Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Probabilidade de Comutar em Grupos Finitos

por

Alexandre Matos da Silva Pires de Moraes

sob orientação do

Prof. Dr. Martino Garonzi

Brasília - DF
2017

À minha esposa, Rachel, pela parceria e compreensão.
Aos meus filhos, Eduardo e Gustavo. Conciliar o Mestrado com as atividades profissionais consumiu, ao longo desses últimos anos, muito do tempo e atenção que eles esperavam receber de mim. Espero, que o fato de sempre me verem estudando sirva como exemplo e não como contra-exemplo.
À minha mãe, Lélia, meu grande exemplo de luta e persistência.
À memória de Seizi Amano, meu eterno guru matemático.

Considerate la vostra semenza:
Fatti non foste a viver come bruti,
Ma per seguir virtute e conoscenza.
(Dante Alighieri - Divina Commedia)

RESUMO

No presente trabalho, estuda-se a probabilidade de dois elementos comutarem quando são aleatoriamente selecionados em um grupo finito. Para obter os resultados principais, que são os Teoremas 9 e 14 constantes do artigo *On the commuting probability in finite groups* (R.M. Guralnick e G. R. Robinson, 2006), são adotadas duas abordagens complementares: uma que recorre à análise das classes de conjugação de um grupo e outra que se apóia não só na teoria de representações lineares de grupos mas também na informação que pode ser obtida a partir dos caracteres que lhes são associados. O primeiro teorema fornece uma cota superior para o valor da probabilidade de comutação. Já o segundo, estabelece uma cota inferior para tal probabilidade, usando informações sobre grau dos caracteres irredutíveis. Um resultado adicional, sob a forma de corolário, garante a existência, em um grupo G de ordem par (superior a 2), de um subgrupo próprio H, cujo cubo da ordem é maior do que a ordem de G.

ABSTRACT

In the current work, we study the commuting probability of two randomly selected elements of a finite group. In order to obtain the main results, which are theorems 9 and 14 of the article *On the commuting probability in finite groups* (R.M. Guralnick e G. R. Robinson, 2006), two complementary approaches are considered: one that takes into account the analysis of conjugacy classes in a group and another that relies not only upon the theory behind the linear representations of groups but also on the information that can be extracted from the associated characters. The first theorem allows an upper bound to be obtained for the value of the commuting probability. The second, on the other hand, establishes a lower bound for this probability, using information about the degree of the irreducible characters. An additional result, under the form of a corollary, ensures the existence, in a finite group G of even order (greater than 2), of a proper subgroup H, whose cube of the order is greater than the order of G.

Conteúdo

1. INTRODUÇÃO

No presente trabalho, estuda-se a probabilidade de dois elementos comutarem quando são aleatoriamente selecionados em um grupo finito. Antes de embarcar em uma busca centrada na determinação dos aspectos quantitativos (que naturalmente acompanham a noção de probabilidade), é interessante refletir sobre potenciais fontes de informação sobre comutatividade.

Amparando-nos na definição básica de que, "*dois elementos* x, g *de um grupo comutam se* $xg = gx$", e recorrendo a algumas equivalências muito conhecidas, podemos obter diferentes perspectivas sobre o significado de "comutar" :

$$xg = gx \Leftrightarrow g^{-1}xg = x \Leftrightarrow x^{-1}g^{-1}xg = 1 \, .$$

Convém não menosprezar o conteúdo subjacente a relações matemáticas tão despretensiosas. De forma similar ao que ocorre em outros campos do conhecimento humano, avaliar indiretamente a comutatividade, em cada cenário específico de estudo, pode ser tarefa mais simples do que o uso direto da definição. Isso não só motiva a escolha da perspectiva mais conveniente em cada contexto mas também inspira a criação de objetos matemáticos que permitam inferir sobre a propriedade de comutar. Dentre os objetos mais relevantes, merecem destaque os comutadores e os automorfismos internos induzidos por elementos do grupo. Dada a importância desses últimos, trataremos freqüentemente da análise da *ação por conjugação*.

Um caso limite importante, no que concerne à determinação da comutatividade, é o dos grupos abelianos. Além destes serem, precisamente, os *grupos comutativos*, possuem estrutura bastante conhecida. Isso conduz a pensar que, se dispusermos de métodos que permitam definir *quão longe de ser abeliano* um grupo está, será possível obter dados sobre a comutação em um grupo não-abeliano.

Nessa linha de análise, devotaremos especial atenção aos quocientes de um grupo G por dois de seus subgrupos característicos mais amplamente conhecidos:

- o centro, $Z(G)$;
- o subgrupo derivado, G' .

Por ser isomorfo a $Inn(G)$, grupo dos automorfismos internos de G, o quociente $G/Z(G)$ fornece informações diretas sobre conjugação. Por outro lado, G/G' fornece a referência de ser o maior quociente abeliano associado a G.

Esses rápidos exemplos ilustram o uso de atributos indiretos para concluir sobre a comutação e terão presença marcante no trabalho a ser desenvolvido, o qual culminará na demonstração de dois teoremas que estabelecem limites para o valor da probabilidade de comutar.

Precedendo o registro inicial dos enunciados dos dois teoremas que constituem o objeto principal de nosso estudo, dedicaremos algum tempo à definição formal da probabilidade de comutação.

Seja G um grupo finito de ordem n. A probabilidade de que dois elementos de G selecionados aleatoriamente (e com reposição) comutem é definida através da seguinte expressão:

$$cp(G) = \frac{|\{(x, y) \in G \times G : xy = yx\}|}{|G \times G|} .$$

Cumpre salientar que, em uma tal definição, assume-se implicitamente uma distribuição uniforme no espaço de probabilidade $G \times G$.

Levando-se em conta que, em um grupo abeliano, por sua própria essência, vale $cp(G) = 1$, o caso de interesse prático é justamente o dos grupos não-abelianos ($cp(G) < 1$). Convém ainda observar que não existe o outro extremo do espectro, isto é, que não ocorre o caso $cp(G) = 0$. Isso porque, em qualquer grupo G, o elemento identidade, 1_G , comuta com todos os elementos de G .

Um fato que chama bastante a atenção é que o valor máximo que pode ser assumido por $cp(G)$ em grupos não-abelianos é 5/8, conforme será demonstrado no texto. Esse curioso resultado foi originalmente apresentado em 1973 ([6]) e contribuiu para despertar o interesse no estudo da probabilidade de comutar.

Mesmo sendo tecnicamente simples e, de certa forma, intuitiva, essa definição de $cp(G)$ não é muito conveniente sob o ponto de vista de manipulação matemática. Isso naturalmente motiva a busca de formas alternativas de calcular a probabilidade, sendo a mais notável a que apresentaremos a seguir.

Se denotarmos por $k(G)$ o número de classes de conjugação no grupo G, veremos que a probabilidade de comutar é dada por:

$$cp(G) = \frac{k(G)}{|G|} .$$

Um aspecto interessante associado a essa nova formulação é que ela evidencia que o problema que estamos estudando pode ser expresso em termos de informações puramente algébricas: a ordem do grupo e número de classes de conjugação. Por estarmos tratando com grupos finitos, o desafio maior reside em obter o valor de $k(G)$, razão pela qual muitos trabalhos se dedicaram a pesquisar tal invariante. Como exemplo, podemos citar [3], [13], [2] e, mais recentemente, [4].

Tal equação ganha ainda mais força ao demonstrarmos que $k(G)$ coincide com o número de caracteres complexos irredutíveis de G. Com o intuito de derivar esse importante resultado, promoveremos uma análise introdutória da Teoria de Representações Lineares e dos caracteres que lhes são associados.

Apesar de estarem disponíveis várias técnicas que se propõem a calcular $cp(G)$, concentraremos os esforços na análise de duas delas. De modo a demonstrar os resultados principais, que correspondem aos Teoremas 9 e 14 constantes em [5], serão adotadas, respectivamente, as seguintes abordagens:

1) Análise da conjugação em um grupo (e vários conceitos associados);
2) Teoria de Representações Lineares e Caracteres.

Passemos, agora, aos enunciados dos dois teoremas.

Teorema 4.1 ([5] - Teorema 9).
Sendo G um grupo finito e $sol(G)$ o seu radical solúvel, vale:

$$cp(G) \leqslant [G : sol(G)]^{-1/2} .$$

Teorema 6.1 ([5] - Teorema 14).

(a) Para qualquer grupo finito G é válida a seguinte desigualdade:

$$cp(G) \geqslant \Big(\frac{1}{|G|} \cdot \sum_{\chi \in Irr(G)} \chi(1) \Big)^2 .$$

(b) Se G é um grupo finito de ordem par e com centro trivial, então:
$|G| < |C_G(x)|^3$, para algum $x \in G - \{1\}$.

O Teorema 4.1 fornece uma cota superior para o valor da probabilidade de comutar e, na pavimentação do caminho para demonstrá-lo, estudaremos vários conceitos auxiliares. Dentre eles podemos listar os de grupos *quasisimple*, *semi-simples*, *almost simple* e o de um subgrupo característico conhecido como o *Fitting Generalizado*, $F^*(G)$. Provaremos também o *Teorema de Bender*, o qual relaciona $F^*(G)$ com o subgrupo de Fitting, $F(G)$, e com outro subgrupo característico denominado o *layer* de G e denotado por $E(G)$.

Já o Teorema 6.1 estabelece uma cota inferior para a probabilidade de comutar, usando informações sobre o grau dos caracteres irredutíveis de um grupo. Todo o suporte necessário para que se possa demonstrá-lo é provido no texto, numa seção que trata de Representações Lineares.

É importante ressaltar que, apesar de utilizar conceitos relativamente simples em seu desenvolvimento, a demonstração do Teorema 4.1 se apóia em dois resultados intermediários ([2] e [13]), que recorrem à Classificação dos Grupos Simples Finitos ($CFSG$). Dessa forma, a despeito de seu enunciado mais compacto, o primeiro teorema pode ser considerado "menos elementar" que o segundo.

Antes de efetivamente iniciarmos o nosso estudo, consideramos relevante registrar que o artigo base para a elaboração desse trabalho ([5]) recorre a técnicas adicionais para derivar outros limites para $cp(G)$. Além disso, o interesse no tema continua vivo, conforme comprovado pela publicação do recente artigo [7].

2. CONCEITOS FUNDAMENTAIS

2.1. CONJUGAÇÃO.

Dizemos que dois elementos x e y de um grupo G são conjugados se existe $g \in G$ tal que $y = g^{-1}xg$. Quando existe um tal g, é comum dizer que y *é conjugado a* x *por* g e usar a notação $y = x^g$. A relação binária em que "$x \sim y$" significa que "existe $g \in G$ tal que $y = g^{-1}xg$" é uma relação de equivalência. A classe de equivalência de $\alpha \in G$ correspondente a tal relação é denominada *classe de conjugação* de α e denotada por α^G ou $Cl(\alpha)$.

A conjugação por um elemento fixo $g \in G$ é também comumente referenciada como o *automorfismo interno induzido por* g :

$$\begin{aligned} &\theta_g : G \to G \\ &\quad x \mapsto \theta_g(x) = x^g = g^{-1}xg \ . \end{aligned}$$

Uma observação básica é que se x e g comutam, então $x = x^g$. Dessa forma, em um grupo abeliano, o único automorfismo interno é a identidade ($Inn(G) = 1$). Por outro lado, se G é não-abeliano, devem existir automorfimos internos distintos da identidade e, nesse caso, o estudo da conjugação pode se mostrar frutífero para a obtenção de informações sobre comutatividade.

2.2. RELAÇÃO ENTRE COMUTATIVIDADE E CONJUGAÇÃO.

Seja g um elemento qualquer de um grupo G. Definimos o *centralizador* de g em G como o conjunto formado pelos elementos x do grupo G que comutam com um dado $g \in G$.

$$C_G(g) = \{x \in G \mid xg = gx\} \ = \{x \in G \mid g^{-1}xg = x\} \ = \{x \in G \mid x^g = x\} \ .$$

Os elementos x que centralizam um dado $g \in G$ geram uma classe de conjugação unitária ou *singleton* ($x^g = x$). Dessa forma, todo $x \in G$ tal que $xg = gx$ permanece fixo quando se promove a conjugação por um elemento de G. É importante ainda notar que o centralizador de um elemento $g \in G$ é um subgrupo de G. ($C_G(g) \leqslant G$)

Em resumo, se estivermos interessados em determinar os elementos do grupo G que comutam com um certo $g \in G$, podemos adotar as seguintes abordagens:

(1) testar cada $x \in G$ e verificar se ocorre $xg = gx$;
(2) deixar $g \in$ G agir por conjugação sobre cada $x \in G$ e identificar todos aqueles elementos que permanecem fixos.

O segundo procedimento é bem mais natural e, por isso, dedicaremos tempo ao estudo da conjugação e suas propriedades.

Dado um grupo G, seja $X \subseteq G$ um subconjunto arbitrário. Definimos:

- o *centralizador* de X em G é o conjunto dos elementos de G que comutam com todos os elementos de X, isto é, $C_G(X) = \{\ g \in G \mid xg = gx,\ \forall x \in X\ \}$.

  Observando que $C_G(X) = \bigcap_{x \in X} C_G(x)$, segue $C_G(X) \leqslant G$.

- o *centro* do grupo G é o conjunto dos elementos $y \in G$ que comutam com todos os elementos de G. Assim, $Z(G) = C_G(G) = \{\ y \in G \mid xy = yx,\ \forall x \in G\ \}$ e decorre que G é abeliano se, e somente se, $Z(G) = G$.

- o *normalizador* de X em G é o subgrupo $N_G(X) = \{\ g \in G \mid X^g = X\ \}$. Dado um subgrupo $H \leqslant G$, tem-se $H \trianglelefteq N_G(H)$.

Compilamos, na proposição a seguir, uma série de fatos sobre centralizadores e normalizadores, que serão amplamente utilizados ao longo do texto. Tais resultados podem ser encontrados em várias referências clássicas de Teoria de Grupos e serão assumidos sem demonstração.

Proposição 2.1 (Propriedades Básicas do Centralizador e do Normalizador)**.** *Seja G um grupo. São válidas as seguintes propriedades:*

(a) *Se X, Y são subconjuntos de G tais que $X \subseteq Y$, então $C_G(Y) \subseteq C_G(X)$;*
(b) *Se $H \leqslant G$ e $g \in G$, então $C_H(g) = C_G(g) \cap H$;*
(c) *Sendo $H \leqslant J \leqslant G$, vale $N_J(H) = N_G(H) \cap J$;*
(d) *Para qualquer subgrupo $H \leqslant G$, vale $C_G(H) \trianglelefteq N_G(H)$;*
(e) *O quociente $N_G(H)/C_G(H)$ é isomorfo a um subgrupo de Aut(H).*

2.3. AÇÃO DE GRUPOS.

Outra maneira bastante freqüente de tratar a conjugação faz uso do conceito de ação de um grupo sobre um conjunto. Dizemos que *um grupo G age sobre um conjunto não-vazio* Ω (ou que G permuta os pontos de Ω) se, a cada $g \in G$ e a cada $\alpha \in \Omega$, corresponde um único elemento α^g de Ω (imagem da ação de g sobre α) tal que:

(i) $\alpha^1 = \alpha, \forall \alpha \in \Omega$;
(ii) $(\alpha^g)^h = \alpha^{gh}, \forall \alpha \in \Omega$ e $\forall g, h \in G$.

Dessa forma, uma ação de G sobre Ω é uma função:

$\mu : \Omega \times G \to \Omega$
$\quad (\alpha, g) \mapsto \alpha^g$, que verifica as condições (i) e (ii).

Notação: Na definição acima, optamos por especificar uma *ação à direita* . Tal convenção será mantida ao longo de todo o texto.

Começaremos a análise, revisando os conceitos de *órbitas* e *estabilizadores* de uma ação e estabelecendo algumas relações importantes entre eles:

- órbita: subconjunto de Ω que contém os possíveis resultados da ação de cada $g \in G$ sobre o elemento $\alpha \in \Omega$.

  $\mathcal{O}(\alpha) = \alpha^G = \{ \alpha^g \mid g \in G \} \subseteq \Omega.$

- estabilizador de um ponto: conjunto dos elementos de G que fixam um dado $\alpha \in \Omega$. (Tal conjunto é um subgrupo de G).

  $G_\alpha = Stab_G(\alpha) = \{ g \in G \mid \alpha^g = \alpha \} \leqslant G$.

Antes de iniciar a demonstração da Proposição 2.2, revisitaremos um resultado clássico, conhecido como *Teorema Órbita-estabilizador*.

Sejam G um grupo agindo sobre Ω e $\mathcal{O}$ uma órbita dessa ação. Seja $\alpha \in \mathcal{O}$ e denotemos $H = G_\alpha$, o estabilizador de α em G. Então existe uma bijeção:
$\mathcal{O} \leftrightarrow \{ Hx \mid x \in G \}$.

Sejam $f : \mathcal{O} \to \{ Hx \mid x \in G \}$ uma função e β um elemento de $\mathcal{O}$.
Tomemos $x \in G$ tal que $\beta = \alpha^x$ e façamos $f(\beta) = Hx$.

(I) f está bem definida, pois:
$\alpha^x = \alpha^y \Rightarrow (\alpha^x)^{y^{-1}} = (\alpha^y)^{y^{-1}} = \alpha^1 = \alpha \ \therefore \ xy^{-1} \in H = G_\alpha \ \therefore \ xy^{-1} = h \in H$

$\therefore \ x = hy, h \in H \ \therefore \ Hx = Hy$.

(II) f é sobrejetiva, pois, dada uma classe Hx, existe $x \in G$ tal que $f(\alpha^x) = Hx$.

(III) f é também injetiva.
Admitamos $f(\beta) = f(\gamma)$. Então $\beta = \alpha^x$ e $\gamma = \alpha^y$, com $Hx = Hy$.
Mas isso significa que $y = hx$ para algum $h \in H = G_\alpha$ e, portanto:

$\gamma = \alpha^y = \alpha^{hx} = (\alpha^h)^x = \alpha^x = \beta$.

Como conseqüência direta de f ser bijetiva, a cardinalidade da órbita de α coincide com o número de classes laterais do estabilizador G_α, ou seja:

$$|\mathcal{O}| = [G : G_\alpha] = \frac{|G|}{|G_\alpha|} \qquad (\textit{Fundamental Counting Principle} \text{ - FCP}).$$

A última equação evidencia ainda que qualquer tamanho de órbita divide $|G|$.

Proposição 2.2. *Dados um grupo G e um conjunto Ω, denotemos por μ uma ação de G sobre Ω:*

$$\begin{aligned}\mu : \Omega \times G &\to \Omega \\ (\omega, x) &\mapsto \omega^x \ .\end{aligned}$$

Se $\alpha, \beta \in \Omega$ estão na mesma órbita, então:

(a) $[G : G_\alpha] = [G : G_\beta]$;
(b) *Existe $x \in G$ tal que $G_\beta = (G_\alpha)^x$, o que significa que G_α e G_β são subgrupos conjugados de G ;*
(c) *Em particular, tem-se $G_{\alpha^x} = (G_\alpha)^x$.*

Demonstração. (a) Dado que α, β estão na mesma órbita, vale $\mathcal{O}(\alpha) = \mathcal{O}(\beta)$. Usando o fato que $|\mathcal{O}(\alpha)| = [G : G_\alpha]$ e $|\mathcal{O}(\beta)| = [G : G_\beta]$, segue a tese.

(b) Lembrando que β está em $\mathcal{O}(\alpha)$, existe $x \in G$ tal que $\beta = \alpha^x$. Tomando $g \in G_\alpha$, tem-se $\alpha^g = \alpha$. Além disso, $g^x \in (G_\alpha)^x$, ou seja, $x^{-1}gx \in (G_\alpha)^x$. Resulta:

$$\beta^{x^{-1}gx} = (\alpha^x)^{x^{-1}gx} = \alpha^{xx^{-1}gx} = \alpha^{gx} = \alpha^x = \beta \ .$$

Mas isso significa que $x^{-1}gx \in G_\beta$, isto é, $(G_\alpha)^x \subseteq G_\beta$. Analogamente, prova-se a inclusão reversa e obtém-se a tese.

