Grupos de Fröbenius

Um estudo sobre um teorema de Fröbenius, Teoria de Representações e Caracteres de Grupos Finitos

Brasília, Brasil, 2017–2018

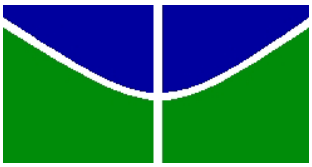
Trabalho por

João Pedro Papalardo Azevedo

Sob a orientação do professor

Emerson Ferreira de Melo
Universidade de Brasília

Programa FAPDF: Edital 03/2016
Modalidade: IC– Iniciação Científica
Projeto: Estruturas Algébricas



Conteúdo

1 Introdução

Este trabalho é o relatório final do projeto de iniciação científica intitulado "Estruturas Algébricas", edital 03/2016, financiado pela Fundação de Apoio à Pesquisa do Distrito Federal - FAPDF. Além disso, o presente texto tem também a intenção de ser um texto introdutório à Teoria de Caracteres, autocontido o suficiente para que um leitor que entende Álgebra Linear e os teoremas básicos da Teoria de Grupos Finitos consiga entender os resultados apresentados, dos quais o principal é o Teorema de Fröbenius, que prova a normalidade e a ordem do núcleo num grupo de Fröbenius. Nesse trabalho, curiosamente, muitos, senão a maioria dos teoremas, é constituída de resultados do próprio Fröbenius, como os teoremas importantes do capítulo 4, e isso acontece em parte porque a atuação desse matemático, apesar de frutuosa em inúmeras áreas, teve resultados particularmente interessantes na Teoria de Representações e na Teoria de Caracteres.

Desse modo, não podemos deixar de citar, ao menos em linhas gerais, alguns aspectos da figura desse homem que esteve na linha de frente da matemática no seu tempo. Nascido em uma cidade da Prússia, hoje Alemanha, em 1849, Fröbenius morre em 1917, antes de completar 68 anos de idade. Foi orientado por Weiesrtrass e Kumming no seu doutorado, que concluiu 1870 na Universidade de Berlim, onde também assistiu às aulas de Kronecker e anos mais tarde ocupou a cadeira que pertencia a ele. O próprio Weierstrass gostava de dizer que Fröbenius era um de seus alunos mais talentosos. A atuação profissinal de Fröbenius começa tão logo ele se forma, mesmo sem licença para lecionar, algo incomum no sistema alemão do século XIX. Fröbenius atuou em vários ramos da matemática de maneira frutuosa, e seus artigos do início do século 20 ainda hoje figuram em vários livros de graduação e pós-graduação ao redor do mundo.

Sem dúvida estamos aqui falando de um matemático bastante competente, que orientou Ernst Landau e Issai Schur, publicando alguns trabalhos com este último. Porém, quando se fala da vida pessoal de Fröbenius, algumas controvérsias aparecem. Alguns historiadores o descrevem com sendo uma pessoa impaciente e explosiva, dada a discussões com outros, fato esse que muitas pessoas atestam. Fröbenius trabalhou na Universidade de Berlim por 25 anos, e mostrava ter verdadeira aversão a matemáticos como Felix Klein e Sophus Lie, que tinham uma forma de pensar matemática menos tradicional que aquela que ele vivia em Berlim. Havia uma certa competição entre a universidade de Berlim e a de Göttinghem, onde Klein trabalhou. Essa disputa foi vencida por Göttinghem com importante papel de Klein, outro matemático que era um dos mais eminentes de seu tempo. A maior parte dos professores de matemática da Universidade de Berlim pensava que a matemática aplicada devia ser deixada para as escolas técnicas e que as universidades eram lugar para a matemática pura; Fröbenius compartilhava desse pensamento. Para a felicidade da ciência (e provável desgosto de nosso matemático) suas descobertas foram mais tarde usadas para fazer avançar a Mecânica Quântica e a Física Teórica.

Apesar do temperamento explosivo e das relações estranhas com alguns matemáticos, há quem descreva Fröbenius como uma figura calorosa e, apesar de

tudo, os resultados dele foram certamente muito interessantes. O presente texto termina com uma prova de um resultado sobre grupos de Fröbenius, e por esse motivo apresentamos aqui a definição do que vêm a ser tais grupos e o enunciado, sem prova, do nosso resultado principal:

Definição 1. ***Grupo de Fröbenius:*** *Um grupo finito G é dito grupo de Fröbenius quando em sua representação por permutações G é transitivo, há um subgrupo não-trivial H fixando um elemento e apenas a identidade fixa mais de um elemento. Tal subgrupo H é chamado* ***complemento de Fröbenius.***

Com isso, apresentamos agora o

Teorema de Fröbenius. *Se G um grupo de Fröbenius e H o subgrupo de G fixando uma letra, então o subconjunto de G que consiste da identidade mais os elementos que não fixam nenhuma letra é um subgrupo normal K de G de ordem $[G : H]$.*

É interessante pensar que apenas com algumas hipóteses simples prova-se que algo que inicialmente era apenas um subconjunto de G é, na verdade, um subgrupo normal. No final da seção 3 mostraremos que esse subgrupo normal que surge, chamado de *núcleo de Fröbenius* tem ainda mais algumas propriedades interessantes que elencamos a seguir:

Teorema 1. *Seja G um grupo de Fröbenius com núcleo K e complemento H. Então:*

(i) $G = HK$*, com* $H \cap K = 1$*, de forma que G é o produto semidireto de K por H.*

(ii) $|H|$ *divide* $|K|$*-1.*

(iii) Todo elemento de $H^{\#}$ *induz por conjugação um automorfismo livre de ponto fixo sobre K.*

(iv) $C_G(y) \leq K, \forall y \in K^{\#}$.

Dito isso, comecemos.

2 Preliminares

Nesta seção mostraremos alguns resultados simples que serão necessários no decorrer do texto. Aqui, G sempre será um grupo finito.

Proposição 1. *Seja A uma matriz $n \times n$ qualquer. O traço de A é igual à soma de seus autovalores.*

Demonstração. De fato, basta notar que o polinômio característico de A, $p(t) = det(A - tI)$, onde I denota a identidade de ordem n, é dado pela expressão

$$p(t) = (-1)^n(t^n - tr(A)t^{n-1} + \cdots + (-1)^n det(A)),$$

ao mesmo tempo em que o Teorema Fundamental da Álgebra garante que

$$p(t) = (-1)^n(t - \lambda_1)\cdots(t - \lambda_n),$$

onde λ_i representa o i-ésimo autovalor de A, $i = 1, \cdots, n$. Comparando os coeficientes dos dois polinômios, o resultado segue. □

Proposição 2. *O conjunto I dos inteiros algébricos é um anel com as operações usuais de adição e multiplicação. Em particular, tal conjunto é subanel de $\mathbb{C}$.*

Demonstração. O Teorema Fundamental da Álgebra garante que $p(X)$ tem $gr(p)$ raízes complexas, o que prova que $I \subset \mathbb{C}$, e como $\mathbb{C}$ é um anel com as operações apresentadas, devemos apenas provar que I é subanel de $\mathbb{C}$. De fato, note que $0 \in I$ visto que 0 satisfaz o polinômio $p(X) = X$. Dados $j, k \in I, j \neq 0$, temos que existem $p(X) \in \mathbb{Z}[X]$ mônico tal que $p(k) = 0$. Note que $k - j$ é uma raiz do polinômio mônico $p(X + j)$, visto que $p(k - j + j) = p(k) = 0$, de forma que $k - j \in I$. Por fim, note que kj é raiz do polinômio mônico $j^{gr(p)}p(X/j)$, o que completa a demonstração. □

Proposição 3. *Sejam X, Y matrizes quadradas de ordem n com entradas complexas, e sejam $\lambda, \mu \in \mathbb{C}$. Então vale que*

(i) $tr\, XY = tr\, YX$.

(ii) $tr(\lambda X + \mu Y) = \lambda tr\, X + \mu tr\, Y$.

(iii) Se X e Y são matrizes similares, então $tr\, X = tr\, Y$.

(iv) $tr\,(X \otimes Y) = (tr\, X)(tr\, Y)$.

(v) $tr\,(X^t) = tr\, X$.

Demonstração. Para (i), veja que

$$tr\, XY = \sum_{i=1}^{n}\sum_{k=1}^{n} x_{ik}y_{ki} = \sum_{k=1}^{n}\sum_{i=1}^{n} y_{ki}x_{ik} = tr\, YX$$

. Note, agora, que

$$tr(\lambda X + \mu Y) = \sum_{k=1}^{n} \lambda x_{kk} + \mu y_{kk} = \lambda \sum_{k=1}^{n} x_{kk} + \mu \sum_{k=1}^{n} y_{kk} = \lambda tr\, X + \mu tr\, Y.$$

Em (iii), veja que, se $X = P^{-1}YP$, usando (i), temos que $tr\, X = tr\,(P^{-1}(YP)) = tr\,(YPP^{-1}) = tr\, Y$. Para (iv), note que, sendo $Y = (y_{ij})$, o produto tensorial entre X e Y é dado em forma de blocos por

$$X \otimes Y = \begin{pmatrix} y_{11}X & \cdots & y_{1n}X \\ \vdots & \ddots & \vdots \\ y_{n1}X & \cdots & y_{nn}X \end{pmatrix},$$

de forma que é fácil ver que $tr\,(X \otimes Y) = (tr\, X)(tr\, Y)$.

Para (v), basta notar que a diagonal principal de uma matriz fica invariante por transposição. □

3 Representações

Nesse capítulo vamos estabelecer as definições e resultados básicos que dizem respeito à Teoria de Representações de grupos dos quais vamos precisar e que não dependem dos resultados da Teoria de Caracteres. Depois de introduzir alguns conceitos da teoria de representações, vamos mostrar alguns resultados envolvendo representações de permutações e mostramos o importante Teorema de Maschke, que garante a redutibilidade completa de algumas representações de grupos finitos. Por fim, terminamos o capítulo com resultados a respeito de representações irredutíveis de grupos finitos e o teorema de Wedderburn.

3.1 Representações de Permutações

Um grupo de permutações G agindo num conjunto S é dito *transitivo* em S dado que, para $s, s' \in S$, exista um $x \in G$ tal que $x(s) = s'$ e é dito *duplamente transitivo* em S dado que para cada conjunto de pares $\{s_1, s_2\}$ e $\{s'_1, s'_2\}$ com $s_i, s'_i \in S$, $i = 1, 2$, $s_1 \neq s_2$ e $s'_1 \neq s'_2$ exista $x \in G$ tal que $x(s_i) = s'_i$, $i = 1, 2$. Transitividade tripla e, de maneira geral, transitividade m-upla são definidas da mesma forma. O inteiro $|S|$ é chamado de *grau* de G.

Em qualquer grupo de permutações G agindo num conjunto S, o subconjunto H de G que deixa qualquer subconjunto T de S invariante, ou como conjunto ou elemento a elemento, é claramente um subgrupo de G.

Seja H um subgrupo de G e seja x_iH, $1 \leq i \leq n$ um conjunto completo de classes laterais de H em G. Denote o conjunto dessas classes laterais por S. Então, para $x \in G$, a função π_x definida por

$$\pi_x(x_iH) = xx_iH, \quad 1 \leq i \leq n,$$

é uma permutação de S porque $xx_iH \in S$ e $xx_iH \neq xx_jH$ se $i \neq j$. Além disso, é imediado que $\pi_x\pi_y = \pi_{xy}$, para $x, y \in G$. Desse modo, a função π_H que leva x em π_x é um homomorfismo de G no grupo simétrico S_n do conjunto S. O núcleo K de π_H é o conjunto dos $x \in G$ fixando cada x_iH. Equivalentemente, $x \in K$ se e somente se $x \in H^{x_i}$ para todo i. Assim,

$$K = \bigcap_{i=1}^{n} H^{x_i}.$$

Temos, assim, que G/K é isomorfo a um grupo de permutações de S. Também temos que G/K age transitivamente em S, porque, se x_iH, x_jH são duas classes laterais distintas de H em G, tomando $x = x_jx_i^{-1}$ temos que $xx_iH = x_jH$, de forma que π_x leva x_iH em x_jH. Podemos assumir que $x_1 = 1$. Verifica-se imediatamente que $\pi_H(H)$ é o subgrupo fixando a letra x_1H, e de maneira geral temos que $\pi_H(H^{x_i})$ é o subgrupo fixando x_iH.

Chamaremos π_H de *representação de permutações* de G nas classes laterais à esquerda de H. Claramente, π_H é determinada inteiramente por H e é independente da escolha dos representantes das classes laterais de H em G.

De uma maneira mais geral, qualquer homomorfismo de G no grupo simétrico de um conjunto S é chamado de representação de permutações de G em S. O inteiro $|S|$ é chamado de *grau* de π. Dizemos que π é (duplamente) transitiva se $\pi(G)$ age de maneira (duplamente) transitiva em S. Se θ é uma função injetora mapeando o conjunto S no conjunto S', então claramente a composição $\pi' = \theta^{-1}\pi\theta$ dá uma representação de G em S'. Também é claro que a ação de $\pi'(G)$ em S' é definida pela ação de $\pi(G)$ em S, juntamente com a ação de θ. Sob essas condições, diremos que as representações π e π' são representações equivalentes ou isomorfas de G.

Temos o seguinte resultado básico, porém importante:

Lema 1. *Toda representação de permutações transitiva de G é equivalente a uma nas classes laterais à esquerda de um subgrupo de G.*

Demonstração. Seja π uma representação de permutações transitiva de G num conjunto S, onde podemos identificar S com $\{1, \cdots, n\}$. Como acima, vamos denotar a imagem do elemento x de G por π por π_x. Seja H o subgrupo de G que fixa o elemento 1. Vamos argumentar que π e π_H são equivalentes.

Como π é transitiva, existe um elemento x_i em G tal que $\pi_{x_i}(1) = i$. Desse modo, como π é um homomorfismo, então $\pi_{x_i h}(1) = i$ para todo $h \in H$. Reciprocamente, se $\pi_x(1) = i$, então $\pi_{x_i^{-1}x} = 1$, o que garante que $x_i^{-1}x \in H$ e que $x \in x_i H$. Dessa forma, $x_i H$ é o conjunto de todos os elementos de G que levam 1 em i. Em particular, $x_i H \neq x_j H$ e $x_i H \cap x_j H = \emptyset$ se $i \neq j$. Por fim, como um elemento x de G transforma 1 em i para algum i, cada elemento de G pertence a uma das classes $x_i H$, $1 \leq i \leq n$. Dessa forma, o conjunto $S' = \{x_i H \,|\, 1 \leq i \leq n\}$ é um conjunto completo de classes laterais de G módulo H.

