq P \in Syl_p(G)$ seja maximal em P, então $|P : Q| = p$ e $Q \lhd P$.

Pelo Corolário 1.75, para todo caráter $\psi \in Irr(P)$ tal que $[\psi_{|_Q}, \alpha] > 0$, temos duas possibilidades para $\psi_{|_Q}$,

(1) $\psi_{|_Q}$ é irredutível, o que implica que $\psi(1) = \alpha(1)$. Logo $\psi(1) \mid \alpha^P(1)$.

(2) $\psi_{|_Q}(1) = p \cdot \alpha(1) = |P : Q|\alpha(1) = \alpha^P(1)$.

Logo para todo $\psi \in Irr(P)$ temos que $\psi(1) \mid \alpha^P(1)$. Em particular, $\chi(1) \mid \alpha^P(1)$, pois por hipótese temos que $\chi_{|_P} \in Irr(P)$.

Caso 2: Suponha que existe $N \lhd P$ tal que N é maximal em P e Q é maximal em N. Assim temos $Q \lhd N \lhd P$ tais que $|P : N| = |N : Q| = p$ e $|P : Q| = p^2$. Pelo Corolário 1.75 temos duas possibilidades para $\psi_{|_N}$

(1) $\psi_{|_N}$ é irredutível. Daí aplicando o Corolário 1.75 aos grupos N e Q, temos duas possibilidades para $\psi_{|_Q}$.

  (1.1) $\psi_{|_Q}$ é irredutível, donde segue que $\alpha(1) = \psi(1)$ e portanto $\psi(1) \mid \alpha^P(1)$.

  (1.2) $\psi_{|_Q} = \sum_{i=1}^{p} \alpha_i$, donde segue que $\psi(1) = p \cdot \alpha(1) = \frac{\alpha^P(1)}{p}$ e portanto $\psi(1) \mid \alpha^P(1)$.

(2) $\psi_{|_N} = \sum_{i=1}^{p} \theta_i$, onde $\theta_i \in Irr(N)$. Então pelo Corolário 1.75, para cada θ_i temos duas possibilidades

  (2.1) $\theta_{i|_Q}$ é irredutível, implicando que $\psi(1) = p \cdot \alpha(1) = \frac{\alpha^P(1)}{p}$. Logo $\psi(1) \mid \alpha^P(1)$.

  (1.2) $\theta_{i|_Q} = \sum_{i=1}^{p} \gamma_i$, com $\gamma_i \in Irr(Q)$. Logo $\psi(1) = p^2 \cdot \alpha(1) = \alpha^P(1)$.

Portanto, $\psi(1) \mid \alpha^P(1)$. Em particular, $\chi(1) \mid \alpha^P(1)$.

Caso 3: Vamos considerar Q um subgrupo qualquer de P.

Como P é um p-grupo, podemos obter uma série subnormal

$$Q \lhd N_1 \lhd \cdots \lhd N_k = P,$$

tal que Q é maximal de índice p em N_1, e N_i é maximal de índice p em N_{i+1}, para todo $i = 1, \ldots, k-1$. Logo aplicando indutivamente o caso anterior, segue que $\chi(1)$ divide $\alpha^P(1)$. Assim concluímos a demonstração da afirmação.

Obtivemos que $\chi(1)$ divide $\alpha^P(1) = |P : Q| = |G : F|_p$ e portanto, $\chi(1)$ divide $|G : F|$.

■

Teorema 2.17 (Wilde). *Sejam G um grupo solúvel finito e $\chi \in Irr(G)$. Então*

$$\chi = \sum_E a_E(\lambda_{(E)})^G,$$

onde $E \subseteq G$ é um subgrupo elementar de G e $\lambda_{(E)} \in Lin(E)$. Além disso, $\chi(1)$ divide cada índice $|G : E|$, para todo E tal que $a_E \neq 0$.

Demonstração. Procederemos por indução sobre $|G|$.

Se $|G| = 1$ o resultado segue. Supondo que $|G| > 1$, vamos dividir a demonstração em dois casos.

Caso 1: Vamos supor que χ não seja um caráter primitivo.

Se $\chi = \theta^G$, onde θ é um caráter de algum subgrupo próprio H de G, então pela Reciprocidade de Frobenius,

$$1 = [\theta^G, \chi] = [\theta, \chi_{|H}]_H.$$

Pelo item (b) do Teorema de Brauer,

$$\theta = \sum_E a_E(\lambda_{(E)})^H,$$

donde segue que $\chi = \sum_E a_E(\lambda_{(E)})^G$ e como $|H| < |G|$, por hipótese de indução temos que $\theta(1) \mid |H : E|$ e portanto $\chi(1) = \theta(1)|G : H|$ divide $|G : E|$.

Caso 2: Se χ é primitivo, supomos que $\chi(1) > 1$ e assim podemos assumir que $\chi(1)$ é divisível por um primo p.

Como G é um grupo solúvel finito, temos que existe uma série normal

$$1 = G_0 < G_1 < \cdots < G_n = G,$$

tal que $\frac{G_i}{G_{i-1}}$ tem ordem prima, para todo $i = 1, \ldots, n$. Além disso, pelo Corolário 1.70, temos que $\chi_{|G_i}$ é homogêneo para todo $i = 0, 1, \ldots, n$. Logo, pelo Teorema 1.48, temos que $\chi = \chi_p \cdot \chi_{p'}$, onde χ_p é p-especial e $\chi_{p'}$ é p'-especial.

Pelo Teorema 1.50, a restrição de χ_p a um p-subgrupo de Sylow de G é um caráter irredutível e então pelo Lema 2.16, temos que

$$\chi_p = \sum_E a_E(\lambda_{(E)})^G,$$

onde E é um subgrupo elementar de G tal que $\chi_p(1) = \chi(1)_p$ divide $|G : E|$.

Afirmamos que

$$\chi_{p'} = \sum_F b_F(\mu_{(F)})^G,$$

onde F é um subgrupo elementar de G, $\mu_{(F)}$ é um caráter linear de F e $|G : F|$ é divisível por $\chi(1)_{p'}$.

Essa demonstração será feita por indução sobre a quantidade de números primos que dividem $\chi(1)$.

Se $p' = \{p_1\}$, pelo que vimos anteriormente,

$$\chi_{p'} = \chi_{p_1} = \sum_H c_H(\theta_{(H)})^G,$$

onde H é um subgrupo elementar de G, o caráter $\theta_{(H)} \in Lin(H)$ e $|G : H|$ é divisível por $\chi_{p'}(1)$.

Se $p' = \{p_1, p_2, \ldots, p_n\}$, pelo Teorema 1.48,

$$\chi_{p'} = \chi_{p_1} \cdot \chi_{p_1{}'}, \text{ onde } p_1{}' = \{p_2, \ldots, p_n\}.$$

Assim, pela hipótese de indução temos que

$$\chi_{p_1{}'} = \sum_K d_K(\gamma_{(K)})^G,$$

com K subgrupo elementar de G, o caráter $\gamma_{(K)} \in Lin(K)$ e $|G : K|$ divisível por $\chi_{p_1{}'}(1)$.

Assim,

$$\chi_{p'} = \chi_{p_1} \cdot \chi_{p_1'} \Rightarrow \sum_{H,K} c_H d_K (\theta_{(H)})^G (\gamma_{(K)})^G. \qquad (*)$$

Escrevendo $G = \dot{\bigcup} HsK$ e utilizando o Teorema 1.62,

$$\begin{aligned}\left((\theta_{(H)})^G\right)_{|K} \gamma_{(K)} &= \sum_{s\in H\backslash G/K} \left(\theta^s{}_{|(H^s\cap K)}\right)^H \gamma_{(K)} \\ &= \sum_{s\in H\backslash G/K} \left(\theta^s{}_{|(H^s\cap K)} \gamma_{|(H^s\cap K)}\right)^K,\end{aligned}$$

onde na última igualdade utilizamos o Teorema 1.42(b). Daí, em $(*)$ temos

$$\begin{aligned}\chi_{p'} &= \sum_{H,K} c_H d_K (\theta_{(H)})^G (\gamma_{(K)})^G \\ &= \sum_{H,K} c_H d_K \left(({\theta_{(H)}}^G)_{|K} \gamma_{(K)}\right)^G, \text{ pelo Teorema 1.42(b)} \\ &= \sum_{H,K} c_H d_K \sum_{s\in H\backslash G/K} \left[\left(\theta^s{}_{|(H^s\cap K)} \gamma_{|(H^s\cap K)}\right)^K\right]^G \\ &= \sum_{H,K} c_H d_K \sum_{s\in H\backslash G/K} \left(\theta^s{}_{|(H^s\cap K)} \gamma_{|(H^s\cap K)}\right)^G, \text{ pelo Teorema 1.42(c).}\end{aligned}$$

Note que $\theta^s{}_{|(H^s\cap K)} \gamma_{|(H^s\cap K)}$ é um caráter linear do subgrupo elementar $H^s \cap K$. Vejamos que cada índice $|G : H^s \cap K|$ é divisível por $\chi_{p'}(1)$.

De fato, como vimos anteriormente,

$$\chi(1)_{p_1} \mid |G : H| \text{ e } \chi(1)_{p_1'} \mid |G : K|.$$

Então escrevendo

$$|G : H^s \cap K| = \frac{|G|}{|H^s|} \frac{|H^s|}{|H^s \cap K|} = |G : H^s| \frac{|H^s|}{|H^s \cap K|}$$

e

$$|G : H^s \cap K| = \frac{|G|}{|K|} \frac{|K|}{|H^s \cap K|} = |G : K| \frac{|K|}{|H^s \cap K|}$$

temos que $\chi(1)_{p_1} \mid |G : H^s \cap K|$ e $\chi(1)_{p_1'} \mid |G : H^s \cap K|$. Portanto como $mdc(\chi(1)_{p_1}, \chi(1)_{p_1'}) = 1$, temos que $\chi(1)_{p_1} \cdot \chi(1)_{p_1'} = \chi_{p'}(1)$ divide $|G : H^s \cap K|$.

Portanto, considerando o subgrupo elementar $F = H^s \cap K$ e o caráter linear $\mu_{(F)} = {\theta^s}_{|(H^s \cap K)}\gamma_{|(H^s \cap K)}$, concluímos que

$$\chi_{p'} = \sum_F b_F (\mu_{(F)})^G,$$

com $|G : F|$ divisível por $\chi_{p'}(1)$.

Agora utilizando o fato de que $\chi = \chi_p \cdot \chi_{p'}$, temos que

$$\chi = \sum_{E,F} a_E b_F (\lambda_{(E)})^G (\mu_{(F)})^G,$$

então por um argumento análogo ao utilizado na demonstração da afirmação anterior, obtemos

$$\chi = \sum_{E,F} a_E b_F \sum_{s \in E \backslash G / F} \left({\lambda^s}_{|(E^s \cap F)} \mu_{|(E^s \cap F)} \right)^G,$$

onde ${\lambda^s}_{|(E^s \cap F)} \mu_{|(E^s \cap F)}$ é um caráter linear do subgrupo elementar $E^s \cap F$ e cada índice $|G : E^s \cap F|$ é divisível por $\chi(1)$.

■

Capítulo 3

Uma aplicação do Teorema de Brauer

Neste capítulo, iremos estudar um resultado de Isaacs [9]. Aplicando o Teorema de Brauer, mostraremos que um múltiplo adequado da função que associa a cada elemento g de um grupo finito G a dimensão do espaço dos vetores fixados por $\Phi(g)$ é um caráter generalizado, onde Φ é uma representação de G.

3.1 - Classes Racionais

Nosso objetivo aqui é mostrar que se α é uma função constante sobre as classes racionais, então $|G|\alpha$ é um caráter generalizado de G. Vamos precisar da seguinte definição.

Definição 3.1. Seja G um grupo e $x, y \in G$. Escrevemos $x \overset{R}{\sim} y$ se os grupos cíclicos $\langle x \rangle$ e $\langle y \rangle$ são conjugados em G.