(c) Por definição de órbita, tem-se $\alpha^x \in \mathcal{O}(\alpha), \forall x \in G$. De (b), segue o resultado. □

2.4. AÇÃO POR AUTOMORFISMOS.

Definição 2.1. *Sejam dois grupos N e H tais que H age sobre o conjunto dos elementos de N. Dizemos que H age por automorfismos sobre N se, $\forall x, y \in N$ e $\forall h \in H$, vale $(xy)^h = x^h y^h$.*

Assim, a função θ_h, induzida por cada $h \in H$, é um automorfismo de N.

$$\begin{aligned}\theta_h : N &\to N \\ n &\mapsto \theta_h(n) = n^h \ ,\end{aligned}$$

Para verificar tal afirmação, deve-se observar inicialmente que ação de H sobre N é, em particular, uma ação do grupo H sobre o conjunto N e, portanto, θ_h é uma permutação dos elementos de N. Assim, dados $x, y \in N$, tem-se:

$$\theta_h(xy) = (xy)^h = x^h \cdot y^h = \theta_h(x) \cdot \theta_h(y).$$

Além disso, o homomorfismo $\theta : H \to Aut(N)$, definido por $\theta : h \mapsto \theta_h$, é denominado a *representação por automorfismos* de H correspondente à ação.

2.5. AÇÃO POR CONJUGAÇÃO.

Definição 2.2. *Dado um grupo G, definimos a ação por conjugação (de G sobre G) da seguinte forma:*

$$\begin{aligned} \mu : G \times G &\to G \\ (\alpha, g) &\mapsto \alpha^g = g^{-1}\alpha g \ . \end{aligned}$$

Reunimos, a seguir, não só a terminologia típica mas também as propriedades básicas associadas à ação por conjugação:

- Dois elementos conjugados possuem a mesma ordem;
- A ação por conjugação (de G sobre G) é uma ação por automorfimos. Isso também acontece com uma ação de G sobre um subgrupo $N \trianglelefteq G$;
- $\mathcal{O}(\alpha) = \alpha^G = \{\ \alpha^g \mid g \in G\ \} = \{\ g^{-1}\alpha g \mid g \in G\ \} = Cl(\alpha)$;
- $G_\alpha = Stab_G(\alpha) = \{\ g \in G \mid \alpha^g = \alpha\ \} = C_G(\alpha)$;
- G é a união disjunta de suas classes de conjugação;
- O número de conjugados de um dado elemento α em um grupo finito G é o índice do centralizador de α em G, ou seja, $|Cl(\alpha)| = [G : C_G(\alpha)]$;
- Dado que $C_G(\alpha)$ é um subgrupo de G, tem-se $|G| = |C_G(\alpha)| \cdot [G : C_G(\alpha)]$ e, portanto, $|G| = |C_G(\alpha)| \cdot |Cl(\alpha)|$. Daí resulta que todos os tamanhos de classes de conjugação dividem $|G|$;
- $|G| = |Z(G)| \ + \sum_{i=l+1}^{k} [G : C_G(x_i)]$, em que $x_{l+1}, \ldots, x_k$ são representantes das classes de conjugação cujo comprimento é maior que 1 .

Dado $\alpha \in G$, o conjunto $\{\alpha\}$ é uma classe de conjugação se, e somente se, $\alpha \in Z(G)$, pois: $\alpha \in Z(G) \Leftrightarrow \alpha g = g\alpha, \forall g \in G \Leftrightarrow g^{-1}\alpha g = \alpha, \forall g \in G \Leftrightarrow \alpha^g = \alpha, \forall g \in G \Leftrightarrow Cl(\alpha) = \{\alpha\}$.

Vale observar que, para um grupo abeliano, tem-se $Z(G) = G$, donde segue $k(G) = |G|$. Isso evidencia que o estudo das classes de conjugação, nesse caso, não traz qualquer informação relevante.

Dentre as propriedades listadas acima, merece especial atenção a que permite calcular o número de elementos numa classe de conjugação.

Sendo $Cl(x) = \{\ x^g \mid x \in G\ \}$ a classe de conjugação de $x \in G$, mostraremos que:

- elementos de uma mesma classe lateral de $C_G(x)$ geram o mesmo conjugado
- elementos em distintas classes laterais de $C_G(x)$ dão origem a conjugados distintos.

Isso nos permitirá concluir que $|Cl(x)| = [G : C_G(x)]$.

Proposição 2.3 (Cálculo do tamanho de uma classe de conjugação)**.** *O número de conjugados de x em um grupo finito G é o índice do centralizador de x em G.*

Demonstração. Antes de iniciar a demonstração propriamente dita, convém notar que tal Proposição é um caso particular do *Teorema Órbita-Estabilizador*. No entanto, sendo a conjugação um conceito bastante utilizado no presente trabalho, o raciocínio usado numa prova direta merece registro específico.

(1) Suponha que a, $b \in G$ estejam na mesma classe lateral à direita de $C_G(x)$ em G. Então $b = ha$, com $h \in C_G(x)$. ($\therefore b^{-1} = (ha)^{-1} = a^{-1}h^{-1}$).

Mas $h \in C_G(x) \Rightarrow hx = xh$ e, portanto:

$x^b = b^{-1}xb = a^{-1}h^{-1}xha = a^{-1}h^{-1}hxa = a^{-1}xa = x^a$.

(2) Se a, $b \in G$ estão em distintas classes laterais à direita de $C_G(x)$ em G, segue $b^{-1}xb \neq a^{-1}xa$. Se tal não fosse o caso, teríamos $b^{-1}xb = a^{-1}xa$ e viria $ab^{-1}xb = xa \therefore ab^{-1}x = xab^{-1}$, o que significa $ab^{-1} \in C_G(x)$, ou seja, isso equivale a dizer a, b pertencem à mesma classe lateral de $C_G(x)$ em G. (Mas isso contraria a escolha inicial de a e b). □

Proposição 2.4 (Número de Classes de Conjugação em um Grupo Finito)**.** *Seja G um grupo finito de ordem n. Denotando por $k(G)$ o número de classes de conjugação em G, valem os seguintes resultados:*

(a) $k(G) = \dfrac{1}{|G|} \cdot \sum_{x \in G} |C_G(x)| = \dfrac{1}{n} \cdot \sum_{x \in G} |C_G(x)|$;

(b) $cp(G) = \dfrac{k(G)}{|G|}$.

Demonstração. (a) Consideremos o conjunto $C = \{ (x, y) \in G \times G : xy = yx \}$, dos pares ordenados cujas entradas são elementos que comutam no grupo G. Para cada $x \in G$ (fixo), o número de pares ordenados do tipo (x,y) em C é dado por $|C_G(x)|$. Sendo $|G| = [G : C_G(x)] \cdot |C_G(x)|$, segue:

$$|C| = \sum_{x \in G} |C_G(x)| = \sum_{x \in G} \frac{|G|}{[G : C_G(x)]} = |G| \cdot \sum_{x \in G} \frac{1}{[G : C_G(x)]} \qquad (*)$$

Pela Proposição 2.2, se dois pontos x e y em G pertencem a uma mesma órbita (classe), seus estabilizadores (centralizadores) são subgrupos conjugados e possuem mesmo índice.

Tomemos um representante x_i da i-ésima classe de conjugação, C_i , e denotemos $|C_i| = m_i$. Cada elemento $y \in C_i$) satisfaz $[G : G_y] = [G : G_{x_i}]$, ou seja:

$[G : C_G(y)] = [G : C_G(x_i)] = |C_i| = m_i$

Dessa forma, para a i-ésima classe de conjugação, vale:

$$\sum_{y \in C_i} \frac{1}{[G : C_G(y)]} = \sum_{y \in C_i} \frac{1}{m_i} = m_i \cdot \frac{1}{m_i} = 1$$

Fazendo $k = k(G)$, podemos reescrever a equação (*):

$$|C| = |G| \cdot \sum_{x \in G} \frac{1}{[G : C_G(x)]} = |G| \cdot \sum_{l=1}^{k} 1 = |G| \cdot k(G)$$

Usando tal fato em (*) , concluímos a prova do item.

(b) Recordemos a definição da probabilidade de comutação, $cp(G)$:

$$cp(G) = \frac{|\{(x, y) \in G \times G : xy = yx\}|}{|G \times G|} = \frac{|C|}{|G|^2}$$

Recorrendo ao item (a), obtemos a expressão básica para o cálculo de $cp(G)$:

$$cp(G) = \frac{k(G)}{|G|} \, . \qquad \square$$

Proposição 2.5 (Cota Superior para $cp(G)$ em grupos não-abelianos)**.** *Se G é um grupo não-abeliano, então $cp(G) \leqslant 5/8$. Além disso, o caso $cp(G) = 5/8$ ocorre se, e somente se, o centro tem indíce 4 .*

Demonstração. Antes de iniciar a demonstração, vale registrar que tal resultado é apresentado em [6] (1973). Apesar de sua simplicidade, pode ser considerado um trabalho que despertou o interesse no estudo da probabilidade de comutar.

(I) A equação das classes se escreve $|G| = |Z(G)| + |C_1| + \cdots + |C_t|$, em que C_i representa uma classe de conjugação não-central (e, portanto, não-unitária). Assim, $|C_i| \geqslant 2$, para cada $i = 1, 2, \ldots, t$ e resulta $(\, |G| - |Z(G)| \,) \geqslant 2 \cdot t$. Sendo k o número total de classes, segue $k = t + |Z(G)|$ e daí $k \leqslant (\, |G| + |Z(G)| \,)/2$.

(II) Sendo G um grupo não-abeliano, temos que o quociente $G/Z(G)$ é não-cíclico e, portanto, $|G/Z(G)| \geqslant 4$. Assim, $|Z(G)| \leqslant |G|/4$ e, aplicando (I), vem $k \leqslant 5/8 \cdot |G|$.

(III) Usando (II) em conjunto com a expressão básica para $cp(G)$ obtida na Proposição 2.4, segue a tese.

(IV) Vejamos agora a situação em que ocorre a igualdade.

Mostramos, na análise anterior, que: $k \leqslant (1/2) \cdot (\, |G| + |Z(G)| \,) \leqslant 5/8 \cdot |G|$.

Se $k = 5/8 \cdot |G|$, vem $k \leqslant (1/2) \cdot (\, |G| + |Z(G)| \,) \leqslant 5/8 \cdot |G| = k$. Isso força que se tenha $(1/2) \cdot (\, |G| + |Z(G)| \,) = 5/8 \cdot |G|$ e daí segue $|Z(G)| = |G|/4$.

Reciprocamente, admitamos que $|Z(G)| = |G|/4$. $Z = Z(G) \leqslant C_G(x), \forall x \in G$. Se x é não-central, seja C o centralizador de x em G. As inclusões $Z < C$ e $C < G$ são estritas, pois:

- Se ocorresse $Z = C$, então x estaria em Z. Mas isso é absurdo, visto que contraria a escolha de x como um elemento não-central.
- Se valesse $C = G$, todos os elementos do grupo comutariam com x. Mas, por definição do centro $Z = Z(G)$, isso significaria $x \in Z$, o que é uma contradição.

Sendo Z um subgrupo de C, devemos ter $|C| = (1/2) \cdot |G|$. Resulta:

$$|Cl(x)| = \frac{|G|}{|C_G(x)|} = \frac{|G|}{|C|} = 2\,.$$

Recorrendo à equação das classes e usando a informação $|Z| = (1/4) \cdot |G|$, segue:

$$|G| = |Z| + (k(G) - |Z|) \cdot 2 \;\therefore\; (3/8) \cdot |G| = k(G) - (1/4) \cdot |G| \;\therefore\; k(G) = (5/8) \cdot |G| \quad \square$$

Exemplo 2.3. *Probabilidade de comutar em Grupos Diedrais*

A título de ilustração, registramos, na tabela a seguir, o valor de $cp(G)$ para grupos diedrais D_n. Os cálculos foram feitos com o software GAP e n e corresponde ao número de lados do polígono regular em análise. É interessante observar que o valor de $cp(G)$ para D_4 é o máximo possível (conforme Proposição 2.5).

diedral	$cp(G)$	***diedral***	$cp(G)$	***diedral***	$cp(G)$
D_3	1/2	D_{20}	13/40	D_{120}	21/80
$\mathbf{D_4}$	**5/8**	D_{30}	3/10	D_{130}	17/65
D_5	2/5	D_{40}	23/80	D_{140}	73/280
D_6	5/14	D_{50}	7/25	D_{150}	13/50
D_7	7/16	D_{60}	11/40	D_{160}	83/320
D_8	1/3	D_{70}	19/70	D_{170}	22/85
D_9	2/5	D_{80}	43/160	D_{180}	31/120
D_{10}	7/22	D_{90}	4/15	D_{190}	49/190
D_{11}	3/8	D_{100}	53/200	D_{196}	101/392
D_{12}	4/13	D_{110}	29/110	D_{200}	103/400

2.6. CLASSES DE CONJUGAÇÃO EM UM SUBGRUPO.

Estudaremos, agora, alguns lemas que estabelecem relações entre os números de classes de conjugação de um grupo e de um seu subgrupo. Tais resultados serão empregados, posteriormente, na demonstração do Primeiro Teorema.

Lema 2.6. *Sendo H um subgrupo de G, são válidas as seguintes relações entre o número de classes de conjugação de H e de G:*

(a) $k(H) < [G : H] \cdot k(G)$, *se* $H \neq G$;
(b) $k(G) \leqslant [G : H] \cdot k(H)$.

Demonstração. (a) Conforme visto na Proposição 2.4, temos:

$$k(H) = \frac{1}{|H|} \cdot \sum_{x \in H} |C_H(x)| = \frac{[G : H]}{|G|} \cdot \sum_{x \in H} |C_H(x)| \quad \text{(I)}$$

Sendo H e G subconjuntos de G em que $H \subseteq G$, a Proposição 2.1 permite escrever:

$$\frac{[G : H]}{|G|} \cdot \sum_{x \in H} |C_H(x)| \leqslant \frac{[G : H]}{|G|} \cdot \sum_{x \in H} |C_G(x)| \quad \text{(II)}$$

Sendo H, por hipótese, um subgrupo próprio de G, temos:

$$\frac{[G : H]}{|G|} \cdot \sum_{x \in H} |C_G(x)| < \frac{[G : H]}{|G|} \cdot \sum_{x \in G} |C_G(x)| \quad \text{(III)}$$

Unindo os fatos (I), (II), e (III), resulta:

$$k(H) = [G : H] \cdot \frac{1}{|G|} \sum_{x \in H} |C_H(x)| < [G : H] \cdot \frac{1}{|G|} \sum_{x \in G} |C_G(x)| = [G : H] \cdot k(G)$$

(b) Sabemos que:

$$|G| = [G : C_G(x)] \cdot |C_G(x)| = [G : H] \cdot |H| = [G : H] \cdot |C_H(x)| \cdot [H : C_H(x)]$$

$$\therefore \ |C_G(x)| = [G : H] \cdot |C_H(x)| \cdot \frac{[H : C_H(x)]}{[G : C_G(x)]} \quad \text{(IV)}$$

A Proposição 2.3 estabelece que, para um grupo qualquer: $|Cl(x)| = [G : C_G(x)]$

Por ser H um subgrupo de G, o número de H-conjugados de um elemento $x \in G$ é, no máximo, igual ao seu número de conjugados em G. Dessa observação, segue:

$[H : C_H(x)] \leqslant [G : C_G(x)]$

Usando tal informação em (IV), vem: $|C_G(x)| \leqslant [G : H] \cdot |C_H(x)|$ (V)

Considerando que o resultado obtido em (V) vale para todo $x \in G$, segue:

$$\sum_{x \in G} |C_G(x)| \leqslant [G : H] \cdot \sum_{x \in G} |C_H(x)| = [G : H] \cdot \sum_{y \in H} |C_G(y)| \quad \text{(VI)}$$

Usando novamente (V) em (VI), resulta:

$$\sum_{x \in G} |C_G(x)| \leqslant [G : H] \cdot \sum_{y \in H} |C_G(y)|$$

$$\leqslant [G : H] \cdot \sum_{y \in H} [G : H] \cdot |C_H(y)| = \frac{|G|}{|H|} \cdot [G : H] \cdot \sum_{y \in H} |C_H(y)|$$

$$\therefore \frac{1}{|G|} \cdot \sum_{x \in G} |C_G(x)| \leqslant [G : H] \cdot \frac{1}{|H|} \cdot \sum_{y \in H} |C_H(y)|$$

A última desigualdade equivale a dizer que: $k(G) \leqslant [G : H] \cdot k(H)$.

□

Lema 2.7. *Sendo N um subgrupo normal de G, são válidas as seguintes relações:*

(a) $\dfrac{C_G(x)N}{N} \subseteq C_{G/N}(xN)$;

(b) $\dfrac{C_G(x)}{C_N(x)} \cong \dfrac{C_G(x)N}{N}$;

(c) $k(G) \leqslant k(G/N) \cdot k(N)$.

Demonstração. (a) Notemos inicialmente que, sendo $N \trianglelefteq G$ e $C_G(x) \leqslant G$, tem-se que $C_G(x)N$ é subgrupo de G. Além disso, dado que $N \trianglelefteq C_G(x)N$, segue que $(C_G(x)N)/N \leqslant G/N$. Tomemos agora uma classe lateral σN em $(C_G(x)N)/N$. Temos $\sigma = y \cdot n$, com $y \in C_G(x)$ e $n \in N$.

$y \in C_G(x) \Rightarrow y \cdot x = x \cdot y \ \therefore \ yN \cdot xN = xN \cdot yN \ \therefore \ yN \in C_{G/N}(xN)$

Sendo $\sigma = y \cdot n$, segue $\sigma N = (y \cdot n)N = yN$ e, portanto, $\sigma N \in C_{G/N}(xN)$

(b) Conforme visto no item (a), $N \trianglelefteq C_G(x)N$ (I)
Sendo $C_G(x) \leqslant C_G(x)N$, temos $(N \cap C_G(x)) \trianglelefteq C_G(x)$.

Pela Proposição 2.1, sabemos que $N \cap C_G(x) = C_N(x)$ e, assim, segue:

$C_N(x) \trianglelefteq C_G(x)$ (II)

Recorremos ao Segundo Teorema do Isomorfismo para mostrar que:

$\frac{C_G(x)N}{N} \cong \frac{C_G(x)}{N \cap C_G(x))}$ e, aplicando (II), obtemos $\frac{C_G(x)N}{N} \cong \frac{C_G(x)}{C_N(x)}$

(c) Combinando os resultados obtidos em (a) e (b), podemos escrever:

$$\frac{C_G(x)}{C_N(x)} \cong \frac{C_G(x)N}{N} \subseteq C_{G/N}(xN)\,.$$

Por estarmos tratando com grupos finitos, podemos passar de tais inclusões a desigualdades que envolvem as ordens dos grupos:

$$|C_G(x)| \leqslant \left|C_{G/N}(xN)\right| \cdot |C_N(x)| \;\text{ e }\; \sum_{x\in G}|C_G(x)| \leqslant \sum_{x\in G}\left|C_{G/N}(xN)\right| \cdot |C_N(x)| \qquad \text{(I)}$$

Sendo ρ um elemento da classe lateral xN, tem-se $\rho N = xN$. Assim, o centralizador $C_{G/N}(\rho N)$ coincide com o centralizador $C_{G/N}(xN), \forall \rho \in xN$. Dessa forma, fazendo $S = xN$, a soma em (I) pode ser reescrita:

$$\sum_{x\in G}\left|C_{G/N}(xN)\right| \cdot |C_N(x)| = \sum_{S\in G/N}\left(\left|C_{G/N}(S)\right| \cdot \sum_{x\in S}|C_N(x)|\right) \qquad \text{(II)}$$

Dados os subconjuntos $A, B \subseteq G$, consideremos os conjuntos:
$Q = \{\ (a,b) \in A \times B : ab = ba\ \}$ e $C_A(x) = \{a \in A\ :\ ax = xa\}$.

Com essas notações, vemos que, para cada $a \in A$ (fixo), o número de pares ordenados (a,b) em Q é dado por $|C_B(a)|$. Por outro lado, para cada $b \in B$ (fixo), o número de pares (a,b) em Q é dado por $|C_A(b)|$. Unindo as duas perspectivas:

$$\sum_{a\in A}|C_B(a)| = |Q| = \sum_{b\in B}|C_A(b)| \qquad \text{(III)}$$

Aplicando (III) aos subconjuntos $N \leqslant G$ e $xN = S \subseteq G$, podemos escrever:

$$\sum_{x\in S}|C_N(x)| = \sum_{\tau\in N}|C_S(\tau)|\,.$$

Esse último fato nos permite voltar a (II) e transformar uma soma sobre a classe lateral S, em outra, sobre o subgrupo normal N:

$$\sum_{S\in G/N}\left(\left|C_{G/N}(S)\right| \cdot \sum_{x\in S}|C_N(x)|\right) = \sum_{S\in G/N}\left(\left|C_{G/N}(S)\right| \cdot \sum_{\tau\in N}|C_S(\tau)|\right) \qquad \text{(IV)}$$

Dado o subgrupo $N \trianglelefteq G$, sejam $t \in N$, $x \in G$, $S := xN$. Com as mesmas notações já utilizadas, vamos mostrar que: $|C_S(t)| \leqslant |C_N(t)|$. De fato:

Quando $C_S(t)$ é vazio, tem-se $0 = |C_S(t)| \leqslant |C_N(t)|$. Com isso em mente, podemos supor $C_S(t)$ não-vazio, ou seja, que existe $y \in C_S(t)$. Dado um tal y, é suficiente mostrar que $C_S(t) \subseteq yC_N(t)$, pois $|yC_N(t)| = |C_N(t)|$.