Agora defina $\theta : S \to S'$ por $\theta(i) = x_i H$, para todo i, e $\pi' = \theta^{-1}\pi\theta$. Perceba que θ é claramente injetora, o que garante que π' é uma representação de permutações de G em S' que é equivalente a π. Por fim, sejam $x \in G$ e $i \in S$, e suponha que $x x_i H = x_j H$. Nesse caso temos que $\pi_{x x_i}(1) = j$ e que $\pi_x(i) = j$, ou seja, que $\pi_x(\theta^{-1}(x_i H)) = j$. Aplicando θ a essa igualdade obtemos $\theta\pi_x\theta^{-1}(x_i H) = \pi'_x(x_i H) = \theta(j) = x_j H = x x_i H$. Nessas igualdades, olhando apenas para $\pi'_x(x_i H) = x x_i H$, percebe-se que de fato $\pi' = \pi_H$ e o resultado está provado. □

O caso em que $H = 1$ é de particular importância. Nesse caso, certamente o núcleo de π_H é 1 e $\rho = \pi_H$ é um isomorfismo de G em um subgrupo do grupo simétrico de grau $|G|$, que é precisamente o conteúdo do Teorema de Cayley. Nos referiremos a essa representação como a representação *regular* (à esquerda) de G. A seguinte propriedade da representação regular segue direto da definição:

Lema 2. *Na representação regular de G apenas a identidade tem pontos fixos.*

Agora, iremos encarar ρ de uma maneira um pouco diferente. Seja $|G| = n$. É fácil ver que, na representação regular de G, cada elemento de $G^{\#}$ induz uma permutação livre de ponto fixo em G, de modo que, ordenando os elementos do

grupo, uma maneira natural de encarar ρ é associando cada elemento g de G à matriz de permutação $n \times n$ que representa a mesma permutação que g induz no grupo. Isso nos fornece uma representação $\rho : G \to M_n(\mathbb{R})$ onde as imagens dos elementos de G são matrizes de permutação com a seguinte propriedade:

Proposição 4. *Se ρ é a representação regular de G, então vale que*

$$tr(\rho(y)) = \begin{cases} 0, & \text{se } y \in G^{\#} \\ |G|, & \text{se } y = 1. \end{cases}$$

Demonstração. Basta observar que a presença de uma entrada 1 na i-ésima posição da diagonal principal de $\rho(g)$ significa que g fixa o i-ésimo elemento de G, segundo a ordenação que demos aos elementos do grupo anteriormente. Ora, veja que, se $x \neq 1$, $gx = x$ implica claramente que $g = 1$. Isso garante que os elementos de $G^{\#}$ não fixam nenhum elemento de G, enquanto $1 \in G$ claramente fixa todos. □

Agora que esses fatos foram estabelecidos, já é possível provar o Teorema 1, mesmo sem demonstrar o resultado principal do texto. Lembramos aqui que um grupo G é dito de Fröbenius se, em sua representação permutacional, existe um subgrupo H chamado complemento de Fröbenius que fixa um elemento e apenas a identidade em G fixa mais de um elemento nessa ação.

Teorema 1. *Seja G um grupo de Fröbenius com núcleo K e complemento H. Então:*

(i) $G = HK$*, com* $H \cap K = 1$*, de forma que G é o produto semidireto de K por H.*

(ii) $|H|$ *divide* $|K|$*-1.*

(iii) Todo elemento de $H^{\#}$ induz por conjugação um automorfismo livre de ponto fixo sobre K.

(iv) $C_G(y) \leq K$, $\forall y \in K^{\#}$.

Demonstração. Para (i), note que como os elementos de H fixam exatamente um elemento e os de $K^{\#}$ não fixam nenhum, segue direto que $H \cap K = 1$. Como $|K| = [G : H]$, $|HK| = |G|$. Sendo $K \triangleleft G$, $HK \leq G$ e deve-se ter $HK = G$. Por fim, pela normalidade de K em G, deve-se ter $G = H \ltimes K$.

Assumindo a validade do Teorema de Fröbenius, temos que $K \triangleleft G$ e que conjugação por um elemento $h \in H$ induz um automorfismo bem definido de K. Como G é transitivo e H é o subgrupo fixando uma letra, a representação de permutações de G é equivalente àquela nas classes laterais de H, pelo Teorema 3.1. No nosso caso, podemos tomar os elementos de K como representantes das classes laterais módulo H. Agora, supondo que $k^h = k$ para algum $k \in K^{\#}$, segue que o elemento $h \in H$ fixa H e kH, e como em G apenas a identidade fixa mais de uma letra, segue que $h = 1$. Note que isso garante que os elementos de $H^{\#}$ agem livres de ponto fixo sobre K. Isso prova (iii).

Para (ii), seja $A_k = \{k^h \,|\, h \in H\}$. Claramente, $|A_k| = |H|$. Suponha que $A_k \cap A_{k^*} \neq 1$ para algum par $k, k^* \in K$. Então, tomando $k' \in A_k \cap A_{k^*}$, temos

$$k' = k^h = (k^*)^{h^*} \Rightarrow k^{h(h^*)^{-1}} = k^*.$$

Fazendo $g = h(h^*)^{-1}$, tem-se $k^g = k^*$, de forma que $(k^*)^h = (k^g)^h = k^{gh}$. Quando h varia em H, gh varia em H, dando $A_k = A_{k^*}$. Segue disso que os conjuntos A_k particionam $K^\#$, de forma que $|H|$ divide $|K| - 1$.

□

Uma consequência disso é que o centro de um grupo de Fröbenius é sempre trivial:

Corolário 1. *Todo grupo de Fröbenius G tem centro trivial.*

Demonstração. De fato, como $C_G(y) \leq K, \forall y \in K$, deve-se ter $Z(G) \leq K$, visto que $Z(G) \leq C_G(y)$ para todo $y \in G$. Desse modo, suponha que exista $g \in Z(G)$ com $g \neq 1$ e note que, dado $h \in H$, teríamos $gh = hg \Rightarrow g^h = g$, contradizendo o ponto (iii) acima. □

Por fim, temos ainda uma segunda forma de caracterizar os grupos de Fröbenius, como segue

Teorema 2. *Seja H um subgrupo não trivial de G. Então G é um grupo de Fröbenius com complemento H se e somente se H é disjunto de seus conjugados e é o seu próprio normalizador em G.*

Demonstração. Seja x_iH, $x_1 = 1$, $i = 1, \cdots, n$ um conjunto completo de representantes de classes laterais de H em G. Se algum elemento de G fixa duas tais classes, então pela transitividade algum elemento de $H^\#$ fixa uma das classes x_iH com $i > 1$:

$$\begin{aligned} gx_iH = x_iH \text{ e } gx_jH = x_jH &\Rightarrow g \in H^{x_i^{-1}} \cap H^{x_j^{-1}} \\ &\Rightarrow x_i^{-1}hx_i = x_j^{-1}hx_j,\ h \in H \\ &\Rightarrow h = h^{x_jx_i^{-1}} \\ &\Rightarrow H \cap H^{x_k^{-1}} \neq 1, \end{aligned}$$

o que garante que algum elemento de H fixa x_kH, onde $x_k = x_ix_j^{-1}$.

Segue daí que G é um grupo de Fröbenius com complemento H se e somente se nenhum elemento de $H^\#$ fixa nenhum x_iH, com $i > 1$. Porém, para $h \in H^\#$, $x_iH = hx_iH$ se e somente se $h^{x_i^{-1}} \in H$ ou, equivalentemente, se $h \in H \cap H^{x_i}$. Dessa forma, G e H têm as propriedades em questão se e só se $H \cap H^{x_i} = 1\,(*)$, para $2 \leq i \leq n$.

Agora assuma que $(*)$ vale. Se H é subgrupo próprio de $N_G(H)$, pode-se tomar $x \in N_G(H)\backslash H$ e ter $H \cap H^x = H$, uma contradição, de forma que $H = N_G(H)$. Além disso, se $x \in G\backslash H$, então $x \in x_iH$ para algum $i > 1$, de forma que $H \cap H^x = H \cap H^{x_i} = 1$. Reciprocamente, se $N_G(H) = H$ e H é disjunto de seus conjugados, então $H \cap H^x = 1$ para todo x em $G\backslash H$, de forma que $(*)$ vale. □

3.2 Propriedades Básicas

Se π é uma representação de permutações de G num conjunto S, podemos enxergar os elementos de S como a base de um espaço vetorial V sobre um corpo arbitrário F e então considerar os elementos de $\pi(G)$ como transformações lineares de V representados com respeito à base dada pelas matrizes de permutação apropriadas. Dessa forma, π induz um homomorfismo de G no grupo das transformações lineares não-singulares de V/F ou, equivalentemente, das matrizes não-singulares com coeficientes em F, uma variação da interpretação da ação de G em S que vimos anteriormente.

Se V é um espaço vetorial de dimensão n sobre um corpo F, denotaremos por $GL(V, F)$ o grupo das transformações lineares não-singulares em V e por $GL(n, F)$ o grupo de todas as matrizes $n \times n$ com coeficientes em F. Como sempre, para cada base $\{v_1, \cdots, v_n\}$ de V/F, associamos a cada $T \in GL(V/F)$ a matriz $T_{(v)}$ de T com respeito à base dada. Então a função $\alpha_{(v)} \colon T \to T_{(v)}$ é um isomorfismo de $GL(V, F)$ em $GL(n, F)$.

Um homomorfismo de um grupo G no grupo $GL(V, F)$ das transformações não-singulares de V/F é chamado de uma *representação* de G. V é chamado de *espaço de representação* ou *módulo de representação*, conforme V seja um espaço vetorial ou apenas um módulo, e, nesse último caso, F seria um anel. Também podemos dizer que ϕ é *representado* em V/F ou que ϕ é uma representação de V *sobre* F. O núcleo K de ϕ é chamado *núcleo* da representação. Se ϕ é injetora, de modo que G é mapeado de maneira isomorfa em $GL(V, F)$ e $K = 1$, dizemos que ϕ é uma representação *fiel*. No outro extremo, dizemos que ϕ é *trivial* se $K = G$, e nesse caso $\phi(G)$ consiste apenas na transformação identidade em V. Em geral, a dimensão de G sobre F, $dim_F V$, é chamada de *grau* de ϕ. Representações de grau 1 são chamadas *lineares*. Aqui, vamos nos restringir apenas a representações de dimensão finita.

A representação ϕ acima induz de maneira natural uma representação ϕ^* de G/K em $GL(V, F)$ que é fiel. Dessa forma, toda representação de G induz uma representação fiel de G módulo $ker(\phi)$ no mesmo espaço.

Agora, a imagem $\phi(G)$ de G sob ϕ é um grupo de transformações lineares de V, de forma que temos as seguintes relações básicas:

$$\phi(xy) = \phi(x)\phi(y), \quad \forall x, y \in G,$$

$$(\phi(x))(av + a'v') = a(\phi(x))(v) + a'(\phi(x))(v'), \quad , \forall a, a' \in F, v, v' \in V.$$

Escolhendo uma base fixa (v) de V/F, a função composta $\alpha_{(v)}\phi$ é um homomorfismo de G em $GL(n, F)$ chamada de representação *matricial* de G em $GL(n, F)$. Para $x \in G$ escreveremos $\phi(x)_{(v)}$ no lugar de $\alpha_{(v)}\phi(x)$, por brevidade.

Se W é um subespaço de V que é invariante sob $\phi(G)$, então ϕ induz um homomorfismo por restrição de G em $GL(W, F)$, que será chamado obviamente de *restrição* de ϕ a W e representado por $\phi|_W$. Uma tal representação também é dita uma *subrepresentação* de ϕ.

Existem dois tipos muito importantes de representações: as *irredutíveis* e as *indecomponíveis*. Uma representação ϕ de G em V/F é dita *irredutível* se

os únicos subespaços $\phi(G)$-invariantes de V são 0 e V. No caso em que isso não ocorre, diremos que ϕ é *redutível*. Diremos que ϕ é indecomponível se não for possível escrever V como a soma direta de dois subespaços de V não-triviais e $\phi(G)$-invariantes. No caso contrário, diremos que ϕ é *decomponível*. Claramente irredutibilidade implica indecomponibilidade, mas a recíproca não necessariamente é verdade. De fato, mais tarde veremos uma condição para uma representação decomponível ser irredutível. Essa questão é intimamente relacionada a outra definição, a de *redutibilidade completa*. Diremos que uma representação ϕ de G em V/F é *completamente redutível* dado que $V = V_1 \oplus \cdots \oplus V_r$, onde V_i é um subespaço não-zero $\phi(G)$-invariante de V e $\phi|_{V_i}$ é irredutível, para todo i.

Já vimos na seção anterior a utilidade do conceito de representações de permutações equivalentes, que permitia enxergar um problema que envolvia uma representação como um problema que envolvia apenas classes laterais módulo algum subgrupo de G. Essa noção tem uma extensão natural para representações em geral, que é igualmente importante e que descreveremos agora. Seja ϕ uma representação de G em V/F e sejam (v) e (v') duas bases de V/F. Então, para $x \in G$, temos

$$(\phi(x))_{(v')} = P^{-1}(\phi(x)_{(v)})P,$$

onde P denota a matriz de mudança de base de (v) para (v'). Assim, uma representação qualquer ϕ de G determina uma quantidade de representações matriciais de G que nós consideraremos equivalentes.

Uma situação similar acontece se ϕ, ϕ' são representações de G nos espaços V, V' sobre F, respectivamente, de mesma dimensão n, com $(v), (v')$ bases de V, V', e tais que P a matriz de um isomorfismo ϕ que mapeia os elementos de (v) nos elementos correspondentes de (v'), de forma que, para cada $x \in G$, temos

$$(\phi'(x))_{(v')} = P^{-1}(\phi(x))_{(v)}P.$$

Novamente, consideraremos que ϕ e ϕ' são representações equivalentes.

Expressa em termos de transformações lineares, a condição acima pode ser lida como $\phi(x) = \psi^{-1}\phi\psi(x)$, onde ψ é um isomorfismo linear entre V e V'. Dessa forma, diremos que duas representações são *isomorfas* ou *equivalentes* se seus espaços de representação forem isomorfos. Por fim, segue de tudo isso que a relação "ser equivalente a " entre representações é de fato uma relação de equivalência na categoria de todas as representações de um grupo G em espaços vetoriais sobre um corpo F.

3.3 Redutibilidade Completa

Vamos estabelecer agora um critério suficiente para uma representação ser completamente redutível.