Proposição 3.2. *Se G é um grupo finito então $x \overset{R}{\sim} y$ define uma relação de equivalência em G.*

Demonstração.

(i) $x \overset{R}{\sim} x$;

(ii) Se $x \overset{R}{\sim} y$ então existe $g \in G$ tal que $\langle x \rangle = \langle y \rangle^g$. Logo $y \overset{R}{\sim} x$, pois $\langle y \rangle = \langle x \rangle^{g^{-1}}$;

(iii) Se $x \overset{R}{\sim} y$ e $y \overset{R}{\sim} z$ então existem $g, h \in G$ tais que $\langle x \rangle = \langle y \rangle^g$ e $\langle y \rangle = \langle z \rangle^h$. Logo $x \overset{R}{\sim} z$, pois $\langle x \rangle = \langle z \rangle^{hg}$.

■

Denotaremos por $[x]_R = \{y \in G; y \overset{R}{\sim} x\}$ e $G/\overset{R}{\sim} = \{[x]_R; x \in G\}$, a classe racional de x e o conjunto das classes racionais de G, respectivamente.

Proposição 3.3. *Sejam G um grupo finito e $\chi \in Irr(G)$. A soma dos valores de χ sobre as classes racionais de G é um número inteiro, isto é, para todo $x \in G$ a soma $\sum_{g \in [x]_R} \chi(g) \in \mathbb{Z}$.*

Demonstração. Primeiramente observamos que se $x \overset{R}{\sim} y$, então $|x| = |y|$, assim $A := \sum_{g \in [x]_R} \chi(g)$ é uma soma de raizes $|x|$-ésimas da unidade. Pelo Lema 1.15, temos que $\Phi(g) = diag(\epsilon_1, ..., \epsilon_{\chi(1)})$ e $\chi(g) = \sum_{i=1}^{\chi(1)} \epsilon_i$, então $A \in \mathbb{Q}(\omega)$, onde ω é uma raiz $|x|$-ésima primitiva de 1 (extensão ciclotômica). Agora note que se i é coprimo com $|x|$, então $x \overset{R}{\sim} x^i$ e assim para todo $f \in Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ temos que $f(A) = A$, pois f é definida por $f(\omega) = \omega^i$, para algum i coprimo com $|x|$ e $f(\chi(g)) = \chi(g^i)$. Logo $A \in \mathbb{Q}$ e portanto $A \in \mathbb{Z}$.

■

Proposição 3.4. *Se G é um grupo finito e $\alpha : G \to \mathbb{Z}$ é uma função constante sobre o conjunto das classes racionais de G, isto é, $\alpha(x) = \alpha(y)$ se $x \overset{R}{\sim} y$, então $|G|\alpha$ é um caráter generalizado de G.*

Demonstração. Seja $\chi \in Irr(G)$, denotaremos por $\{x_i\}$ um conjunto completo de representantes das classes de equivalência com respeito à relação $\overset{R}{\sim}$. Temos

$$\begin{aligned} [|G|\alpha, \chi] &= \tfrac{1}{|G|} \sum_{g \in G} |G|\alpha(g)\overline{\chi(g)} \\ &= \sum_i \sum_{g \in [x_i]_R} \alpha(g)\overline{\chi(g)} \\ &= \sum_i \alpha(x_i) \sum_{g \in [x_i]_R} \overline{\chi(g)}. \end{aligned}$$

Como $\sum_{g \in [x_i]_R} \overline{\chi(g)} \in \mathbb{Z}$, pela Proposição 3.3, segue que $[|G|\alpha, \chi] \in \mathbb{Z}$ e portanto $|G|\alpha$ é um caráter generalizado de G.

∎

3.2 - Uma particular função de classe

Vamos agora considerar uma particular função de classe, constante sobre as classes racionais e mostrar que para esta função o resultado da Proposição 3.4 pode ser melhorado.

Seja Φ uma representação complexa de um grupo finito G com caráter associado χ. Podemos definir a função $\alpha_\chi : G \to \mathbb{Z}$ sendo

$$\alpha_\chi(g) = dim(E_1(\Phi(g))),$$

onde $g \in G$ e $E_1(\Phi(g)) = \{v \in \mathbb{C}^{\chi(1)} : \Phi(g)(v) = v\} = Ker(\Phi(g) - Id)$.

No próximo Lema vamos obter outra forma de escrever a função α_χ.

Lema 3.5. *Seja G um grupo finito e Φ uma representação complexa de G que determina o caráter χ. Para todo $g \in G$,*

$$\alpha_\chi(g) = [\chi|_{\langle g \rangle}, 1_{\langle g \rangle}]_{\langle g \rangle}.$$

Demonstração. Pelo Lema 1.15, podemos escolher uma base de V de modo que $\Phi(g) = diag(1, \ldots, 1, \epsilon_1, \ldots, \epsilon_t)$, onde $\epsilon_i \neq 1$, $\epsilon_i^{|g|} = 1$ e a quantidade de autovalores 1 é a dimensão do espaço dos vetores fixados por $\Phi(g)$, ou seja, $\alpha_\chi(g)$. Assim temos

$$\begin{aligned}
\chi(g^0) &= \alpha_\chi(g) + \epsilon_1^0 + \cdots + \epsilon_t^0 \\
\chi(g^1) &= \alpha_\chi(g) + \epsilon_1^1 + \cdots + \epsilon_t^1 \\
&\vdots \\
\chi(g^{|g|-1}) &= \alpha_\chi(g) + \epsilon_1^{|g|-1} + \cdots + \epsilon_t^{|g|-1}
\end{aligned}$$

Daí, $\sum_{k=0}^{|g|-1} \chi(g^k) = |g|\alpha_\chi(g) + \sum_{k=0}^{|g|-1} \epsilon_1^k + \sum_{k=0}^{|g|-1} \epsilon_2^k + \cdots + \sum_{k=0}^{|g|-1} \epsilon_t^k = |g|\alpha_\chi(g)$ e portanto,

$$[\chi|_{\langle g \rangle}, 1_{\langle g \rangle}]_{\langle g \rangle} = \frac{1}{|g|} \sum_{k=0}^{|g|-1} \chi(g^k) = \alpha_\chi(g).$$

∎

Agora vamos provar o seguinte resultado.

Teorema 3.6. *Seja G é um grupo finito de expoente e. Se χ é um caráter de G, então $e\alpha_\chi$ é um caráter generalizado.*

Pelo Teorema de Brauer, é suficiente provarmos que a restrição $(e\alpha_\chi)_{|N}$ é um caráter generalizado de N, para todo subgrupo nilpotente $N \leq G$. Portanto basta demonstrarmos o Teorema 3.6 para o caso em que N é nilpotente. Neste caso, devemos verificar que $e[\alpha_\chi, \zeta] \in \mathbb{Z}$, para todo caráter irredutível ζ de N. Para isso, vamos tornar geral esse resultado, supondo que ζ é um caráter generalizado.

Proposição 3.7. *Seja G um grupo nilpotente e suponha que χ é um caráter de G e ζ é um caráter generalizado. Então $m[\alpha_\chi, \zeta]_G \in \mathbb{Z}$, para todo inteiro positivo m tal que $\zeta(g) = 0$ sempre que $g^m \neq 1$.*

Em particular, se m é o expoente de G, a condição $\zeta(x) = 0$ sempre que $x^m \neq 1$ é satisfeita por vacuidade. Portanto a Proposição 3.7 inclui o caso nilpotente do Teorema 3.6 e implica o caso geral, pelo Teorema de Brauer.

Vamos precisar da próxima definição e dos seguintes resultados.

Definição 3.8. Se G é um grupo finito, $\chi : G \to \mathbb{C}$ é uma função arbitrária e n é um inteiro positivo, definimos

$$\chi^{(n)} : G \to \mathbb{C} \text{ por } \chi^{(n)}(x) = \chi(x^n)$$

e

$$\chi^{(1/n)} : G \to \mathbb{C} \text{ por } \chi^{(1/n)}(x) = \sum_{\substack{y \in G \\ y^n = x}} \chi(y).$$

Proposição 3.9. *Se χ é um caráter generalizado de G, então $\chi^{(n)}$ é um caráter generalizado de G.*

Demonstração. Considere o polinômio simétrico $t_n(x_1, \ldots, x_m) = \displaystyle\sum_{j=1}^{m} x_j^n$, onde $m = \chi(1)$. Pelo Teorema de Newton em [4], existe $f \in \mathbb{Z}[x_1, \ldots, x_m]$ tal que $t_n = f(s_1, \ldots, s_m)$, onde os s_i são os polinômios simétricos elementares. Se $a_1(g), \ldots, a_m(g)$ são os autovalores da matriz $\Phi(g)$, então

$$\chi^{(n)}(g) = \chi(g^n) = \sum_{i=1}^{m} a_i(g)^n = t_n(a_1(g), \ldots, a_m(g)) = f(\hat{s}_1, \ldots, \hat{s}_m),$$

onde $\hat{s}_i = s_i(a_1(g), \ldots, a_m(g))$ é a avaliação em g de um caráter de G, pelo Teorema 8.12 em [7]. Como os caracteres generalizados formam um anel, $\chi^{(n)}$ é um caráter generalizado.

■

Proposição 3.10. *Se χ é um caráter generalizado de G, então $\chi^{(1/n)}$ é também um caráter generalizado de G.*

Demonstração. Em primeiro lugar, vejamos que $\chi^{(1/n)}$ é constante sobre as classes de conjugação.

$$\begin{aligned}
\chi^{(1/n)}(gxg^{-1}) &= \sum_{\substack{y\in G\\ y^n = gxg^{-1}}} \chi(y) = \sum_{\substack{y\in G\\ (g^{-1}yg)^n = x}} \chi(y)\\
&= \sum_{\substack{z\in G\\ z^n = x}} \chi(gzg^{-1}) = \sum_{\substack{z\in G\\ z^n = x}} \chi(z)\\
&= \chi^{(1/n)}(x).
\end{aligned}$$

Seja $\zeta \in Irr(G)$. Então

$$\begin{aligned}
[\chi^{(1/n)}, \zeta] = & \frac{1}{|G|}\sum_{x\in G} \chi^{(1/n)}(x)\overline{\zeta(x)}\\
= & \frac{1}{|G|}\sum_{x\in G}\sum_{\substack{y\in G\\ y^n = x}} \chi(y)\overline{\zeta(x)}\\
= & \frac{1}{|G|}\sum_{y\in G} \chi(y)\overline{\zeta(y^n)}\\
= & [\chi, \zeta^n].
\end{aligned}$$

Como $\zeta^{(n)}$ é um caráter generalizado, temos que $[\chi, \zeta^n] \in \mathbb{Z}$ e portanto $\chi^{(1/n)}$ é um caráter generalizado.

■

Lema 3.11. *Seja G um grupo finito e $N \lhd G$ tal que $\frac{G}{N}$ é cíclico. Suponha que χ é um caráter generalizado de G tal que $\chi(g) = 0$, para todo $g \in G \setminus N$. Então $\chi = \psi^G$, para algum caráter generalizado ψ em N.*

Demonstração. Como $\frac{G}{N}$ é cíclico, todos os seus caracteres irredutíveis são lineares, desse modo $Irr(\frac{G}{N})$ é um grupo abeliano e portanto, pelo Lema 1.23, pode ser identificado com o grupo cíclico

$$C = \{\psi \in Irr(G); N \leq Ker(\psi)\}$$

de caracteres lineares de G.

Pelo Corolário 1.27, para todo $\phi \in Irr(G)$ e todo $\lambda \in C \leq Lin(G)$, $\lambda\phi \in Irr(G)$ e o grupo C age por multiplicação sobre $Irr(G)$. Como $\chi(g) = 0$ se $\lambda(g) \neq 1$, temos que $\chi = \chi\lambda$.

Afirmação 1: χ é uma $\mathbb{Z}$-combinação linear das somas das órbitas da ação de C sobre $Irr(G)$.