Tomemos um $z \in C_S(t)$. Então existe $n \in N$ tal que $z = xn$ e vale $xnt(xn)^{-1} = t$. Lembrando que $yt = ty$, segue:

$t = y^{-1}ty = y^{-1}xntn^{-1}x^{-1}y$, mostrando que $y^{-1}xn \in C_G(t)$.

Por outro lado $y^{-1}x \in N$ (pois $y \in S = xN$). Assim $y^{-1}xn \in N$ e, portanto, $y^{-1}xn \in C_N(t)$. Finalmente, $z = xn = y(y^{-1}xn) \in yC_N(t)$ e daí $C_S(t) \subseteq yC_N(t)$.

Combinando esse último resultado com a expressão em (IV), segue:

$$\begin{aligned}\frac{1}{|G|}\sum_{x\in G}|C_G(x)| &\leqslant \frac{1}{|G|}\sum_{S\in G/N}\big|C_{G/N}(S)\big|\cdot\sum_{\tau\in N}|C_S(\tau)| \\ &\leqslant \frac{1}{|G/N|}\sum_{S\in G/N}\big|C_{G/N}(S)\big|\cdot\Big(\frac{1}{|N|}\sum_{\tau\in N}|C_N(\tau)|\Big)\end{aligned}$$

Recorrendo à expressão para $k(G)$ dada na Proposição 2.4, obtemos a tese. □

O item (c) do Lema 2.7 é de grande utilidade, pois permite dividir o problema de calcular uma cota superior para $k(G)$. Caso seja possível identificar um subgrupo normal N e um quociente G/N para os quais se consiga limitar o número de classes de conjugação, teremos um limite para $k(G)$. Veremos também, no lema a seguir, como obter o resultado correspondente para $cp(G)$. Tal estratégia terá papel importante na demonstração do Teorema 4.1.

Lema 2.8. *Seja G um grupo finito.*

(a) *Para todo subgrupo próprio $H < G$, vale:*

$$[G:H]^{-2}\cdot cp(H) < cp(G) \leqslant cp(H)\ ;$$

(b) *Quando $N \trianglelefteq G$, $cp(G) \leqslant cp(N)\cdot cp(G/N)$.*
Em particular, vale $cp(G) \leqslant cp(G/N)$;

(c) *Uma seção de um grupo finito G é qualquer imagem homomórfica de um subgrupo de G. Para toda seção X de G, tem-se $cp(G) \leqslant cp(X)$;*

(d) *Se H é outro grupo finito, então $cp(G \times H) = cp(G)\cdot cp(H)$;*

(e) *Se o grupo G é não-abeliano, $cp(G) < 3/2 \cdot [G : C_G(x)]^{-1}$, para algum $x \in (G - Z(G))$. Se o centro $Z(G)$ é trivial, vale $cp(G) \leqslant [G : C_G(x)]^{-1}$ para algum $x \in G - \{1\}$.*

Demonstração. (a) Usando os ítens (a) e (b) do Lema 2.6, obtemos:

$[G : H]^{-1} \cdot k(H) < k(G) \leqslant [G : H] \cdot k(H)$, quando H é subgrupo próprio de G .

Lembrando que $k(G) = |G| \cdot cp(G)$ e $k(H) = |H| \cdot cp(H)$, vem:

$[G : H]^{-1} \cdot |H| \cdot cp(H) < |G| \cdot cp(G) \leqslant [G : H] \cdot |H| \cdot cp(H)$.

Dividindo todos os membros das desigualdades por $|G|$, obtemos a tese.

(b) Usamos o fato que $k(G/N) = \dfrac{|G|}{|N|} \cdot cp(G/N)$ e aplicamos o Lema 2.7 (c).

Dado que $cp(N) \leqslant 1$, temos, em particular, $cp(G) \leqslant cp(G/N)$.

(c) Notemos que, pela definição, uma seção de G é um grupo da forma Y/N, em que $N \trianglelefteq Y$ e $Y \leqslant G$. Seja $X = Y/N$ uma seção de G. Pelo item (b), temos $cp(Y) \leqslant cp(Y/N)$. Mas $cp(G) \leqslant cp(Y)$, por (a). Combinando (a) e (b), segue:

$cp(G) \leqslant cp(Y) \leqslant cp(Y/N) \therefore cp(G) \leqslant cp(X)$.

(d) Segue do fato que $k(G \times H) = k(G) \cdot k(H)$.

(e) Fazendo $Z = Z(G)$ e $k = k(G)$, a equação das classes se escreve:

$$|G| = |Z| + \sum_i [G : C_G(x_i)] ,$$

em que os x_i são representantes das classes de tamanho superior a 1.

(I) Para provar a desigualdade proposta, basta mostrar que:

$k < 3/2 \cdot |G| \cdot [G : C_G(x)]^{-1}$, para algum $x \in (G - Z)$,

ou, equivalentemente, que: $k < 3/2 \cdot |C_G(x)|$, para algum x não-central.

Denotando por c a máxima ordem de $C_G(x)$ para $x \in G - Z$, precisamos mostrar que $k < 3/2 \cdot c$ para um tal x . Retornando à equação das classes, obtemos:

$$|G| = |Z| + \sum_i [G : C_G(x_i)] \geqslant |Z| + (k - |Z|) \cdot \frac{|G|}{c} \therefore |G| > |G| - |Z| \geqslant (k - |Z|) \cdot \frac{|G|}{c} .$$

Assim, $k < c + |Z|$ e, por estarmos tratando com números inteiros, $k \leqslant c + |Z| - 1$.

Lembrando que $Z \leqslant C_G(x)$ e levando em conta a escolha de x (não-central), segue que Z deve ser um subgrupo próprio de $C_G(x)$. Assim:

$[C_G(x) : Z] \geqslant 2 \ \therefore |Z| \leqslant 1/2 \cdot |C_G(x)| \ \therefore |Z| \leqslant 1/2 \cdot c$

Usando este último fato em $k < c + |Z|$, segue $k < 3/2 \ \cdot c$

(II) Dado $x \in (G - Z)$, com $Z = 1$, precisamos mostrar que:

$k \ \leqslant |G| \ \cdot [G : C_G(x)]^{-1}$ (ou, de forma equivalente, $k \leqslant |C_G(x)| \leqslant c$).

Mas, no caso específico $Z = 1$, a inequação $k \leqslant c + |Z| - 1$ se reduz a $k \leqslant c$. □

2.7. SUBGRUPO COMUTADOR E SUBGRUPO DERIVADO.

O *comutador* de dois elementos $x, y \in G$ é o elemento $[x, y] = x^{-1}y^{-1}xy$. Dado que $xy = yx[x, y]$, o comutador pode ser visto como uma espécie de "correção" aplicada ao termo yx para que se torne igual a xy. Pela definição, pode-se ainda ver que $[x, y] = 1 \Leftrightarrow x$ e y comutam.

Sejam $H \leqslant G$ e $K \leqslant G$ subgrupos de G:

- $[H, K] = \langle\ [h, k] \mid h \in H \ e \ k \in K\ \rangle$ denota o subgrupo gerado por todos os comutadores de elementos de H com elementos de K e é chamado o *subgrupo comutador* de H e K.
- Em particular, definimos $G' = [G, G] = \langle\ [x, y] \mid x, y \in G\ \rangle$, o chamado *subgrupo derivado* de G (subgrupo gerado por todos os comutadores em G). É interessante notar que $G' = 1 \Leftrightarrow G$ é abeliano.
- Dizemos que H *centraliza* K se $H \leqslant C_G(K)$.
- Dizemos que H *normaliza* K se $H \leqslant N_G(K)$.

Proposição 2.9 (Subgrupo Derivado e Quocientes Abelianos)**.** *Dados um grupo G e seu subgrupo derivado G', tem-se:*

(a) *Dado $N \trianglelefteq G$, o quociente G/N é abeliano se, e somente se, $G' \subseteq N$;*
(b) *Seja $\varphi : G \to A$ um homomorfismo de grupos, em que A é um grupo abeliano. Então $G' \subseteq Ker(\varphi)$;*
(c) *Todo subgrupo H de G que contém G' é normal em G .*

Demonstração. Vide ([16], item 2.23, pg 33) e ([15], item 3.52, pg 59). □

É interessante observar que G' é o menor subgrupo normal N de G tal que G/N é abeliano. O quociente G/G' é chamado *resíduo abeliano* e é o maior quociente abeliano de G.

A Proposição a seguir apresenta uma coletânea de propriedades associadas ao subgrupo comutador. Recorreremos muitas vezes a tais fatos para provar resultados que envolvem os conceitos de um subgrupo *centralizar* ou *normalizar* outro subgrupo. Isso será particularmente importante no estudo do Subgrupo de Fitting Generalizado (Seção 3.2).

Proposição 2.10 (Propriedades do Subgrupo Comutador)**.** *Sejam $H \leqslant G$ e $K \leqslant G$ subgrupos de G. São válidas as seguintes propriedades:*

(a) $[H, K] = [K, H]$;
(b) *H centraliza K se, e somente se,* $[H, K] = 1$;
(c) *H normaliza K se, e somente se,* $[H, K] \leqslant K$;
(d) *Se $H \leqslant G$ e $K \trianglelefteq G$, então* $[H, K] \leqslant K$;
(e) *Se $H, K \trianglelefteq G$, então* $[H, K] \leqslant H \cap K$. *Além disso, se $H \cap K = 1$, então* $H \leqslant C_G(K)$;
(f) $H \subseteq N_G([H, K])$, *ou seja, H normaliza o subgrupo* $[H, K]$;
(g) *Sejam $K \leqslant H \leqslant G$ com $K \trianglelefteq G$. Então* $[H, G] \leqslant K$ *se, e somente se,* $H/K \leqslant Z(G/K)$;
(h) *Se $H, K \leqslant G$ e $\varphi : G \to L$ é homomorfismo, então* $\varphi([H, K]) = [\varphi(H), \varphi(K)]$;
(i) *(Lema dos 3 Subgrupos) - Sejam dados três subgrupos $H, K, L \leqslant G$, que satisfazem* $[H, K, L] = 1$ *e* $[K, L, H] = 1$. *Então vale* $[L, H, K] = 1$.

Demonstração. Vide, por exemplo, ([16], pg 112) e ([9], item 4.9, pg 126). □

Vale atentar para alguns casos particulares interessantes do item (g):
(I) $[G, G] \leqslant K$ se, e somente se, $G/K \leqslant Z(G/K)$. Dado que a inclusão reversa é sempre verdadeira, segue $G' \leqslant K \Leftrightarrow G/K$ é abeliano. (vide Proposição 2.9)
(II) Fazendo agora $K = Z(G)$, segue $G' \leqslant Z(G) \Leftrightarrow G/Z(G)$ é abeliano. Vemos ainda que se $G/Z(G)$ é não-abeliano, então $G' \nsubseteq Z(G)$.

Proposição 2.11. *Dados os grupos G e K, seja H um subgrupo de G. São válidas as seguintes propriedades:*

(a) $H \leqslant G \Rightarrow H' \leqslant G'$;
(b) $\varphi : G \to K$ *é homomorfismo* $\Rightarrow \varphi(G') \leqslant K'$;
(c) $\varphi : G \to K$ *é homomorfismo sobrejetivo* $\Rightarrow \varphi(G') = K'$.

Demonstração. Vide, por exemplo, ([16], item 5.30, pg 112). □

3. A CAMINHO DO TEOREMA DE BENDER

3.1. GRUPOS NILPOTENTES E SOLÚVEIS.

Uma *série normal* de um grupo G é uma seqüência finita de subgrupos normais ($G_i \trianglelefteq G$) tais que $1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G$. Cada quociente G_{i+1}/G_i é denominado um *grupo fator* da série. O comprimento da série normal é o número de inclusões estritas, ou seja, o número de fatores não-triviais.

Uma *série abeliana* ou *série solúvel* para um grupo G é uma série normal, cujos grupos fatores (G_{i+1}/G_i) são abelianos.

Uma *série central* para um grupo G é uma série normal, cujos fatores satisfazem:

$$\frac{G_{i+1}}{G_i} \leqslant Z\Big(\frac{G}{G_i}\Big)\ ,\ \forall i \in \{0, 1, \ldots, n-1\}\ .$$

Um grupo é dito *solúvel* quando possui uma série solúvel.
Um grupo é dito *nilpotente* quando possui uma série central.

Complementamos essa revisão inicial sobre grupos nilpotentes e solúveis, apresentando uma coletânea de termos que serão relevantes no desenvolvimento dos demais tópicos tratados nesse texto:

- Um subgrupo $S \leqslant G$ é dito *subnormal* em G se existir uma série finita de subgrupos $H_i \leqslant G$ tais que $S = H_0 \lhd H_1 \lhd \cdots \lhd H_r = G$.

- Um subgrupo próprio $M < G$ é dito um *subgrupo maximal* de G se não existe subgrupo L tal que $M < L < G$. ($M < G$ é dito maximal se, sempre que $M \leqslant H \leqslant G$, então $H = M$ ou $H = G$).

- Para um grupo finito G, define-se o subgrupo de Frattini, $\Phi(G)$, como a interseção de todos os subgrupos maximais de G.

  $$\Phi(G) = \bigcap_{M max G} M\ .$$

  Um elemento $x \in G$ é dito um *não-gerador* se pode ser omitido de qualquer conjunto de geradores de G . Dessa forma, se x é um não gerador de G, vale: $G = \langle x, Y\rangle \Rightarrow G = \langle Y\rangle$.

  O subgrupo de Frattini de um grupo G é característico em G e pode ser definido, de forma equivalente, como o conjunto de elementos de G que são *não-geradores*.

- O *subgrupo de Fitting* de G, denotado por $F(G)$, é o subgrupo característico gerado por todos os subgrupos normais nilpotentes de G.

$$F(G) = \langle\, M \leqslant G \mid M \trianglelefteq G \text{ e } M \text{ é nilpotente} \,\rangle\,.$$

Quando G é um grupo finito, demonstra-se que $F(G)$ é o maior subgrupo normal nilpotente de G (vide [9], item 1.28, pg 26).

- Dado um subgrupo $H \leqslant G$, o *normal core* de H em G é o seguinte subgrupo normal:

$$core_G(H) = \bigcap_{x \in G} H^x \trianglelefteq G\,.$$

O normal core de H em G é o maior subgrupo normal de G contido no subgrupo H.

- A interseção de todos os p-subgrupos de Sylow de um grupo G é denominada o p-core de G. Se p é um primo e $P \in Syl_p(G)$, então:

$$O_p(G) = \bigcap Syl_p(G) = \bigcap_{x \in G} P^x = core_G(P)\,.$$

O p-core de G é o maior p-subgrupo normal de G.

- Sendo p um primo que divide a ordem de um grupo G, o subgrupo de Fitting pode também ser caracterizado da seguinte forma:

$$F(G) = \prod_{p\ divide\ |G|} O_p(G)\,.$$

- Seja K um subgrupo tal que $1 < K \trianglelefteq G$. Então K é dito um subgrupo *normal minimal* de G se não existir subgrupo normal L de G tal que $1 < L < K$. (K tem a propriedade de minimalidade dentre todos os subgrupos normais não-triviais). Vale notar que, à exceção do grupo trivial, todos os grupos finitos possuem subgrupos normais minimais. Além disso, se G é simples, então G é um subgrupo normal minimal de G.

- O *socle* de um grupo finito G, denotado $Soc(G)$, é o subgrupo característico gerado por todos os subgrupos normais minimais de G :

$$Soc(G) = \langle\, M \leqslant G \mid M \text{ é normal minimal} \,\rangle\,.$$

Pode-se mostrar que o socle é o produto direto de alguns desses subgrupos normais minimais ([14], pg 87). Vale notar que, para qualquer G finito, todo subgrupo normal não-trivial $1 < N \trianglelefteq G$ contém um subgrupo normal minimal de G , garantindo que $N \cap Soc(G) > 1$.

Proposição 3.1. *Sendo G um grupo não-trivial, são válidos os seguintes fatos:*

(a) *Se $K \leqslant M < G$ e $K \trianglelefteq G$, então: M/K é um subgrupo maximal de G/K se, e somente se, M é um subgrupo maximal de G.*
(b) *Se G é finito, então todo subgrupo próprio de G está contido em algum subgrupo maximal de G.*
(c) *Se $M < G$ e $[G:M] = p$ (primo), então M é um subgrupo maximal de G.*
(d) *Se G é finito, então G possui um único subgrupo maximal se, e somente se, G é cíclico e $|G| = p^m$ (para algum primo p e algum inteiro positivo m).*

Demonstração. Veja [15], item 140, pg 51. □

Proposição 3.2. *Algumas propriedades de Grupos Nilpotentes.*

(a) *Grupos nilpotentes não-triviais possuem centros não-triviais.*
(b) *Cada termo de uma série central de um grupo nilpotente está contido em algum termo da série central ascendente de tal grupo. Em particular, sendo G nilpotente, G é um termo de sua série central ascendente.*
(c) *Grupos abelianos não-triviais possuem classe de nilpotência $r = 1$.*
(d) *Os grupos G que possuem classe de nilpotência $r = 2$ são os grupos não-abelianos em que o quociente $G/Z(G)$ é abeliano.*
(e) *Todo subgrupo próprio de um grupo nilpotente está propriamente contido em seu normalizador.*
(f) *Seja G um grupo nilpotente. Se o subgrupo $N \trianglelefteq G$ é não-trivial, então $N \cap Z(G) \neq 1$. Em particular, todo subgrupo normal minimal de G está contido no centro de G e possui ordem prima.*
(g) *Todo subgrupo maximal de um grupo nilpotente G é normal em G e possui índice primo.*
(h) *Seja $H \leqslant Z(G)$. Se o quociente G/H é nilpotente, então G é nilpotente. Em particular, se $G/Z(G)$ é nilpotente, G também o é.*
(i) *p-grupos finitos são nilpotentes.*
(j) *Para G finito, $\Phi(G)$ é nilpotente.*

Demonstração. As demonstrações dos fatos gerais reunidos na Proposição podem ser obtidas, por exemplo, em ([9], cap 1), ([14], cap 5) e ([16], cap 5). □

Proposição 3.3. *Caracterização de Grupos Nilpotentes Finitos.*

Para um grupo G finito as seguintes condições são equivalentes:

(a) *G é nilpotente.*
(b) *$H < N_G(H)$ para todo subgrupo próprio $H < G$.*
(c) *Todo subgrupo maximal de G é normal.*
(d) *$G' \leqslant \Phi(G)$.*
(e) *Todo subgrupo de Sylow de G é normal.*
(f) *G é o produto direto (interno) de de seus subgrupos de Sylow não-triviais.*

Demonstração. A demonstração dessas variadas maneiras de caracterizar grupos nilpotentes finitos pode ser encontrada, por exemplo, em ([12], item 5.12, pg 214). □

Proposição 3.4. *Para um grupo finito G valem as seguintes propriedades:*

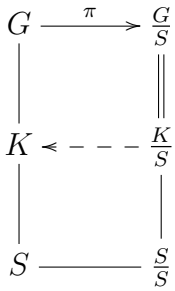
(a) *G possui um único subgrupo solúvel normal maximal (subgrupo maximal dentre os que são normais e solúveis). Tal grupo é denominado o radical solúvel de G e denotado por sol(G).*
(b) *$G/sol(G)$ não contém subgrupos solúveis normais não triviais. Além disso, tem-se $sol(G/sol(G)) = 1$.*

Demonstração. (a) Seja $S \trianglelefteq G$ um subgrupo solúvel de G com a maior ordem possível e consideremos $N \trianglelefteq G$ tal que N é solúvel. Temos $SN \trianglelefteq G$ e, pela combinação dos fatos a seguir, o produto SN é solúvel:

- $SN/N \cong S/(N \cap S)$;
- $S/(N \cap S)$ é solúvel (quociente do solúvel S);
- O subgrupo $N \trianglelefteq G$ é solúvel (hipótese).

Pela maximalidade de S, segue $|SN| \leqslant |S|$. Dado que $S \leqslant SN$, resulta $S = SN$. Por outro lado, $N \leqslant SN$ e, portanto, $N \leqslant SN = S$. Mas isso significa que S contém todos os subgrupos normais solúveis de G.