Teorema 3. ***(Maschke)*** *Seja ϕ uma representação de G em V/F e assuma que F é de característica 0 ou coprima a $|G|$. Então ϕ é completamente redutível.*

Demonstração. Perceba que, tanto no caso de F ter característica zero quando no caso de característica prima, $\frac{1}{|G|}$ é um elemento bem definido de F, visto que ou F tem característica zero ou coprima a $|G|$. Seja W um G-submódulo de V, e seja U um complemento para W em V. Note que tal complemento existe, basta completar uma base de W para uma base de V; o que não sabemos é se W é G-invariante. Defina $\theta : V \to W$ como sendo a projeção canônica de V sobre W. Agora definiremos $\psi : V \to V$ dada por

$$\psi(v) = \frac{1}{|G|} \sum_{x \in G} x^{-1}(\theta(xv)).$$

Antes de mais nada, perceba que ψ, da maneira como foi definida, é um G-homomorfismo. Que ψ é linear com relação à adição segue direto do fato de θ também o ser, de modo que iremos mostrar apenas que $\psi(gv) = g\phi(v)$. De fato, veja que

$$\begin{aligned}
\psi(gv) =& \frac{1}{|G|} \sum_{x \in G} x^{-1}(\theta(xgv)) \\
=& \frac{1}{|G|} \sum_{x \in G} gg^{-1}x^{-1}(\theta(xgv)) \\
=& \frac{1}{|G|} \sum_{x \in G} g(xg)^{-1}(\theta(xgv)) \\
=& \frac{1}{|G|} \sum_{x \in G} gx^{-1}(\theta(xgv)), \quad \text{pois } xg \text{ percorre } G \text{ quando } x \text{ o faz,} \\
=& g\psi(v).
\end{aligned}$$

Agora, note que se $v \in W$, então $\theta(v) = v$. Isso garante que $\psi(v) = v$. Perceba, ainda, que como ψ depende da projeção θ sobre W, temos que $Im(\psi) \subseteq W$. O fato de que, restrita a W, ψ age como a identidade garante, por fim, que $Im(\psi) = W$. O que provaremos a seguir é que, sendo $K = ker(\psi)$ um G-submódulo de V, teremos $V = W \oplus K$. De fato, tome $v \in W \cap K$. Sendo v um vetor de W, segue por um lado que $\psi(v) = v$, e sendo v um elemento do núcleo também segue que $\psi(v) = 0$, provando que $W \cap K = \{0\}$. Agora, veja que como $\psi(v) \in W$ para todo $v \in V$, e como ψ age como a identidade em W, segue que $\psi(\psi(v)) = \psi(v)$. Sendo assim, dado um $v \in V$ qualquer, defina $u = v - \psi(v)$. Veja que $\psi(u) = \psi(v - \psi(v)) = \psi(v) - \psi(\psi(v)) = 0$, o que garante que $u \in K$ e que $v = \psi(v) + u \in W + K$. Tudo isso nos garante que $V = W \oplus K$, como queríamos demonstrar. □

3.4 Representações Irredutíveis

Ao estudar objetos algébricos, com frequência surge o problema de decompô-los em estruturas mais simples que funcionam como "blocos" para a construção desses objetos. Com representações de grupos finitos não é diferente, de forma

que o objetivo dessa seção é estudar as possíveis representações irredutíveis de um grupo finito G.

Uma conjunto que tenha simultaneamente estrutura de anel e espaço vetorial sobre um corpo $\mathbb{F}$ é chamado de *álgebra* sobre $\mathbb{F}$. Considere, então, um grupo finito $(G, *)$, uma ordenação de seus elementos dada por $B = \{g_1, \cdots, g_{|G|}\}$ e considere o seguinte conjunto:

$$\mathbb{C}[G] = \{\sum a_i g_i \, : \, a_i \in \mathbb{C}, \, g_i \in G\},$$

o conjunto de todas as somas formais de elementos do grupo com coeficientes complexos. Perceba que $\mathbb{C}[G]$ tem estrutura de $\mathbb{C}$ espaço vetorial, com base ordenada B e, além disso, é possível definir a partir da operação do grupo uma operação de multiplicação, distributiva em relação à adição do espaço vetorial, dada por $g \cdot h \coloneqq g * h$. Dessa maneira, $\mathbb{C}[G]$ tem uma estrutura de álgebra e será chamada de *álgebra grupo* do grupo G.

A noção de álgebra grupo será muito útil no estudo das representações de um grupo G visto que, dada uma representação ϕ de G é possível estendê-la por linearidade para uma representação de $\mathbb{C}[G]$ e reciprocamente, dada uma representação θ de $\mathbb{C}[G]$ é sempre possível obter uma representação de G por restrição de θ aos elementos da base de $\mathbb{C}[G]$. Além disso, uma representação de G é irredutível se e somente se a representação correspondente de $\mathbb{C}[G]$ o é. Nosso objetivo com a presente seção é o de, dado um grupo finito qualquer, determinar exatamente quais são todas as suas possíveis representações irredutíveis, a menos de isomorfismos. As álgebras aqui citadas serão sempre de dimensão finita sobre o corpo base. Alguns resultados irão precisar de álgebras unitárias, que nada mais são do que álgebras com elemento neutro multiplicativo.

Antes de começarmos de fato daremos algumas definições. A *álgebra dos endomorfismos de* V é dada por $End_A(V) = E_A(V) = \{f \, : \, V \to V \, : \, f$ é homomorfismo de A-módulos$\}$, e é obviamente o conjunto de todos os endomorfismos de V, com multiplicação dada por composição de funções. Diremos que uma álgebra A é *semi-simples* quando o A-módulo regular A°, que nada mais é do A agindo sobre si mesma por multiplicação à direita, for completamente redutível. Uma álgebra será dita simples quando seus únicos ideais forem os triviais.

Lema 3. ***(Schur (1))*** *Sejam V, W A-módulos irredutíveis e seja $f : V \to W$ um homomorfismo de A-módulos. Se $f \neq 0$, então f é um isomorfismo.*

Demonstração. O que precisamos para provar esse resultado é apenas usar o fato de que $ker(f)$ e $im(f)$ são A-módulos. As propriedades que fazem de $ker(f)$ e $im(f)$ são imediatamente verificadas, à exceção da ação de A sobre tais estruturas ser uma operação fechada. Para ver isso, tome $c \in A$ e $v \in ker(f)$ primeiramente, e veja que $f(cv) = f(v)c = 0$, visto que f é um A-homomorfismo. Agora, tome $w \in im(f)$ e note que $w = f(v)$ para algum $v \in V$ apropriado. Assim, temos que $wc = f(v)c = f(vc) \in im(f)$, como queríamos. Agora, sendo $f \neq 0$, temos que $ker(f) < V$ é um submódulo próprio de V, forçando $f = \{0\}$. O mesmo argumento garante que $im(f) \neq \{0\}$ e força $im(f) = W$, completando a prova. □

Lema 4. ***(Schur (2))*** *Seja $f : V \to V$ um A-endomorfismo do A-módulo irredutível V, sendo A uma álgebra sobre um corpo algebricamente fechado F. Nesse caso, temos $End_A(V) \cong F$, isomorfismo de corpos.*

Demonstração. Perceba que o enunciado do lema em questão equivale a dizer que todo A-endomorfismo de V é na verdade uma transformação escalar. A prova é como segue: tome $c \in F$ um autovalor de f em F. É possível obter tal autovalor pelo fato de que F é algebricamente fechado. Seja, então, $v \in V$ um autovetor correspondente ao autovalor c. Temos que $f(v) = cv$. Considere agora o A-endomorfismo θ dado por $\theta(v) = f(v) - cv$. Sendo V irredutível, temos que ou θ é zero ou um isomorfismo, de acordo com o lema 3 acima. Nesse caso, como $0 \neq v \in ker(\theta)$, deve-se ter $\theta = 0$, o que garante que $\theta(w) = 0$ para todo $w \in V$, ou seja, que $f(w) - cw = 0$, que é equivalente a dizer que $f(w) = cw$ e que f é de fato uma transformação escalar. No caso da transformação nula n, que mapeia V em $0 \in V$, ela é tal que $n(v) = 0 \cdot v$. Isso tudo mostra que é possível mapear $End_A(V)$ em F por uma aplicação $\phi : End_A(V) \to F$ de forma que se $f \in End_A(V)$ é tal que $f(v) = cv$ para todo $v \in V$, então $\phi(f) = c$. Tal função é sobrejetora, visto que para cada escalar $c \in F$ a transformação $g(v) = cv$ é um A-endomorfismo de V, e é injetora porque se $\phi(f) = \phi(g) = c$, então $f(v) = g(v) = cv$ e f e g coincidem. Que $End_A(V)$ é um corpo tem verificação imediata: todo elemento não-nulo de $End_A(V)$ tem inverso, pelo lema acima, e a multiplicação, dada por composição de funções, é comutativa pois todo endomorfismo de V é uma transformação escalar. Que ϕ é homomorfismo verifica-se diretamente. □

Seja V um A-módulo completamente redutível e seja M um A-módulo irredutível. A parte M-homogênea de V, indicada com $M(V)$, é a soma de todos os submódulos de V que são isomorfos a M. Observe que $M \cong N$ implica $M(V) = N(V)$.

Lema 5. *Seja $V = \oplus_i W_i$ uma soma direta de A-módulos com W_i irredutível para todo i. Seja M um A-módulo irredutível. Então teremos*

(i) *$M(V)$ é um $E_A(V)$-submódulo de V;*

(ii) *$M(V) = \sum_i \{W_i : W_i \cong M\}$;*

(iii) *O número $n_M(V)$ de W_i que são isomorfos a M é um invariante de V, não depende da decomposição $\oplus_i W_i$;*

(iv) *Se N é um A-módulo irredutível não isomorfo a M, então $M(V) \cap N(V) = \{0\}$.*

Demonstração. (i). Precisamos mostrar que se $\theta \in E_A(V)$, então $M(V)\theta \subseteq M(V)$, e para isso basta mostrar que se $M \cong W \leq V$ então $W\theta \subseteq M(V)$. Se $W\theta = \{0\}$ o resultado segue direto, de onde podemos assumir que $W\theta \neq \{0\}$. Nesse caso, sendo W irredutível, o Lema de Schur (1) garante que θ é um isomorfismo, ou seja, que $W\theta \cong W \subseteq M(V)$.

(ii). A inclusão $\supseteq$ é clara. Mostraremos agora a inclusão $\subseteq$. Seja $M \cong W \leq V$, queremos mostrar que $W \subseteq \sum_M = \sum\{W_i \;\; W_i \cong M\}$. Seja $\pi_j : V \to V$ a projeção canônica na componente W_j de $\sum_M$; lembre-se de que π_j é um A-endomorfismo com imagem W_j. Se $\pi_j(W) \neq \{0\}$, então $\pi_j(W) = W_j$, pela irredutibilidade de W_j, e $ker(\pi_j) = \{0\}$, sendo W irredutível. Isso garante $W \cong W_j$, e isso mostra que $\pi_j(W) \subseteq \sum_M$ para todo j. Por outro lado, $W \subseteq \sum_j \pi_j(W)$, sendo todo elemento de W soma de projeções de W nos W_j. Isso garante que $W \subseteq \sum_M$.

(iii). Pelo ponto (2) temos

$$dim(M(V)) = n_M(V)dim(M),$$

logo $n_M(V)$ não depende da decomposição $\oplus_i W_i$.

(iv). É imediato do ponto (2). □

Lema 6. *Seja A uma F-álgebra com unidade. Todo A-módulo irredutível é isomorfo a um quociente de A°. Se A é semi-simples, então todo A-módulo irredutível é isomorfo a um submódulo de A°.*

Demonstração. Seja V um A-módulo irredutível e seja $0 \neq v \in V$. Seja $\theta : A^\circ \to V$ dado por $\theta(x) : vx$. É fácil ver que θ é um homomorfismo de A-módulos. Como A possui unidade, $1 \cdot v = v \in Im(\theta) \subseteq V$, temos $Im(\theta) = V$ sendo V irredutível. Seja $W = ker(\theta)$. Pelo teorema de isomorfismo temos $V \cong A^\circ/W$, isomorfismo de A-módulos. Se A é semi-simples, então W admite um complemento U em A° que é submódulo de A°, daí $A^\circ = W \oplus V$, de forma que $V \cong A^\circ/W \cong U$. □

Perceba que esse resultado revela qual é a estrutura de A° quando A é semi-simples: o módulo regular de A contém dentro de si, como submódulos, cópias isomorfas de todos os possíveis A-módulos irredutíveis M, de forma que $M(A^\circ) \neq \{0\}$ para todo M A-módulo irredutível. Isso motiva então a criação do seguinte conjunto: seja $\mathcal{M}(A)$ um conjunto de representantes de A-isomorfismos de A-módulos irredutíveis. Usando os lemas 5.2 e 6, temos que se A é uma álgebra semi-simples então temos um isomorfismo de A-módulos

$$A^\circ \cong \oplus_{M \in \mathcal{M}(A^\circ)} M(A^\circ).$$

Escreveremos $M(A)$ no lugar de $M(A^\circ)$ para simplificar a notação. O teorema de Wedderburn, abaixo, implicará que na verdade esse isomorfismo é um isomorfismo de álgebras (ou seja, o isomorfismo vale sem a "bolinha" $\circ$).

A ideia do teorema de Wedderburn é mostrar que toda álgebra semi-simples é uma soma direta de álgebras simples, às quais nós também iremos entender melhor.

Teorema 4. ***(Wedderburn)*** *Seja A uma F-álgebra semi-simples com unidade e seja M um A-módulo irredutível.*

(i) $M(A)$ é um ideal minimal de A;

(ii) *Se W é um A-módulo irredutível, então $W \cdot M(A) = 0$ a menos que $W \cong M$.*

(iii) *Para $x \in A$, seja $x_M : M \to M$ dado por $x_M(m) : mx$ e seja $A_M = \{x_M : x \in A\} \subseteq End_F(V)$. A função $M(A) \to A_M$, que leva x em x_M, é uma bijeção;*

(iv) *$\mathcal{M}(A)$ é um conjunto finito.*

Demonstração. (i). Se $x \in A$, a função $\theta_x : A \to A$ definida por $(y)\theta_x : xy$ é um A-endomorfismo do A-módulo regular A°. Sabendo que $M(A)$ é um $E_A(A^\circ)$-submódulo de A°, temos $xM(A) = M(A)\theta_x \subseteq M(A)$, logo $M(A)$ é ideal à esquerda de A. Sendo $M(A)$ um A-submódulo, segue direto que $M(A)$ é ideal à direita de A também. Mostraremos a minimalidade de $M(A)$ abaixo.