Primeiramente, observamos que a ação de C em $Irr(G)$ é fiel. Se $\psi_1, \psi_2 \in Irr(G)$ são tais que $\lambda\psi_1 = \lambda\psi_2$, então

$$\begin{aligned} 1 &= [\lambda\psi_1, \lambda\psi_2] = \frac{1}{|G|}\sum_{g\in G}\lambda(g)\psi_1(g)\overline{\lambda(g)}\,\overline{\psi_2(g)} \\ &= \frac{1}{|G|}\sum_{g\in G}\psi_1(g)\psi_2(g) = [\psi_1, \psi_2]. \end{aligned}$$

Daí, $\psi_1 = \psi_2$. Logo, pondo $\chi = \sum\limits_{\psi\in Irr(G)} a_\psi \psi$ a relação $\chi = \lambda\chi$ implica que

$$\sum_{\psi\in Irr(G)} a_{\lambda\psi}\lambda\psi = \sum_{\psi\in Irr(G)} a_\psi\lambda\psi \Rightarrow \sum_{\psi\in Irr(G)} (a_{\lambda\psi} - a_\psi)\lambda\psi = 0 \Rightarrow a_{\lambda\psi} = a_\psi,$$

pois $Irr(G)$ é uma base para o espaço das funções de classe de G. Sejam $\theta_1, \ldots, \theta_k$ as órbitas dessa ação, podemos escrever

$$\chi = \sum_{i=1}^{k}\sum_{\psi\in\theta_i} a_\psi\psi = \sum_{i=1}^{k} a_i \sum_{\psi\in\theta_i}\psi\,,$$

onde $a_i \in \mathbb{Z}$.

Visto isso, é suficiente provar que toda soma de órbitas é induzida por algum caráter de N.

Considere então $\xi \in Irr(G)$ e η a soma da C-órbita contendo ξ. Se α é uma componente irredutível de $\xi_{|_N}$, completaremos a demonstração verificando que $\alpha^G = \eta$.

Ora, mas para todo $g \in G \setminus N$ existe $\lambda \in C$ tal que $\lambda(g) \neq 1$. Como η é a soma de uma C-órbita, temos $\eta\lambda = \eta$ e

$$\eta(g) = (\eta\lambda)(g) = \eta(g)\lambda(g) \Rightarrow \eta(g)(\lambda(g) - 1) = 0 \Rightarrow \eta(g) = 0.$$

Por outro lado, se $x \in G$ e $g \in G \setminus N$, então $x^{-1}gx \notin N$ e

$$\alpha^G(g) = \frac{1}{|N|}\sum_{x\in G}\alpha^\circ(x^{-1}gx) = 0.$$

Logo $\eta = \alpha^G$ em $G \setminus N$. Vamos mostrar que $\eta = \alpha^G$ em N.

Cada componente irredutível de η é da forma $\xi\mu$ para algum $\mu \in C$. Como $\mu_{|_N} = 1_{_N}$, temos $(\xi\mu)_{|_N} = \xi_{|_N}\mu_{|_N} = \xi_{|_N}$, donde $\eta_{|_N}$ é um múltiplo de $\xi_{|_N}$ que é um múltiplo da soma da G-órbita de α, pelo Teorema de Clifford (Teorema 1.63).

Afirmação 2: $(\alpha^G)_{|_N}$ é um múltiplo da soma da G-órbita de α.

De fato, pelo Teorema 1.62, temos que

$$(\alpha^G)_{|_N} = \sum_{j=1}^{m} \left((\alpha^{r_j})_{|_{N^{r_j} \cap N}} \right)^N = \sum_{j=1}^{m} \left((\alpha^{r_j})_{|_N} \right)^N = \sum_{j=1}^{m} \alpha^{r_j},$$

onde $r_j \in G = \dot{\bigcup}_{j=1}^{m} N r_j N$.

Assim, para mostrar que $\eta = \alpha^G$ em N é suficiente verificarmos que $\eta(1) = \alpha^G(1)$.

Se $B \subseteq C$ o estabilizador de ξ com respeito à ação definida no Corolário 1.27, então $\eta(1) = |C : B|\xi(1)$. Seja $T = I_G(\alpha) \subseteq G$ o estabilizador de α. Pelo Teorema 1.67(b), temos que $\xi = \beta^G$, onde $\beta \in Irr(T)$ e $[\beta_{|_N}, \alpha]_N \neq 0$.

Afirmação 3: $\beta_{|_N} = \alpha$.

Como $N < T < G$ e $N \lhd G$, temos que $N \lhd T$. Por outro lado, β é uma componente irredutível de α^T pois

$$1 \leq [\beta_{|_N}, \alpha]_N = [\beta, \alpha^T]_T.$$

Agora, $\frac{T}{N} \leq \frac{G}{N}$ é um grupo cíclico e $\alpha \in Irr(N)$ é invariante em T, donde segue que α é extensível a T, pelo Corolário 11.22 em [8], ou seja, existe $\gamma \in Irr(T)$ tal que $\gamma_{|_N} = \alpha$. Pelo Teorema de Gallagher (Corolário 1.73), temos que para distintos $\hat{\sigma} \in Irr\left(\frac{T}{N}\right)$ os caracteres $\sigma\gamma$ são distindos, irredutíveis e são todos os constituintes de α^T. Logo $\beta = \sigma\gamma$, para algum $\hat{\sigma} \in Irr\left(\frac{T}{N}\right)$. Como $\hat{\sigma} \in Irr\left(\frac{T}{N}\right)$ implica que $N \subseteq Ker(\sigma)$, temos

$$\beta_{|_N} = (\sigma\gamma)_{|_N} = 1_{_N}\gamma_{|_N} = \gamma_{|_N} = \alpha.$$

Consequentemente, $\xi(1) = |G : T|\alpha(1)$ e $\eta(1) = |C : B||G : T|\alpha(1)$. Como $\alpha^G(1) = |G : N|\alpha(1)$, resta mostrar que $|G : N| = |G : T||C : B|$, ou seja, que $|T : N| = |C : B|$, já que $|G : N| = |G : T||T : N|$.

Pelo terceiro Teorema do Isomorfismo, $\frac{G}{T} \simeq \frac{\frac{G}{N}}{\frac{T}{N}}$. Então, se mostrarmos que $B = \{\psi \in Irr(G);\ T \leq Ker(\psi)\}$ teremos

$$|C : B| = \frac{|C|}{|B|} = \frac{|G : N|}{|N : T|} = |T : N|.$$

Seja $\mu \in B$. Utilizando o Teorema 1.42(b), temos

$$\xi = \xi\mu = \beta^G\mu = (\beta\mu_{|_T})^G$$

e $(\beta\mu_{|_T})_{|_N} = \beta_{|_N}\mu_{|_N} = \beta_{|_N} = \alpha$. Contudo, pelo Teorema 1.67(c), β é o único com tais propriedades. Logo $\beta\mu_{|_T} = \beta$ e assim, pelo Teorema de Gallagher, $\mu_{|_T} = 1_T$. Então $T \subseteq Ker(\mu)$.

Reciprocamente, seja $\mu \in Irr(G)$ tal que $T \subseteq Ker(\mu)$. Temos que $\mu \in B$, pois

$$\xi\mu = \beta^G\mu = (\beta\mu_{|_T})^G = \beta^G = \xi.$$

Portanto, $B = \{\psi \in Irr(G); T \leq Ker(\psi)\}$ finalizando a demonstração.

■

Agora vamos demonstrar a Proposição 3.7.

Demonstração. Primeiramente observamos que a aplicação $\chi \mapsto \alpha_\chi$ é aditiva. De fato, se Φ_1 e Φ_2 são representações complexas de G que determinam os caracteres χ_1 e χ_2 respectivamente, então

$$\Phi(g) = \begin{bmatrix} \Phi_1(g) & 0 \\ 0 & \Phi_2(g) \end{bmatrix}$$

é uma representação complexa de G que determina o caráter $\chi_1 + \chi_2$. Logo

$$\begin{aligned} \alpha_{\chi_1+\chi_2}(g) = &\ dim(E_1(\Phi(g))) \\ = &\ dim(E_1(\Phi_1(g))) + dim(E_1(\Phi_2(g))) \\ = &\ \alpha_{\chi_1}(g) + \alpha_{\chi_2}(g). \end{aligned}$$

Deste modo, podemos assumir que χ é um caráter irredutível de G e então procedermos por indução sobre $\chi(1)$.

Se $\chi(1) = 1$, então χ é linear. Denotando $K = Ker(\chi)$, segue que

$$\alpha_\chi(g) = \begin{cases} 1, & \text{se } g \in K \\ 0, & \text{se } g \notin K \end{cases}.$$

Considerando a projeção $\pi : G \to \frac{G}{K}$, seja $Kg \in \frac{G}{K}$ cuja ordem divide m, temos que $K = (Kg)^m = Kg^m$, ou seja, $g^m \in K$. Então

$$N = \{g \in G; g^m \in K\}$$

é a pré imagem dos elementos de $\frac{G}{K}$ cuja ordem divide m.

Sejam $g_1, g_2 \in N$, então $g_1^m, g_2^m \in K$ e $(g_1^{-1})^m = (g_1^m)^{-1} \in K \leq G$, ou seja, $g_1^{-1} \in N$. Como $\frac{G}{K}$ é cíclico, em particular é abeliano, segue que

$$K = Kg_1^m Kg_2^m = (Kg_1)^m (Kg_2)^m = (Kg_1g_2)^m = K(g_1g_2)^m,$$

isto é, $g_1g_2 \in N$. Portanto, $N \leq G$.

Como $K \trianglelefteq N$, temos que $\frac{N}{K} \leq \frac{G}{K}$ é cíclico e então $\left|\frac{N}{K}\right|$ divide m. Assim, $m\alpha_\chi$ é um múltiplo de $\left|\frac{N}{K}\right| \alpha_\chi$ e

$$(1_K)^N(g) = \frac{1}{|K|} \sum_{x \in N} (1_K)^\circ(xgx^{-1}) = \begin{cases} |N:K|, & \text{se } g \in K \\ 0, & \text{se } g \notin K \end{cases} = \left|\frac{N}{K}\right| \alpha_\chi(g).$$

Em particular, $(m\alpha_\chi)_{|N}$ é um caráter de N.

Se $g \in G \setminus N$, então $g^m \notin K$ e por hipótese temos $\zeta(g) = 0$. Como $\frac{G}{N}$ é cíclico, pelo Lema 3.11, existe um caráter generalizado η de N tal que $\zeta = \eta^G$. Então

$$m[\alpha_\chi, \zeta] = [m\alpha_\chi, \eta^G] = [(m\alpha_\chi)_{|N}, \eta] \in \mathbb{Z},$$

pois $(m\alpha_\chi)_{|N}$ é um caráter de N.

Suponha que $\chi(1) > 1$. Como G é nilpotente, pelo Corolário 1.68 podemos escrever $\chi = \lambda^G$, onde λ é um caráter linear de algum subgrupo K de G e neste caso, observamos que K é um subgrupo próprio de G, pois $\chi(1) > 1$. Sejam H um subgrupo maximal de G que contém K e $\psi = \lambda^H$. Pelo Teorema 1.42(c) temos $\psi^G = \lambda^G = \chi$ e $\psi \in Irr(H)$, pois se ψ é soma de caracteres, então ψ^G é também uma soma de caracteres, contradizendo o fato de χ ser irredutível. Portanto temos que $\chi = \psi^G$, para algum $\psi \in Irr(H)$, onde $H \lhd G$ tem índice primo p. Então,

$$[\chi_{|H}, \psi] = [(\psi^G)_{|H}, \psi] = [\psi^G, \psi^G] = [\chi, \chi] = 1.$$

Além disso, pelo Teorema de Clifford e pelo Corolário 1.75

$$\chi_{|H} = \psi_1 + \psi_2 + \cdots + \psi_p,$$

onde $\psi = \psi_1$ e $\{\psi_1, \psi_2, \ldots, \psi_p\}$ é uma órbita da ação de G sobre $Irr(H)$. Então $(\alpha_\chi)_{|_H} = \sum_{i=1}^{p} \alpha_{\psi_i}$ e os α_{ψ_i} são tais que para todo $g \in G$,

$$\begin{aligned}(\alpha_{\psi_i})^g(h) &= \alpha_{\psi_i}(ghg^{-1}) = \frac{1}{|h^g|}\sum_{k=0}^{|h^g|-1} \psi_i((ghg^{-1})^k) \\ &= \frac{1}{|h|}\sum_{k=0}^{|h|-1} \psi_i(gh^kg^{-1}) = \frac{1}{|h|}\sum_{k=0}^{|h|-1} {\psi_i}^g(h^k) = \alpha_{{\psi_i}^g}(h).\end{aligned}$$

Agora vamos utilizar módulos para calcular $\alpha_\chi(g)$ se $g \in G \setminus H$.