(b) Seja $S = \text{sol}(G)$ o radical solúvel de G e admitamos a existência de um subgrupo $K/S \trianglelefteq G/S$ que seja solúvel normal não-trivial. Sendo S e K/S solúveis, segue que K é solúvel. Com uma tal construção, ao subgrupo $K/S \trianglelefteq G/S$ corresponde um subgrupo $K \trianglelefteq G$ (com K solúvel). Mas, pela maximalidade de S, segue $K \leqslant S$. Por outro lado, sendo $S \trianglelefteq K$, vem $K/S = 1$, o que significa que o subgrupo K/S de G/S é trivial.



Uma conseqüência de (b) é que o radical solúvel do quociente $G/\text{sol}(G)$ é trivial, ou seja, $\text{sol}(G/\text{sol}(G)) = 1$. □

Proposição 3.5. *Para um grupo finito G valem as seguintes propriedades:*

(a) *Um subgrupo normal minimal de um grupo finito solúvel G é um p-grupo abeliano elementar para algum primo p.*
(b) *G é nilpotente se, e somente se, todo subgrupo de G é subnormal.*
(c) *Se S é subnormal em G e M é um subgrupo normal minimal de G, então $M \leqslant N_G(S)$.*

Demonstração. As demonstrações dos resultados compilados em tal Proposição, podem ser obtidas em:

(a) ([12], item 5.46, pg 239).
(b) ([9], item 2.1, pg 46).
(c) ([9], item 2.6, pg 48).

□

Proposição 3.6. *Para um grupo finito G valem as seguintes propriedades:*

(a) $\Phi(G) \leqslant F(G)$ *e* $Z(G) \leqslant F(G)$.
(b) *Sejam G um grupo finito e N um subrupo tal que $\Phi(G) \leqslant N \trianglelefteq G$. Então: N é nilpotente $\Leftrightarrow N/\Phi(G)$ é nilpotente.*
(c) $F(G)/\Phi(G) = F(G/\Phi(G))$.
(d) $F(G)/Z(G) = F(G/Z(G))$.
(e) *$F(G)$ centraliza todos os subgrupos normais minimais de G.*
(f) *Se G é um grupo finito solúvel, então um subgrupo normal minimal de G está contido no centro de F(G). Além disso, a interseção de um subgrupo normal não-trivial de G com $F(G)$ é não-trivial.*
(g) *Versão do Teorema de Bender para Grupos Solúveis.*
Se G é um grupo finito solúvel, então $C_G(F(G)) \leqslant F(G)$.

Demonstração. (a) O subgrupo característico $\Phi(G)$ é nilpotente para G finito (Proposição 3.2). Usando o fato de $F(G)$ ser gerado pelos subgrupos normais nilpotentes de G, segue $\Phi(G) \leqslant F(G)$. Por outro lado, lembrando que o centro é um subgrupo nilpotente (por ser abeliano) e que $Z(G)$ char G, segue $Z(G) \leqslant F(G)$.

(b) ($\Rightarrow$) Quocientes de grupos nilpotentes são nilpotentes.

($\Leftarrow$) Mostraremos que um p-subgrupo de Sylow arbitrário $P \in Syl_p(N)$ é normal em N, pois isso garante que o grupo finito N é nilpotente (vide Proposição 3.3). Sendo $\Phi(G) \trianglelefteq N$, segue $P\Phi(G) \leqslant N$ e $(P\Phi(G))/\Phi(G) \in Syl_p(N/\Phi(G))$.

$N/\Phi(G)$ é nilpotente (por hipótese), logo $(P\Phi(G))/\Phi(G) \trianglelefteq N/\Phi(G)$. Dado que um Sylow normal é característico, vem $(P\Phi(G)/\Phi(G))$ char $N/\Phi(G)$. Mas $N/\Phi(G) \trianglelefteq G/\Phi(G)$ e, portanto, $(P\Phi(G)/\Phi(G)) \trianglelefteq G/\Phi(G)$.

O Teorema da Correspondência fornece $P\Phi(G) \trianglelefteq G$. Notando que P é um subgrupo de $Syl_p(P\Phi(G))$, recorremos ao *Argumento de Frattini*, para concluir

que $G = N_G(P)(P\Phi(G))$. Sendo $P \trianglelefteq N_G(P)$, vem $G = N_G(P)\Phi(G)$ e, pela caracterização de $\Phi(G)$ como conjunto dos elementos não-geradores de G, vem $G = N_G(P)$. Assim, $P \trianglelefteq G$ e $P \trianglelefteq N$, evidenciado que um qualquer p-Sylow P de N é normal em N, como queríamos.

(c) Temos $\Phi(G) \trianglelefteq F(G) \trianglelefteq G$. Considerando o quociente por $\Phi(G)$, vemos que $F(G)/\Phi(G)$ é normal em $G/\Phi(G)$ e nilpotente (quociente do nilpotente, $F(G)$). Além disso, $F(G)/\Phi(G) \subseteq F(G/\Phi(G))$, por ser este último o maior subgrupo normal nilpotente em $G/\Phi(G)$.

Provaremos agora a inclusão contrária. Seja $K/\Phi(G) = F(G/\Phi(G)) \trianglelefteq G/\Phi(G)$. Tal subgrupo é normal e nilpotente, pela definição do Fitting. A esse $K/\Phi(G)$ corresponde o subgrupo normal $K \trianglelefteq G$. Considerando que $\Phi(G) \leqslant K \trianglelefteq G$ e sendo $K/\Phi(G)$ nilpotente, usamos (b) para concluir que K é nilpotente. Assim, o subgrupo K é normal em G e nilpotente, o que garante $K \leqslant F(G)$.

Unindo os dois resultados, obtemos a tese: $F(G/\Phi(G)) = K/\Phi(G) \leqslant F(G)/\Phi(G)$.

(d) Por (a), sabemos que $Z(G) \trianglelefteq F(G) \trianglelefteq G$. Temos $F(G)/Z(G) \trianglelefteq G/Z(G)$ (correspondência). Além disso, sendo $F(G)$ nilpotente, o quociente $F(G)/Z(G)$ também o é. Por definição do subgrupo de Fitting, temos $F(G)/Z(G) \subseteq F(G/Z(G))$.

Mostremos agora a inclusão contrária. $F(G/Z(G)) \trianglelefteq G/Z(G)$ e sabemos que o Fitting $F(G/Z(G))$ é nilpotente. Por outro lado, $F(G/Z(G))$ é um subgrupo normal da forma $M/Z(G)$ e a ele corresponde um subgrupo $M \trianglelefteq G$. Mas sabemos (pela Proposição 3.2) que se $M/Z(G)$ é nilpotente, então M também o é. Assim, o subgrupo M é normal em G e nilpotente, logo $M \leqslant F(G)$. Segue $F(G/Z(G)) = M/Z(G) \subseteq F(G)/Z(G)$, concluindo a prova.

(e) Dados os subgrupos $N, H \trianglelefteq G$, sejam N normal minimal e H normal e nilpotente. Temos dois cenários a analisar:

Caso 1: $N \cap H = 1$. Nessa situação, os elementos de N comutam com os elementos de H e, portanto, H centraliza N.

Caso 2: $N \cap H \neq 1$. Sendo N normal minimal e H normal, segue $N \leqslant H$. Dado que o grupo nilpotente H é não-trivial, segue $N \cap Z(H) \neq 1$ (conforme Proposição 3.2). $Z(H)$ char H e $H \trianglelefteq G$, logo $Z(H) \trianglelefteq G$. Em decorrência da minimalidade de N, segue $N \leqslant Z(H)$, logo H centraliza N.

Isso completa a prova de que qualquer subgrupo normal nilpotente centraliza um subgrupo normal minimal arbitrário e, pela definição de $F(G)$, deduz-se a tese.

(f) Façamos $F = F(G)$ e $Z = Z(G)$.

Seja N um subgrupo normal minimal de G. Sendo G finito e solúvel, a Proposição 3.5 garante que N é um p-grupo abeliano elementar (para algum primo p). Sendo um p-grupo finito, N é nilpotente. Pela definição do Fitting, segue $N \leqslant F$. Sendo $1 < N \leqslant G$ (normal minimal é não-trivial), segue F não-trivial. Pela Proposição 3.2, o centro, $Z(F)$, do nilpotente não-trivial, F, é também não-trivial.

Se N é subgrupo normal não-trivial do grupo nilpotente F, vale $N \cap Z(F) \neq 1$ (Proposição 3.2). Em particular, sendo N normal minimal em G e $Z(F) \trianglelefteq G$ (pois $Z(F)$ char F e $F \trianglelefteq G$) , segue $N \leqslant Z(F)$.

Para provar a segunda afirmação, tomemos um grupo $M \trianglelefteq G$, não-trivial e selecionemos um subgrupo N, normal minimal, tal que $N \leqslant M$. Mostramos, na primeira parte, que $1 < N \cap Z(F) \leqslant N \leqslant F$. Assim, $1 < N \cap Z(F) \leqslant N \leqslant F \cap M$, o que evidencia que a interseção do normal M com F é não-trivial.

(g) Sejam $F = F(G)$, $C = C_G(F)$ e $Z = Z(F)$. Se mostrarmos que C/Z é trivial, ficará demonstrada a tese.

Notemos, inicialmente, que se G é solúvel, então seu subgrupo C e o quociente C/Z também são solúveis.

Admitamos, por contradição, que $C/Z \neq 1$ e seja M/Z um subgrupo normal minimal de C/Z. Temos $Z < M \leqslant C$ e, pela Proposição 3.5, M/Z é p-grupo abeliano elementar e, portanto, nilpotente.

Sendo $M \leqslant C = C_G(F)$, temos, $F \leqslant C_G(M)$ e $Z \leqslant C_G(M)$. Mas $Z \leqslant M$ e, portanto, $Z \leqslant C_G(M) \cap M = Z(M)$. Usando tal informação em conjunto com o fato de M/Z ser abeliano, temos $M/Z(M)$ é abeliano. Recorrendo à Proposição 3.2, obtemos que M é nilpotente. Daí segue que $M \leqslant F(C)$.

Dado que $F \trianglelefteq G$, temos que $C = C_G(F) \trianglelefteq G$. Mas $F(C)$ char C e, portanto, $F(C) \trianglelefteq G$. Lembrando que $F(C)$ é nilpotente, segue $F(C) \leqslant F$. Assim, $M \leqslant F(C) \leqslant F$. Observando que $M \leqslant C$, segue $M \leqslant F \cap C = Z(F) = Z$. Entretanto, isso contradiz a escolha de M . □

3.2. O SUBGRUPO DE FITTING GENERALIZADO.

Vimos na Proposição 3.6 que, no caso específico em que G é um grupo finito solúvel, o subgrupo de Fitting de G, $F(G)$, contém seu próprio centralizador (ou seja, $C_G(F(G)) \leqslant F(G)$). A definição do subgrupo de Fitting generalizado, $F^*(G)$, que será apresentada mais adiante, permite que se formule uma inclusão similar ($C_G(F^*(G)) \leqslant F^*(G)$), conhecida como o *Teorema de Bender* (Proposição 3.13), para o caso de um grupo finito que não seja, necessariamente, solúvel.

Para facilitar referências futuras, registramos a seguir uma série de definições que tratam, principalmente, de subgrupos característicos e de algumas classes (não tão usuais) de grupos. Convém mencionar que, numa tentativa de evitar ambigüidades técnicas, optou-se por não traduzir os termos *quasisimple* e *almost simple*.

- Dado um grupo finito G, consideremos pares de grupos (X,Y) que verifiquem $Y \leqslant Z(X)$ e $X/Y \cong G$. Nessas condições, diz-se que X é uma *extensão central* de G.

- Um grupo é dito *perfeito* se coincide com o seu subgrupo derivado, o que equivale a dizer que não possui nenhum quociente abeliano não-trivial. Todo grupo finito *não-solúvel* contém um subgrupo característico não-trivial que é perfeito. Por outro lado, se um grupo G possui um subgrupo perfeito não-trivial, G é não-solúvel.
- Um grupo G é dito *quasisimple* se é perfeito e o quociente $G/Z(G)$ é simples. De forma equivalente, um grupo é quasisimple se, além de ser perfeito, é uma extensão central de um grupo simples. É interessante ainda notar que todo grupo não-abeliano simples é quasisimple.
- Um subgrupo subnormal quasisimple de um grupo finito arbitrário G é denominado um *componente* de G.
- Denomina-se *layer* de G, e denota-se por $E(G)$, o subgrupo gerado por todos os componentes de G. $E(G) = \langle\ H : H \text{ é componente de } G\ \rangle$. A Proposição 3.9 demonstra que dois distintos componentes de um grupo finito se centralizam e, portanto, são normais no subgrupo $E(G)$, por eles gerado. Quando G não possui componentes, define-se $E(G) = 1$.
- Dado um grupo finito G, definimos o *subgrupo de Fitting generalizado* por meio da relação: $F^*(G) = F(G)E(G)$
- Um grupo G é dito *semi-simples* quando é um produto de subgrupos normais simples não-abelianos (os quais são quasisimple). Um grupo semi-simples não possui subgrupos normais abelianos não-triviais e pode ser expresso como um produto direto de grupos simples não-abelianos.
- Um grupo G é dito *almost simple* se existe um subgrupo normal simples não-abeliano $N \trianglelefteq G$ cujo centralizador $C_G(N)$ é trivial.

  Equivalentemente, G é *almost simple* se existe um subgrupo simples não-abeliano S e que satisfaz $S \leqslant T \leqslant \mathrm{Aut}(S)$ para algum grupo $T \cong G$.

Proposição 3.7. *Dado um grupo finito G em que o quociente $G/Z(G)$ é simples, são válidos os seguintes fatos:*

(a) *O quociente $G/Z(G)$ é não-abeliano.*
(b) *O subgrupo derivado, G', é perfeito.*
(c) $G'/Z(G') \cong G/Z(G)$.
(d) *G' é quasisimple.*

Demonstração. Recordemos dois fatos básicos antes de começar a demonstração:

(I) Todo subgrupo de um grupo abeliano é normal. Dessa forma, um grupo abeliano simples não pode conter nenhum subgrupo não-trivial. Isso nos permite concluir que *um grupo abeliano simples é cíclico de ordem prima.*

(II) *Se G é não-abeliano, então $G/Z(G)$ não é cíclico.* Para validar tal afirmação, admitamos que o quociente $G/\mathrm{Z}(G)$ seja cíclico e seja $\overline{a}$ um gerador de tal grupo. Sejam x e y dois elementos quaisquer de G. Então $x = a^i \cdot z_1$ e $y = a^j \cdot z_2$ para

convenientes $i, j \geqslant 0$ e $z_1, z_2 \in \mathrm{Z}(G)$. Daí segue $xy = (a^i \cdot z_1)(a^j \cdot z_2) = a^{i+j} z_1 z_2 = a^{j+i} z_2 z_1 = a^j z_2 a^i z_1 = yx$ ($\therefore$ G é abeliano, o que contraria a hipótese).

(a) Seja $Z = \mathrm{Z}(G)$. Se o grupo simples G/Z fosse abeliano, então deveria, de acordo com a observação (I), ser cíclico. Mas G/Z cíclico obrigaria G abeliano ($\therefore$ $Z = G$), conforme (II), contrariando a hipótese G/Z simples. Assim, G/Z é um grupo simples não-abeliano (donde decorre $G' \nsubseteq \mathrm{Z}(G)$, conforme Proposição 2.10).

(b) Se G fosse solúvel, o quociente (não-abeliano) G/Z seria solúvel. Dado que G/Z é simples, sua série solúvel se reduziria a $1 \leqslant G/Z$, o que implicaria G/Z abeliano (contrariando a hipótese). Concluímos que G é não-solúvel, o que garante $G''' \neq 1$. Segue que G'' é não-abeliano e, portanto, $G'' \nsubseteq \mathrm{Z}(G)$.

Sendo G/Z simples e não-abeliano, o Teorema da Correspondência nos garante que Z é normal maximal. Usando o fato $G'' \nsubseteq \mathrm{Z}(G)$, vem $G''Z > Z$. Sendo $G''Z \trianglelefteq G$, a maximalidade do subgrupo normal Z impõe $G''Z = G$. Resulta:

$$\frac{G}{G''} = \frac{G''Z}{G''} \cong \frac{Z}{(Z \cap G'')}$$

Sendo Z abeliano, segue G/G'' abeliano. Pela Proposição 2.9, isso só pode ocorrer se o subgrupo $G'' \trianglelefteq G$ for tal que $G' \subseteq G''$. Dado que a inclusão reversa é sempre válida, resulta $G'' = G'$ e, por definição, G' é perfeito.

(c) Usando o fato $G'' = G'$, obtém-se $G'Z = G$. Além disso:

$$\frac{G'}{(Z \cap G')} \cong \frac{G'Z}{Z} = \frac{G}{Z}, \text{ o que mostra que o quociente } \frac{G'}{(Z \cap G')} \text{ é simples.}$$

Segue que $(Z \cap G')$ é subgrupo normal maximal de G' e, conseqüentemente, $\mathrm{Z}(G') \leqslant Z \cap G'$. Por definição $(Z \cap G')$ é o conjunto dos elementos de G' que comutam com todos os elementos de G. Em particular, os elementos de tal conjunto comutam com os elementos de G'. Daí $(Z \cap G') \leqslant \mathrm{Z}(G')$ e decorre $(Z \cap G') = \mathrm{Z}(G')$. Finalmente:

$$\frac{G'}{Z(G')} = \frac{G'}{(Z \cap G')} \cong \frac{G'Z}{Z} = \frac{G}{Z} = \frac{G}{Z(G)}$$

(d) Sendo G' perfeito e $G'/\mathrm{Z}(G')$ simples, tem-se, por definição, que G' é quasisimple.

□

Proposição 3.8. *Seja G um grupo quasisimple. São válidos os seguintes fatos:*

(a) *Se $N \lhd G$ (inclusão própria), então $N \leqslant Z(G)$.*
(b) *Toda imagem homomórfica não-trivial de G é quasisimple.*

Demonstração. (a) Façamos $Z = \mathrm{Z}(G)$. Sendo G quasisimple, temos G perfeito e $G/Z(G)$ não-abeliano simples ($\therefore$ Z é normal maximal). Consideremos um subgrupo normal próprio $N \lhd G$. Admitindo-se $N \nsubseteq Z$, deve-se ter $NZ > Z$ e, pela maximalidade de Z, isso implica $NZ = G$. Resulta:

$$\frac{G}{N} = \frac{NZ}{N} \cong \frac{Z}{(N \cap Z)}.$$

A última relação garante que G/N é abeliano (por ser isomorfo a um quociente de $Z = Z(G)$). Pela Proposição 2.9 isso só pode ocorrer se $G' \subseteq N$. Unindo tal informação à hipótese de G ser perfeito, obtém-se $G = G' \subseteq N < G$. Tal contradição mostra que se deve ter $N \leqslant Z(G)$.

(b) Sendo $N \lhd G$ (normal próprio), G/N é uma imagem homomórfica não-unitária de G. Vamos mostrar que G/N é quasisimple.

(I) Dado que o homomorfismo canônico é sobrejetivo, a Proposição 2.11 nos assegura que $G'/N = (G/N)'$. Usando o fato de G ser perfeito, escrevemos:

$$\frac{G}{N} = \frac{G'}{N} = \left(\frac{G}{N}\right)', \text{ evidenciando que } G/N \text{ é perfeito.}$$

(II) Considerando que $Z(G)$ contém N, temos:

$$\frac{(G/N)}{(Z/N)} \cong \frac{G}{Z}$$

Sendo G quasisimple, tem-se que G/Z é simples não-abeliano. Dessa forma, o primeiro quociente na expressão acima também o é.

Por outro lado, sendo $x \in Z$, tem-se $xN \cdot gN = xgN = gxN = gN \cdot xN, \forall g \in G$. Assim, uma classe lateral $xN \in Z/N$ comuta com qualquer classe lateral gN de G/N, mostrando que $Z/N \subseteq Z(G/N)$.

Mas o fato de $\dfrac{(G/N)}{(Z/N)}$ ser simples impõe $Z/N = Z(G/N)$. Resulta:

$$\frac{(G/N)}{Z(G/N)} = \frac{(G/N)}{(Z/N)} \cong \frac{G}{Z} \text{ , mostrando que o quociente } \frac{(G/N)}{Z(G/N)} \text{ é simples.}$$

□

É interessante notar que há dois aspectos envolvidos na definição de um subgrupo componente, K, de um grupo G:

- Ser quasisimple é uma propriedade intrínseca ao subgrupo e não depende do grupo ambiente.
- Ser subnormal descreve como o subgrupo K se insere em G.