(ii). Se W é um A-submódulo irredutível e $W \ncong M$, então $W(A) \cap M(A) = \{0\}$, como já provamos. Como $W(A)$ e $M(A)$ são ideais de A, segue que $W(A)M(A) \subseteq W(A) \cap M(A) = \{0\}$. Pelo lema 6, A° tem um submódulo $W_0 \cong W$ e $W_0 \subseteq W(A)$, logo $W_0 M(A) = 0$. Como $W \cong W_0$ (isomorfismo de A-módulos), segue que $WM(A) = 0$, pois, se $f : W \to W_0$ é um A-isomorfismo, $x \in M(A)$ e $v \in W_0$ temos $f(v)x = f(vx) = f(0) = 0$).

(iii). Pelo ponto (2), temos $x_W = 0$ se $x \in M(A)$ e $M \ncong W$. Como A é a soma direta dos $M(A)$, onde $M \in \mathcal{M}(A)$, se $y \in A$ então escrevendo $y = \sum_{N \in \mathcal{M}(A)} y(N)$ temos $y_M = \sum_N y(N)_M = x_M$ onde $x = y(N)_M$, pois as componentes $y(N)_M$ de y com N não-isomorfo a M são tais que $y(N)_M = 0$, pelo ponto (2) acima. Logo, a restrição $M(A) \to A_M$ é sobrejetiva. Por outro lado, se $x \in M(A)$ e $x_M = 0$, então $x_W = 0$ para todo $W \cong M$. Com efeito, se $f : M \to W$ é um isomorfismo de A-módulos, e $w \in W$, então para $m \in M$ apropriado temos $x_W(w) = wx = f(m)x = f(mx) = f(0) = 0$. O ponto (2) garante que $x_W = 0$ para todo A-módulo irredutível U, logo $Vx = 0$ para todo A-módulo completamente redutível V, sendo V soma de submódulos irredutíveis. Escolhendo $U = A^\circ$, obtemos que $x = 1x = 0$. Isso mostra que $M(A) \to A_M$, $x \mapsto x_M$, que é homomorfismo de A-módulos, é injetiva.

(i). Agora mostraremos que o ideal $M(A)$ é minimal. Seja $I < M(A)$ um ideal de A contido propriamente em $M(A)$. Mostraremos que $I = 0$. De fato, sabemos que $M(A)$ é uma soma direta de submódulos de A isomorfos a M, e sendo $I < M(A)$ segue que existe algum $M_0 \cong M$ tal que $M_0 \nsubseteq I$. Sendo M_0 irredutível, segue que $M_0 \cap I = \{0\}$, de forma que $M_0 I \subseteq M_0 \cap I = \{0\}$ (pois M_0 é A-submódulo e I é ideal). Agora, pelo mesmo argumento apresentado no parágrafo anterior, segue que se $M \cong M_0$ então $MI = 0$ também, o que garante que, tomando $x \in I$ qualquer temos $x_M = 0$. Sendo a aplicação $x \mapsto x_M$ uma bijeção $M(A) \to A_M$ e $x \in I \subseteq M(A)$, isso garante $x = 0$.

(iv). Já observamos que se tem $M(A) \neq 0$ para todo M irredutível e que $A = \oplus_{M \in \mathcal{M}(A)} M(A)$ tem dimensão finita. Segue que $|\mathcal{M}(A)|$ é finito. □

Corolário 2. *Toda álgebra semi-simples com unidade é isomorfa a uma soma direta de álgebras simples com unidade*

$$A \cong \oplus_{M \in \mathcal{M}(A)} M(A),$$

e com a multiplicação feita por componentes. Se M é um A-módulo irredutível a álgebra $M(A)$ é isomorfa a A_M.

Demonstração. Já temos a decomposição escrita no nível dos A-módulos. Lembrando que se W e M são A-módulos irredutíveis não isomorfos então $W(A)M(A) = 0$, segue, usando a distributividade da multiplicação em A que

$$\left(\sum_{M\in\mathcal{M}(A)} x(M)\right)\left(\sum_{M\in\mathcal{M}(A)} y(M)\right) = \sum_{M\in\mathcal{M}(A)} x(M)y(M),$$

ou seja, a multiplicação em A é feita por componentes. O elemento $1 \in A$ pode ser escrito como uma soma $\sum_{M\in\mathcal{M}(A)} e_M$, onde $e_M \in M(A)$, e se $x \in N(A)$ temos que $x = 1x = \sum_{M\in\mathcal{M}(A)} e_M x = e_N x$, e o mesmo prova que $x = x1 = xe_N$, garantindo que e_N é o elemento neutro da multiplicação de $N(A)$. Isso mostra que $N(A)$ é uma álgebra com unidade.

Para mostrar que $M(A)$ é simples, tomamos I ideal próprio de $M(A)$ e mostramos que $I = \{0\}$, e para isso provaremos que I é, na verdade, um ideal de A, de forma que a minimalidade de $M(A)$ em A completa a prova. Se $x \in A$ e $y \in I$, então escrevendo $x = \sum_{M\in\mathcal{M}(A)} x(M)$ com $x(M) \in M(A)$ temos $xy = x(M)y \in I$, sendo I ideal de $M(A)$. Isso prova que I é ideal de A.

Por fim, seja M um A-módulo irredutível. A_M é uma álgebra dada por $m(cx_M) \coloneqq c\cdot(m)x_M$ para todo $c \in F$, e com multiplicação dada pela composição de funções, sendo $x_M y_M = (xy)_M$. A função $\phi : M(A) \to A_M$, $\phi(x) = x_M$ é claramente um homomorfismo de álgebras, e é bijetiva pelo ponto (3) do teorema de Wedderburn. □

Nosso próximo objetivo é entender a estrutura de $M(A) \cong A_M$. Seja A uma álgebra unitária sobre o corpo F e seja M um A-módulo. Denotaremos aqui simplesmente por $End(M)$ a álgebra dos endomorfismos F-lineares de M para M, para não carregar a notação. Lembre-se que para $x \in A$ temos $x_M : M \to M$ definido por $x_M(m) = mx$ e $A_M = \{x_M : x \in A\}$ é uma subálgebra de $End(M)$, sendo $(xy)_M = x_M y_M$ para $x, y \in A$. Já vimos que a função $x \to x_M$ induz um isomorfismo de álgebras $M(A) \cong A_M$.

Teorema 5. ***(Centralizador Duplo)*** *Sejam A uma F-álgebra unitária semi-simples e M um A-módulo irredutível. Seja $D = E_A(M) = End_A(M) = Hom_A(M, M)$. Então $E_D(M) = A_M$, ou seja,*

$$C_{End(M)}(C_{End(M)}(A_M)) = A_M.$$

Demonstração. Sendo A semi-simples, M é isomorfo a um submódulo de A°, logo podemos supor M submódulo de A°. E, lembrando que A e A° são isomorfos como álgebras, podemos assumir também que M é uma subálgebra de A. Seja $I = M(A)$. Sabemos que I é um ideal de A e que $M \subseteq I$. A inclusão $A_M \subseteq E_D(M)$ é clara, pois se $x_M \in A_M$ e $\phi \in D$, então $x_M(\phi(m)) = \phi(m)x = \phi(mx) = \phi(x_M(m))$, já que todo $\phi \in D$ respeita a ação de A. Mostraremos agora a inclusão $E_D(M) \subseteq A_M$. Seja $\theta \in E_D(M)$, ou seja, $((m)\alpha)\theta = ((m)\theta)\alpha$

para todo $\alpha \in D$. Se $m \in M$, seja $\alpha_m : M \to A$ dada por $(x)\alpha_m = mx$. Como M é ideal direito de A (ou seja, submódulo de A°), segue que $mx \in M$ para todo $x \in M$, e isso implica que $\alpha_m : M \to M$. Se $a \in A$ e $x \in M$, temos

$$(xa)\alpha_m = m(xa) = (mx)a = (x)\alpha_m a,$$

logo $\alpha_m \in E_A(M) = D$. Se $m, n \in M$, então

$$(mn)\theta = (n\alpha_m)\theta = (n\theta)\alpha_m = m(n\theta). \qquad (*)$$

Fixamos $0 \neq n \in M$ e seja e a unidade da álgebra I. Considere AnA o ideal de A gerado pelos elementos da forma anb, com $a, b \in A$ quaisquer. Temos $AnA \subseteq I$ sendo I ideal e $n \in M \subseteq I$, e como AnA é ideal de A e I é ideal minimal, obtemos $I = AnA$, visto que $n = ene \in AnA \neq \{0\}$. Isso garante que existem $a_i, b_i \in A$ tais que $\sum_i a_i n b_i = e \in I$. Se $m \in M$, então

$$m = me = m\sum_i a_i n b_i = \sum_i (ma_i)(nb_i).$$

Agora, sendo M ideal de A, temos que ma_i e nb_i pertencem a M, de forma que, usando $(*)$, temos

$$m\theta = (\sum_i (ma_i)(nb_i))\theta = \sum_i ((ma_i)(nb_i))\theta \sum_i (ma_i)((nb_i)\theta) = m\sum_i a_i((nb_i)\theta).$$

Definindo $u = \sum_i a_i((nb_I)\theta) \in A$, obtemos $\theta = u_M \in A_M$. □

Observe que, pelo Lema de Schur (1), todo elemento não-nulo de $D = End_A(M)$, onde M é um A-módulo irredutível, é um isomorfismo. Isso garante que D é um anel de divisão. O teorema acima garante que $A_M = E_D(M)$ se M é irredutível. Isso, junto com o que já sabíamos, garante que se A é semi-simples, então pode-se escrever

$$A \cong \oplus_{M \in \mathcal{M}(A)} A_M \cong \oplus_{M \in \mathcal{M}(A)} End_D(M),$$

onde cada elemento de $E_D(M)$ pode ser encarado como uma matriz sobre um anel de divisão. O Teorema de Wedderburn é às vezes formulado assim.

Corolário 3. *Seja A uma álgebra semi-simples com unidade sobre um corpo algebricamente fechado F. Seja M um A-módulo irredutível. Seja $\mathcal{M}(A)$ um conjunto de representantes de A-isomorfismo de A-módulos. Valem as seguintes afirmativas:*

(i) $A_M = End(M)$;

(ii) $dim(A_M) = dim(M(A)) = dim(M)^2$;

(iii) $n_M(A^\circ) = dim(M)$;

(iv) $dim(A) = \sum_{M \in \mathcal{M}(A)} dim(M)^2$;

(v) $dim(Z(A)) = |\mathcal{M}(A)|$.

Demonstração. Como F é algebricamente fechado, $D = E_A(M) = F \times 1$ pelo Lema de Schur (2), logo, pelo Teorema do Centralizador Duplo, temos que $A_M = E_D(M) = E_F(M) = End(M)$ e ponto (i) segue. Sendo $M(A) \cong A_M$, isomorfismo de álgebras, provando (ii). $M(A^\circ)$ é soma direta de $n_M(A^\circ)$ cópias de M. Logo, se $d = dim(M)$, temos

$$d^2 = dim(M(A)) = n_M(A^\circ).dim(M) = n_M(A^\circ) \times d,$$

o que mostra que $d = n_M(A^\circ)$ e prova (iii). Sendo $A = \sum_{M \in \mathcal{M}(A)} M(A)$, (iv) segue direto de (ii). Seja $Z^M = Z(M(A))$. Sendo $E_A(M) = C_{End(M)}(A_M)$, temos $Z(A_M) = A_M \cap E_A(M) = A_M \cap F \times 1 = F \times 1$, logo $dim(Z^M) = dim(Z(A_M)) = 1$, daí $dim\left(\sum_M Z^M\right) = |\mathcal{M}(A)|$. Para concluirmos, basta mostrar que $\sum_M Z^M = Z(A)$. Se $z \in Z(A)$, podemos escrever $z = \sum_M z^M$ com $z^M \in M(A)$ para todo M, e usando o fato de que A é soma direta (como álgebra) dos $M(A)$, temos que $zx = xz$ significa $\sum_M z^M x^M = \sum_M x^M z^M$. Isso garante que $z \in Z(A)$ se e somente se $z^M \in Z(M(A))$ para todo $M \in \mathcal{M}(A)$, ou seja, $Z(A) = \sum_{M \in \mathcal{M}(A)} Z(M(A))$. □

Teorema 6. *Se G é um grupo finito, então $dim(Z(C[G]))$ é igual ao número de classes de conjugação de G.*

Demonstração. Dada uma classe de conjugação C de G, defina $\gamma_C : \sum_{x \in C} x \in \mathbb{C}[G]$. Temos que $\gamma_C \in Z(\mathbb{C}[G])$, pois, dado qualquer $g \in G$, lembrando que $C = \{t_i^{-1} c t_i \,|\, i = 1, \cdots, r\}$, com $r = |C|$, vale que

$$\gamma_C g = \sum_{i=1}^{r} xg = \sum_{i=1}^{r} t_i^{-1} c t_i g = g \sum_{i=1}^{r} (t_i g)^{-1} t_i^{-1} c t_i g = g\gamma_C.$$

Agora, basta concluir que os γ_C formam uma base do espaço $Z(\mathbb{C}[G])$. Para concluir a independência linear dos elementos de $Z(\mathbb{C}[G])$, sabendo que $\mathbb{C}[G]$ é um espaço vetorial de dimensão $|G|$, podemos ordenar os elementos do grupo e associar a cada um deles um vetor da base canônica de $\mathbb{C}^{|G|}$, de forma que o i-ésimo elemento de G segundo a ordenação dada a ele seja mapeado no vetor canônico e_i. Como as classes de conjugação de um grupo o particionam, isso garante que cada γ_C é uma soma de vetores distintos da base de $\mathbb{C}[G]$, de forma que γ_C e $\gamma_{C'}$ não possuem a mesma entrada não-nula simultaneamente. Com o produto interno usual em $\mathbb{C}^|G|$, tais vetores γ_C são sempre ortogonais dois a dois. Agora, suponha que $z = \sum_{g \in G} \lambda_g g \in Z(\mathbb{C}[G])$. Se $h \in G$, temos

$$\sum_{g \in G} \lambda_g g = z = h^{-1} z h = \sum_{g \in G} \lambda_g h^{-1} g h = \sum_{g \in G} \lambda_{hgh^{-1}} g,$$

e, sendo a escrita em função dos elementos da base de $\mathbb{C}[G]$ única, comparando coeficientes segue que $\lambda_g = \lambda_{hgh^{-1}}$ para todo $h \in G$. Isso mostra que os coeficientes λ_g são constantes nas classes de conjugação de G e implica que z é combinação linear dos γ_C. □

Perceba que esse resultado nos diz muitas coisa sobre a decomposição da álgebra $\mathbb{C}[G]$. Já sabíamos do Teorema de Maschke que $\mathbb{C}[G]$ é completamente redutível sempre que G é um grupo finito, e sabíamos também que tal álgebra se decompõe em subálgebras simples que são isomorfas a álgebras de matrizes. O que esse novo resultado agrega de interessante é o fato de que agora sabemos que $dim(A) = \sum_{M \in \mathcal{M}(A)} dim(M)^2$. Ou seja, se n_i é o grau da i-ésima representação irredutível de G, vale a igualdade $\sum_{i=1}^{k} n_i^2 = |G|$. Em certos casos, como por exemplo no caso do grupo S_3 de ordem 6, isso assegura que, como S_3 tem três classes de conjugação, escrevendo 6 como soma de três quadrados temos necessariamente $6 = 1^2 + 1^2 + 2^2$, garantindo que S_3 possui uma representação irredutível de grau 2. Em outros casos, como por exemplo no caso do grupo diedral D_4, que possui ordem 8 e 5 classes de conjugação, tal argumento pode ser repetido para concluirmos que D_4 possui quatro representações irredutíveis de grau 1 e uma de grau 2.