Seja V um $\mathbb{C}[G]$-módulo que determina o caráter χ, então $V = V_1 \oplus V_2 \oplus \cdots \oplus V_p$, onde para todo $i = 1, \ldots, p$ temos que V_i é o $\mathbb{C}[H]$-submódulo irredutível de V que determina o caráter $\psi_i \in Irr(H)$. Esses submódulos são permutados por G pois, se $g \in G \setminus H$, então $\langle g \rangle$ permuta V_i transitivamente e então podemos assumir que g leva V_i em V_{i+1}, para todo $i = 1, \ldots, p-1$ e g leva V_p em V_1.

Fixando $g \in G \setminus H$, definimos uma $\mathbb{C}$-transformação linear $\varphi : V_1 \to V$ por $\varphi(w) = w + wg + wg^2 + \cdots + wg^{p-1}$. Se $w \in Ker(\varphi)$, então

$$\varphi(w) = w + wg + wg^2 + \cdots + wg^{p-1} = 0$$

logo $w = 0$, pois $V = V_1 \oplus V_2 \oplus \cdots \oplus V_p$. Portanto φ é injetiva.

Agora note que se w é um ponto fixado por g^p em V_1, então $\varphi(w)$ é fixado por g. Reciprocamente, suponha que $v \in V$ é um ponto fixado por g. Escrevendo $v = v_1 + v_2 + \cdots + v_p$, com $v_i \in V_i$ temos que

$$v = vg \Rightarrow v_1 + v_2 + \cdots + v_p = v_1g + v_2g + \cdots + v_pg.$$

Comparando as projeções, segue que $v_1g = v_2$, $v_2g = v_3, \ldots, v_{p-1}g = v_p$, e $v_pg = v_1$. Logo, $v_1g^p = v_1g^{p-1}g = v_pg = v_1$ e

$$\varphi(v_1) = v_1 + v_1g + v_1g^2 + \cdots + v_1g^{p-1} = v_1 + v_2 + \cdots + v_p = v.$$

Desse modo, φ define um isomorfismo do subespaço de V_1, formado pelos pontos fixados por g^p, no subespaço de V, formado pelos pontos fixados por g. Por outro lado, como $\left|\frac{G}{H}\right| = p$, para todo $g \in G \setminus H$ temos que $H = (Hg)^p = Hg^p$, ou seja, $g^p \in H$. Portanto, $\alpha_\chi(g) = \alpha_\psi(g^p)$ para todo $g \in G \setminus H$.

Agora,

$$m[\alpha_\chi, \zeta] = \frac{m}{|G|}\sum_{g \in G} \alpha_\chi(g)\overline{\zeta(g)} = \frac{m}{|G|}S_1 + \frac{m}{|G|}S_2,$$

onde $S_1 = \sum_{g \in H} \alpha_\chi(g)\overline{\zeta(g)}$ e $S_2 = \sum_{g \in G \setminus H} \alpha_\chi(g)\overline{\zeta(g)}$.

Se $g \in H$, então $\alpha_\chi(g) = \sum_{i=1}^{p} \alpha_{\psi_i}(g)$ e

$$S_1 = |H| \left[\left(\sum_{i=1}^{p} \alpha_{\psi_i} \right), \zeta_{|_H} \right] = |H| \sum_{i=1}^{p} [\alpha_{\psi_i},\, \zeta_{|_H}] = p|H|[\alpha_\psi, \zeta_{|_H}],$$

pois, pelo Lema 1.61(d) $[\alpha_{\psi_i}, \zeta_{|_H}] = [\alpha_\psi, \zeta_{|_H}]$, para todo $1 \leq i \leq p$.

Note que $\psi(1) < \chi(1)$. Assim, por hipótese de indução temos

$$\frac{m}{|G|} S_1 = \frac{m}{|G|} p|H|[\alpha_\psi,\, \zeta_{|_H}] = m[\alpha_\psi,\, \zeta_{|_H}] \in \mathbb{Z}.$$

Para calcularmos S_2, vamos aplicar indução sobre m.

Se $m = 1$, então $\zeta(g) = 0$, sempre que $g \neq 1$. Daí,

$$[\alpha_\chi, \zeta] = \frac{1}{|G|} \sum_{g \in G} \alpha_\chi(g)\overline{\zeta(g)} = \frac{1}{|G|} \alpha_\chi(1)\overline{\zeta(1)} = \frac{1}{|G|} \chi(1)\overline{\zeta(1)} = [\chi, \zeta] \in \mathbb{Z}.$$

Para $h \in H$ defina $\xi(h) = \sum_{\substack{g \in G \setminus H \\ g^p = h}} \zeta(g)$. Então

$$\begin{aligned} S_2 &= \sum_{g \in G \setminus H} \alpha_\chi(g)\overline{\zeta(g)} \\ &= \sum_{g \in G \setminus H} \alpha_\psi(g^p)\overline{\zeta(g)} \\ &= \sum_{h \in H} \sum_{\substack{g \in G \setminus H \\ g^p = h}} \alpha_\psi(g^p)\overline{\zeta(g)} \\ &= \sum_{h \in H} \alpha_\psi(h) \sum_{\substack{g \in G \setminus H \\ g^p = h}} \overline{\zeta(g)} \\ &= \sum_{h \in H} \alpha_\psi(h)\overline{\xi(h)} \\ &= |H|[\alpha_\psi, \xi]. \end{aligned}$$

Vamos mostrar que

$$\frac{m}{|G|} S_2 = \frac{m}{|G|} |H|[\alpha_\psi, \xi] = \frac{m}{p}[\alpha_\psi, \xi] \in \mathbb{Z}.$$

Note que se $g \in G \setminus H$ e $g^p = h \in H$, então p divide a ordem de g. De fato, se p não divide $|g|$ então $mdc(p, |g|) = 1$. Assim, existem $a, b \in \mathbb{Z}$ tais que $ap + b|g| = 1$, logo

$$g = g^{ap+b|g|} = (g^p)^a = h^a \in H,$$

contradizendo o fato de que $g \in G \setminus H$.

Se $p \nmid m$ então $g^m \neq 1$ e por hipótese temos $\zeta(g) = 0$. Dessa forma, ξ é identicamente zero e portanto, $\frac{m}{|G|}S_2 \in \mathbb{Z}$.

Agora suponha que $p \mid m$.

Se $g^m = 1$ e $g^p = h \in H$, então $h^{(m/p)} = 1$. Assim, se $h^{(m/p)} \neq 1$, então $g^m \neq 1$ e por hipótese segue que $\zeta(g) = 0$, para todo $g \in G \setminus H$ tal que $g^p = h$ e portanto $\xi(h) = 0$.

Agora

$$\xi(h) = \sum_{\substack{g \in G \\ g^p = h}} \zeta(g) - \sum_{\substack{g \in H \\ g^p = h}} \zeta(g)$$

e então $\xi = (\zeta^{(1/p)})_{|H} - (\zeta_{|H})^{(1/p)}$, que é um caráter generalizado pela Proposição 3.10. Como $\xi(h) = 0$ se $h^{(m/p)} \neq 1$, por hipótese de indução temos que $\frac{m}{p}[\alpha_\psi, \xi_{|H}] \in \mathbb{Z}$. Logo, $\frac{m}{|G|}S_2 \in \mathbb{Z}$ e portanto $m[\alpha_\chi, \zeta] \in \mathbb{Z}$.

■

Usando a Proposição 3.7, vamos provar um resultado mais forte do que o Teorema 3.6.

Teorema 3.12. *Seja G um grupo finito e suponha que χ é um caráter de G e ζ é um caráter generalizado. Então $m[\alpha_\chi, \zeta] \in \mathbb{Z}$, para todo inteiro positivo m tal que $\zeta(g) = 0$, sempre que $g^m \neq 1$.*

Demonstração. Pelo Teorema de Brauer, o caráter principal 1_G pode ser escrito como soma de caracteres lineares induzidos λ_i^G, onde os λ_i são caracteres de certos grupos nilpotentes $N_i \subseteq G$. Assim, pelo Teorema 1.42(c)

$$\zeta = \zeta 1_G = \sum_i \zeta(\lambda_i)^G = \sum_i (\zeta_{|N_i}\lambda_i)^G.$$

Portanto,

$$m[\alpha_\chi, \zeta] = \sum_i m[\alpha_\chi, (\zeta_{|N_i}\lambda_i)^G] = \sum_i m[(\alpha_\chi)_{|N_i}, \zeta_{|N_i}\lambda_i].$$

Por outro lado, $\zeta_{|N_i}\lambda_i$ é um caráter generalizado tal que $(\zeta_{|N_i}\lambda_i)(n) = 0$, para todo $n \in N_i$ que satisfaz $n^m \neq 1$. Logo, pela Proposição 3.7, $m[(\alpha_\chi)_{|N_i}, \zeta_{|N_i}\lambda_i] \in \mathbb{Z}$. Portanto $m[\alpha_\chi, \zeta]$ é inteiro.

■

Na Proposição 3.4, mostramos que se $\alpha : G \to \mathbb{Z}$ é uma função constante sobre o conjunto das classes racionais, então $\alpha|G|$ é um caráter generalizado, ou seja, $|G|[\alpha, \zeta] \in \mathbb{Z}$, para qualquer $\zeta \in Irr(G)$. No Teorema 3.6, para uma função α particular e para todo $\zeta \in Irr(G)$ mostramos que $e[\alpha, \zeta] \in \mathbb{Z}$, onde e é o expoente de G. Agora se ζ é um caráter particular, vamos mostrar que podemos reduzir o coeficiente de $[\alpha, \zeta]$ para qualquer função $\alpha : G \to \mathbb{Z}$ que seja constante sobre o conjunto das classes racionais.

Teorema 3.13. *Se $\alpha : G \to \mathbb{Z}$ é uma função constante sobre o conjunto das classes racionais de G, então para todo $\zeta \in Irr(G)$ temos que*

$$\frac{|G|}{\zeta(1)}[\alpha, \zeta]$$

é um inteiro.

Demonstração. Seja $\{x_1, x_2, \ldots, x_k\}$ um conjunto representativo das classes de conjugação $Cl_1, \ldots, Cl_k$ de G. Temos que

$$\frac{|G|}{\zeta(1)}[\alpha, \zeta] = \sum_{x \in G} \alpha(x) \frac{\overline{\zeta(x)}}{\zeta(1)} = \sum_{i=1}^{k} \alpha(x_i) \frac{\overline{\zeta(x_i)}}{\zeta(1)} |Cl_i|,$$

onde $\frac{\overline{\zeta(x_i)}}{\zeta(1)}|Cl_i|$ é um inteiro algébrico, pelo Teorema 1.35 e portanto $\frac{|G|}{\zeta(1)}[\alpha, \zeta]$ é um inteiro algébrico, pelo Corolário 1.32. Por outro lado, pela Proposição 3.4, $|G|[\alpha, \zeta] \in \mathbb{Z}$. Dessa forma, $\frac{|G|}{\zeta(1)}[\alpha, \zeta]$ é racional e portanto inteiro, pelo Lema 1.30.