Dessa forma, os componentes tendem a compartilhar algumas propriedades dos subgrupos subnormais. Por exemplo, temos:

- Se K é um componente de G tal que $K \leqslant L \leqslant G$, então K é também um componente de L. (Basta notar que se S é subnormal em G e $Q \leqslant G$ é um subgrupo arbitrário então $S \cap Q$ é subnormal em Q).
- Se S é subnormal em G e K é um componente de S então K é componente de G. (Decorre do fato de a subnormalidade ser transitiva).

Proposição 3.9. *Seja G um grupo finito.*

(a) *Se N é um subgrupo normal minimal de G e H é um componente de G tal que $H \nsubseteq N$, então $[N, H] = 1$.*
(b) *Se H e K são componentes distintos de G, então $[H, K] = 1$. (De forma equivalente, dizemos que dois componentes de G se centralizam).*

Demonstração. (a) Levando em conta que $H \nsubseteq N$, obtemos $(H \cap N) < H$ e $(H \cap N) \lhd H$. Usando a Proposição 3.8, segue $(H \cap N) \subseteq \mathrm{Z}(H)$. Sendo H subnormal em G e N normal minimal em G, pode-se mostrar que $N \subseteq N_G(H)$ (vide, por exemplo, [9], item 2.6, pg 48). Isso significa que N normaliza H e $[N,H] \leqslant H$ (conforme Proposição 2.10). Dado que $N \trianglelefteq G$, a mesma Proposição garante que $[N,H] \leqslant N$, donde $[N,H] \leqslant (N \cap H) \leqslant \mathrm{Z}(H) \leqslant C_G(H)$. Isso equivale a dizer que $[N,H]$ centraliza H, acarretando $[[N,H],H] = 1$. Lembrando que $[N,H] = [H,N]$, vem $[[H,N],H] = 1$. Recorrendo ao Lema dos 3 subgrupos, escrevemos $[[H,H],N] = 1$ ou, equivalentemente, $[H', N] = 1$. Usando o fato de H ser perfeito, obtém-se $[H,N] = 1$.

(b) Vamos utilizar indução sobre $|G|$. Nossa hipótese indutiva é que o resultado é válido para qualquer grupo cuja ordem é inferior à de G. Se H e K estão ambos contidos em algum subgrupo próprio $X < G$, então eles são componentes distintos de X. Aplicando a hipótese de indução a X, segue $[H, K] = 1$.

Assumimos agora que nenhum subgrupo próprio de G contenha, simultaneamente, H e K. Se G fosse simples, então os subgrupos H e K, sendo não-triviais e subnormais em G, coincidiriam com G. Mas isso não ocorre, permitindo-nos afirmar que G não é simples. Sendo G não-trivial, G contém um subgrupo normal minimal N. Um tal N é próprio e, por hipótese, não contém, ao mesmo tempo, H e K. Digamos que $K \leqslant N$ e $H \nsubseteq N$. Pelo item (a), temos $[H, N] = 1$. Por outro lado, dado que $K \leqslant N$, segue $[H, K] \subseteq [H, N] = 1$.

Consideremos agora o cenário em que $H \nleq N$ e $K \nleq N$ para qualquer normal minimal N. Denotemos por $\overline{G}$ o quociente G/N. Os subgrupos $\overline{H} = HN/N$ e $\overline{K} = KN/N$ são imagens homomórficas não-triviais, respectivamente, dos componentes H e K. Segue, pela Proposição 3.8, que ambos são *quasisimple*. Unindo tal conclusão ao fato desses subgrupos serem subnormais em $\overline{G}$, resulta que são componentes de $\overline{G}$. Se $\overline{H} \neq \overline{K}$, obtemos $[\overline{H}, \overline{K}] = 1$, aplicando a hipótese de indução ao grupo $\overline{G}$ (cuja ordem é menor que $|G|$). Além disso, $\overline{[H, K]} = 1$ (Proposição 2.10) e, portanto, $[H, K] \leqslant N$. Recorrendo ao item (a), obtemos $[N, H] = 1$. Assim, $[H, K, H] = 1$ e $[K, H, H] = 1$ e, aplicando o Lema dos 3 Subgrupos, obtemos $[H, H, K] = 1$. Sendo $H = [H, H]$, pois H é quasisimple, vem $[H, K] = 1$.

O caso ainda não tratado é $\overline{H} = \overline{K}$, o que equivale a $HN = KN$. Podemos assumir que a última equação vale para qualquer escolha de N normal minimal em G, pois, se tivéssemos $HN \neq KN$, recairíamos no caso anterior. Observemos agora que HN contém os componentes H e K, donde segue $HN = G$ (pois partimos da hipótese que nenhum $Y < G$ próprio contém H e K). Aplicamos o resultado em ([9], item 2.6, pg 48) aos subgrupos N (normal minimal) e H (subnormal em G), o que nos permite concluir que $N \leqslant N_G(H)$. Sendo $H \trianglelefteq N_G(H)$, segue $HN \leqslant N_G(H)$. Mas $N_G(H) \leqslant G = HN$ e resulta $H \trianglelefteq G$. Por argumento idêntico, obtemos $K \trianglelefteq G$ e recorrendo à Proposição 2.10, vemos que $[H, K] \leqslant H \cap K$. Supondo, por absurdo, que $[H, K]$ fosse não-trivial, poderíamos escolher um normal minimal N contido em $H \cap K$ e isso acarretaria $H = HN = KN = K$. Mas esse não é o caso, pois, por hipótese, os componentes H e K são distintos. Fica, então, claro que o erro foi admitir $[H, K] \neq 1$, não restando outra opção além de $[H, K] = 1$. Isso completa a demonstração. □

Proposição 3.10. *Sejam G um grupo finito e $\mathcal{F}$ uma família de subgrupos normais simples não-abelianos de G. Se G é o produto dos membros de $\mathcal{F}$, então tal produto é direto e $\mathcal{F}$ é o conjunto de todos os subgrupos normais minimais de G.*

Demonstração. vide [9], item 9.5, pg 274. □

Proposição 3.11. *Se N é um subgrupo normal minimal de G, então N é abeliano ou N é semi-simples.*

Demonstração. Seja S um subgrupo normal minimal em N. Temos $1 < S \trianglelefteq N$.

Se S é abeliano, então S é nilpotente e, portanto, $S \leqslant F(N)$. Temos que $F(N)$ é normal em G e não-trivial (por conter S). Assim, o subgrupo $F(N) \trianglelefteq G$ é tal que $1 < F(N) \trianglelefteq N$ (com N normal minimal). Isso impõe $F(N) = N$. Mas, por definição, $F(N)$ é o maior normal nilpotente de N e daí segue que N é nilpotente. Sendo N não-trivial, decorre da Proposição 3.2 que $Z(N) > 1$. Sendo $Z(N) \trianglelefteq G$

(com $Z(N) \subseteq N$), segue, pela minimalidade de N, que $Z(N) = N$, permitindo concluir que N é abeliano.

Assumindo, agora, S não-abeliano, afirmamos que S deve ser simples. Se $K \lhd S$ e K subnormal em G, então o normal minimal N normaliza K (vide [9], item 2.6, pg 48). Assim $K \lhd S \trianglelefteq N \leqslant N_G(K)$, donde segue $K \lhd N$. Mas S é normal minimal em N, obrigando $K = 1$ ou $K = S$, permitindo concluir que S é simples.

Consideremos agora o caso específico em que S é não-abeliano simples. Nessa situação, cada conjugado, S^g, de S em G é também um subgrupo simples não-abeliano e tal que $S^g \trianglelefteq N$. Segue que o produto $S^G = \langle\ S^g \mid g \in G\ \rangle$ de tais conjugados de S é, por definição, semi-simples. Temos ainda que $1 < S^G \trianglelefteq G$ (com $S^G \subseteq N$). Mais uma vez, a minimalidade de N acarreta $S^G = N$, concluindo a prova de que, se N é não-abeliano, então N é semi-simples. □

Proposição 3.12. *Dado um grupo finito G, denotemos por $E = E(G)$ o subgrupo layer e $Z = Z(E)$ o centro de E. São válidos os seguintes fatos:*

(a) *E é perfeito. ($E' = E$).*
(b) *O quociente E/Z é semi-simples.*
(c) *Se o subgrupo $M \trianglelefteq G$ é solúvel então $[E, M] = 1$.*

Demonstração. Denotando por $\mathcal{F}$ o conjunto dos componentes de G, escrevemos $E = E(G) = \langle \mathcal{F} \rangle$. Vimos na Proposição 3.9 que dois componentes distintos de um grupo finito se normalizam. Assim, cada componente é normal em $E(G)$.

(a) Para um dado $H \in \mathcal{F}$, vale $H = H'$. Temos $H \leqslant E$ e, pela Proposição 2.11, isso assegura que $H' \leqslant E'$. Assim, $H \leqslant E'$ para qualquer componente H, donde segue $E \leqslant E'$. Sendo natural a inclusão contrária, obtemos $E' = E$.

(b) Sendo $Z(H) \leqslant C_G(H)$, temos $[Z(H), H] = 1$. Por outro lado, se $K \in \mathcal{F}$ é um componente de G tal $K \neq H$, a Proposição 3.9 garante que $[H, K] = 1$. Logo:

$[Z(H), K] \leqslant [H, K] = 1$ ($\therefore$ $Z(H)$ centraliza qualquer membro de $\mathcal{F}$).

Assim, $Z(H)$ é central em E (ou seja, $Z(H) \leqslant Z(E) = Z$ $\therefore Z(H) \leqslant H \cap Z$).

Por outro lado, Z centraliza E e $H \leqslant E$. Assim, Z centraliza H (ou seja, $Z \subseteq C_G(H)$. Sendo $Z(H) = C_G(H) \cap H$, temos $Z \cap H \subseteq C_G(H) \cap H = Z(H)$. Unindo as duas inclusões, resulta $Z(H) = Z \cap H$, para todo $H \in \mathcal{F}$.

Seja $\overline{E} = E/Z$. Temos $\overline{H} = (HZ)/Z \cong H/(H \cap Z) = H/Z(H)$. H é quasisimple (por ser um componente de G) e, portanto, $H/Z(H)$ é simples e não-abeliano (Proposição 3.7). O isomorfismo garante que o mesmo ocorre com $\overline{H}$.

A imagem $\overline{X}$ de um qualquer componente $X \in \mathcal{F}$ (gerador de E) é normal em $\overline{E}$. O subgrupo gerado pelos $\overline{X}$ é, então, um produto de subgrupos simples, não-abelianos e que são normais em $\overline{E}$. Ou seja, $\overline{E}$ é semi-simples.

(c) Sendo $M \trianglelefteq G$, temos $(M \cap E) \trianglelefteq E$. Pela hipótese de ser M solúvel, seu subgrupo $(M \cap E)$ também o é. Fazendo o quociente E/Z, obtemos uma imagem homomórfica solúvel do subgrupo $(M \cap E)$, que será denotada por X/Z:

$$\frac{X}{Z} = \frac{(M \cap E)Z}{Z} \trianglelefteq \frac{E}{Z} \text{ (correspondência)}$$

Os subgrupos normais minimais do grupo semi-simples E/Z são não-abelianos e simples (Proposição 3.10) e, em particular, não-solúveis. O subgrupo solúvel X/Z não pode conter nenhum desses normais minimais de E/Z e, portanto, deve ser o grupo trivial. Decorre $(M \cap E)Z = Z$, o que implica $(M \cap E) \subseteq Z$. Sendo $M, E \trianglelefteq G$, a Proposição 2.10 assegura que $[M, E] \leqslant M \cap E$. Assim:

$[M, E] \leqslant M \cap E \subseteq Z = Z(E) \leqslant C_G(E)$. Isso significa que $[M, E]$ centraliza E, ou seja, $[M, E, E] = 1$ e $[E, M, E] = 1$. Pelo *Lema dos 3 Subgrupos*, vem $[E, E, M] = 1$, ou seja, $[E, M] = 1$. □

Proposição 3.13 (Teorema de Bender)**.** *Seja G um grupo finito. Sendo $F^*(G)$ o Subgrupo de Fitting Generalizado, é válida a seguinte relação:*

$$C_G(F^*(G)) \leqslant F^*(G) .$$

Demonstração. Sejam $C := C_G(F^*(G))$ e $Z := C \cap F^*(G)$. Precisamos mostrar que $Z = C$ e, para tanto, argumentaremos por contradição.

Admitamos que $Z \neq C$. Temos, por construção, $Z \subseteq C$, o que obriga $Z < C$.

Sendo $F^*(G) \trianglelefteq G$, temos $C = C_G(F^*(G)) \trianglelefteq G$ (Proposição 2.1). Além disso, por ser Z uma interseção de subgrupos normais de G, temos $Z \trianglelefteq G$. Fazendo o quociente G/Z, temos $1 \neq C/Z \trianglelefteq G/Z$. Logo, existe um subgrupo normal minimal M/Z de G/Z tal que $M/Z \trianglelefteq C/Z$ e, portanto, $M \trianglelefteq C$.

Por construção, temos que C centraliza $F^*(G)$. Dado que $Z \subseteq F^*(G)$, segue que C centraliza Z. Considerando que $M \subseteq C$, segue que Z centraliza M. Lembrando que $Z \subseteq M$, obtemos $Z \subseteq Z(M)$.

Pela Proposição 3.11, o subgrupo normal mininal M/Z do grupo finito G/Z ou é abeliano ou é semi-simples.

Caso 1: Se M/Z é abeliano é também nilpotente. Dado que $Z \subseteq Z(M)$, a Proposição 3.2 garante que M é nilpotente. Notando que $M \trianglelefteq G$, segue:

$M \subseteq F(G) \subseteq F^*(G)$. Mas $M \subseteq C$, logo $M \subseteq C \cap F^*(G) = Z$.

Mas isso é uma contradição, pois sabemos que $M/Z \neq 1$. Isso evidencia que o caso abeliano não pode ocorrer.

Caso 2: Admitamos M/Z semi-simples e seja S/Z um subgrupo normal minimal de M/Z. Assim, S/Z é um fator simples não-abeliano de M/Z (conforme Proposição 3.10). Resulta $Z = Z(S)$ e, portanto, $S/Z(S)$ é simples não-abeliano. Pela Proposição 3.7, segue que S' é quasisimple. Além disso, S' é subnormal em G (pois $S \trianglelefteq M$ e $M \trianglelefteq G$), de modo que S' é uma componente de G. Por definição do subgrupo *layer* de G, obtemos $S' \subseteq E(G) \subseteq F^*(G)$. Levando em conta que $S' \subseteq S \subseteq C$, decorre $S' \subseteq C \cap F^*(G) = Z$. Mas o fato que $S' \subseteq Z \trianglelefteq G$, garante que S/Z é abeliano (conforme Proposição 2.9). Mas isso contraria o fato de S/Z ser não-abeliano e, portanto, não pode ocorrer.

Concluímos que as contradicões (em ambos os casos previstos na Proposição 3.9) derivaram de termos assumido $Z \neq C$. Fica, pois, demonstrado que $Z = C$. □

Corolário 3.14. *Conseqüências do Teorema de Bender*

Sendo G um grupo finito, são válidos os seguintes fatos:

a) $F(G) = F^*(G)$ *se, e somente se,* $C_G(F(G)) \subseteq F(G)$.

b) *Se* $F^*(G) = 1$, *então* $G = 1$.

Demonstração. (a) ($\Rightarrow$) Suponha $F(G) = F^*(G)$. Pelo *Teorema de Bender*, sempre vale $C_G(F^*(G)) \leqslant F^*(G)$. Da hipótese inicial, segue $C_G(F(G)) \leqslant F(G)$.

($\Leftarrow$) Reciprocamente, admitamos $C_G(F(G)) \leqslant F(G)$. Dado que $F(G)$ é solúvel, $E(G) \leqslant C_G(F(G))$ (vide Proposição 3.12) e, portanto, $E(G) \leqslant F(G)$. Sendo $F^*(G) = F(G)E(G)$, segue $F^*(G) = F(G)$.

(b) $G = C_G(1) = C_G(F^*(G)) \leqslant F^*(G) = 1$ □

4. DEMONSTRAÇÃO DO PRIMEIRO TEOREMA

Teorema 4.1. ([5] - *Theorem 9*).
Sendo G um grupo finito e $sol(G)$ o seu radical solúvel, vale:

$$cp(G) \leqslant [G : sol(G)]^{-1/2} .$$

Demonstração. (I) Pela Proposição 3.4, temos $sol(G/sol(G)) = 1$, o que mostra que existe pelo menos um grupo finito com radical solúvel trivial. Aplicando a tese do Teorema ao grupo $H = G/sol(G)$, vem $cp(H) \leqslant [H : sol(H)]^{-1/2}$, ou seja:

$$\begin{aligned} cp\Big(\frac{G}{sol(G)}\Big) &\leqslant \Big[\Big(\frac{G}{sol(G)}\Big) : sol\Big(\frac{G}{sol(G)}\Big)\Big]^{-\frac{1}{2}} \\ = \Big[\Big(\frac{G}{sol(G)}\Big) : 1\Big)\Big]^{-\frac{1}{2}} &= \Big[G : sol(G)\Big]^{-\frac{1}{2}} \end{aligned}$$

Sendo $sol(G) \trianglelefteq G$, o Lema 2.8 fornece $cp(G) \leqslant cp(G/sol(G))$.
Daí decorre $cp(G) \leqslant [G : sol(G)]^{-1/2}$, de modo que podemos assumir, sem perda de generalidade, que $sol(G) = 1$.

(II) Seja $F(G)$ o subgrupo de Fitting de G. Sendo tal subgrupo nilpotente, ele também é solúvel. Dado que assumimos $sol(G) = 1$, decorre $F(G) = 1$. Fazendo $I = F^*(G) = F(G)E(G)$, obtemos $I = E(G)$.
Caso ocorresse $E(G) = 1$, teríamos $F^*(G) = 1$ e, pelo corolário 3.14, viria $G = 1$. Vamos assumir, daqui em diante que estamos lidando com $E(G)$ não-trivial.

(III) Sabemos que o subgrupo *layer* $E(G)$ é gerado por subgrupos subnormais *quasisimple* (*componentes* de G). No caso geral, E(G) não é necessariamente o produto direto de $H_1, \ldots, H_t$, em que os H_i são os componentes de G. Sabemos, no entanto, que $H_i \trianglelefteq E(G)$ $(\forall i, 1 \leqslant i \leqslant t)$ e que $Z(H_i)$ *char* H_i, o que garante $Z(H_i) \trianglelefteq E(G)$. Sendo H_i um componente de G, H_i é quasisimple e, portanto, cada quociente $H_i/Z(H_i)$ é simples (e não-abeliano), conforme Proposição 3.7.

(IV) Façamos $E = E(G)$. O centro $Z(E)$ é abeliano ($\therefore$ solúvel) e normal em G, de modo que $Z(E) \leqslant sol(G)$. Mas estamos assumindo $sol(G) = 1$, logo $Z(E) = 1$ e $E/Z(E) \cong E$. Pela Proposição 3.12, o quociente $E/Z(E)$ é *semi-simples*. Dessa forma, sob as hipóteses do Teorema:

$$\frac{E}{Z(E)} \cong E = F^*(G) = I$$

Logo, I é o produto direto de normais simples não-abelianos. Temos ainda que cada fator de I, por ser não-abeliano simples, possui centro trivial.

(V) Consideremos a ação por conjugação do grupo G sobre o conjunto $\Omega = \{S_1, S_2, \ldots, S_t\}$ dos fatores simples do subgrupo $S_1 \times S_2 \times \cdots \times S_t = I \trianglelefteq G$:

$$\begin{aligned} \rho : \Omega \times G &\to \Omega \\ (S_i, g) &\mapsto S_i{}^g \end{aligned}$$

Cada subgrupo $S_i{}^g$ é isomorfo a S_i ($g^{-1}S_ig \cong S_i$, $\forall g \in G$) e podemos mostrar que a ação definida produz o efeito de permutar os fatores de I.

Dado o subgrupo $g^{-1}S_ig = S_i{}^g \leqslant G$, tomemos elementos $x \in I$, $s \in S_i$ e $g \in G$. Ao conjugar um elemento $(g^{-1}sg)$ de $S_i{}^g$ por um $x \in I$, obtemos:

$$x^{-1}(g^{-1}sg)x = g^{-1}(gx^{-1}g^{-1})s(gxg^{-1})g = g^{-1}(gxg^{-1})^{-1}\ s(gxg^{-1})g.$$

Mas $y = (gxg^{-1}) \in I$, pois $I \trianglelefteq G$. Sendo $S_i \trianglelefteq I$, vem $y^{-1}sy \in S_i$. Além disso, $g^{-1}(y^{-1}sy)g \in S_i{}^g$ ($\therefore\ S_i{}^g \trianglelefteq I$). Temos ainda que o subgrupo normal $S_i{}^g$ de I é um produto direto de alguns dos fatores de I ([14], item 3.3.16, pg 88). Mas sendo cada um dos S_i um grupo simples, um subgrupo conjugado $S_i{}^g$ também deve ser, de modo que $S_i{}^g = S_j$ para algum j (potencialmente distinto de i). Isso evidencia que ρ permuta os fatores de I.