Com isso, a pergunta principal dessa seção é respondida: se um G-módulo M é completamente redutível então M possui componentes irredutíveis retiradas de um conjunto com representantes de classe de isomorfismo de G-módulos irredutíveis que possui um número de elementos igual ao número de classe de G. Além disso, a fórmula da soma dos quadrados é muito útil ao determinar precisamente, em alguns casos, as dimensões de tais módulos irredutíveis. Por fim, vale ressaltar que a existência de um G-módulo irredutível N implica a existência de uma representação irredutível de G pois o que acontece de fato na ação de G sobre N é que se mapeia G em $GL(N)$. Isso, junto com as demais informações desse parágrafo, nos mostra um caminho para conhecer as representações irredutíveis de um grupo finito. Para alguns grupos, porém, tal tarefa não é tão simples, e determinar uma representação inteira de G envolve o problema de encontrar uma quantidade grande de entradas numa matriz quadrada, coisa que nem sempre é possível fazer. Além disso, em certos casos, com $|G|$ e o número de classe de G fixos, é possível escrever $|G|$ como soma de quadrados de algumas maneiras distintas, o que dificulta saber os graus das representações irredutíveis de G. Então surgem novas perguntas aqui: é possível, de alguma forma, conhecer pelo menos todos os graus de representações irredutíveis de G? E uma, mais importante, cabe aqui: numa representação de G sobre um G-módulo V, cada elemento do grupo é mapeado numa transformação linear de V, associada a uma matriz quadrada com $dim(V)^2$ entradas. Qual informação a respeito dessas matrizes que é preciso capturar para entender de uma maneira boa as representações irredutíveis de G? Essas duas perguntas são respondidas na próxima seção.

4 Caracteres e o Teorema de Fröbenius

Os caracteres de grupo são uma ferramenta poderosa para o estudo dos grupos finitos. Essa contribuição para a matemática, junto com uma parte importante da teoria de representações, se deve ao trabalho do próprio G. Fröbenius. Este capítulo inclui muitos fatos simples sobre esse ente matemático

que culminam na demonstração do celebrado Teorema de Fröbenius. Em ordem, apresentaremos as definições e primeiras propriedades dos caracteres, derivadas da teoria de representações, para depois introduzirmos as relações de orto-gonalidade e comentarmos sobre a teoria dos caracteres induzidos, com ênfase especial no caso em que o subgrupo do qual se induz o caractere é disjunto de seus conjugados. Por fim, o capítulo termina com uma prova do teorema de Fröbenius.

4.1 Primeiras Propriedades

Sabe-se do corolário 3.5 que um grupo G tem apenas uma quantidade finita de representações irredutíveis inequivalentes, que chamaremos de r e sabemos ser o número de classe de G, pelo teorema 6.

Para qualquer representação ϕ de G sobre $\mathbb{C}$, com espaço de representação $V/\mathbb{C}$, definimos o *caractere* χ de ϕ colocando, para $y \in G$,

$$\chi(y) = tr(\phi(y)).$$

Aqui, $tr(\phi(y))$ denota o traço da transformação linear $\phi(y)$ de V, o que mostra que χ é uma função de G em $\mathbb{C}$. Vamos nos referir a χ como um *caractere* de G.

Nós já tivemos a ocasião de considerar um caractere particular no nosso estudo de representações, quando vimos a representação regular π de um grupo G qualquer. De fato, $\chi(y)$ é precisamente o número de vezes em que o número 1 aparece na diagonal principal de $\pi(y)$, que é o número de elementos fixados pela transformação $\pi(y)$. Em particular, o caractere ρ_0 da representação regular é 0 para $y \in G^{\#}$ e $|G|$ para $y = 1$.

O caractere *principal* ou *trivial* de G é o caractere da representação trivial de G que, por definição, mapeia cada elemento de G em $1 \in \mathbb{C}$. Obviamente o grau dessa representação é 1. A notação padrão para o caractere principal é 1_G.

Como primeiro resultado básico temos a

Proposição 5. *Se G é um grupo, valem as seguintes afirmações*

(i) Representações equivalentes de G sobre F têm o mesmo caractere.

(ii) Se χ é um caractere de G, então o valor de χ é constante em todos os elementos de uma mesma classe de conjugação.

Demonstração. Se ϕ e ψ são representações equivalentes de G, de grau d, então sabe-se que existe uma matriz não-singular $d \times d$ P com entradas em F tal que $\psi(y) = P^{-1}\phi(y)P$ para todo $y \in G$. Desse modo, $\psi(y)$ e $\phi(y)$ são similares e temos, pela proposição 3.1 que $tr(\phi(y)) = tr(\psi(y))$. Conclui-se, assim, que ψ e ϕ têm o mesmo caractere.

Similarmente, se χ denota o caractere da representação matricial ϕ e x e y são conjugados em G, então $y = z^{-1}xz$ para algum $z \in G$, de modo que $\phi(y) = \phi^{-1}(z)\phi(x)\phi(z)$, já que ϕ é um homomorfismo. Então, do mesmo modo como argumentamos antes, sendo $\phi(z)$ uma matriz não singular, segue também que $\chi(x) = \chi(y)$. □

Devido ao segundo ponto desse teorema, diremos que χ é uma *função de classe* em G.

Uma segunda propriedade elementar dos caracteres é a seguinte:

Proposição 6. *Se χ é um caractere de G, então $\chi(y)$ é uma soma de raízes $|G|$-ésimas da unidade para qualquer $y \in G$. Em particular, $\chi(y)$ é um inteiro algébrico.*

Demonstração. Temos, pelo Teorema de Lagrange, que $y^m = 1$, onde $m = |G|$. Dessa forma, se ϕ é uma representação matricial de G com caractere χ, então $\phi(y^m)$ é a identidade de ordem n, I, onde $n = deg\,\phi$. Porém, peloa proposição 1, $\chi(y) = tr(\phi(y))$ é a soma dos autovalores ϵ_i, $1 \leq i \leq n$ de $\phi(y)$. Entretanto, os autovalores de $\phi^j(y)$ são ϵ_i^j, e como os autovalores de $\phi^m(y) = I$ são todos iguais a 1, temos que $\epsilon_i^m = 1$, de forma que cada autovalor de $\phi(y)$ é uma raiz $|G|$-ésima da unidade. Como ϵ_i satisfaz o polinômio mônico $X^m - 1$ com coeficientes inteiros, segue que tal valor é um inteiro algébrico. Como os inteiros algébricos formam um anel, conforme a proposição 2, segue que $\chi(y)$ é, também, um inteiro algébrico. □

Também temos o seguinte resultado básico:

Proposição 7. *Seja χ o caractere de uma representação ϕ de G de grau n e seja $y \in G$. Então*

(i) $|\chi(y)| \leq n$.

(ii) $|\chi(y)| = n$ *se e somente se* $\phi(y)$ *é uma transformação escalar.*

(iii) $\chi(y) = n$ *se e somente se* $\phi(y)$ *for a transformação identidade.*

Demonstração. Já sabemos que $\chi(y) = \sum_{i=1}^{n} \epsilon_n$, onde cada ϵ_i é uma raiz da unidade e também um autovalor de $\phi(y)$. Então

$$|\chi(y)| = \left| \sum_{i=1}^{n} \epsilon_n \right| \leq \sum_{i=1}^{n} |\epsilon_i| = n, \tag{1}$$

provando (i).

Se $\phi(y)$ é uma transformação escalar, todos os seus autovalores são iguais a, digamos, ϵ, raiz $|G|$-ésima da unidade. Dessa forma, $\chi(y) = n\epsilon$ e $|\chi(y)| = n$. Reciprocamente, se $|\chi(y)| = n$, então o número complexo $\chi(y) = \sum_{i=1}^{n} \epsilon_i$ precisa estar sobre o círculo de centro na origem do plano complexo e raio n. Como cada ϵ_i tem comprimento unitário, é claro que isso só é possível caso todos os autovalores de $\phi(y)$ sejam iguais. Então (ii) é reduzida a mostrar que $\phi(y)$ é uma transformação escalar sempre que seus autovalores são todos iguais.

Chamando esse valor comum de ϵ, então o polinômio característico de $\phi(y)$ é $(X - \epsilon)^n$. Por outro lado, $\phi(y)$ também satisfaz o polinômio $X^m - 1$. Como este último tem todas as raízes distintas, segue que o máximo divisor comum entre esses dois polinômios é $X - \epsilon$. Assim, $\phi(y)$ satisfaz o polinômio $X - \epsilon$,

que agora sabemos ser seu polinômio minimal, de forma que $\phi(y)$ de fato é a transformação escalar ϵI.

Finalmente, se $\chi(y) = n$, então em particular temos que $|\chi(y)| = n$ e que $\phi(y) = \epsilon I$ por (ii), de forma que $\chi(y) = n\epsilon$, o que força $\epsilon = 1$ e $\phi(y)$ é de fato a identidade. A recíproca de (iii) segue trivialmente. □

Proposição 8. *Seja χ um caractere de G e tome*

$$H = \{y \in G | \chi(y) = \chi(1)\}.$$

Então H é subgrupo normal de G.

Demonstração. Seja ϕ uma representação de G com caractere χ e grau n. Dessa forma, como $\phi(1)$ é a transformação identidade, segue que $\chi(1) = n$ e os elementos de H são aqueles que têm o caractere associado igual a n. Ora, o terceiro ponto do teorema anterior garante, então que $\phi(y) = I$ para todo $y \in H$, de forma que H corresponde ao núcleo de ϕ e, por isso, é normal em G, visto que ϕ é homomorfismo de grupos. □

Se χ é o caractere de uma representação ϕ de G, então definimos $ker\,\chi = ker\,\phi$ e $deg\,\chi = deg\,\phi$. Então $ker\,\chi = \{y \in G | \chi(y) = \chi(1)\}$, e, além disso, temos que

$$\deg\,\chi = \chi(1). \tag{2}$$

Também chamaremos χ de *irredutível, redutível, fiel* ou *linear* conforme as representações associadas a χ também o sejam. Como representações equivalentes de G têm o mesmo caractere, segue em particular que o número de caracteres irredutíveis distintos de G, k, é menor ou igual ao número de classe de G, r. No final da próxima seção mostraremos que, de fato, $k = r$.

Suponha que para inteiros apropriados m_i e representações ϕ_i de G, $1 \leq i \leq h$, tenhamos

$$\phi = m_1\phi_1 \oplus \cdots \oplus m_h\phi_h, \tag{3}$$

onde $m_i\phi_i$ representa uma soma direta de m_i cópias da representação ϕ_i. Perceba que tal representação ϕ tem uma representação matricial simples: é simplesmente uma matriz com blocos dados pelas ϕ_i, tantas vezes quantas apareçam. Então, se χ_i denotar o caractere de ϕ_i, pode-se escrever

$$\chi = m_1\chi_1 + \cdots + m_h\chi_h.$$

Isso mostra que uma soma direta de representações, irredutíveis ou não, induz um caractere que é dado pela soma dos caracteres dos fatores da soma direta.

Em particular, pelo Teorema de Maschke, qualquer representação de G sobre $\mathbb{C}$ é completamente redutível e pode ser expressa na forma (3) com cada ϕ_i irredutível. Segue disso que todo caractere de G pode ser expresso como combinação linear dos caracteres irredutíveis de G com coeficientes não-negativos inteiros.

Reciprocamente, ressaltamos que para quaisquer representações ϕ_i de G e quaisquer inteiros não-negativos m_i, $1 \leq i \leq h$, sempre pode-se construir uma

representação ϕ da forma (3): de fato, considere uma soma direta V de h espaços vetoriais $V_i/\mathbb{C}$, onde cada V_i é a soma direta de m_i cópias do espaço de representação de ϕ_i, para todo i, e então defina ϕ em V de acordo com a ação de ϕ_i em V_i. Isso significa que qualquer combinação linear de caracteres com coeficientes inteiros não-negativos é, novamente, um caractere de G.

Também existe uma definição natural para o produto de dois caracteres, relacionada ao produto tensorial das representações associadas a eles. De fato, se ϕ_i são representações de G sobre $V_i/\mathbb{C}$, $i = 1, 2$, então a função $\phi_1 \otimes \phi_2$ definida por

$$(\phi_1 \otimes \phi_2)(y) = (\phi_1(y)) \otimes (\phi_2(y))$$

para $y \in G$ é imediatamente verificada como sendo uma representação de G com espaço de representação $V_1 \otimes V_2$. De fato, é claro que essa representação é apenas a restrição da representação produto $\phi_1 \otimes \phi_2$ à diagonal $\{(y, y) : y \in G\}$ de $G \times G$. Além disso, se ϕ_i é uma representação com relação a uma base apropriada de V_i, $i = 1, 2$, então a matriz $\phi_1 \otimes \phi_2(y)$ será o produto tensorial das matrizes $\phi_1(y)$ e $\phi_2(y)$. Dessa forma, pela proposição 3.4, temos que

$$tr(\phi_1(y) \otimes \phi_2(y)) = tr(\phi_1(y))tr(\phi_2(y)) \tag{4}$$

para todo $y \in G$. Então vê-se que o caractere de $\phi_1 \otimes \phi_2$ é o produto dos caracteres de χ_1 de ϕ_1 e χ_2 de ϕ_2, que denotaremos por $\chi_1\chi_2$. Segue direto da equação (4) que $\chi_1\chi_2 = \chi_2\chi_1$.