■

3.3 - Uma aplicação computacional

Vamos concluir nossa dissertação com uma aplicação da teoria dos caracteres no problema da geração de um grupo por um conjunto de elementos. Em particular, iremos aplicar a função de classe α_χ definida e estudada anteriormente. Nossa referência principal é o livro de Lux e Phalings [12].

Vamos precisar das seguintes definições e observações.

Definição 3.14. Seja V um $\mathbb{C}[G]$-módulo. Definimos

$$Inv^G(V) = \langle (g-1)v;\ g \in G,\ v \in V \rangle .$$

Observação 3.15. $Inv^G(V)$ e $Fix_G(V) = \{v \in V;\ g \cdot v = v, \forall\ g \in G\}$ são dois $\mathbb{C}[G]$-módulos. Além disso, $Fix_G(V)$ é o maior submódulo de V, sobre o qual G age trivialmente, enquanto $Inv^G(V)$ é o menor submódulo W de V, tal que G age trivialmente sobre $\frac{V}{W}$.

Definição 3.16. Sejam G um grupo finito e $\mathscr{C} = (\mathscr{C}_1, \ldots, \mathscr{C}_m)$, tal que cada $\mathscr{C}_i$ é um subconjunto normal de G, isto é, $\mathscr{C}_i$ é união de classes de conjugação de elementos de G.

Para $H \leqslant G$, definimos

$$\Sigma_G^H(\mathscr{C}) = \{(g_1, \ldots, g_m);\ g_i \in \mathscr{C}_i,\ g_1 \cdots g_m = 1,\ \langle g_1, \ldots, g_m \rangle =_G H\}$$

e

$$\Sigma_G^{\leqslant H}(\mathscr{C}) = \{(g_1, \ldots, g_m);\ g_i \in \mathscr{C}_i,\ g_1 \cdots g_m = 1,\ \langle g_1, \ldots, g_m \rangle \leqslant_G H\},$$

onde $U =_G H$, significa que U é conjugado em G ao subgrupo H e $U \leqslant_G H$, significa que U é conjugado em G a um subgrupo de H.

Denotaremos $\alpha_G(\mathscr{C}) = \left|\Sigma_G^{\leqslant G}(\mathscr{C})\right|$ e $\gamma_G(\mathscr{C}) = \left|\Sigma_G^G(\mathscr{C})\right|$. Claramente $\alpha_G(\mathscr{C}) \geq \gamma_G(\mathscr{C}) \geq 0$.

Observação 3.17. Seja $\mathscr{L}$ um conjunto completo de representantes das classes de conjugação de subgrupos de G. Então

$$\Sigma_G^{\leqslant G}(\mathscr{C}) = \dot{\bigcup_{H \in \mathscr{L}}} \Sigma_G^H(\mathscr{C}),$$

ou ainda,

$$\Sigma_G^{\leqslant G}(\mathscr{C}) = \dot{\bigcup_{H \leqslant G}} \Sigma_H^H(\mathscr{C}_1 \cap H, \ldots, \mathscr{C}_m \cap H).$$

Daí,

$$\begin{aligned} \alpha_G(\mathscr{C}) &= \left|\Sigma_G^{\leqslant G}(\mathscr{C})\right| = \sum_{H \leqslant G} \left|\Sigma_H^H(\mathscr{C}_1 \cap H, \ldots, \mathscr{C}_m \cap H)\right| \\ &= \sum_{H \leqslant G} \gamma_H(\mathscr{C}_1 \cap H, \ldots, \mathscr{C}_m \cap H). \end{aligned}$$

Definição 3.18. Um conjunto não vazio X é dito *parcialmente ordenado*, se podemos definir uma relação binária $x \preceq y$ em X, de forma que para quaisquer $x, y, z \in X$, temos

(a) $x \preceq x$;

(b) Se $x \preceq y$ e $y \preceq x$, então $x = y$;

(c) Se $x \preceq y$ e $y \preceq z$, então $x \preceq z$.

Se X é um conjunto parcialmente ordenado, diremos simplesmente que X é um poset.

Definição 3.19. Um poset $(P, \preceq)$ é dito *localmente finito*, se o conjunto $\{z \in P;\ x \preceq z \preceq y\}$ é finito, para todo par $x, y \in P$.

Estamos interessados em calcular γ_G a partir de α_H, onde H é um subgrupo de G. Para isso, vamos precisar da função de Möbius.

Definição 3.20. A *função de Möbius* de um poset localmente finito $(P, \preceq)$ é uma função $\mu_P : P \times P \to \mathbb{Z}$, definida por

(i) $\mu_P(x, y) = 0$, se x e y não satisfazem $x \preceq y$;

(ii) se $x \preceq y$, definimos $\mu_P(x, y)$ recursivamente por $\mu_P(x, x) = 1$ e para $x \prec y$, $\sum\limits_{x \preceq z \preceq y} \mu_P(x, z) = 0$.

Observação 3.21. Seja $P = \{x_1, \dots, x_n\}$ um poset. Vamos assumir que $x_i \preceq x_j$ se $i \leqslant j$. Então a matriz

$$[z_{ij}]_{1 \leqslant i,j \leqslant n} \text{ tal que } z_{ij} = \begin{cases} 1, & \text{se } x_i \preceq x_j \\ 0, & \text{caso contário} \end{cases}$$

é uma matriz triangular superior tal que $z_{ii} = 1$. Logo $[z_{ij}]$ é inversível e sua inversa é dada pela matriz

$$[\mu_{ij}]_{1 \leqslant i,j \leqslant n} \text{ onde } \mu_{ij} = \mu_P(x_i, x_j).$$

Como $[\mu_{ij}]$ é também uma inversa à esquerda, obtemos

$$\sum_{x \preceq z \preceq y} \mu_P(z, y) = \delta_{x,y}.$$

Vamos utilizar a equação acima para demonstrar o próximo resultado.

Lema 3.22. *Sejam μ a função de Möbius do reticulado dos subgrupos de G e $\mathscr{C} = (\mathscr{C}_1, \ldots, \mathscr{C}_m)$, tal que cada $\mathscr{C}_i$ é um subconjunto normal de G. Então*

$$\gamma_G(\mathscr{C}) = \sum_{H \leqslant G} \mu(H, G) \cdot \alpha_H(\mathscr{C}_1 \cap H, \ldots, \mathscr{C}_m \cap H).$$

Demonstração. Pela Observação 3.17, temos que

$$\alpha_H(\mathscr{C}_1 \cap H, \ldots, \mathscr{C}_m \cap H) = \sum_{U \leqslant H} \gamma_U(\mathscr{C}_1 \cap U, \ldots, \mathscr{C}_m \cap U).$$

Multiplicando esta equação por $\mu(H, G)$ e somando sobre todos os subgrupos de G, obtemos

$$\begin{aligned} & \sum_{H \leqslant G} \mu(H, G) \cdot \alpha_H(\mathscr{C}_1 \cap H, \ldots, \mathscr{C}_m \cap H) = \\ = & \sum_{H \leqslant G} \sum_{U \leqslant H} \mu(H, G) \cdot \gamma_U(\mathscr{C}_1 \cap U, \ldots, \mathscr{C}_m \cap U) \\ = & \sum_{U \leqslant G} \left(\sum_{U \leqslant H \leqslant G} \mu(H, G) \right) \gamma_U(\mathscr{C}_1 \cap U, \ldots, \mathscr{C}_m \cap U) \\ = & \ \gamma_G(\mathscr{C}_1, \ldots, \mathscr{C}_m), \text{ pela Observação 3.21.} \end{aligned}$$

∎

Agora vamos obter uma fórmula para calcular α_G.

Teorema 3.23. *Sejam $Cl_1, \ldots, Cl_m$ classes de conjugação (não necessariamente distintas) de G e $\mathscr{C} = (Cl_1, \ldots, Cl_m)$. Então*

$$\alpha_G(\mathscr{C}) = \frac{|Cl_1| \cdots |Cl_m|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(g_1) \cdots \chi(g_m)}{\chi(1)^{m-2}},$$

onde $\{g_1, \ldots, g_m\}$ é um conjunto representativo das classes $Cl_1, \ldots, Cl_m$.

Demonstração. Sejam Cl uma classe de conjugação de G e g um representante dessa classe. Definindo $Cl' = \{x^{-1}; x \in Cl\}$ e denotando $C = \sum_{x \in Cl'} x \in \mathbb{C}[G]$ e $C_i = \sum_{x \in Cl_i} x$, temos que

$$\alpha_G(\mathscr{C}) = |C_m| \cdot |\{(x_1, \ldots, x_{m-1});\ x_j \in Cl_j,\ x_1 \cdots x_{m-1} = g_m^{-1}\}|.$$

Portanto,

$$C_1 \cdots C_{m-1} = \sum_{Cl \in Cl(G)} \frac{\alpha_G(Cl_1, \ldots, Cl_{m-1}, Cl)}{|Cl|} C.$$

Para um caráter $\chi \in Irr(G)$, consideramos a função $\mathbb{C}$-linear ω_χ definida na seção 1.2. Aplicando ω_χ à equação anterior e utilizando a Observação 1.34, temos

$$\begin{aligned} &\frac{|Cl_1|}{\chi(1)}\chi(g_1)\cdots\frac{|Cl_{m-1}|}{\chi(1)}\chi(g_{m-1}) = \\ = &\sum_{Cl\in Cl(G)} \alpha_G(Cl_1,\ldots,Cl_{m-1},Cl)\frac{1}{\chi(1)}\chi(g^{-1}). \end{aligned}$$

Multiplicando dos dois lados dessa igualdade por $\frac{|Cl_m|}{|G|}\chi(1)\chi(g_m)$ e somando sobre todos os caracteres irredutíveis de G, segue que

$$\begin{aligned} &\frac{|Cl_1|\cdots|Cl_m|}{|G|}\sum_{\chi\in Irr(G)}\frac{\chi(g_1)\cdots\chi(g_m)}{\chi(1)^{m-2}} = \\ = &\sum_{Cl\in Cl(G)} \alpha_G(Cl_1,\ldots,Cl_{m-1},Cl)\frac{|Cl_m|}{|G|}\sum_{\chi\in Irr(G)}\chi(g_m)\chi(g^{-1}), \end{aligned}$$

onde

$$\sum_{\chi\in Irr(G)}\chi(g_m)\chi(g^{-1}) = |C_G(g_m)|\delta_{g_m,g} = \frac{|G|}{|Cl_m|}\delta_{g_m,g},$$

pela Segunda Relação de Ortogonalidade (Teorema 1.19).

Portanto,

$$\alpha_G(\mathscr{C}) = \frac{|Cl_1|\cdots|Cl_m|}{|G|}\sum_{\chi\in Irr(G)}\frac{\chi(g_1)\cdots\chi(g_m)}{\chi(1)^{m-2}}.$$

■

Agora vamos estudar alguns resultados sobre módulos.

Definição 3.24. Se V é um $\mathbb{C}$-módulo (à esquerda), então

$$V^* = \{x : V \to \mathbb{C};\ x(av_1+v_2) = ax(v_1)+x(v_2)\} = Hom_{\mathbb{C}}(V,\mathbb{C})$$

se torna um $\mathbb{C}$-módulo (à direita) se definirmos

$$(x * a)(v) = x(av),\ \text{para quaisquer } a\in\mathbb{C},\ x\in V^* \text{ e } v\in V.$$

Diremos que V^* é o *módulo dual* de V.

Lema 3.25. *Seja V um $\mathbb{C}$-módulo de dimensão finita n. Se W é um submódulo de V e $W^\circ = \{x\in V^*;\ x(w)=0,\ \forall\ w\in W\}$, então a aplicação $W\mapsto W^\circ$ é uma bijeção que reverte inclusão e*

$$dim(W^\circ) = n - dim(W).$$

Demonstração. Ver [12, Theorem 1.1.34].

∎

Definição 3.26. Se V é um $\mathbb{C}[G]$-módulo, definimos

$$\left(\sum_{g \in G} \alpha_g g\right) \cdot x = x * \left(\sum_{g \in G} \alpha_g g^{-1}\right),$$

para $x \in V^*$ e $\alpha_g \in \mathbb{C}$. Dessa forma, $(V^*, \cdot)$ é um $\mathbb{C}[G]$-módulo.