Fazendo $J = \mathrm{Ker}(\rho)$ e tomando um $x \in J$, obtém-se $S_i{}^x = S_i$ ($\forall i$, $1 \leqslant i \leqslant t$). Dessa forma, a ação de J fixa cada S_i em I e tem o efeito de permutar os elementos pertencentes a tal fator.

Denotando por α_i o homomorfismo de J em $Aut(S_i)$ que representa a ação de J sobre um dado S_i, podemos construir o seguinte homomorfismo de grupos:

$$\begin{aligned} \alpha : J &\to Aut(S_1) \times \cdots \times Aut(S_t) \\ x &\mapsto (\alpha_1(x), \ldots, \alpha_t(x)) \end{aligned}$$

O núcleo de α consiste nos elementos de J que preservam todos os fatores:
$Ker(\alpha) = \{\ x \in J \mid s^x = s, \forall i, \forall s \in S_i\ \} = \{\ x \in J \mid a^x = a, \forall a \in I\ \} \subseteq C_G(I)$

No caso em análise, temos $I = \mathrm{F}^*(G)$. Assim, recorrendo à Proposição 3.13, obtemos $C_G(I) \leqslant I$. Mas, pela definição de centralizador de um subgrupo, isso significa que $C_G(I) = \mathrm{Z}(I)$. Além disso, vimos no item (IV) que $\mathrm{Z}(I) = \mathrm{Z}(E) = 1$, e daí segue que $C_G(I)$ é trivial e, portanto, $Ker(\alpha) = 1$. Sendo α injetivo, podemos considerar a inclusão $J \leqslant Aut(S_1) \times \cdots \times Aut(S_t)$.

(VI) Vamos mostrar agora que a conjugação de qualquer $(s_1, \ldots, s_t) \in S_1 \times \cdots \times S_t = I$ por um elemento $(y_1, \ldots, y_t) = y \in I$ preserva cada um dos fatores S_i. Levando-se em conta que o núcleo J fixa (simultaneamente) todos os fatores, isso significa que $I \subseteq J = \mathrm{Ker}(\rho)$.

Notemos, de início, que um S_i arbitrário pode ser identificado com $1 \times \cdots \times 1 \times S_i \times 1 \times \cdots \times 1$, que é um produto direto de t termos. Visando facilitar a análise, consideremos o caso $I = S_1 \times S_2$. Tomando $(a, 1) \in S_1$ e $(1, b) \in S_2$, obtemos:

$(a,1)^{(1,b)} = (a,1)$, donde $(1 \times S_2) \subseteq C_I(S_1)$

Estendendo tal raciocínio para t fatores, podemos supor, sem perda de generalidade, que a entrada não-trivial em I ocorra para $i = 1$. Nessas condições, segue $(1 \times S_2 \times \cdots \times S_t) \subseteq C_I(S_1)$.

De forma ainda mais geral, vale $(s_1, 1, \ldots, 1)^{(y_1,\ldots,y_t)} = ({s_1}^{y_1}, 1, \ldots, 1) \in S_1$, demonstrando que a conjugação de um fator S_i por elemento de I preserva S_i ($\therefore I \subseteq J$). Da observação final em (V), decorre:

$$S_1 \times \cdots \times S_t = I \leqslant J \leqslant Aut(S_1) \times \cdots \times Aut(S_t) = A.$$

(VII) A Proposição 5.3 em [2] estabelece que, para um grupo finito *almost simple* H, vale $k(H) \leqslant |H|^{0,41}$. A mesma desigualdade é obedecida por um grupo H que verifique:
$S_1 \times \cdots \times S_t \leqslant H \leqslant Aut(S_1) \times \cdots \times Aut(S_t)$

E, se isso acontece, digamos que H tem t componentes.

Para demonstrar a validade de tal fato para o grupo J definido em (V), vamos utilizar o *princípio do menor inteiro* no conjunto dos inteiros não superiores a t, em que t é o número de componentes em J.

No caso particular em que $t = 1$, temos $I = S_1$. Unindo as conclusões de (V) e (VI), resulta $S_1 = I \leqslant J \leqslant Aut(S_1)$, caracterizando que J é almost simple.

Já para $t > 1$, façamos $L = S_1 \times 1 \times \cdots \times 1 \cong S_1$ e seja $C = C_J(L)$. C é o núcleo da ação por conjugação de J sobre L e, usando a Proposição 2.1, segue $J/C \leqslant Aut(L)$. Pelas considerações em (VI), temos a seqüência de inclusões $(1 \times S_2 \times \cdots \times S_t) \subseteq C_I(L) \subseteq C \subseteq C_A(L) \subseteq A$. Por outro lado, considerando $(y_1, \ldots, y_t) \in C_A(L)$ e lembrando que y_i é um automorfismo, segue que y_1 deve ser a função identidade em A. Isso permite concluir que $C_A(L) = 1 \times Aut(S_2) \times \cdots \times Aut(S_t)$ (logo C tem $t-1$ componentes). Temos ainda que:

$$\frac{LC}{C} \cong \frac{L}{(L \cap C)} \cong L, \text{ pois a interseção } (L \cap C) \text{ é trivial.}$$

Em resumo: $L \cong \dfrac{LC}{C} \leqslant \dfrac{J}{C} \leqslant Aut(L)$, mostrando que $\dfrac{J}{C}$ é almost simple.

Recorrendo ao Lema 2.7, obtemos: $k(J) \leqslant k(C) \cdot k(J/C)$

Dado que $k(J/C) \leqslant |J/C|^{0,41}$, segue:

$$k(J) \leqslant k(C) \cdot |J/C|^{0,41} = k(C) \cdot \frac{|J|^{0,41}}{|C|^{0,41}}$$

Admitamos agora que o resultado não valha a partir de um J que possua t componentes, isto é, que $k(J) > |J|^{0,41}$. Com essa hipótese, $C = C_J(L)$ verifica o resultado (pois C possui um número de componentes igual a $t-1$), ou seja:

$$k(C) \leqslant |C|^{0,41} \text{ e, portanto: } \frac{k(C)}{|C|^{0,41}} \leqslant 1$$

Novamente pelo Lema 2.7:

$$k(J) \leqslant k(C) \cdot \frac{|J|^{0,41}}{|C|^{0,41}} \leqslant |J|^{0,41} \text{ (o que é uma contradição).}$$

(VIII) $S_1 \times \cdots \times S_t = I \leqslant J$, em que os t fatores S_i são grupos simples não-abelianos. Dado que o grupo simples não-abeliano de menor ordem é A_5, temos: $|J| \geqslant 60 \cdot 60 \cdot \cdots \cdot 60 = 60^t$.

Por outro lado, usando o resultado principal em [13], tem-se $k(X) < 3^{t/2}$, quando X é um grupo finito de permutações com $t > 2$. Mas:

$$3^{t/2} = 60^{\,log_{60}(3^{t/2})} = 60^{(t/2)\cdot(log_{60}3)} \leqslant 60^{(t/2)\cdot(0,27)} \leqslant (60^t)^{0,14}$$

Aplicando os dois fatos ao grupo G/J, vem:

$$|J|^{0,14} \geqslant (60^t)^{0,14} \geqslant 3^{t/2} > k(G/J)$$

Por outro lado, $k(G) \leqslant k(J) \cdot k(G/J) \leqslant |J|^{0,41} \cdot |J|^{0,14} = |J|^{0,55}$

Vamos analisar dois casos: $|G/J| > |J|^{0,1}$ e $|G/J| \leqslant |J|^{0,1}$

a) $|G/J| > |J|^{0,1} \Rightarrow |G| > |J|^{1,1} \Rightarrow |J|^{0,55} < |G|^{1/2} \therefore k(G) < |G|^{0,5}$

b) $|G/J| \leqslant |J|^{0,1} \Rightarrow |G| \leqslant |J|^{1,1} \Rightarrow |G|^{0,5} \leqslant |J|^{0,55} < |J|^{0,59}$

Sendo $cp(G) \leqslant cp(J)$ (Lema 2.8), segue: $k(G) \leqslant k(J) \cdot \frac{|G|}{|J|} = k(J) \cdot |G/J|$

Assim, $k(G) \leqslant |J|^{0,41} \cdot |G/J| = |G| \cdot \frac{1}{|J|^{0,59}} = |G|^{0,5} \cdot \left(\frac{|G|^{0,5}}{|J|^{0,59}} \right) < |G|^{0,5}$

Fica provado que $k(G) < \sqrt{|G|}$ para um G não-trivial em que $\text{sol}(G) = 1$. $\square$

Corolário 4.2. *Sendo G um grupo finito, tem-se $cp(G) = [G : sol(G)]^{-1/2}$, se, e somente, se, G é abeliano.*

Demonstração. ($\Rightarrow$) Asumindo $cp(G) = [G : sol(G)]^{-1/2}$, vamos provar que G é abeliano. Já sabemos que:

(I) $cp(X) \leqslant [X : sol(X)]^{-1/2}$;
(II) $cp(X) < [X : sol(X)]^{-1/2}$, quando $sol(X) = 1$ e $E(X) \neq 1$.

Consideremos o grupo $X = G/sol(G)$. Usando a hipótese, em conjunto com os fatos (I) e (II), obtemos:

$$\Big[G : sol(G)\Big]^{-\frac{1}{2}} = cp(G) \leqslant cp\Big(\frac{G}{sol(G)}\Big)$$
$$\leqslant \Big[\Big(\frac{G}{sol(G)}\Big) : sol\Big(\frac{G}{sol(G)}\Big)\Big]^{-\frac{1}{2}} = \Big[\Big(\frac{G}{sol(G)}\Big) : 1\Big)\Big]^{-\frac{1}{2}} = \Big[G : sol(G)\Big]^{-\frac{1}{2}}$$

Na cadeia de igualdades e desigualdades acima, vemos que o primeiro e o último membro são iguais, o que implica a igualdade entre todos os termos intermediários. Em particular, vale:

$$cp\Big(\frac{G}{sol(G)}\Big) = \Big[\Big(\frac{G}{sol(G)}\Big) : sol\Big(\frac{G}{sol(G)}\Big)\Big]^{-\frac{1}{2}}$$

Lembrando que $X = G/sol(G)$ e $sol(G/sol(G)) = 1$, segue:

$cp(X) = [X : sol(X)]^{-\frac{1}{2}}$, com $sol(X) = 1$ (III)

Se ocorresse $E(X) \neq 1$ (com $sol(X) = 1$), o fato (II) acarretaria:

$cp(X) < [X : sol(X)]^{-\frac{1}{2}}$

O resultado obtido em (III) mostra que esse não é o caso. Logo devemos ter $E(X) = 1$ com $sol(X) = 1$. Isso significa que $F^*(X) = 1$ e, pelo corolário 3.14, segue $X = 1$. Pela escolha de X, segue $G = sol(G)$ e, recorrendo mais uma vez à hipótese, segue $cp(G) = 1$. Mas esse último fato, significa que G é abeliano.

($\Leftarrow$) Reciprocamente, se G é abeliano, temos $cp(G) = 1$.
Por outro lado, G é solúvel (por ser abeliano) e, portanto, $G = sol(G)$.

Resulta: $[G : sol(G)]^{-1/2} = 1 = cp(G)$. □

5. REPRESENTAÇÕES LINEARES DE GRUPOS

Já vimos que a ação de um grupo G sobre um conjunto Ω origina um homomorfismo de G no grupo simétrico de Ω, possibilitando que a ação sobre Ω de cada $g \in G$ seja descrita como uma permutação dos elementos de Ω. Tal abordagem permite que propriedades estabelecidas no grupo $\mathrm{Sym}(\Omega)$ sejam mapeadas de volta para o grupo abstrato G (via homomorfismo), constituindo uma importante ferramenta para obtenção de informações sobre G.

Na presente seção, lançamos mão de outra técnica interessante para o estudo das propriedades de um grupo G. Em vez de analisar a ação de G sobre um conjunto genérico, concentramos a atenção na ação de cada $g \in G$ sobre um espaço vetorial de dimensão finita (definido sobre o corpo dos números complexos). A motivação para optar por uma tal estratégia é transformar alguns problemas, originalmente associados à Teoria de Grupos, em problemas de Álgebra Linear.

5.1. CONCEITOS BÁSICOS.

Definição 5.1. *Sejam V um espaço vetorial de dimensão n (finita) sobre $\mathbb{C}$ e G um grupo finito. Uma representação de G sobre V é um homomorfismo ρ de G sobre o grupo $GL(V)$ das transformações lineares invertíveis de V.*

$$\begin{aligned} \rho : G &\to GL(V) \\ g &\mapsto (g)\rho = \rho_g \, . \end{aligned}$$

O homomorfismo de grupos $\rho : G \to GL(V)$ associa a cada $g \in G$ uma transformação linear invertível (isomorfismo linear) $\rho_g : V \to V$. Além disso, temos:

- O espaço V que aparece na definição é denominado espaço de representação e sua dimensão é o grau da representação.
- Se V tem dimensão n finita, $GL(V) \cong GL(n, \mathbb{C})$ (grupo das matrizes $n \times n$ invertíveis com entradas no corpo dos números complexos).
- $(1)\rho = I_n$ (matriz identidade de ordem n).
- $(g \cdot h)\rho = (g)\rho \cdot (h)\rho$, $\forall g, h \in G$. (Outra notação usual: $\rho_{gh} = \rho_g \rho_h$).
- Por uma questão de simplificação da linguagem, é bem comum referir-se à representação $\rho : G \to GL(V)$ apenas como "*a representação V*".

Dado que a representação $\rho : G \to GL(V)$ é um homomorfismo, a transformação $\rho_{gh} : V \to V$ pode ser escrita como $\rho_{gh} = \rho_g \circ \rho_h$ (sempre usando a referência de ação à direita) ou, de forma correspondente, $[\rho_{gh}] = [\rho_h][\rho_g]$, pensando em produto de matrizes. Além disso, pode-se tratar $(\mathbf{v})(\rho_g \circ \rho_h)$ como o produto $[\rho_h][\rho_g][\mathbf{v}]$, em que $[\mathbf{v}]$ denota o vetor coluna correspondente a $\mathbf{v}$.

Com essas definições em mente, consideremos a função:

$$\begin{aligned}\mu : V \times G &\to V \\ (\mathbf{v}, g) &\mapsto \mathbf{v}^g = (\mathbf{v})\rho_g\end{aligned}$$

Pode-se observar que a função μ satisfaz as seguintes condições:

(a) $\mu(\mathbf{v}, 1) = \mathbf{v}^1 = I_n(\mathbf{v}) = \mathbf{v}$
(b) $\mu(\mathbf{v}, gh) = \mathbf{v}^{gh} = (\mathbf{v})(\rho_g \circ \rho_h) = ((\mathbf{v})\rho_g)\rho_h = (\mu(\mathbf{v}, g))\rho_h = \mu(\mu(\mathbf{v}, g), h)$
(c) $\mu(c\mathbf{v}, g) = (c\mathbf{v})\rho_g = c \cdot ((\mathbf{v})\rho_g) = c \cdot \mu(\mathbf{v}, g)$
(d) $\mu(\mathbf{v_1} + \mathbf{v_2}, g) = (\mathbf{v_1} + \mathbf{v_2})\rho_g = (\mathbf{v_1})\rho_g + (\mathbf{v_2})\rho_g = \mu(\mathbf{v_1}, g) + \mu(\mathbf{v_2}, g)$

Isso significa que, além de ser um ação (à direita) do grupo G sobre o conjunto V, a função induzida por μ para cada g fixo é linear:

$$\mu(c\mathbf{v} + d\mathbf{w}, g) = c\mu(\mathbf{v}, g) + d\mu(\mathbf{w}, g),\ \forall \mathbf{v}, \mathbf{w} \in V,\ \forall c, d \in \mathbb{C}$$

Dessa forma, dada uma representação $\rho : G \to GL(V)$, pode-se associar uma *ação linear* de G em V tal que $\mathbf{v}^g = (\mathbf{v})\rho_g$, $\forall \mathbf{v} \in V$ e $\forall g \in G$. Reciprocamente, se G age linearmente sobre o espaço vetorial V, a função $\rho : G \to GL(V)$, que associa a cada elemento g de G uma transformação linear invertível $\rho_g : V \to V$ (induzida pela ação de g), é uma representação de G.

Terminologia Alternativa: Sejam G um grupo finito e V um espaço vetorial de dimensão n (finita) sobre o corpo $\mathbb{C}$. Diz-se que V é um *G-módulo* se existe uma multiplicação $\mathbf{v}g$, de elementos de V por elementos de G (com $\mathbf{v}g \in V$), que satisfaça:

(a) $\mathbf{v}1 = \mathbf{v}$
(b) $\mathbf{v}(gh) = ((\mathbf{v})g)h$
(c) $(c\mathbf{v})g = c\,(\mathbf{v}g)$
(d) $(\mathbf{v} + \mathbf{w})g = \mathbf{v}g + \mathbf{w}g$,

$\forall g, h \in G,\ \forall \mathbf{v}, \mathbf{w} \in V$ e $\forall c \in \mathbb{C}$

A partir da ação de um grupo G sobre um conjunto $S = \{s_1, s_2, \ldots, s_n\}$, podemos construir um G-módulo de dimensão$|S|$. Nessa construção, os elementos de S farão o papel de vetores e, para enfatizar tal fato, passarão a ser escritos em negrito.

- Definimos um espaço vetorial $\mathbb{C}S$, em que o conjunto S constitui uma base.
  $\mathbb{C}S = \mathbb{C}\{\mathbf{s_1}, \mathbf{s_2}, \ldots, \mathbf{s_n}\} = \{c_1\mathbf{s_1} + c_2\mathbf{s_2} + \cdots + c_n\mathbf{s_n},\ c_i \in \mathbb{C}\}$

- A adição de vetores em $\mathbb{C}S$ é definida por:
  $(c_1\mathbf{s_1} + \cdots + c_n\mathbf{s_n}) + (d_1\mathbf{s_1} + \cdots + d_n\mathbf{s_n}) = (c_1 + d_1)\mathbf{s_1} + \cdots + (c_n + d_n)\mathbf{s_n}$

- A multiplicação por escalar em $\mathbb{C}S$ é dada por:
  $c(c_1\mathbf{s_1} + \cdots + c_n\mathbf{s_n}) = (cc_1)\mathbf{s_1} + \cdots + (cc_n)\mathbf{s_n}$

- A ação de G sobre o espaço vetorial $\mathbb{C}S$ é obtida usando linearidade e o fato que $\mathbf{s_i}g \in S$
  $(c_1\mathbf{s_1} + \cdots + c_n\mathbf{s_n})g = c_1(\mathbf{s_1}g) + \cdots + c_n(\mathbf{s_n}g) \in \mathbb{C}S, \forall g \in G$

Exemplo 5.2. *Representação Trivial*
Todos os grupos possuem a representação trivial, a qual associa a todo $g \in G$ a matriz identidade (que, naturalmente, corresponde à transformação identidade). Isso significa que cada elemento de G age trivialmente sobre o espaço vetorial V.

Exemplo 5.3. *Representação Sinal para um Grupo de Permutações*
Seja $G = S_n$, em que S_n é o grupo das permutações de um conjunto de n elementos. Uma permutação $\pi \in S_n$ pode ser expressa como um produto de transposições ($\pi = \tau_1\tau_2 \ldots \tau_k$). Apesar de tal decomposição não ser única, a paridade de k está bem definida (independente do valor de k, π terá sempre um número par de transposições ou sempre um número ímpar).

Definindo $sgn(\pi) = (-1)^k$, vemos que $(\pi \cdot \sigma)sgn = (\pi)sgn \cdot (\sigma)sgn$.

O homomorfismo X: $S_n \to \{1, -1\}$ definido por:

$$X(\pi) = sgn(\pi) = \begin{cases} 1, & \text{se } \pi \text{ é uma permutação par;} \\ -1, & \text{se } \pi \text{ é uma permutação ímpar;} \end{cases}$$

é denominado representação sinal de S_n. (X é uma representação não-trivial de grau 1. Além disso, os valores 1 e -1 devem ser vistos como números complexos).