Devido às propriedades associativas e distributivas dos produtos tensoriais e somas diretas de espaços vetoriais, que são herdadas pelas representações e, portanto, pelos caracteres de G, pode-se mostrar diretamente que essa definição de multiplicação é associativa e distributiva em relação à adição.

É conveniente e útil estender a definição de caractere para permitir coeficientes inteiros negativos nas combinações lineares, para obter uma estrutura de anel para o conjunto de todo os caracteres de G. Para fazer isso, definiremos um *caractere generalizado* de G como sendo a diferença entre quaisquer dois caracteres ordinários de G, e isso nos permite estender as definições de adição e multiplicação aos caracteres generalizados de uma maneira óbvia. O conjunto de todos os caracteres se torna, desse modo, um módulo sobre os inteiros com a adição, enquanto a multiplicação permanece associativa e distributiva. Dessa forma, o conjunto de todos os caracteres generalizados forma um anel comutativo, chamado de *anel de caracteres* de G, que denotaremos por $ch(G)$. Claramente, os caracteres irredutíveis de G formam uma base para $ch(G)$.

Por fim, vamos estender a definição de grau para os caracteres generalizados colocando $deg\chi = deg\chi_1 - deg\chi_2$ se $\chi = \chi_1 - \chi_2$, com χ_1, χ_2 caracteres ordinários de G, e vê-se que (2) também vale para caracteres generalizados, e $deg\chi$ é independente da representação particular de χ como diferença de dois caracteres, visto que tais diferenças devem ter a mesma imagem em todos os elementos do grupo G.

O anel $ch(G)$ é munido de uma involução natural. De fato, se ϕ é qualquer representação matricial de G, definimos a representação *contragradiente* ϕ' de

ϕ pela relação

$$\phi'(y) = ((\phi(y)^{-1})^t, \tag{5}$$

$y \in G$, onde t denota transposição. Como as operações de inversão e transposição de matrizes são anti-isomorfismos do grupo $GL(n, \mathbb{C})$, segue que ϕ' é um homomorfismo e é de fato uma representação de G. Claramente, representações equivalentes originam representações contragradientes equivalentes. Se χ for o caractere de ϕ, então chamaremos de χ' o caractere de ϕ'.

Segue direto de (5) que $(\phi')' = \phi$ e consequentemente $(\chi')' = \chi$, o que mostra que a função $\chi \to \chi'$ é involutória. Além do mais, temos que, para quaisquer caracteres χ_1, χ_2 de G temos que $(\chi_1 + \chi_2)' = \chi_1' + \chi_2'$ e que $(\chi_1\chi_2)' = \chi_1'\chi_2'$, e se estendermos $'$ aos caracteres generalizados e, assim, a $ch(G)$ teremos que a função resultante dessa extensão é um automorfismo de $ch(G)$ de ordem 2. O próximo teorema lista as propriedades básicas dessa função. Aqui, $\overline{\lambda}$ denota o conjugado complexo de λ.

Proposição 9. *Para qualquer caractere χ de G temos*

(i) $\chi'(y) = \overline{\chi(y)} = \chi(y^{-1})$, $\forall y \in G$.

(ii) $deg\,\chi' = deg\,\chi$ *e* $ker\,\chi' = ker\,\chi$.

(iii) χ' *é irredutível se, e somente se,* χ *é irredutível.*

Demonstração. Seja ϕ uma representação com caractere χ. Por (5) e pela proposição 3.5, temos

$$\chi'(y) = tr(\phi'(y)) = tr(\phi(y^{-1}))^t = tr(\phi(y^{-1})) = \chi(y^{-1}). \tag{6}$$

Por outro lado, pela proposição 1, temos que

$$\chi(y) = tr(\phi(y)) = \epsilon_1 + \cdots + \epsilon_n, \tag{7}$$

onde os ϵ_i são raízes da unidade e também são os autovalores de $\phi(y)$, $1 \leq i \leq n$ e $deg\,\phi = n$. Porém, os autovalores de $\phi(y^{-1})$ são ϵ_i^{-1}, $1 \leq i \leq n$ e, como cada ϵ_i tem módulo 1, segue que $\epsilon_i^{-1} = \overline{\epsilon_i}$, de forma que

$$tr(\phi^{-1}(y)) = \overline{\epsilon_1} + \cdots + \overline{\epsilon_n} = \overline{\epsilon_1 + \cdots + \epsilon_n} = \overline{\chi(y)}. \tag{8}$$

Além do mais, como ϕ é um homomorfismo, $\chi(y^{-1}) = tr(\phi(y^{-1})) = tr(\phi^{-1}(y)))$ e (i) segue de (6) e (8).

Segue direto de (5) que $deg\,\phi' = deg\,\phi$, o que garante que $deg\,\chi' = deg\,\chi$. Além do mais, para $y \in G$, $\phi(y)$ é uma transformação escalar se, e somente se, $(\phi(y)^{-1})^t$ o é. Desse modo, χ' e χ têm os mesmos núcleos, provando (ii).

Finalmente, se a matriz $\phi(y)$ pode ser decomposta em blocos que são zero fora da diagonal, $(\phi^{-1}(y))^t)$ também pode. Isso mostra que χ' é irredutível se e só se χ o é, provando (iii). □

O caractere χ' pode ser construído de uma maneira alternativa. Se ϕ é uma representação matricial de G tendo χ' como caractere, pode-se construir uma nova representação $\bar{\phi}$ de G tendo χ como caractere, simplesmente fazendo as entradas de $\bar{\phi}(y)$ serem os conjugados complexos das entradas correspondentes em $\phi(y)$. Como conjugação é um automorfismo de $\mathbb{C}$, é trivial verificar que $\bar{\phi}$ é uma representação de G. Se $\bar{\chi}$ denota o caractere de $\bar{\phi}$, então $\bar{\chi}(y) = \overline{\chi(y)}$ para todo $y \in G$, de forma que $\chi' = \chi$ pela proposição 9.1. Veremos na próxima seção que as representações ϕ' e $\bar{\phi}$, tendo o mesmo caractere, são equivalentes.

4.2 As Relações de Ortogonalidade

Queremos, agora, obter algumas relações importantes entre os caracteres irredutíveis de G e algumas consequências importantes dessas relações. Daqui para a frente, denotaremos por $\{\phi_i\}$ um conjunto completo de representações irredutíveis inequivalentes de G, $1 \leq i \leq n$, com χ_i sendo o caractere de ϕ_i e $\chi_1 = 1_G$ sendo o caractere de ϕ_1, a representação trivial de G. Como já dissemos, tal caractere será chamado de caractere principal de G. Também adotaremos e preservaremos a notação de que $n_i = deg\, \chi_i$.

Vamos introduzir um produto interno hermitiano em $ch(G)$ pela fórmula

$$(\theta, \chi) = \frac{1}{|G|} \sum_{y \in G} \theta(y)\overline{\chi(y)} \tag{1}$$

para $\theta, \chi \in ch(G)$. Vamos provar que $(\ ,\ )$ é de fato um produto interno hermitiano. Note que, dados $\theta_1, \theta_2, \chi \in ch(G)$,

$$\begin{aligned}(\theta_1 + \theta_2, \chi) =& \frac{1}{|G|} \sum_{y \in G} (\theta_1(y) + \theta_2(y))\overline{\chi(y)} \\ =& \frac{1}{|G|} \sum_{y \in G} \theta_1(y)\overline{\chi(y)} + \theta_2(y)\overline{\chi(y)} \\ =& (\theta_1, \chi) + (\theta_2, \chi),\end{aligned}$$

e que

$$\begin{aligned}(\chi, \theta_1 + \theta_2) =& \frac{1}{|G|} \sum_{y \in G} \chi(y)(\overline{\theta_1(y) + \theta_2(y)}) \\ =& \frac{1}{|G|} \sum_{y \in G} \chi(y)(\overline{\theta_1(y)} + \overline{\theta_2(y)}) \\ =& \frac{1}{|G|} \sum_{y \in G} \chi(y)\overline{\theta_1(y)} + \chi(y)\overline{\theta_2(y)} \\ =& \frac{1}{|G|} \sum_{y \in G} \chi(y)\overline{\theta_1(y)} + \frac{1}{|G|} \sum_{y \in G} \chi(y)\overline{\theta_2(y)} \\ =& (\chi, \theta_1) + (\chi, \theta_2).\end{aligned}$$

Agora, os únicos escalares que podemos multiplicar por caracteres são números inteiros. Veja que substituindo χ ou θ em alguma entrada acima, o escalar inteiro sai de fato do produto interno. Por fim, vale ressaltar que sendo tal escalar um número real, a conjugação complexa que aparece sobre o segundo membro do produto interno não o altera. Isso tudo garante que $(\ ,\ )$ é bilinear. Que esse aplicação bilinear é positiva definida segue do fato que, quando calculamos (θ, θ) o somatório se torna um somatório de normas de números complexos $\theta(y)\overline{\theta(y)} = ||\theta(y)||$ e que, por isso, é maior ou igual a zero. Por fim, note que

$$\overline{(\theta, \chi)} = \overline{\frac{1}{|G|}\sum_{y\in G}\theta(y)\overline{\chi(y)}} = \frac{1}{|G|}\sum_{y\in G}\chi(y)\overline{\theta(y)} = (\chi, \theta),$$

e esse produto interno é de fato Hermitiano.

Como de costume, diremos que θ e χ são ortogonais se $(\theta, \chi) = 0$ e definimos a norma do caractere χ como sendo

$$\|\chi\| = \sqrt{(\theta, \theta)}. \tag{2}$$

Antes de começarmos a provar os resultados que queremos, temos a

Proposição 10. *Se $\chi_1, \cdots, \chi_k$ são os caracteres irredutíveis de G, vale que*

(i)
$$\sum_{g\in G}\chi_i(g) = \begin{cases} 0, & \text{se } i = 1, \\ |G|, & \text{se } i \neq 1. \end{cases}$$

(ii)
$$\sum_{i=1}^{k} n_i\chi_i(y) = \begin{cases} 0, & \text{se } y \neq 1, \\ |G|, & \text{se } y = 1. \end{cases}$$

(iii) $\sum_{i=1}^{k} n_i^2 = |G|$

Demonstração. Veja que (iii) segue direto do corolário 3.4. Para (i), tome $u = \sum_{g\in G} g \in \mathbb{C}[G] = A$. Sabemos que $u \in Z(A)$ e que, sendo assim, $\phi_i(u) = \lambda I$ para toda representação irredutível ϕ_i de A e para λ e I apropriados. Perceba que $\chi_i(u) = \sum_{g\in G} tr(\phi_i(g)$, de forma que só precisamos mostrar que $tr(\phi_i(u)) = 0$ ou $|G|$, conforme for o caso. O resultado segue claramente para o caso em que $i = 1$; dessa forma suponha $i \neq 1$. Nessa situação, sendo ϕ_i não-trivial, certamente existe $x \in G$ tal que $\phi_i(x) \neq I$. Para um tal x, temos que $xu = u$. Dessa equação, segue que

$$\phi_i(xu) = \phi_i(u) \Rightarrow \lambda(\phi_i(x) - I) = 0.$$

Como assumimos $\phi_i(x) \neq I$, deve-se ter $\lambda = 0$, provando o resultado. □

A importância fundamental desse produto interno está no fato de que, sob ele, os caracteres irredutíveis são ortonormais, conforme atestam os próximos dois resultados.

Teorema 7. *Os caracteres χ_i de G, $1 \leq i \leq n$, formam uma base ortonormal de $ch(G)$ sobre os inteiros:*

$$(\chi_i, \chi_j) = \begin{cases} 0, & \text{se } i \neq j \\ 1, & \text{se } i = j. \end{cases}$$

Vamos encontrar a prova do teorema acima enquanto estabelecemos a seguinte propriedade adicional de $ch(G)$:

Proposição 11. *Se $\chi_i\chi_j = \sum_{k=1}^{r} m_{ijk}\chi_k$, com m_{ijk} inteiros não-negativos, de forma que m_{ij1} é o número de vezes que o caractere trivial χ_1 aparece como constituinte de $\chi_i\chi_j$, então*

$$m_{ij1} = \begin{cases} 0, & \text{se } i \neq j \\ 1, & \text{se } i = j \end{cases}$$

Demonstração. Seja $V_i/\mathbb{C}$ o espaço de representação de ϕ_i, $1 \leq i \leq r$, de forma que, sem perda de generalidade, podemos assumir

$$\phi_i \otimes \phi_j = \sum_{k=1}^{r} m_{ijk}\phi_k. \tag{3}$$

Suponha que para algum par i, j se tenha $m_{ij1} \neq 0$. Por simplicidade de notação, escreveremos ϕ no lugar de ϕ_i e ψ no lugar de ϕ_j, U no lugar de V_i, V no lugar de V_j e $W = V \otimes_{\mathbb{C}} W$. Note que, como a representação trivial ϕ_1 mapeia todo elemento do grupo que é representado em $1 \in \mathbb{C}$, tal representação leva todos os elementos de G na transformação identidade de V_1, que tem dimensão 1. Dessa forma, considere um r-vetor $w \in W$ onde cada entrada é um vetor do espaço $m_{ijk}V_k$ da forma $w = (v, 0, \cdots, 0)$. Perceba que $v = (v_1, \cdots, v_{m_{ij1}})$ é um vetor de $m_{ij1}V_1$, e cada zero que aparece é, na verdade, um vetor de zeros em cada $m_{ijk}V_k$. Note que w é invariante sob a ação de $\phi \otimes \psi(y)$ para todo $y \in G$. Como cada V_k é irredutível, o operador $m_{ijk}\phi(y)$ é uma matriz em blocos, todos iguais e todos representando uma transformação escalar, conforme o Lema 4. Isso faz com que as entradas que são zeros permaneçam invariantes, e além disso temos que $m_{ij1}\phi_1(y)$ atua como a identidade para todo $y \in G$, preservando cada entrada de v. Dessa forma, podemos afirmar que

$$(\phi \otimes \psi)(y)w = w, \, \forall y \in G. \tag{4}$$

A base do espaço W é dada por tensores da forma $u_i \otimes v_j$, onde os vetores da forma u_i formam uma base de U e os da forma v_j uma base de V, $1 \leq i \leq dim\, U$, $1 \leq j \leq dim\, V$. Assim, pode-se escrever w sob a forma $w = \sum_{i,j} a_{ij}u_i \otimes v_j$. Agora, dado que o produto tensorial é distributivo em relação à soma direta de vetores, ressaltamos que o somatório apresentado anteriormente pode ser escrito como

$$w = \sum_{k=1}^{s} u_k \otimes v_k, \tag{5}$$

onde $u_k \otimes v_k = u_k \otimes \left(\bigoplus_{j=1}^{dim\, V} a_{kj} v_j\right)$. Perceba que $s \leq dim\, U$, que os u_k são todos linearmente independentes em U e que cada v_k é diferente de zero. Seja U_1 o subespaço de U gerado pelos u_k. Por (4) e (5), temos que

$$\sum_{k=1}^{s} (\phi(y))(u_k) \otimes (\psi(y))(v_k) = \sum_{k=1}^{s} u_k \otimes v_k. \tag{6}$$

Como os u_k são linearmente independentes e os v_k são não-nulos, segue de (6) e da definição de produto tensorial que cada $(\phi(y))(u_k) \in U_1$, de forma que U_1 é $\phi(G)$-invariante e precisa ser igual a U pela irredutibilidade de ϕ. Dessa forma, $(u) = \{u_k | 1 \leq k \leq s\}$ é uma base para U. Similarmente, o subespaço gerado pelos v_k é invariante sob ψ, de forma que $V_1 = V$, onde V_1 é o subespaço gerado pelos v_k, pela irredutibilidade de ψ. Isso garante que $dim\, V \leq s = dim\, U$. Entretanto, como o argumento é claramente simétrico em U e V, também segue que $dim\, U \leq dim\, V$. A igualdade vale e, desse modo, $(v) = \{v_k \,|\, 1 \leq k \leq s\}$ é uma base para V.