Corolário 3.27. *Se V é um $\mathbb{C}[G]$-módulo de dimensão finita n, então*

$$(Inv^G(V))^\circ = Fix_G(V^*).$$

Demonstração. Por definição,

$$Fix_G(V^*) = \{x \in V^*;\ g \cdot x = x,\ \forall\ g \in G\}.$$

Assim, para todo $v \in V$,

$$(g \cdot x)(v) = x(v) \Leftrightarrow x(g^{-1}v) = x(v) \Leftrightarrow x((g^{-1} - 1)v) = 0.$$

Logo $Fix_G(V^*) \subseteq (Inv^G(V))^\circ = \{x \in V^*;\ x(w) = 0, \forall\ w \in Inv^G(V)\}$. Por outro lado, seja $x \in (Inv^G(V))^\circ$. Para todo $v \in V$, temos que $(g^{-1} - 1)v \in Inv^G(V)$ e assim $x((g^{-1} - 1)v) = 0$. Logo

$$(Inv^G(V))^\circ \subseteq Fix_G(V^*).$$

Portanto $(Inv^G(V))^\circ = Fix_G(V^*)$.

∎

Corolário 3.28. *Se G é um grupo cíclico e V é um $\mathbb{C}[G]$-módulo, então*

$$dim(Fix_G(V)) = dim(Fix_G(V^*)).$$

Demonstração. Pelo Corolário 3.27, $(Inv^G(V))^\circ = Fix_G(V^*)$. Logo

$$dim(Fix_G(V^*)) = dim(V) - dim(Inv^G(V)).$$

Por outro lado, se g é o gerador do grupo G, definimos

$$\begin{aligned} f : V &\rightarrow V \\ v &\mapsto (g - 1)v. \end{aligned}$$

Assim,

$$Ker(f) = \{v \in V;\ g \cdot v = v\} = Fix_G(V)$$

e

$$Im(f) = \langle (g-1)v;\ v \in V \rangle = Inv^G(V).$$

Logo,

$$\begin{aligned} dim(V) &= dim(Fix_G(V)) + dim(Inv^G(V)) \\ &= dim(Fix_G(V)) + dim(V) - dim(Fix_G(V^*)) \end{aligned}$$

e portanto,

$$dim(Fix_G(V)) = dim(Fix_G(V^*)).$$

■

Lema 3.29. *Sejam $G = \langle g_1, \ldots, g_r \rangle$ e V um $\mathbb{C}[G]$-módulo. Então*

$$\begin{aligned} Inv^G(V) &= (1-g_1)V + (1-g_2)V + \cdots + (1-g_r)V \\ &= (1-g_1)V + g_1(1-g_2)V + \cdots + g_1 \cdots g_{r-1}(1-g_r)V. \end{aligned}$$

Demonstração. Para demonstrar a primeira igualdade, observamos que

$$g_i(1-g_j)v = (1-g_i)g_jv - (1-g_i)v + (1-g_j)v,$$

para $1 \leqslant i, j \leqslant r$.

Assim, $W_j := (1-g_1)V + \cdots + (1-g_j)V$ é invariante sob a ação dos geradores g_i, para todo $i = 1, \ldots j$.

Logo W_r é um $\mathbb{C}[G]$-submódulo de V e todos os geradores g_i agem trivialmente sobre $\frac{V}{W_r}$. Daí, pela Observação 3.15, temos que $Inv^G(V) \subseteq W_r$. Por outro lado, do fato de $\frac{V}{Inv^G(V)}$ ser invariante sob a ação de G, segue que para todo $v \in V$,

$$g_i(v + Inv^G(V)) = v + Inv^G(V) \Rightarrow (1-g_i)v \in Inv^G(V),$$

então $W_r \subseteq Inv^G(V)$. Portanto $Inv^G(V) = W_r$.

Para a segunda igualdade, vamos mostrar por indução, que

$$W_j = (1-g_1)V + g_1(1-g_2)V + \cdots + g_1 \cdots g_{j-1}(1-g_j)V,$$

para todo $j = 1, \ldots, r$.

Escrevendo

$$\begin{aligned}(1-g_j)v &= (1-g_1)v + g_1(1-g_2)v + g_1g_2(1-g_3)v + \cdots + \\ &\quad + g_1\cdots g_{j-1}(1-g_j)v - (1-g_1\cdots g_{j-1})g_jv\end{aligned}$$

e observando que

$$(1-g_1\cdots g_{j-1})g_jv = (1-g_{j-1})g_jv + (1-g_{j-2})g_{j-1}g_jv + \cdots + (1-g_1)g_2\cdots g_jv$$

pertence a W_{j-1}, segue que

$$(1-g_j)v - g_1\cdots g_{j-1}(1-g_j)v \in W_{j-1}, \text{ para todo } v \in V.$$

Daí,

$$\begin{aligned}W_j &= (1-g_1)V + \cdots + (1-g_{j-1})V + (1-g_j)V \\ &= (1-g_1)V + \cdots + (1-g_{j-1})V + g_1\cdots g_{j-1}(1-g_j)V + W_{j-1} \\ &= W_{j-1} + g_1\cdots g_{j-1}(1-g_j)V \\ &= (1-g_1)V + g_1(1-g_2)V + \cdots + g_1\cdots g_{j-1}(1-g_j)V.\end{aligned}$$

Portanto,

$$\begin{aligned}Inv^G(V) &= (1-g_1)V + (1-g_2)V + \cdots + (1-g_r)V \\ &= (1-g_1)V + g_1(1-g_2)V + \cdots + g_1\cdots g_{r-1}(1-g_r)V.\end{aligned}$$

■

Teorema 3.30 (L. Scott). *Sejam $G = \langle g_1, \ldots, g_r\rangle$ um grupo tal que $g_1\cdots g_r = 1$ e V um $\mathbb{C}[G]$-módulo de dimensão finita n. Então*

$$\sum_{i=1}^{r}\left(n - dim(Fix_{\langle g_i\rangle}(V))\right) \geq 2n - dim(Fix_G(V)) - dim(Fix_G(V^*)).$$

Demonstração. Seja K o $\mathbb{C}$-subespaço de $V^r = V\oplus\cdots\oplus V$, definido por

$$K = \{(v_1, \ldots, v_r);\ v_i \in (1-g_i)V,\ 1 \leq i \leq r\}.$$

Defina as funções $\mathbb{C}$-lineares

$$\begin{aligned}\beta : V &\to K \\ v &\mapsto ((1-g_1)v, \ldots, (1-g_r)v),\end{aligned}$$

e

$$\begin{array}{rcl} \delta : K & \to & V \\ (v_1, \ldots, v_r) & \mapsto & v_1 + g_1 v_2 + \cdots + g_1 \cdots g_{r-1} v_r. \end{array}$$

Como

$$0 = 1 - g_1 \cdots g_r = (1 - g_1) + g_1(1 - g_2) + \cdots + g_1 \cdots g_{r-1}(1 - g_r),$$

temos que $Im(\beta) \subseteq Ker(\delta)$. Além disso,

$$\begin{array}{rcl} Im(\delta) & = & (1 - g_1)V + g_1(1 - g_2)V + \cdots + g_1 \cdots g_{r-1}(1 - g_r)V \\ & = & (1 - g_1)V + \cdots + (1 - g_r)V \\ & = & Inv^G(V), \text{ pelo Lema 3.29.} \end{array}$$

Daí, pelo Lema 3.25 e Corolário 3.27,

$$dim(Im(\delta)) = n - dim(Fix_G(V^*)).$$

Por outro lado,

$$Ker(\beta) = Fix_G(V) \text{ e } Inv^{\langle g_i \rangle}(V) = (1 - g_i)V.$$

Então pelo Lema 3.25 e pelos Corolários 3.27 e 3.28,

$$\begin{array}{rcl} dim(Inv^{\langle g_i \rangle}(V)) & = & n - dim(Fix_{\langle g_i \rangle}(V^*)) \\ & = & n - dim(Fix_{\langle g_i \rangle}(V)), \end{array}$$

donde segue que

$$\begin{array}{rcl} \displaystyle\sum_{i=1}^{r} \big(n - dim(Fix_{\langle g_i \rangle}(V))\big) & = & \displaystyle\sum_{i=1}^{r} \big(dim(Inv^{\langle g_i \rangle}(V))\big) \\ & = & \displaystyle\sum_{i=1}^{r} dim((1 - g_i)V) \\ & = & dim(K) \\ & = & dim(Im(\delta)) + dim(Ker(\delta)) \\ & = & n - dim(Fix_G(V^*)) + dim(Im(\beta)) + \\ & & +dim\left(\dfrac{Ker(\delta)}{Im(\beta)}\right) \\ & = & n - dim(Fix_G(V^*)) + n + \\ & & - dim(Ker(\beta)) + dim\left(\dfrac{Ker(\delta)}{Im(\beta)}\right) \\ & \geq & 2n - dim(Fix_G(V^*)) - dim(Fix_G(V)). \end{array}$$

■

Corolário 3.31. *Seja G um grupo finito tal que $G = \langle g_1, \ldots, g_r \rangle$ e $g_1 \cdots g_r = 1$. Se $1_G \neq \chi \in Irr(G)$, então*

$$\sum_{i=1}^{r} \alpha_\chi(g_i) \leq (r-2)\chi(1).$$

Demonstração. Seja V um $\mathbb{C}[G]$-módulo irredutível de dimensão finita associado ao caráter χ. Lembramos que

$$\begin{array}{rcl} G & \to & GL(V) \\ g & \mapsto & g_L \end{array}$$

é a representação de G associada ao módulo V. Sendo $Fix_G(V)$ um submódulo de V, temos somente duas possibilidades:

$$Fix_G(V) = \{0\} \text{ ou } Fix_G(V) = V.$$

Se $Fix_G(V) = V$, então para todo $v \in V$ e para todo $g \in G$ temos $\Phi(g)v = v$, ou seja, $\Phi(g) = Id$ contradizendo a hipótese de que $\chi \neq 1_G$. Portanto, $Fix_G(V) = \{0\}$.

Agora vamos verificar que $Fix_G(V^*) = \{0\}$. Como V é um $\mathbb{C}[G]$-módulo irredutível, V^* é também um $\mathbb{C}[G]$-módulo irredutível, pelo Lema 3.25. Logo $Fix_G(V^*) = \{0\}$ ou $Fix_G(V^*) = V^*$.

Se $Fix_G(V^*) = V^*$, então pelo Corolário 3.27 e pelo Lema 3.25,

$$\begin{aligned} dim(V^*) &= dim(Fix_G(V^*)) = dim(Inv^G(V))^\circ \\ &= dim(V) - dim(Inv^G(V)). \end{aligned}$$

Logo $dim(Inv^G(V)) = 0$ e assim $Fix_G(V) = V$, contradizendo o que demonstramos anteriormente. Portanto $Fix_G(V^*) = \{0\}$.

Por outro lado, pelo Lema 3.5

$$\alpha_\chi(g_i) = dim(Fix_{\langle g_i \rangle}(V)).$$

Logo, pelo Teorema 3.30,

$$\sum_{i=1}^{r} (n - \alpha_\chi(g_i)) \geq 2n$$

e portanto,

$$\sum_{i=1}^{r} \alpha_\chi(g_i) \leq (r-2)n = (r-2)\chi(1).$$

■

Corolário 3.32. *Para cada $g \in G$, denote por $d(g)$ o menor número de conjugados de g em G, que geram o grupo G. Então*

$$d(g) \geq \frac{\chi(1)}{\chi(1) - \alpha_\chi(g)},$$

para qualquer caráter irredutível $\chi \neq 1_G$.