Exemplo 5.4. *Representações de grau 1 para um grupo cíclico*
Seja $C_n = \langle g \rangle = \{g, g^2, \ldots, g^n = 1\}$ o grupo cíclico de ordem n. Para obter as representações de dimensão 1 de tal grupo, façamos $(g)\rho = c$, em que $c \in \mathbb{C}$.
Sendo ρ um homomorfismo, temos:

$c^n = ((g)\rho)^n = (g^n)\rho = (1)\rho = 1$, *ou seja, c é uma raiz n-ésima da unidade.*

De forma geral, dado o grupo C_n, existem n possibilidades para a imagem ρ_g do gerador g através de cada representação (homomorfismo). Como exemplo concreto, vamos construir a tabela de representações de grau 1 para $C_4 = \{1, g, g^2, g^3\}$.

representação	***elementos do Grupo***			
	$\mathbf{1}$	$\mathbf{g}$	$\mathbf{g^2}$	$\mathbf{g^3}$
ρ	1	1	1	1
τ	1	-1	1	-1
ψ	1	i	-1	$-i$
ϕ	1	$-i$	-1	i

Na montagem da tabela, levamos em conta os seguintes fatos:

- *como em qualquer homomorfismo, a imagem da identidade é* 1 *;*
- *a segunda coluna mostra a imagem escolhida para o gerador* g *naquela representação. Assim:* $(g)\rho = 1$, $(g)\tau = -1$, $(g)\psi = i$, $(g)\phi = -i$ *;*
- *as imagens de* g^2 *e* g^3 *são obtidas a partir da imagem do gerador.*

Exemplo 5.5. *Representação Regular à direita*

Essa é a representação associada à ação regular à direita de G *(sobre* G*).*

Dado um grupo finito $G = \{g_1, g_2, \ldots, g_n\}$*, tomemos um elemento fixo* $x \in G$*. Multiplicando, à direita, cada elemento de* G *por tal* x*, obtemos o conjunto* $\{g_1x, g_2x, \ldots, g_nx\} = G$*, mostrando que tal produto é uma permutação dos elementos de* G *e remetendo ao conhecido fato de que todo grupo é isomorfo a um grupo de permutações de seu conjunto associado (Teorema de Cayley). O isomorfismo assim produzido é denominado representação regular à direita de* G*. (Vale notar que, nesse caso, o espaço vetorial é* $\mathbb{C}G$*).*

É interessante lembrar, nesse ponto, que uma matriz de permutação é uma matriz quadrada obtida a partir da matriz identidade de mesma dimensão, por meio de permutação de linhas. Cada coluna e cada linha de uma matriz desse tipo possui exatamente uma entrada não-nula (cujo valor é 1). Multiplicar à direita, por uma matriz de permutação, produz o efeito de rearranjar as colunas da matriz original. Vejamos um exemplo:

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} c_1 & a_1 & b_1 \\ c_2 & a_2 & b_2 \\ c_3 & a_3 & b_3 \end{pmatrix}$$

Podemos fazer o seguinte resumo da multiplicação à direita de uma matriz A (a_{ij}) *por uma matriz* P (p_{jk}) *de permutação* $(A \cdot P = B)$*:*

- *Se* P *possui uma entrada igual a* 1 *na posição* p_{jk}*, tal "*1*" terá influência sobre a coluna* j *de* A*, fazendo com que ela seja movida para a coluna* k *da matriz resultante* (B)*.*
- *Se a matriz* P *possui um elemento não-nulo na posição* p_{jj} *(diagonal principal), a coluna* j *permanecerá fixa na matriz resultante* (B)*.*

Seja $\pi \in S_n$ *a permutação associada à ação de multiplicação à direita por um elemento* $x \in G$*. Tal ação pode ser representada por uma matriz de permutação* $P(x)_{n\times n}$*, cujas linhas e colunas são indexadas pelo conjunto finito* G *:*

$$P(x)_{i,j} = P(\pi)_{i,j} = \begin{cases} 1, & se\ \pi(j) = i \\ 0, & se\ \pi(j) \neq i \end{cases}$$

Como exemplo prático, vamos registrar a representação regular de C_4 , a qual tem grau $4 = |C_4|$. Naturalmente, temos $\rho_1 = (1)\rho = I_4$.

$$\rho_g = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \rho_{g^2} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \rho_{g^3} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Exemplo 5.6. *Sejam V e W espaços vetoriais complexos e consideremos duas representações $\rho : G \to GL(V)$ e $\tau : G \to GL(W)$ do grupo G. É possível construir uma nova representação de G, recorrendo ao conceito de soma direta.*

$$\begin{aligned} \rho \oplus \tau : G &\to GL(V \oplus W) \\ g &\mapsto \rho_g \oplus \tau_g \ , \end{aligned}$$

em que $V \oplus W = \{ \ (\mathbf{v}, \mathbf{w}) \mid \mathbf{v} \in V \ , \ \mathbf{w} \in W \ \}$ e as operações envolvendo pares ordenados desse espaço são efetuadas componente a componente.

A função $\rho_g \oplus \tau_g$, definida a seguir, é uma transformação linear invertível em $V \oplus W$, $\forall g \in G$:

$$\begin{aligned} \rho_g \oplus \tau_g : V \oplus W &\to V \oplus W \\ (\mathbf{v}, \mathbf{w}) &\mapsto ((\mathbf{v})\rho_g, (\mathbf{w})\tau_g) \end{aligned}$$

Sejam $\mathcal{B}_1 = \{\mathbf{v_1}, \ldots \mathbf{v_n}\}$ e $\mathcal{B}_2 = \{\mathbf{w_1}, \ldots \mathbf{w_m}\}$, respectivamente, bases para os espaços V e W. Pela definição de soma direta, tem-se $\mathcal{B}_1 \cap \mathcal{B}_2 = \varnothing$. Além disso, $\mathcal{B}_1 \cup \mathcal{B}_2$ é uma base para $V \oplus W$.

É interessante notar que, se $M_1(g)$ e $M_2(g)$ são, respectivamente, as matrizes associadas a ρ_g e τ_g, então a matriz $M(g)$, associada à representação $\rho_g \oplus \tau_g$, terá o seguinte formato:

$$M(g) = \left[\begin{array}{c|c} M_1(g) & 0 \\ \hline 0 & M_2(g) \end{array}\right]$$

Definição 5.7. *Sejam $\rho : G \to GL(V)$ uma representação de G e $W \subseteq V$ um subespaço vetorial de V. W é dito um subespaço G-invariante (ou G-estável) se $(\mathbf{w})\rho_g \in W$, $\forall \mathbf{w} \in W$ e $\forall g \in G$.*

A partir de um subespaço $W \subseteq V$ que seja G-invariante, pode-se definir (por restrição a W) uma nova representação $\rho_W : G \to GL(W)$, em que $(g)\rho_W = (g)\rho$, $\forall g \in W$. Nessas condições, $\rho_W = \rho|_W$ é dita uma *subrepresentação*.

Uma representação V, em que V é não-nulo, é dita *irredutível* se seus únicos subespaços G-invariantes são os triviais (V e $\{0\}$). Por outro lado, diz-se que uma representação não-nula é *completamente redutível* se é uma soma direta de representações irredutíveis. (Ou seja, $V = W_1 \oplus W_2 \oplus \cdots \oplus W_r$, em que cada W_i é uma representação irredutível de G).

Exemplo 5.8. *Uma representação $\rho : G \to GL(V)$ de grau 1 é irredutível.*

Seja W um subespaço próprio de V, em que $dim(V) = 1$. Devemos ter $dim(W) < dim(V)$ e só nos resta a opção $dim(W) = 0$. Daí decorre $W = \{\mathbf{0}\}$. Mas tal W é trivial, o que mostra que V não possui subespaços próprios não-triviais. Dessa forma, por definição, ρ é uma representação irredutível.

Exemplo 5.9. *Representação redutível de grau 3 para S_3 .*

Vamos construir, agora, uma representação de grau 3 para o grupo S_3. Podemos pensar no grupo $D_3 \cong S_3$ e considerar que cada vetor $\{e_1, e_2, e_3\}$ descreve um vértice do triângulo equilátero. As rotações (3-ciclos) e reflexões (2-ciclos) movem tais vértices e podem ser representadas por matrizes de permutação.

$$\rho_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_{(1\,2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_{(1\,3)} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\rho_{(2\,3)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \rho_{(1\,2\,3)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \rho_{(1\,3\,2)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Definição 5.10. *Sejam $\rho : G \to GL(V)$ e $\tau : G \to GL(W)$ duas representações do grupo G. Um homomorfismo de representações (ou G-homomorfismo) é uma transformação linear $\psi : V \to W$ que satisfaz:*

$$(\mathbf{v})(\psi \circ \tau_g) = (\mathbf{v})(\rho_g \circ \psi),\ \forall g \in G,\ \forall \mathbf{v} \in V$$

É interessante registrar algumas formas alternativas de fazer referência ao conceito de G-homomorfismo:

- Se recorrermos à terminologia de G-módulos, podemos dizer que ψ é um G-homomorfismo se $(\mathbf{v}g)\psi = (\mathbf{v})\psi \cdot g$, $\forall g \in G$, $\forall \mathbf{v} \in V$, o que corresponde a dizer que ψ *preserva a ação de G.*
- Um G-homomorfismo é também chamado de homomorfismo *G-invariante.*
- Diz-se que um G-homomorfismo, ψ, é um *intertwining operator.*

Definição 5.11. *Sejam $\rho : G \to GL(V)$ e $\tau : G \to GL(W)$ duas representações do grupo G. ρ e τ são ditas equivalentes se existe um isomorfismo linear $\psi : V \to W$ tal que $\rho_g = \psi\tau_g\psi^{-1}$, $\forall g \in G$.*

Notando que $\rho_g = \psi\tau_g\psi^{-1} \Leftrightarrow \rho_g\psi = \psi\tau_g$, podemos também dizer que as representações ρ e τ são equivalentes se existe um *G-isomorfismo* entre os espaços vetoriais que as definem.

Proposição 5.1. *Sejam $\rho : G \to GL(V)$ e $\tau : G \to GL(W)$ duas representações do grupo G e $\psi : V \to W$ um G-homomorfismo. Valem as seguintes propriedades:*

(a) *$Ker(\psi)$ é uma subrepresentação de V ;*
(b) *$Im(\psi)$ é uma subrepresentação de W ;*
(c) *A aplicação $\psi_0 : V \to W$ definida a seguir é G-invariante:*

$$\psi_0 : \mathbf{v} \ \mapsto \ \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{v})(\rho_{g^{-1}}\, \psi\, \tau_g) \, .$$

Demonstração. (a) Sejam $g \in G$ e $\mathbf{v} \in Ker(\psi)$. Sabemos que $Ker(\psi)$ é um subespaço de V e, além disso, pela definição de núcleo, $(\mathbf{v})\psi = 0$. Sendo ψ um G-homomorfismo, tem-se $\psi \circ \tau_g = \rho_g \circ \psi$, $\forall g \in G$. Assim:

$((\mathbf{v})\psi)\tau_g = (\mathbf{v})(\psi \circ \tau_g) = (\mathbf{v})(\rho_g \circ \psi)$. Usando o fato $(\mathbf{v})\psi = 0$, segue:

$\mathbf{0} = (\mathbf{0})\tau_g = ((\mathbf{v})\psi)\tau_g = (\mathbf{v})(\rho_g \circ \psi) = ((\mathbf{v})\rho_g)\psi \ \therefore (\mathbf{v})\rho_g \in Ker(\psi), \forall \mathbf{v} \in Ker(\psi)$

Isso significa que $Ker(\psi)$ é uma subrepresentação de V .

(b) Já sabemos que $Im(\psi)$ é um subespaço de W .
Sejam $g \in G$ e $\mathbf{w} \in Im(\psi)$. Então, existe $\mathbf{v} \in V$ tal que $(\mathbf{v})\psi = \mathbf{w}$.
Sendo ψ um G-homomorfismo, tem-se $\psi \circ \tau_g = \rho_g \circ \psi$, $\forall g \in G$. Assim:

$(\mathbf{w})\tau_g = ((\mathbf{v})\psi)\tau_g = (\mathbf{v})(\psi \circ \tau_g) = (\mathbf{v})(\rho_g \circ \psi) = ((\mathbf{v})\rho_g)\psi$

Mas $((\mathbf{v})\rho_g)\psi \in Im(\psi)$ e, portanto, $(\mathbf{w})\tau_g \in Im(\psi)$.

Isso mostra que $Im(\psi)$ é uma subrepresentação de W .

(c) Dados $g, h \in G$, temos que $k = gh^{-1}$ assume todos os valores possíveis em G à medida que o elemento g percorre o grupo. Assim:

$$\begin{aligned}((\mathbf{v})\rho_h)\psi_0 &= \frac{1}{|G|} \cdot \sum_{g\in G}((\mathbf{v})\rho_h)(\rho_{g^{-1}}\ \psi\ \tau_g) \\ &= \frac{1}{|G|} \cdot \sum_{g\in G}((\mathbf{v})\rho_h)(\rho_{g^{-1}}\ \psi\ \tau_g\tau_{h^{-1}}\tau_h) = \frac{1}{|G|} \cdot \sum_{g\in G}((\mathbf{v})(\rho_{hg^{-1}}\ \psi\ \tau_{gh^{-1}}))\tau_h \\ &= \Big(\frac{1}{|G|} \cdot \sum_{k\in G}(\mathbf{v})(\rho_{k^{-1}}\ \psi\ \tau_k)\Big)\tau_h = ((\mathbf{v})\psi_0)\tau_h\end{aligned}$$

O fato $((\mathbf{v})\rho_h)\psi_0 = ((\mathbf{v})\psi_0)\tau_h$ evidencia que ψ_0 é G-invariante. □

Proposição 5.2 (Lema de Schur)**.** *Sejam $\rho : G \to GL(V)$ e $\tau : G \to GL(W)$ duas representações irredutíveis do grupo G. Se $\psi : V \to W$ é um G-homomorfismo não-nulo, então ψ é um G-isomorfismo.*

Demonstração. Estamos assumindo, inicialmente, que ψ é não-nulo. Sendo V irredutível, seu subespaço G-invariante $Ker(\psi)$ (vide Proposição 5.1) admite duas possibilidades extremas: $Ker(\psi) = \{\mathbf{0}\}$ ou $Ker(\psi) = V$. Mas esta última não pode subsistir, pois em tal caso teríamos ψ identicamente nulo, o que contraria nossa hipótese. Concluímos que $Ker(\psi) = \{\mathbf{0}\}$, o que significa que ψ é injetivo.

Sendo $Ker(\psi) = \{\mathbf{0}\}$, devemos ter $Im(\psi) \neq \{\mathbf{0}\}$. Sendo W irredutível, a opção que resta para seu subespaço G-invariante $Im(\psi)$ (vide Proposição 5.1) é coincidir com W. Mas o fato que $Im(\psi) = W$ corresponde a dizer que ψ é sobrejetivo. □

Usando o fato de que $\mathbb{C}$ é um corpo algebricamente fechado, podemos estabelecer um importante corolário do Lema de Schur.

Corolário 5.3. *Seja $\rho : G \to GL(V)$ uma representação irredutível de G. Dado um G-endomorfismo $\psi : V \to V$, existe um $\lambda \in \mathbb{C}$, tal que $(\mathbf{v})\psi = \lambda\mathbf{v}, \forall \mathbf{v} \in V$.*

Demonstração. Sendo $\mathbb{C}$ algebricamente fechado, ψ possui um autovalor λ (raiz de seu polinômio característico).

Consideremos a função linear $f : V \to V$, definida por $(\mathbf{v})f = (\mathbf{v})\psi - \lambda\mathbf{v}$.

Tal f é G-invariante, pois:

$$(\mathbf{v}g)f = (\mathbf{v}g)\psi - \lambda\mathbf{v}g = (\mathbf{v})\psi \cdot g - \lambda\mathbf{v}g = ((\mathbf{v})\psi - \lambda\mathbf{v}) \cdot g = (\mathbf{v})f \cdot g,\ \forall g \in G\ .$$

Pela Proposição 5.2, existem, a princípio, duas possibilidades para f:

- f é nula;
- f é um isomorfismo.

No entanto, podemos garantir que f não é um isomorfismo.

Se $\mathbf{w}$ fosse um autovetor associado a λ, teríamos $(\mathbf{w})\psi = \lambda\mathbf{w}$, logo $(\mathbf{w})f = \mathbf{0}$. Isso significa que existiria um $\mathbf{w} \in Ker(\psi)$, com $\mathbf{w} \neq \mathbf{0}$. Se f possui núcleo não-trivial, f não pode ser injetiva. Resulta $f = 0$ e concluímos que $(\mathbf{v})\psi = \lambda\mathbf{v}$, concluindo a demonstração. □

É interessante notar que o autovalor λ de ψ_0 pode ser calculado explicitamente. Para tanto, consideremos a aplicação $\psi_0 : V \to V$ tal que:

$$\psi_0 : \mathbf{v} \;\mapsto\; \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{v})(\rho_{g^{-1}}\ \psi\ \rho_g)$$

Convém observar que simplesmente consideramos o caso particular $\rho = \tau$ para a função ψ_0 definida na Proposição 5.1. Tomando o *traço*, $tr(\psi_0)$, do operador linear ψ_0 e lembrando que o traço é invariante por conjugação, obtemos:

$$\begin{aligned} tr(\psi_0) = tr\Big(\frac{1}{|G|} \cdot \sum_{g \in G} (\rho_{g^{-1}}\ \psi\ \rho_g)\Big) &= \frac{1}{|G|} \cdot \sum_{g \in G} tr(\rho_{g^{-1}}\ \psi\ \rho_g) \\ = \frac{1}{|G|} \cdot \sum_{g \in G} tr(\rho_g(\rho_{g^{-1}}\ \psi\ )) &= \frac{1}{|G|} \cdot \sum_{g \in G} tr(\ \psi\ ) = tr(\ \psi\ ) \end{aligned}$$

Por outro lado, sendo $(\mathbf{v})\psi_0 = \lambda\mathbf{v}$, temos $\psi_0 = \lambda \cdot Id_V$. Daí segue:

$tr(\psi_0) = tr(\lambda \cdot Id_V) = \lambda \cdot tr(Id_V) = \lambda \cdot dim(V)$

Comparando as duas expressões para $tr(\psi_0)$, obtemos $\lambda = tr(\psi)/dim(V)$

Corolário 5.4. *Seja G um grupo abeliano finito. Então todas as representações irredutíveis complexas de G possuem grau* 1 .

Demonstração. Sejam $\rho : G \to GL(V)$ uma representação irredutível complexa e g um elemento fixo de G. Sendo G um grupo abeliano, vale:
$\rho_g\rho_h = \rho_{gh} = \rho_{hg} = \rho_h\rho_g$, $\forall h \in G$.

Assim, $\rho_h : V \to V$ é um G-homomorfismo para todo $h \in G$ e, pela Proposição 5.2, é um operador escalar (para qualquer elemento h de G). Dessa forma, existe $\lambda_h \in \mathbb{C}$ tal que $\rho_h = \lambda_h Id_V$, $\forall \mathbf{v} \in V$.

Seja W um subespaço de dimensão 1 em V. Tomando $w \in W$, temos:
$(w)\rho_h = \lambda_h\mathbf{w} \in W$, o que mostra que W é G-invariante.

Sendo V, por hipótese, irredutível, V não pode ter subespaços G-invariantes diferentes dos triviais. Isso obriga $V = W$, acarretando $dim(V) = 1$. □

Proposição 5.5 (Teorema de Maschke)**.** *Sejam G um grupo finito e K um corpo cuja característica não divide $|G|$. Sejam $\rho : G \to GL(V)$ uma representação de G e W_1 um subespaço G-invariante de V. Então existe um subespaço G-invariante W_2 tal que $V = W_1 \oplus W_2$.*

A característica é a ordem aditiva (comum) aos elementos não-nulos de K :

- seu valor é zero, quando todos os elementos não nulos de K possuem ordem infinita
- as únicas características não nulas possíveis são números primos.
- A exigência, presente no Teorema, de que um inteiro $|G|$ não seja divisível pela característica de K, é naturalmente satisfeita por corpos de característica zero. (Esse é o caso de $\mathbb{C}$, corpo de base considerado nesse texto).

Demonstração. W_1 é G-invariante, ou seja, $(\mathbf{w})\rho_g \in W_1$, $\forall \mathbf{w} \in W_1$ e $\forall g \in G$.