Agora, para um dado $y \in G$, sejam

$$(\phi(y))_{(u)} = (a_{kh}) \qquad \text{e} \qquad (\psi(y))_{(v)} = (b_{kg}). \tag{7}$$

Então, aplicando essas transformações nos vetores da base de U e V, obtemos

$$(\phi(y))u_k = \sum_{h=1}^{s} a_{kh} u_h \qquad \text{e} \qquad (\psi(y))v_k = \sum_{h=1}^{s} b_{kg} v_h. \tag{8}$$

Substituindo (8) em (6) obtemos as relações

$$\sum_{k=1} a_{kh} b_{kg} = \begin{cases} 0 & \text{se } h \neq g \\ 1 & \text{se } h = g. \end{cases} \tag{9}$$

Porém, a equação (9) garante simplesmente que a matriz $\psi(y)$ é a inversa transposta de $\phi(y)$. Como isso vale para todo $y \in G$ concluímos que $\psi_{(v)} = \phi'_{(u)}$ e segue daí que $\phi' = \psi$.

Até aqui nós já provamos que se $m_{ij1} \neq 0$ então necessariamente $\chi_i = \chi'_j$. Com o auxílio desse resultado, agora podemos argumentar que $(\chi_i, \chi_j) = 0$ se $i \neq j$. De fato, escrevemos

$$\chi_i \chi'_j = \sum_{k=1}^{t} m_{ijk} \chi_k \tag{10}$$

para inteiros não-negativos m_{ijk} apropriados. Como $\chi''_j = \chi_j \neq \chi_i$, segue que deve-se ter $m_{ij1} = 0$. Porém, avaliando (10) para cada $y \in G$ e somando sobre G, temos

$$\sum_{y \in G} \chi_i(y) \chi'_j(y) = \sum_{k=2}^{r} m_{ijk} \left(\sum_{y \in G} \chi_k(y) \right). \tag{11}$$

Porém, sabe-se que $\sum_{y\in G}\chi_k(y)=0$ se $k>1$, pela proposição 10. Como o lado direito dessa equação é 0, segue o resultado desejado: $(\chi_i,\chi_j)=0$ se $i\neq j$.

Um cálculo formal agora nos fornecerá as partes restantes do nosso teorema. Multiplicando a relação da proposição 10(ii) para $y\in G^{\#}$ por $\chi_j'(y)$ e somando sobre $G^{\#}$, teremos

$$0=\sum_{1=1}^{r} n_i \sum_{y\in G^{\#}} \chi_i(y)\chi_j(y). \tag{12}$$

Como $(\chi_i,\chi_j)=0$ se $i\neq j$, e como $\chi_i(1)\chi_j(1)=n_in_j$ para todo i,j, incluindo $i=j$, pode-se reescrever (12) como

$$0=n_j\sum_{y\in G}\chi_j(y)\chi_j'(y)-\sum_{i=1}^{r} n_jn_i^2. \tag{13}$$

Agora, dividindo por n_j e usando a proposição 10(iii), segue que

$$0=\sum_{y\in G}\chi_j(y)\chi_j'(y)-|G| \Rightarrow 1=\frac{1}{|G|}\sum_{y\in G}\chi_j(y)\chi_j'(y), \tag{14}$$

completando a prova do teorema 7.

Suponha, finalmente que $\chi_j=\chi_i'$. Avaliando a relação $\chi_i\chi_j'=\sum_{k=1}^{r} m_{ijk}\chi_k$ para cada $y\in G$ e somando sobre G, temos pela proposição 10(i) que

$$\sum_{y\in G}\chi_i(y)\chi_j(y)=m_{ij1}|G|, \tag{15}$$

o que mostra que $m_{ij1}=(\chi_i,\chi_j)$, de forma que $m_{ij1}=1$ nesse caso e a proposição 11 também está provada. □

As relações de ortogonalidade, junto com a linearidade do produto interno, dão o seguinte corolário:

Corolário 4. *Se $\chi=\sum_{i=1}^{r} a_i\chi_i$, a_i inteiros, então*

(i) $(\chi,\chi_i)=a_i$, $1\leq i\leq r$.

(ii) $\|\chi\|^2=(\chi,\chi)=\sum_{i=1}^{r} a_i^2$.

Em particular, (χ,χ_i) é a multiplicidade de χ_i em χ. Além disso, χ é irredutível se, e somente se $(\chi,\chi)=1$. Essas fórmulas se estendem para caracteres generalizados também.

Como um último corolário, temos ainda o

Corolário 5. *Duas representações de G têm o mesmo caractere se, e somente se, são equivalentes.*

Demonstração. Já vimos que representações equivalentes têm o mesmo caractere. Reciprocamente, sejam ϕ, ψ duas representações de G com o mesmo caractere χ. Sem perda de generalidade, podemos escrever $\phi = \sum_{i=1}^{r} a_i\phi_i$ e $\psi = \sum_{i=1}^{r} b_i\phi_i$, com a_i, b_i inteiros não-negativos, $1 \leq i \leq r$. Dessa forma, teremos que $\chi = \sum_{i=1}^{r} a_i\chi_i = \sum_{i=1}^{r} b_i\chi_i$, de forma que $(\chi, \chi_i) = a_i = b_i$, $1 \leq i \leq r$, pelo teorema anterior. Isso garante que $\phi = \psi$ e o teorema está provado. □

Note que isso garante que a quantidade de caracteres irredutíveis inequivalentes deve ser igual à quantidade de representações inequivalentes, dada pelo número de classe de G.

4.3 Caracteres Induzidos e Conjuntos de Interseção Trivial

As relações entre os caracteres de um grupo G e os de seus subgrupos H são de fundamental importância para o estudo da estrutura de G. Nesta seção nós vamos desenvolver os fatos gerais que dizem respeito a essas relações. Em seguida, vamos nos especializar no caso particular em que o subgrupo em questão é disjunto de seus conjugados, onde resultados consideravelmente mais fortes podem ser obtidos.

Em primeiro lugar, se $H \leq G$, uma representação ϕ de G sobre $\mathbb{C}$ induz de maneira trivial uma representação $\phi|_H$ por restrição de ϕ a H. Se χ é o caractere de ϕ, vamos denotar por $\chi|_H$ o caractere de $\phi|_H$. Por definição, $\chi|_H$ e χ assumem os mesmos valores nos elementos de H. Claramente essa função de restrição é linear e preserva produtos de caracteres. Dessa forma, essa restrição induz um homomorfismo natural de $ch(G)$ em $ch(H)$.

O que não é tão óbvio assim é que cada caractere de H induz também um caractere de G de uma maneira bem menos trivial. Essa relação entre os caracteres de H e os de G depende da noção de *caracteres induzidos*. Seja x_i, $1 \leq i \leq m$ um conjunto completo de representantes de classes laterais de H em G. Seja ψ uma representação matricial de H de grau d. Vamos estender a definição de ψ definindo $\psi(y)$ em todo o grupo G, fazendo $\psi(y)$ ser igual à matriz 0 de ordem $d \times d$ para $y \in G \backslash H$. Agora definimos uma função de G em $M_{md}(\mathbb{C})$, o espaço das matrizes quadradas de ordem md com entradas complexas, pela regra

$$\psi^*(y) = [(x_i y x_j^{-1})] \qquad y \in G. \tag{1}$$

Dessa forma, ψ^* é uma matriz $m \times m$ de blocos cuja (i, j)-ésima entrada é a matriz $d \times d$ $\psi(x_i y x_j^{-1})$. Agora provamos a

Proposição 12. *Seja H um subgrupo de G e ψ uma representação de H. Então a função ψ^* dada em (1) é uma representação de G de grau $[G : H] \cdot deg\, \psi$.*

Demonstração. Tome $x, y \in G$ e considere o produto $\psi^*(x)\psi^*(y)$. O (i, j)-ésimo bloco desse produto é dado por

$$B_{ij}(x, y) = \sum_{k=1}^{m} \psi(x_i x x_k^{-1})\psi(x_k y x_j^{-1}). \tag{2}$$

Agora, para um dado i, existe uma única classe lateral x_tH à qual o elemento x_ix pertence e, assim, tal que $x_ixx_t^{-1} \in H$. Mas então, se $k \neq t$, $\psi(x_ixx_k^{-1})$ é a matriz 0. Dessa forma, (2) se reduz a

$$B_{ij}(x,y) = \psi(x_ixx_t^{-1})\psi(x_tyx_j^{-1}). \tag{3}$$

Por outro lado, $x_ixyx_j^{-1} \in H$ se e somente se $x_ixx_t^{-1} \in (x_jy^{-1}x_t^{-1})H$. Como, no caso em que estamos lidando, $x_ixx_t^{-1} \in H$, então isso acontece se e somente se $x_jy^{-1}x_t^{-1}H = H$, ou seja, se $x_tyx_j^{-1} \in H$. Dessa forma,

$$B_{ij}(x,y) = \begin{cases} 0, & \text{se } x_ixyx_j^{-1} \notin H \\ \psi(x_ixx_t^{-1})\psi(x_tyx_j^{-1}), & \text{se } x_ixyx_j^{-1} \in H. \end{cases} \tag{4}$$

Entretanto, no segundo caso, como ψ é uma representação de H, teremos que $\psi(x_ixx_t^{-1})\psi(x_tyx_j^{-1}) = \psi(x_ixyx_j^{-1})$. Junto com (4) isso nos dá

$$\psi^*(xy) = [B_{ij}(x,y)]. \tag{5}$$

Porém, como $[B_{ij}(x,y)] = \psi^*(x)\psi^*(y)$, fica provado que ψ^* é de fato um homomorfismo.

Finalmente, é imediato que $\psi^*(1)$ é a matriz identidade. Dessa forma, como $\psi^*(x)\psi^*(x^{-1}) = \psi^*(xx^{-1}) = \psi^*(1)$, segue que a imagem desse homomorfismo é composta apenas por matrizes não-singulares, de modo que ψ^* é um homomorfismo de G em $GL(md, \mathbb{C})$ e é de fato um homomorfismo do grau dito no enunciado. □

Como uma ilustração, temos o

Teorema 8. *Seja H um subgrupo de G e seja ψ a representação trivial de H. Então ψ^* é a representação de permutações nas classes laterais à esquerda de H. Em particular, se $H \triangleleft G$, então ψ^* é a representação regular de G/H.*

Demonstração. Com a notação usada acima, temos, para qualquer $y \in G$ e um x_i dado, que $x_iyx_j^{-1} \in H$ se e somente se $x_iy \in x_jH$. Então j é unicamente determinado por y e x_i, e $\psi(x_iyx_k^{-1}) = 1$ ou 0 conforme $k = j$ ou $k \neq j$. Percebemos, assim, que $\psi^*(y)$ é simplesmente a matriz de permutação determinada pela função $x_iH \to yx_iH = x_jH$, provando a primeira afirmação. Se $H \triangleleft G$, a representação de permutações de G nas classes laterais de H tem H em seu núcleo e induz a representação regular em G/H, como queríamos. □

Em geral, vamos nos referir a ψ^* como a representação *induzida* pela representação ψ de H. Se ψ tem o caractere χ, denotaremos o caractere de ψ^* por χ^* e o chamaremos de caractere *induzido* por χ.

Com frequência iremos considerar mais de um subgrupo de G e, às vezes, caracteres induzidos de um subgrupo de G a outro. Nesses casos, χ^* sempre irá denotar o caractere induzido de G por um caractere χ de um subgrupo.

Proposição 13. *Seja H um subgrupo de G e χ um caractere de H. Faça $\chi(y) = 0$ para todo $y \in G \backslash H$. Então temos que*

(i) $\chi^*(y) = \frac{1}{|H|}\sum_{u\in G}\chi(uyu^{-1})$, *para todo* $y \in G$.

(ii) $\chi^*(y) = 0$ *se* y *não pertence a nenhum conjugado de* H.

(iii) Se $ker\,\chi \triangleleft G$, *então* $ker\,\chi \leq ker\chi^*$.

(iv) Representações equivalentes de H *induzem o mesmo caractere em* G.

Demonstração. Seja χ o caractere da representação ϕ de H e use a notação conforme a da proposição 12. Então

$$\chi^*(y) = tr(\psi^*(y)) = \sum_{i=1}^{m} tr\,\psi(x_i y x_i^{-1}) = \sum_{i=1}^{m}\chi(x_i y x_i^{-1}). \tag{6}$$

Agora, para $z \in H$, $zx_iyx_i^{-1}z^{-1} \in H$ se e somente se $x_iyx_i^{-1} \in H$. Como χ é constante nas classes de conjugação de H e 0 fora de H, segue que $\chi(zx_iyx_i^{-1}z^{-1}) = \chi(x_iyx_i^{-1})$ para todo $z \in H$. Dessa forma, pode-se escrever (3.7) como

$$\chi^*(y) = \frac{1}{|H|}\sum_{i=1}^{m}\sum_{z\in H}\chi(zx_iyx_i^{-1}z^{-1}). \tag{7}$$

Mas, como x_i é um conjunto completo de representantes de classes laterais de H em G, $u = zx_i$ percorre todo G à medida que z percorre H e i varia de 1 a m, provando (i).