Demonstração. Se V é um $\mathbb{C}[G]$-módulo irredutível de dimensão finita associado ao caráter χ, então $Fix_G(V) = \{0\}$ e $Fix_G(V^*) = \{0\}$, pois $1_G \neq \chi \in Irr(G)$. Denotando $d = d(g)$, temos que $G = \langle g_1, \ldots, g_d \rangle$, onde g_i é conjugado a g em G. Assim, definindo $g_{d+1} = (g_1 \cdots g_d)^{-1}$ e aplicando o Teorema 3.30 temos

$$\sum_{i=1}^{d+1} \big(dim(V) - dim(Fix_{\langle g_i \rangle}(V))\big) \geq 2dim(V),$$

onde $dim(V) = \chi(1)$ e $dim(Fix_{\langle g_i \rangle}(V)) = dim(Fix_{\langle g \rangle}(V)) = \alpha_\chi(g)$, para todo $i = 1, \ldots, d$.

Assim,

$$\begin{aligned} d \cdot (\chi(1) - \alpha_\chi(g)) &\geq \chi(1) + dim(Fix_{\langle g_{d+1} \rangle}(V)) \\ &\geq \chi(1) \end{aligned}$$

e portanto,

$$d(g) \geq \frac{\chi(1)}{\chi(1) - \alpha_\chi(g)}.$$

■

Teorema 3.33. *Sejam G um grupo finito e $Cl_1, \ldots, Cl_m$ classes de conjugação de G. Se $\gamma_G(Cl_1, \ldots, Cl_m) > 0$, então*

$$\gamma_G(Cl_1, \ldots, Cl_m) \geq |G : Z(G)|.$$

Demonstração. Fixando $g_m \in Cl_m$, temos que $\gamma_G(Cl_1, \ldots, Cl_m)$ é igual a

$$|Cl_m| \cdot |\{(g_1, \ldots, g_{m-1});\ g_i \in Cl_i,\ g_1 \cdots g_{m-1} = {g_m}^{-1}, \langle g_1, \ldots, g_m \rangle = G\}|.$$

Daí, por hipótese, existe pelo menos uma $(m-1)$-upla $(g_1, \ldots, g_{m-1})$, tal que

$$g_i \in Cl_i, \quad g_1 \cdots g_{m-1} = {g_m}^{-1} \quad \text{e} \quad \langle g_1, \ldots, g_m \rangle = G.$$

Se $x \in C_G({g_m}^{-1})$, então $(xg_1x^{-1}, \ldots, xg_{m-1}x^{-1})$ é tal que $xg_ix^{-1} \in Cl_i$, para todo $i = 1, \ldots, m-1$,

$$xg_1x^{-1} \cdots xg_{m-1}x^{-1} = x{g_m}^{-1}x^{-1} = {g_m}^{-1}$$

e $\langle xg_1x^{-1}, \ldots, xg_{m-1}x^{-1}\rangle = G$. Por outro lado, se $x, y \in C_G({g_m}^{-1})$, então

$$\begin{aligned} & (xg_1x^{-1}, \ldots, xg_{m-1}x^{-1}) = (yg_1y^{-1}, \ldots, yg_{m-1}y^{-1}) \Leftrightarrow \\ \Leftrightarrow \quad & xg_ix^{-1} = yg_iy^{-1}, \text{ para todo } i = 1, \ldots, m-1 \\ \Leftrightarrow \quad & y^{-1}x \in Z(G). \end{aligned}$$

Assim temos que

$$\begin{aligned} & |\{(g_1, \ldots, g_{m-1});\ g_i \in Cl_i,\ g_1 \cdots g_{m-1} = {g_m}^{-1}, \langle g_1, \ldots, g_m\rangle = G\}| \geq \\ & \geq \frac{|C_G({g_m}^{-1})|}{|Z(G)|}, \end{aligned}$$

donde

$$\gamma_G(Cl_1, \ldots, Cl_m) \geq |Cl({g_m}^{-1})| \cdot |C_G({g_m}^{-1}) : Z(G)|.$$

Portanto,

$$\gamma_G(Cl_1, \ldots, Cl_m) \geq |G : Z(G)|.$$

■

Vamos agora aplicar os resultados anteriores para provar que o grupo simples $PSp(4, 3)$ e o grupo $Sp(4, 3)$ não são $(2, 3)$-gerados. Demonstrações mais gerais podem ser encontradam em [11] e [14]. No primeiro, Liebeck e Shalev demonstram que $PSp(4, q)$ não é $(2, 3)$-gerado para $q = 2^a$ ou 3^a. No segundo, os autores demonstram que $Sp(4, q)$ não é $(2, 3)$-gerado quando q é potência de primo.

Lembramos brevemente a definição de grupo simplético.

Definição 3.34. Sejam V um espaço vetorial de dimensão finita n sobre um corpo K. Uma *forma bilinear* sobre V é uma aplicação $f : V \times V \to K$ tal que

(1) $f(x + \lambda y, z) = f(x, z) + \lambda f(y, z)$

(2) $f(x, \lambda y + z) = \lambda f(x, y) + f(x, z)$,

para todos $x, y, z \in V$ e $\lambda \in K$.

Definição 3.35. Sejam V um espaço vetorial de dimensão finita sobre um corpo K e β uma base de V. Dizemos que f é *não-degenerada*, se o determinante da matriz que representa a forma f com respeito à base β é diferente de zero.

Definição 3.36. Sejam V um espaço vetorial de dimensão finita n sobre um corpo K e $f : V \times V \to K$ uma forma bilinear não-degenerada. Se f satisfaz

$$f(x, x) = 0 \text{ e } f(x, y) = -f(y, x),$$

para todo $x, y \in V$, dizemos que f é uma forma *simplética* sobre V.

Dizemos que (V, f) é um espaço simplético se f é simplética.

Definição 3.37. Seja (V, f) um espaço simplético. O conjunto das *isometrias simpléticas* de V é definido por

$$I(V, f) = \{g \in GL(V); f(g(x), g(y)) = f(x, y), \forall\ x, y \in G\}.$$

Pode ser demonstrado que o conjunto $I(V, f)$ é um subgrupo de $SL(V)$. Além disso, se f_1 e f_2 são duas formas simpléticas, então os respectivos grupos $I(V, f_1)$ e $I(V, f_2)$ são isomorfos. Para qualquer escolha de f vamos denotar o grupo $I(V, f)$ por $Sp(V)$, $Sp(n, K)$ ou $Sp(n, q)$ no caso em que $|K| = q$. O leitor pode obter mais informações em [5].

O grupo *simplético projetivo* é definido pelo quociente $\frac{Sp(V)}{Z(Sp(V))}$ e é denotado por $PSp(V)$, $PSp(n, K)$ ou $PSp(n, q)$ no caso em que $|K| = q$.

Definição 3.38. Um grupo finito G é dito (m, n)-gerado, se existem dois elementos $x, y \in G$ tais que $|x| = m, |y| = n$ e $G = \langle x, y\rangle$.

Vamos escrever a tabela de caracteres de $G = PSp(4, 3)$, na qual utilizaremos a seguinte notação

$$A = \frac{1 + 3\sqrt{-3}}{2},\quad B = \frac{-7 + 3\sqrt{-3}}{2},\quad C = \frac{-3 + 9\sqrt{-3}}{2},$$
$$D = -5 - 3\sqrt{-3},\quad E = \frac{9 - 9\sqrt{-3}}{2},\quad F = \frac{-3 - \sqrt{-3}}{2},$$
$$G = 1 - \sqrt{-3},\quad H = \frac{-3 + 3\sqrt{-3}}{2},\quad I = \sqrt{-3},\quad J = \frac{1 - \sqrt{-3}}{2}.$$

e $/P$ significa o conjugado complexo de P, para $P = A, B, \ldots, J$.

Tabela de caracteres do grupo $PSp(4,3)$.

	2	6	6	5	3	3	2	1	4	3	.	3	3	2	2	1	2	.	.	2	2
	3	4	2	1	4	4	3	3	1	.	.	2	2	2	2	2	1	2	2	1	1
	5	1	.	.	.	.	.	.	.	.	1	.	.	.	.	.	.	.	.	.	.
		1a	2a	2b	3a	3b	3c	3d	4a	4b	5a	6a	6b	6c	6d	6e	6f	9a	9b	12a	12b
	2P	1a	1a	1a	3b	3a	3c	3d	2a	2b	5a	3b	3a	3c	3c	3d	3c	9b	9a	6b	6a
	3P	1a	2a	2b	1a	1a	1a	1a	4a	4b	5a	2a	2a	2a	2a	2a	2b	3a	3b	4a	4a
	5P	1a	2a	2b	3b	3a	3c	3d	4a	4b	1a	6b	6a	6d	6c	6e	6f	9b	9a	12b	12a
X.1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
X.2		5	-3	1	A	/A	-1	2	1	-1	.	F	/F	I	-I	.	1	J	/J	-J	-/J
X.3		5	-3	1	/A	A	-1	2	1	-1	.	/F	F	-I	I	.	1	/J	J	-/J	-J
X.4		6	-2	2	-3	-3	3	.	2	.	1	1	1	1	1	-2	-1	.	.	-1	-1
X.5		10	2	-2	B	/B	1	1	2	.	.	A	/A	-1	-1	-1	1	-/J	-J	J	/J
X.6		10	2	-2	/B	B	1	1	2	.	.	/A	A	-1	-1	-1	1	-J	-/J	/J	J
X.7		15	-1	-1	6	6	3	.	3	-1	.	2	2	-1	-1	2	-1	.	.	.	.
X.8		15	7	3	-3	-3	.	3	-1	1	.	1	1	-2	-2	1	.	.	.	-1	-1

	1a	2a	2b	3a	3b	3c	3d	4a	4b	5a	6a	6b	6c	6d	6e	6f	9a	9b	12a	12b
2P	1a	1a	1a	3b	3a	3c	3d	2a	2b	5a	3b	3a	3c	3c	3d	3c	9b	9a	6b	6a
3P	1a	2a	2b	1a	1a	1a	1a	4a	4b	5a	2a	2a	2a	2a	2a	2b	3a	3b	4a	4a
5P	1a	2a	2b	3b	3a	3c	3d	4a	4b	1a	6b	6a	6d	6c	6e	6f	9b	9a	12b	12a
X.9	20	4	4	2	2	5	-1	.	.	.	-2	-2	1	1	1	1	-1	-1	.	.
X.10	24	8	.	6	6	.	3	.	.	-1	2	2	2	2	-1	.	.	.	.	.
X.11	30	-10	2	3	3	3	3	-2	.	.	-1	-1	-1	-1	-1	-1	.	.	1	1
X.12	30	6	2	C	/C	-3	.	2	.	.	/F	F	-I	I	.	-1	.	.	/J	J
X.13	30	6	2	/C	C	-3	.	2	.	.	F	/F	I	-I	.	-1	.	.	J	/J
X.14	40	-8	.	D	/D	-2	1	.	.	.	G	/G	G	/G	1	.	-/J	-J	.	.
X.15	40	-8	.	/D	D	-2	1	.	.	.	/G	G	/G	G	1	.	-J	-/J	.	.
X.16	45	-3	-3	E	/E	.	.	1	1	.	H	/H	.	.	.	.	.	.	-J	-/J
X.17	45	-3	-3	/E	E	.	.	1	1	.	/H	H	.	.	.	.	.	.	-/J	-J
X.18	60	-4	4	6	6	-3	-3	.	.	.	2	2	-1	-1	-1	1	.	.	.	.
X.19	64	.	.	-8	-8	4	-2	.	.	-1	.	.	.	.	.	.	1	1	.	.
X.20	81	9	-3	.	.	.	.	-3	-1	1	.	.	.	.	.	.	.	.	.	.

Agora, usando a fórmula descrita no Teorema 3.23, obtemos

$Cl:$	$1a$	$2a$	$2b$	$3a$	$3b$	$3c$	$3d$	$4a$	$4b$
$\alpha_G(2a,3a,Cl)$	0	0	0	0	0	0	0	0	0
$\alpha_G(2a,3b,Cl)$	0	0	0	0	0	0	0	0	0
$\alpha_G(2a,3c,Cl)$	0	0	0	0	0	0	0	0	0
$\alpha_G(2a,3d,Cl)$	0	1440	0	0	0	0	0	0	12960
$\alpha_G(2b,3a,Cl)$	0	0	0	0	0	0	0	0	0
$\alpha_G(2b,3b,Cl)$	0	0	0	0	0	0	0	0	0
$\alpha_G(2b,3c,Cl)$	0	0	4320	0	0	6480	0	0	12960
$\alpha_G(2b,3d,Cl)$	0	0	4320	0	0	0	12960	0	12960

$Cl:$	$5a$	$6a$	$6b$	$6c$	$6d$	$6e$	$6f$	$9a$
$\alpha_G(2a,3a,Cl)$	0	0	360	1440	0	0	0	0
$\alpha_G(2a,3b,Cl)$	0	360	0	0	1440		0	0
$\alpha_G(2a,3c,Cl)$	0	0	0	720	720	2880	6480	0
$\alpha_G(2a,3d,Cl)$	0	2880	2880	0	0	1440	0	0
$\alpha_G(2b,3a,Cl)$	0	0	0	0	0	0	4320	0
$\alpha_G(2b,3b,Cl)$	0	0	0	0	0	0	4320	0
$\alpha_G(2b,3c,Cl)$	25920	0	0	6480	6480	0	2160	0
$\alpha_G(2b,3d,Cl)$	25920	0	0	0	0	12960	8640	25920

$Cl:$	$9b$	$12a$	$12b$
$\alpha_G(2a,3a,Cl)$	0	0	0
$\alpha_G(2a,3b,Cl)$	0	0	0
$\alpha_G(2a,3c,Cl)$	0	0	0
$\alpha_G(2a,3d,Cl)$	0	0	0
$\alpha_G(2b,3a,Cl)$	0	0	6480
$\alpha_G(2b,3b,Cl)$	0	6480	0
$\alpha_G(2b,3c,Cl)$	0	0	0
$\alpha_G(2b,3d,Cl)$	25920	0	0

Observação 3.39. Sejam G um grupo finito, Cl_1, Cl_2, Cl_3 três classes de conjugação, não necessariamente distintas, de G tais que os elementos de Cl_1 possuem ordem m e os elementos de Cl_2 possuem ordem n. Observamos que

$$\alpha_G(Cl_1, Cl_2, Cl_3) \geq \gamma_G(Cl_1, Cl_2, Cl_3) \geq 0.$$

Além disso:

(1) Se $\alpha_G(Cl_1, Cl_2, Cl_3) = 0$, então $\gamma_G(Cl_1, Cl_2, Cl_3) = 0$ e portanto G não é gerado por um par de elementos x, y tais que $x \in Cl_1$, $y \in Cl_2$ e $(xy)^{-1} \in Cl_3$. Se isso acontece para qualquer escolha da classe Cl_3, então G não é (m, n)-gerado.

(2) Se supomos que G é (m, n)-gerado, então para alguma escolha da classe Cl_3, temos

$$\gamma_G(Cl_1, Cl_2, Cl_3) > 0$$

e portanto, pelo Teorema 3.33

$$\alpha_G(Cl_1, Cl_2, Cl_3) \geq \gamma_G(Cl_1, Cl_2, Cl_3) \geq |G : Z(G)|.$$

Assim, considerando o caso particular em que $G = PSp(4, 3)$, temos que analisar apenas os casos em que $\alpha_G(Cl_1, Cl_2, Cl_3) \geq |G| = 25920$. Ou seja, devemos analisar os seguintes casos

$$(Cl_1, Cl_2, Cl_3) = (2b, 3c, 5a),\ (2b, 3d, 5a),\ (2b, 3d, 9a) \text{ e } (2b, 3d, 9b).$$

Utilizando a tabela de caracteres de $G = PSp(4, 3)$, temos

$g \in$	$1a$	$2b$	$3c$	$3d$	$5a$	$9a$	$9b$
$\alpha_{\chi_2}(g)$	5	3	1	3	1	1	1
$\alpha_{\chi_{20}}(g)$	81	39	27	27	17	9	9

Assim,

(1) Para o caso $(2b, 3c, 5a)$, suponha que existem $g_1, g_2, g_3 \in G$ tais que $g_1 \in 2b,\ g_2 \in 3c,\ g_3 \in 5a$, o produto $g_1 \cdot g_2 \cdot g_3 = 1$ e $G = \langle g_1, g_2 \rangle$. Pelo Corolário 3.32, devemos ter

$$\sum_{i=1}^{3} \alpha_\chi(g_i) \leq \chi(1),$$

para todo caráter irredutível $\chi \neq 1_G$. Mas

$$\sum_{i=1}^{3} \alpha_{\chi_{20}}(g_i) = 83 > 81 = \chi_{20}(1).$$

Portanto $G \neq \langle g_1, g_2 \rangle$.

(2) Analogamente, para os casos $(2b, 3d, 5a)$, $(2b, 3d, 9a)$ e $(2b, 3d, 9b)$, temos que

$$\sum_{i=1}^{3} \alpha_{\chi_2}(g_i) = 7 > 5 = \chi_2(1),$$

contradizendo o Corolário 3.32.

Portanto, $PSp(4, 3)$ não é $(2, 3)$-gerado.

Utilizando o GAP também podemos obter os subgrupos de $PSp(4, 3)$ que são $(2, 3)$-gerados. Esses subgrupos possuem ordens $6, 12, 18, 24, 48, 60$ e 324.

Agora vamos mostrar que $G = Sp(4, 3)$ não é $(2, 3)$-gerado. Vamos apresentar uma parte da tabela de caracteres de $Sp(4, 3)$, o leitor pode consultar esta tabela completa em [2].

Utilizaremos a seguinte notação

$$A = \frac{1 + 3\sqrt{-3}}{2},\ B = \frac{-7 + 3\sqrt{-3}}{2},$$
$$H = \frac{-3 - \sqrt{-3}}{2},\ K = -\sqrt{-3},\ L = \frac{1 - \sqrt{-3}}{2}.$$

Tabela de caracteres do grupo $Sp(4,3)$.

2	7	7	6	5	4	4	4	4	3	3	2	2	5	5	3	1	1	4	4	4	4	2	2	2	2	2	1	1
3	4	4	2	1	4	4	4	4	3	3	3	3	1	1	.	.	.	2	2	2	2	2	2	2	2	1	2	2
5	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	1	1	.	.	.	.	.	.	.	.	.	.	.
	1a	2a	2b	4a	3a	6a	3b	6b	3c	6c	3d	6d	4b	4c	8a	5a	10a	6e	6f	6g	6h	6i	6j	6k	6l	12a	9a	18a
2P	1a	1a	1a	2a	3b	3b	3a	3a	3c	3c	3d	3d	2b	2b	4a	5a	5a	3b	3b	3a	3a	3c	3c	3d	3d	6c	9b	9b
3P	1a	2a	2b	4a	1a	2a	1a	2a	1a	2a	1a	2a	4b	4c	8a	5a	10a	2b	2b	2b	2b	2b	2b	2b	2b	4a	3a	6a
5P	1a	2a	2b	4a	3b	6b	3a	6a	3c	6c	3d	6d	4b	4c	8a	1a	2a	6g	6h	6e	6f	6j	6i	6l	6k	12a	9b	18b
X.1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
X.2	5	5	-3	1	A	A	/A	/A	-1	-1	2	2	1	1	-1	.	.	H	H	/H	/H	-K	K	.	.	1	L	L
X.3	5	5	-3	1	/A	/A	A	A	-1	-1	2	2	1	1	-1	.	.	/H	/H	H	H	K	-K	.	.	1	/L	/L
X.4	6	6	-2	2	-3	-3	-3	-3	3	3	.	.	2	2	.	1	1	1	1	1	1	1	1	-2	-2	-1	.	.
X.5	10	10	2	-2	B	B	/B	/B	1	1	1	1	2	2	.	.	.	A	A	/A	/A	-1	-1	-1	-1	1	-/L	-/L
X.6	10	10	2	-2	/B	/B	B	B	1	1	1	1	2	2	.	.	.	/A	/A	A	A	-1	-1	-1	-1	1	-L	-L
X.7	15	15	-1	-1	6	6	6	6	3	3	.	.	3	3	-1	.	.	2	2	2	2	-1	-1	2	2	-1	.	.
X.8	15	15	7	3	-3	-3	-3	-3	.	.	3	3	-1	-1	1	.	.	1	1	1	1	-2	-2	1	1	.	.	.

Utilizando o GAP, temos que

$$\alpha_G(2b, 3d, 8a) = 25920 = \frac{|G|}{|Z(G)|}$$

e esse é o único caso que devemos analisar.

Suponha que existem $g_1, g_2, g_3 \in G$ tais que $g_1 \in 2b,\ g_2 \in 3d,\ g_3 \in 8a$, o produto $g_1 \cdot g_2 \cdot g_3 = 1$ e $G = \langle g_1, g_2 \rangle$. Pelo Corolário 3.32, devemos ter

$$\sum_{i=1}^{3} \alpha_\chi(g_i) \leq \chi(1),$$

para todo caráter irredutível $\chi \neq 1_G$. Mas utilizando a tabela de caracteres de $Sp(4,3)$, temos que

$g \in$	$1a$	$2b$	$3d$	$8a$
$\alpha_{\chi_8}(g)$	15	11	7	5

assim

$$\sum_{i=1}^{3} \alpha_{\chi_8}(g_i) = 23 > 15 = \chi_8(1),$$

logo $G \neq \langle g_1, g_2 \rangle$. Portanto $Sp(4,3)$ não é $(2,3)$-gerado.

Como observação final, os subgrupos de $Sp(4,3)$ que são $(2,3)$-gerados possuem ordens $6, 18$ e 48.

Referências Bibliográficas

[1] R. Brauer and J. Tate, 'On the characters of finite groups', *Annals of Mathematics.* **62** (1955), n°. 1, 1-7.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups*, Oxford University Press, Eynsham, 1985.

[3] L. Dornhoff, *Group Representation Theory (part A)*, Marcel Dekker, New York, 1972.

[4] A. Garcia e Y. Lequain, *Elementos de Álgebra*, 5. edição, Rio de Janeiro, Projeto Euclides, 2010.

[5] L. C. Grove, *Classical Groups and Geometric Algebra*, American Mathematical Society, Rhode Island, 2002.

[6] J. F Humphreys, *A Course in Group Theory*, Oxford, New York, 2001.

[7] B. Huppert, *Character Theory of Finite Groups*, Walter de Gruyter, Berlim, New York, 1998.

[8] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[9] I. M. Isaacs, 'The fixed-point-space dimension function for a finite group representation', *Proceedings of the American Mathematical Society.* **107** (1989), n°. 4, 867-872.

[10] S. Lang, *Algebra*, Springer-Verlag, New York, 2002.

[11] M. W. Liebeck and A. Shalev, 'Classical Groups, Probabilistic Methods and the $(2,3)$-Generation Problem', *Annals of Mathematics.* **144** (1996), n°. 1, 77-125.

[12] K. Lux and H. Pahlings, *Representations of Groups. A Computational Approach*, Cambridge University Press, New York, 2010.

[13] O. Manz and T. R. Wolf, *Representations of solvable groups*, Cambrige, New York, 1993.

[14] M. A. Pellegrini, M. C. Tamburini and M. A. Vsemirnov, 'Uniform $(2,k)$-generation of the 4-dimensional classical groups', *Journal of Algebra.* **369** (2012), 322-350.

[15] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer, 4th edition, November 1994.

[16] J. J. Rotman, *Advanced Modern Algebra*, Prentice Hall, 1st edition, 2002, 2th printing 2003 .

[17] J. P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.

[18] R. W. van der Waall, 'On Brauer's induction formula of characters of groups', *Archiv Mathematik.* **63** (1994), n°. 4, 208-210.

[19] T. Wilde, 'A Note on Brauer's Induction Theorem in a Soluble Group', *Communications in Algebra.* **34** (2006), n°. 5, 867-872.