Se y não está em nenhum conjugado de H, então $uyu^{-1} \notin H$ para todo $u \in G$, de modo que $\chi(uyu^{-1}) = 0$ sempre e (ii) segue de (i). Também temos que, se $y \in ker\,\chi$ e $ker\,\chi \triangleleft G$ então $uyu^{-1} \in ker\,\chi$ e $\chi(uyu^{-1}) = \chi(1)$. Porém, nesse caso, $\chi^*(y) = \frac{1}{|H|}|G|\chi(1) = deg\,\chi^*$, provando (iii). Finalmente, se ψ_1 é uma representação de H, equivalente a ψ, então elas têm o mesmo caractere χ. Porém, de novo por (i), como ψ^* e ψ_1^* só dependem dos valores de χ, segue que tais caracteres estendidos são dados pela mesma fórmula, sendo, portanto, iguais em cada ponto. □

A função de indução $\chi \to \chi^*$ se estende a uma função de $ch(H)$ em $ch(G)$. A proposição 13(i) implica que essa função é linear. Assim, 13(i) e 13(ii) também valem para caracteres generalizados. Em particular, se χ é um caractere generalizado de grau 0, então χ^* também tem grau zero.

Se $H \leq K \leq G$, pode-se induzir um caractere de H em K e, depois, induzir esse caractere em G ou pode-se fazer a indução diretamente de H em G que obtemos o mesmo caractere. O nosso próximo resultado atesta isso.

Proposição 14. *Sejam* H, K *subgrupos de* G *com* $H \leq K \leq G$. *Seja* χ *um caractere de* H *e* $\tilde{\chi}$ *o caractere induzido em* K *por* χ. *Nesse caso,*

$$\chi^* = (\tilde{\chi})^*.$$

Demonstração. Faça $\chi(y) = 0$ para $y \in G \backslash H$. Então, por 13(i),

$$\tilde{\chi}(y) = \frac{1}{|H|} \sum_{v \in K} \chi(vzv^{-1}), \qquad v \in K. \tag{8}$$

Agora, faça $\tilde{\chi}(y) = 0$ se $y \in G \backslash K$. Então, pela proposição 13(i), para $y \in G$,

$$\tilde{\chi}^*(y) = \frac{1}{|K|} \sum_{u \in G} \chi(uyu^{-1}). \tag{9}$$

Mas se $z \notin K$, certamente $vzv^{-1} \notin H \leq K$ para qualquer $v \in K$, de forma que (9) vale também para $z \in G \backslash H$. Dessa forma, por (9) e (10), obtemos

$$\tilde{\chi}^*(y) = \frac{1}{|K|} \frac{1}{|H|} \sum_{u \in G} \sum_{v \in K} \chi(uvyv^{-1}u^{-1}). \tag{10}$$

Entretanto, qualquer elemento de G pode ser escrito exatamente $|K|$ vezes na forma uv, $u \in G$, $v \in K$, de forma que (11) se reduz a

$$\tilde{\chi}(y) = \frac{1}{|H|} \sum_{w \in G} \chi(wzw^{-1}) = \chi^*(y), \tag{11}$$

completando a prova. □

Se H é um subgrupo de G, temos produto interno tanto em $ch(H)$ quando $ch(G)$. Para distingui-los iremos denotá-los por $(*,*)_H$ e $(*,*)_G$ respectivamente. Agora, se $\chi \in ch(G)$ e $\theta \in ch(H)$, podemos considerar χ restrito a H e θ induzido a G, e computar os produtos internos $(\chi|_H, \theta)_H$ e $(\chi, \theta^*)_G$. Que relação existe entre essas multiplicidades? Essa pergunta é respondida pelo teorema da reciprocidade de Fröbenius, que precisa do seguinte lema para ser provado:

Lema 7. *Sejam A um subconjunto de G e $N = N_G(A)$. Então A tem exatamente $[G : N]$ conjugados em G.*

Demonstração. De fato, seja $x_1, \cdots, x_n$ um conjunto completo de representantes de classes laterais à direita de G módulo N, onde $[G : N] = n$. Nesse caso, tomando dois elementos de G que pertencem à classe Nx_i, xx_i e yx_i, perceba que $A^{xx_i} = A^{yx_i}$, pois $A^{xx_i} = (A^x)^{x_i} = A^{x_i}$, pois $x \in N$. Do mesmo modo mostra-se que $A^{x_i y} = A^{x_i}$. Por fim, também temos que os conjugados A^{x_i} e A^{x_j} têm interseção trivial pois, supondo que tal interseção não o fosse, haveria $z \in A^{x_i} \cap A^{x_j}$ tal que

$$z = x_i a_1 x_i^{-1} = x_j a_2 x_j^{-1} \Rightarrow x_j x_i a_1 x_i^{-1} x_j^{-1} = a_2 \in A \Rightarrow x_i x_j^{-1} \in N \Rightarrow x_i N = x_j N.$$

□

Teorema 9. ***(Reciprocidade de Fröbenius)*** *Seja H um subgrupo de G, θ um caractere generalizado de H e χ um caractere generalizado de G. Então*

$$(\chi|_H, \theta)_H = (\theta^*, \chi)_G.$$

Demonstração. Pelas definições e pelo fato de que χ' é uma função de classe, temos

$$\begin{aligned}(\theta^*, \chi)_G =& \frac{1}{|G|} \sum_{y \in G} \theta^*(y)\chi'(y) \\ =& \frac{1}{|G|}\frac{1}{|H|} \sum_{u,y \in G} \theta(uyu^{-1})\chi'(y) \\ =& \frac{1}{|G|}\frac{1}{|H|} \sum_{u,y \in G} \theta(uyu^{-1})\chi'(uyu^{-1}),\end{aligned} \tag{12}$$

onde θ é definido como assumindo o valor zero em $G \backslash H$. Como uyu^{-1} percorre todo G para u fixo quando y percorre G, podemos reescrever (12) como

$$\begin{aligned}(\theta^*, \chi)_G =& \frac{1}{|G|}\frac{1}{|H|} \sum_{u,y \in G} \theta(y)\chi'(y) \\ =& \frac{1}{|H|} \sum_{y \in G} \theta(y)\chi'(y).\end{aligned} \tag{13}$$

Porém, $\theta(y) = 0$ para $y \in G \backslash H$, enquanto em H, $\chi'(y) = \chi'|_H(y)$, de forma que (13) se reduz a

$$(\theta^*, \chi)_G = \frac{1}{|H|} \sum_{y \in G} \theta(y)(\chi|_H)'(y) = (\theta, \chi|_H)_H, \tag{14}$$

provando o teorema. □

Existe um caso especial no qual conclusões mais fortes sobre a relação entre χ e χ^* podem ser encontradas. Esse é o caso no qual H é o normalizador de um subconjunto A de H que é disjunto de seus conjugados em G e o caractere χ é 0 em $H \backslash A$. Por exemplo, o teorema 2 mostra que essas condições valem se G é um grupo de Fröbenius com $H = A$ sendo o complemento; nesse caso χ é um caractere qualquer de H. O resultado básico é o seguinte:

Proposição 15. *Seja A um subconjunto de G que é disjunto de seus conjugados. Faça $N = N_G(A)$ e sejam χ, θ caracteres generalizados de N que são 0 em $N \backslash A$. Então temos*

(i) $\chi^*(y) = \chi(y)$ *para* $y \in A^\#$.

(ii) Se $\deg \chi = 0$, *então* $(\chi, \theta)_N = (\chi^*, \theta^*)_G$.

Demonstração. Faça $\chi(y) = 0$ para $y \in G \backslash N$. Então, para cada $y \in G^\#$ temos, pela proposição 13(i),

$$\chi^*(y) = \frac{1}{|N|} \sum_{u \in G} \chi(uyu^{-1}). \tag{15}$$

Como $\chi(y) = 0$ por hipótese se $y \in N \backslash A$, temos que $\chi(uyu^{-1}) = 0$ a não ser que $uyu^{-1} \in A$. Em particular, $\chi(y) = 0$ a não ser que y pertença a algum conjugado de A. Além disso, para $y \in A^{\#}$, temos que ou $\chi(uyu^{-1}) = 0$ ou que $y \in A \cap A^{u^{-1}}$. Mas, sabe-se que no último caso $A = A^{u^{-1}}$ e $u \in N$, porque A é disjunto de seus conjugados. E, como χ é uma função de classe em N, teremos que $\chi(uyu^{-1}) = \chi(y)$. Dessa forma, para $y \in A^{\#}$,

$$\chi^*(y) = \frac{1}{|N|} \sum_{u \in N} \chi(uyu^{-1}) = \frac{1}{|N|} |N| \chi(y) = \chi(y), \tag{16}$$

provando (i).

Agora, assuma que $deg\, \chi = 0$, de forma que $deg\, \chi^* = 0$. Temos que

$$(\chi^*, \theta^*)_G = \frac{1}{|G|} \sum_{y \in G} \chi^*(y) \overline{\theta^*(y)}. \tag{17}$$

Porém, pelo parágrafo anterior, $\chi^*(y) = 0$ para todo y que não pertence a nenhum conjugado de $A^{\#}$, enquanto $\chi^*(y) = \chi(y)$ e $\theta^*(y) = \theta(y)$ se y está em um conjugado de A. Além disso, pelo lema anterior, sabemos que A tem exatamente $[G : N]$ conjugados, e nenhum deles tem um elemento em comum, pois A é disjunto de seus conjugados. Como $\chi(1) = \chi^*(1) = 0$, (18) se reduz a

$$(\chi^*, \theta^*)_G = \frac{1}{|N|} \sum_{y \in A} \chi(y) \overline{\theta(y)}. \tag{18}$$

Como $\chi * (y) = 0$ para $y \in N \backslash A$ por hipótese, isso nos dá, finalmente,

$$(\chi^*, \theta^*)_G = \frac{1}{|N|} \sum_{y \in N} \chi(y) \overline{\theta(y)} = (\chi, \theta)_N, \tag{19}$$

provando (ii). □

Finalmente, terminaremos essas anotações com uma demonstração do celebrado teorema de Fröbenius:

Teorema de Fröbenius. *Se G é um grupo de Fröbenius com H sendo o subgrupo fixando uma letra, então a identidade, juntamente com os elementos de G que não fixam letra alguma, formam um subgrupo normal de G de ordem $[G : H]$.*

Demonstração. Faça G agir no conjunto $S = \{1, 2, \cdots, n\}$, considere que H fixa 1 e seja $|H| = h$. Como G é uma ação transitiva em S, pelo lema 1 segue que $|G| = hn$. Além do mais, pelo teorema 2, H é disjunto de seus conjugados, $H = N_G(H)$ e $H \neq 1$, de forma que a proposição é aplicável com H no papel de A e N.

Sejam θ_i os caracteres irredutíveis de H, $1 \leq i \leq t$, com $\theta_1 = 1_H$. Também defina $d_i = deg\, \theta_i$, $1 \leq i \leq t$. Lembrando que t é o número de classe de H e como $H \neq 1$, $t > 1$. Considere

$$\phi_i = d_i \theta_1 - \theta_i, \qquad 2 \leq i \leq t, \tag{20}$$

de forma que $deg\,\phi_i = 0$. Então a reciprocidade de Fröbenius e a ortogonalidade dos caracteres garantem que

$$\begin{aligned}(\phi_i^*, \phi_i^*)_G &= (d_i\theta_1 - \theta_i, d_i\theta_1 - \theta_i)_G \\ &= d_i^2(\theta_1, \theta_1)_H - 2d_i(\theta_1, \theta_i)_H + (\theta_i, \theta_i)_H \\ &= d_i^2 + 1.\end{aligned} \tag{21}$$

Por outro lado, temos que

$$(\phi_i^*, 1_G)_G = (\phi_i, \theta_1)_H = d_i, \tag{22}$$

porque $\theta_1 = 1_H$ é a restrição de 1_G a H. Dessa forma, 1_G é um constituinte de multiplicidade d_i em ϕ_i^*. Aplicando produtos internos, segue agora de (21) que $\phi_i^* = d_i 1_G + \epsilon_i\chi_i$, onde $\epsilon = \pm 1$. Entretanto, $deg\,\phi_i^* = 0$, pois $deg\,\phi_i = 0$, o que força $\epsilon_i = -1$ e assim temos

$$\phi_i^* = d_i 1_G - \chi_i \qquad \text{e} \qquad deg\,\chi_i = d_i, 2 \leq i \leq t. \tag{23}$$

Com essa informação, construiremos agora o subgrupo normal que desejamos. Colocaremos $\chi_1 = 1_G$, $d_1 = 1$ e seja

$$\chi = \sum_{i=1}^{t} d_i\chi_i. \tag{24}$$

Por (23) e pela proposição 10(iii), temos que $\chi(1) = \sum_{i=1}^{t} d_i^2 = |H|$. Além disso, se $y \in G$ e y não está em nenhum conjugado de H, então $\phi^*(y) = 0$ e então teremos $\chi_i(y) = d_i$ por (23), $2 \leq i \leq t$. Mas então também vale que $\chi(y) = \sum_{i=1}^{t} d_i^2 = \chi(1)$, e isso garante que $y \in ker\,\chi = K$, ou seja, o núcleo K desse caractere contém todo elemento de G que não pertence a nenhum conjugado de H.

Por outro lado, se $y \in H^{\#}$, $\phi_i^*(y) = \phi_i(y)$, o que nos dá $\chi_i(y) = \theta_i(y)$, $2 \leq i \leq t$, por (20) e (23). Mas então $\chi(y) = \sum_{i=1}^{t} d_i\overline{\chi_i(y)} = 0$. Dessa forma, $H \cap K = 1$ e $\chi(y) = 0$ se y está em algum conjugado de H. Porém, sabemos que os conjugados de H são os subgrupos que fixam apenas uma letra em S. Concluímos, então que $K^{\#}$ consiste precisamente dos elementos de G que não estão em nenhum conjugado de H, ou seja, que não fixam nenhuma letra de S. por fim, temos que

$$(\chi, 1_G) = \frac{1}{|G|}\sum_{y\in G}\chi(y). \tag{25}$$

Como $\chi(y) = 0$ a não ser que $y \in K$, e nesse caso $\chi(y) = |H|$, segue de (25) que $(\chi, 1_G) = |K||H|/|G|$. Porém, KH é um subgrupo de G de ordem $|H||K|$, visto que $K \lhd G$ e $K \cap H = 1$. Como $(\chi, 1_G)$ é um inteiro, isso força que tenhamos $|G| = |H||K|$ e $KH = G$, de forma que $|K| = [G : H]$, como queríamos provar. □

Referências

[1] D.Gorenstein. *Finite Groups.* AMS Chelsea Publishing, American Mathematical Society, Nova York, 1980.

[2] M. Garonzi *Notas de aula do curso de Representações de Grupos Finitos 1.* Universidade de Brasília, Brasília, 2017.