Seja U um subespaço de V complementar a W_1, isto é, tal que $V = W_1 \oplus U$. Consideremos a função ϕ (projeção de V sobre W_1 ao longo de U):

$$\begin{array}{rcl} \phi : V & \to & W_1 \\ \mathbf{v} & \mapsto & (\mathbf{v})\phi = \mathbf{w} \end{array}$$

em que $\mathbf{v} = \mathbf{w} + \mathbf{u}$ é uma expressão única , com $\mathbf{w} \in W_1$ e $\mathbf{u} \in U$

Consideremos agora uma nova aplicação, G-invariante (conforme Proposição 5.1), definida a partir de ρ_g e ϕ :

$$\phi_0 : \mathbf{v} \mapsto \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{v})(\rho_{g^{-1}}\, \phi\, \rho_g)$$

Convém ressaltar que é possível construir ϕ_0 contendo $|G|$ no denominador, pois escolhemos um corpo cuja característica não divide a ordem de G.

Podemos simplificar a notação:

$$\phi_0 : \mathbf{v} \mapsto \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{v})(g^{-1}\phi g)$$

(I) Notemos, inicialmente, que ϕ_0 é uma função de V em W_1. De fato:
$(\mathbf{v})g^{-1} = \mathbf{v}g^{-1}$ e, portanto, $(\mathbf{v}g^{-1})\phi \in W_1, \forall \mathbf{v} \in V$. Além disso, sendo W_1 G-invariante, segue $((\mathbf{v}g^{-1})\phi)g \in W_1$, mostrando que $Im(\phi_0) \subseteq W_1$.

(II) Seja $\mathbf{w} \in W_1$. Vamos mostrar que ϕ_0 restrita a W_1 é a identidade de W_1.
Temos $\mathbf{w}g^{-1} \in W_1$ e, portanto:

$$(\mathbf{w})\phi_0 = \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{w})(g^{-1}\phi g) = \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{w}g^{-1})\phi \cdot g = \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{w}g^{-1}) \cdot g$$

A última igualdade é válida, pois, sendo ϕ uma projeção de V sobre W_1, temos $(\mathbf{w})\phi = \mathbf{w}$, para qualquer $\mathbf{w}$ em W_1. Segue:

$$(\mathbf{w})\phi_0 = \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{w}g^{-1}) \cdot g = \frac{1}{|G|} \cdot \sum_{g \in G} \mathbf{w} = \mathbf{w} \ \therefore \ W_1 \subseteq Im(\phi_0)$$

Por (I) e (II), temos que ϕ_0 é uma projeção de V sobre W_1 e $Im(\phi_0) = W_1$.

(III) Já vimos, na Proposição 5.1, que ϕ_0 é G-invariante. Assim, dados $h \in G$ e $\mathbf{v} \in V$, vale $(\mathbf{v})\phi_0 \cdot h = (\mathbf{v}h)\phi_0$.

(IV) A mesma Proposição 5.1 garante que $Ker(\phi_0)$ é G-invariante.

(V) Pelos fatos demonstrados até aqui, o núcleo de ϕ_0 é um candidato natural ao subespaço U que estamos buscando. Dessa forma, fazendo $W_2 = Ker(\phi_0)$, falta mostrar que $V = W_1 \oplus W_2$.

Tomando $\mathbf{v} \in W_1 \cap W_2$, temos:

- $\mathbf{0} = (\mathbf{v})\phi_0$, pois $\mathbf{v} \in Ker(\phi_0) = W_2$
- $(\mathbf{v})\phi_0 = \mathbf{v}$, pois $\mathbf{v} \in W_1$ (conforme (II))

Resulta: $W_1 \cap W_2 = \{\mathbf{0}\}$

Por outro lado, dada a transformação linear $\phi_0 : V \ \rightarrow \ W_1$, em que V é um espaço vetorial de dimensão finita, sabemos que:

$$dim(V) = dim(Im(\phi_0)) + dim(Ker(\phi_0))$$

Assim, $dim(V) = dim(W_1) + dim(W_2)$ e segue $V = W_1 \oplus W_2$. □

Corolário 5.6 (Decomposição em Representações Irredutíveis)**.** *Sejam G um grupo finito e K um corpo cuja característica não divide a ordem de G. Se V é um espaço vetorial de dimensão finita sobre K, então uma representação $\rho : G \rightarrow GL(V)$ de G é completamente redutível (soma direta de representações irredutíveis).*

Demonstração. Faremos indução sobre $dim(V)$. Se $dim(V) = 1$, a representação é irredutível (vide exemplo 5.8). Admitamos, pois, $dim(V) \geqslant 2$. Se V for irredutível, não há mais o que provar. Se V é redutível, seja $W_1 \subseteq V$ um subespaço não-trivial e G-invariante V. Pelo Teorema de Maschke, podemos construir um novo subespaço G-invariante, $W_2 \subseteq V$, que é complemento de W_1. Temos $dim(W_1) < dim(V)$, $dim(W_2) < dim(V)$ e $V = W_1 \oplus W_2$. Se W_1 e W_2 forem irredutíveis, teremos concluído a prova. Se algum deles for redutível, repetimos o procedimento. □

5.2. FUNÇÕES DE CLASSE.

Na Proposição 2.4, estabelecemos a relação entre a probabilidade de comutar, $cp(G)$, e o número de classes de conjugação, $k(G)$, em um grupo finito. Na presente seção, definimos funções que são constantes em classes de conjugação. Veremos ainda que o conjunto de tais funções é um espaço vetorial de dimensão $k(G)$. Na seção seguinte, trataremos dos caracteres associados às representações lineares, os quais constituem importante exemplo de *funções de classe*.

Definição 5.12. *Sejam G um grupo finito e K um corpo. Uma função $\varphi : G \to K$ é dita uma função de classe quando assume valores constantes em cada classe de conjugação de G, ou seja, $(h^{-1}gh)\varphi = (g)\varphi, \forall g, h \in G$.*

Seja $\mathcal{C}(G) = \{f : G \to \mathbb{C} : (h^{-1}gh)f = (g)f, \forall g, h \in G\}$ o conjunto das funções de classe do grupo G com valores em $\mathbb{C}$. Definamos as operações de soma de funções de classe e multiplicação de função de classe por escalar, respectivamente, por: $f_1 + f_2 : g \to (g)f_1 + (g)f_2$ e $\lambda \cdot f : g \to (g)f \cdot \lambda$ com $\lambda \in \mathbb{C}$. O conjunto $\mathcal{C}(G)$, munido dessas duas operações, forma um $\mathbb{C}$-espaço vetorial.

Denotemos por $C_1, C_2, \ldots, C_k$ as $k = k(G)$ classes de conjugação em G e sejam $1 = g_1, g_2, \ldots, g_k$, respectivamente, representantes de cada uma dessas classes.

As *funções características*, δ_j, das k classes de conjugação, são definidas a seguir:

$$\delta_j(g) = \begin{cases} 1, & \text{se } g \in C_j \\ 0, & \text{se } g \notin C_j \end{cases}$$

As δ_j, assim definidas, são funções de classe e formam uma base de $\mathcal{C}(G)$ e tem-se $dim_{\mathbb{C}}(\mathcal{C}(G)) = k$. De fato:

- As δ_j são linearmente independentes, pois, se $\sum_{j=1}^{k} a_j\delta_j = 0$, com $a_j \in \mathbb{C}$, para cada uma das k classes, então, para g em uma classe fixa C_m, tem-se $0 = \sum_{j=1}^{k} a_j\delta_j(g) = a_m$. Dado que isso vale para todas as classes, segue $a_j = 0,\ \forall j \in \{1, 2, \ldots, k\}$.
- As δ_j são um conjunto gerador de $\mathcal{C}(G)$, pois, dada uma função $f \in \mathcal{C}(G)$, pode-se expressá-la como $f = \sum_{j=1}^{k} f_j \cdot \delta_j$, em que f_j é o valor constante assumido por f na classe C_j.

Definição 5.13 (Produto Interno de Funções de Classe)**.** *Seja G um grupo finito. Se K é um corpo cuja característica não divide $|G|$, definimos o produto interno de duas funções de classe, α e β, através da relação:*

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g) \cdot \overline{\beta(g)} \quad \text{, em que } \overline{z} \text{ indica o complexo conjugado de } z.$$

Veremos que tal produto interno é um recurso capaz de facilitar, substancialmente, a demonstração de várias propriedades associadas a funções de classe.

5.3. CARÁTER DE UMA REPRESENTAÇÃO.

Trataremos, nessa seção, do importante conceito de caráter associado a uma representação linear. Veremos que o sistema de caracteres de uma representação tem a propriedade de ser invariante por transformações lineares semelhantes, ou seja, não dependem de uma escolha específica de base para o espaço vetorial.

Dessa forma, a análise do sistema de caracteres provê um meio para identificar representações irredutíveis, pois, mesmo que uma representação pareça diferente (por ser expressa por matrizes semelhantes), o seu caráter não será alterado. Por outro lado, as representações irredutíveis que forem efetivamente distintas (ou não-equivalentes), possuirão sistemas de caracteres diferentes.

Um resultado de grande importância será derivado na Proposição 5.10. Ali será estabelecida a conexão entre o conjunto de caracteres irredutíveis e o número de classes de conjugação em um grupo finito.

Definição 5.14. *Seja $\rho : G \to GL(V)$ uma representação de grau $\underline{n}$ do grupo finito G. O caráter de ρ (ou caráter correspondente à representação ρ) é a função:*

$$\begin{aligned}&\chi : G \to \mathbb{C}\\ &\quad g \mapsto \chi(g) = tr(\rho_g),\end{aligned}$$

em que $tr(M)$ denota o traço da matriz $M = (a_{ij})$, isto é, $tr(M) = \sum_{k=1}^{n} a_{kk}$.

Com essa definição, vemos que o caráter, $\chi(g)$, de um elemento $g \in G$ é o traço da matriz que o representa. Além disso, dado o grupo finito $G = g_1, g_2, \ldots, g_n$, dizemos que $\chi(g_1), \chi(g_2), \ldots, \chi(g_n)$ é um sistema de caracteres para a representação em análise. Conforme veremos mais adiante, caracteres são funções de classe e, portanto, para obter o sistema de caracteres de um grupo é necessário considerar apenas um representante de cada classe de conjugação.

O caráter de uma representação irredutível será chamado de *caráter irredutível*.

Proposição 5.7 (Propriedades Básicas dos Caracteres)**.** *Sejam ρ uma representação de grau $\underline{n}$ e χ o caráter associado. São válidas as seguintes propriedades:*

(a) $\chi(1) = n$
(b) $\chi(g^{-1}) = \overline{\chi(g)}$, *para $g \in G$. (Nota: $\overline{z}$ denota o complexo conjugado de z).*
(c) *Para um qualquer $g \in G$, vale $|\chi(g)| \leqslant n$.*
(d) $|\chi(g)| = n$ *se, e somente se, ρ_g é escalar.*
(e) $\chi(g) = n$ *se, e somente se, ρ_g é a identidade.*
(f) $\chi(tgt^{-1}) = \chi(g)$, $\forall t, g \in G$, *ou seja, o caráter de uma representação é constante em classes de conjugação. (χ é uma função de classe).*
(g) *Se χ é um caráter irredutível de G, então a função $\overline{\chi}$, em que $\overline{\chi}(g) = \overline{\chi(g)}$, é também um caráter irredutível.*
(h) *Sejam $\rho : G \to GL(V)$ e $\tau : G \to GL(W)$ duas representações do grupo G. Se χ_ρ e χ_τ são, respectivamente, os caracteres associados a ρ e τ, o caráter $\chi_{\rho\oplus\tau}$, associado à soma direta $\rho \oplus \tau$, é dado por $\chi_{\rho\oplus\tau} = \chi_\rho + \chi_\tau$.*
(i) *O caráter de uma representação é uma soma de caracteres irredutíveis.*

Demonstração. (a) $\rho(1) = I_n \therefore \chi(1) = tr(I_n) = n$

(b) (I) Fixemos $g \in G$. Sendo G um grupo finito, vale $g^{|G|} = 1$.

(II) Se λ é um autovalor de ρ_g, então existe vetor não-nulo $\mathbf{v} \in V$, satisfazendo $(\mathbf{v})\rho_g = \mathbf{v}\lambda$. Assim, $(\mathbf{v})\rho_{g^{|G|}} = (\mathbf{v})\rho_g^{|G|} = \mathbf{v}\lambda^{|G|}$. Usando (a) e lembrando que $(\mathbf{v})\rho_1 = \mathbf{v}$, segue: $\mathbf{v} = \mathbf{v}\lambda^{|G|}$, com $\mathbf{v} \neq \mathbf{0}$, o que significa que $\lambda^{|G|} = 1$. Em particular, tem-se $|\lambda| = 1$ e, portanto, $\overline{\lambda} = \lambda^{-1}$.

(III) Por outro lado, sendo λ autovalor de ρ_g, tem-se:

$\mathbf{v} = ((\mathbf{v})\rho_g)\rho_{g^{-1}} = (\mathbf{v}\lambda)\rho_{g^{-1}} = (\mathbf{v})\rho_{g^{-1}} \cdot \lambda$

Assim: $\mathbf{v} \cdot \lambda^{-1} = (\mathbf{v})\rho_{g^{-1}}$, ou seja, λ^{-1} é autovalor de $\rho_{g^{-1}}$

(IV) Usando agora o fato que o traço de ρ_g é a soma dos autovalores dessa matriz, podemos finalizar a prova de (b):

$$\chi(g^{-1}) = tr(\rho_{g^{-1}}) = \sum_{i=1}^{n} {\lambda_i}^{-1} = \sum_{i=1}^{n} \overline{\lambda_i} = \overline{\sum_{i=1}^{n} \lambda_i} = \overline{tr(\rho_g)} = \overline{\chi(g)}$$

(c) Seja $g \in G$ um elemento de ordem m. Conforme visto em (b), $\chi(g) = \sum_{i=1}^{n} \lambda_i$, em que os autovalores λ_i são raízes m-ésimas da unidade. Assim:

$$|\chi(g)| = \left| \sum_{i=1}^{n} \lambda_i \right| \leqslant \sum_{i=1}^{n} |\lambda_i| = \sum_{i=1}^{n} 1 = n$$

(d) Se ρ_g é escalar, todos os autovalores λ_i são iguais. Fazendo $\lambda_i = \lambda$, obtemos $\chi(g) = n \cdot \lambda$. Sendo $|\lambda| = 1$, segue $|\chi(g)| = n$.

Reciprocamente, admitamos $|\chi(g)| = n$. Dado que $|\lambda_i| = 1$, devemos ter $\lambda_i = \lambda$. O polinômio característico de ρ_g é $(x-\lambda)^n$. Se m é a ordem de g, um autovalor λ de ρ_g também satisfaz $x^m - 1$. Mas $x^m - 1 = (x-\lambda)(x^{m-1} + \lambda^2 x^{m-2} + \cdots + \lambda^{m-1}x)$ e, portanto, λ é raiz do mdc, $(x - \lambda)$, dos dois polinômios. Dessa forma, ρ_g é a multiplicação por λ, evidenciando que ρ_g é escalar.

(e) Se $\chi(g) = n$, então $|\chi(g)| = n$ e, portanto, $\chi(g)$ é escalar (d). Desse último fato, decorre $\chi(g) = n \cdot \lambda$, donde segue $\lambda = 1$, demonstrando que ρ_g é a identidade. A recíproca já foi demonstrada em (a).

(f) Usamos o fato que $tr(AB) = tr(BA)$

$$\chi(tgt^{-1}) = tr(\rho_{tgt^{-1}}) = tr(\rho_{tg}\rho_{t^{-1}}) = tr(\rho_{t^{-1}}\rho_{tg}) = tr(\rho_{t^{-1}tg}) = tr(\rho_g) = \chi(g)$$

(g) Seja χ o caráter associado à representação irredutível $\rho : G \to GL(V)$. Denotemos por $\overline{V}$ o espaço vetorial obtido conjugando as coordenadas dos vetores de V. Temos que $\overline{\rho} : G \to GL(\overline{V})$, definida por $\overline{\rho}(g) := \overline{\rho(g)}$, é uma representação de G, pois corresponde à composição de ρ com a conjugação complexa, que é homomorfismo de grupos. Além disso:

$$\chi_{\overline{\rho}}(g) = Tr(\overline{\rho}(g)) = Tr(\overline{\rho(g)}) = \overline{Tr(\rho(g))} = \overline{\chi_\rho(g)}$$

Assim, $\overline{\chi}$ é, especificamente, o caráter associado à representação $\overline{\rho}$.

Admitamos agora que χ é irredutível. Se $W < \overline{V}$ é um subespaço próprio e $\overline{\rho}$-invariante de $\overline{V}$, então $\overline{W}$ é um subespaço próprio ρ-invariante de V. Dado que ρ é irredutível, devemos ter $\overline{W} = \{0\}$ e, conseqüentemente, $W = \{0\}$. Daí segue que $\overline{\chi}$ é irredutível.

(h) Decorre diretamente de $tr(A \oplus B) = tr(A) + tr(B)$ (vide Proposição 7.1).

(i) Unindo o fato expresso em (h) ao Teorema de Maschke, vemos que o caráter de uma representação é a soma dos caracteres das representações irredutíveis em que ela se decompõe, ou seja, a soma de seus caracteres irredutíveis.

□

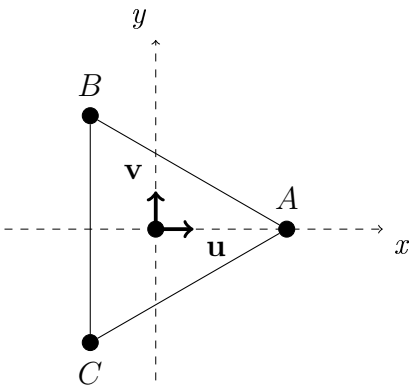
Exemplo 5.15. *Tabela de Caracteres do grupo cíclico C_4*

É interessante revisitar os Exemplos 5.4 e 5.8 . Representações complexas de grau 1 são irredutíveis (e correspondem a matrizes 1×1). Dessa forma, tais representações coincidem com seus caracteres. Outro ponto importante é que os caracteres mostrados na tabela abaixo são todos irredutíveis. A tabela ainda ilustra que, por estarmos trabalhando com funções de $G \to \mathbb{C}$, é perfeitamente normal que alguns caracteres assumam valores imaginários.

caráter	***elementos do Grupo***			
	$\mathbf{1}$	$\mathbf{g}$	$\mathbf{g^2}$	$\mathbf{g^3}$
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	i	-1	$-i$
χ_4	1	$-i$	-1	i

Exemplo 5.16. *Representações de grau 2 para S_3 e caracteres associados*

Assim como fizemos no Exemplo 5.9, vamos considerar o isomorfismo $S_3 \cong D_3$. Nossa proposta é construir duas representações distintas de grau 2 para esse grupo. Inicialmente, usaremos um sistema de 2 eixos ortogonais com origem no baricentro do triângulo equilátero. Em vez de pensar na representação dos vértices, veremos o efeito de cada simetria (rotação, reflexão) sobre o par de eixos considerados. Essa simples mudança de perspectiva permite que tenhamos uma representação de grau inferior àquela do exemplo original.

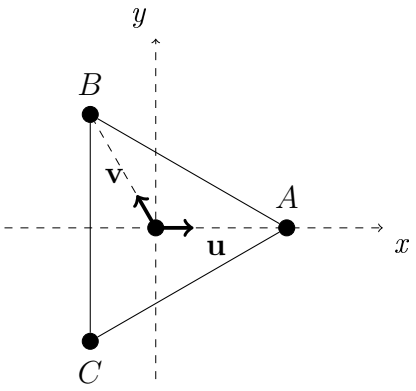


$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad R = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \quad R^2 = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad S_2 = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix} \quad S_3 = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$$

Para o mesmo triângulo, consideremos um novo sistema de eixos $\mathbf{u}, \mathbf{v}$*:*

- *o ângulo entre os eixos coordenados* $\mathbf{u}$ *e* $\mathbf{v}$ *é de* $120°$
- *a origem do sistema de eixos coincide com o baricentro do triângulo*



$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad R = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad R^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \quad RS = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \quad R^2S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Esse exemplo reforça vários aspectos já discutidos:

- *Caracteres são funções de classe. Para uma dada representação, o valor do caráter independe do representante escolhido para a classe;*
- *Caracteres são invariantes por mudança de base.*

A tabela de caracteres a seguir, resume tais fatos. Ao comparar as duas representações equivalentes, é interessante observar que $S_2 = RS$ e $S_3 = R^2S$. Sugere-se ao leitor, calcular os traços das matrizes que representam os elementos do grupo.

caráter	***representante da classe***		
	Id	***R***	***S***
χ	2	-1	0

Proposição 5.8 (Relações de Ortogonalidade de Schur)**.** *Sejam $\rho : G \to GL(V)$ e $\tau : G \to GL(W)$ duas representações irredutíveis do grupo G. Sejam χ_ρ e χ_τ os caracteres associados, respectivamente, a ρ e τ. São válidos os seguintes fatos:*

(a) $\langle \chi_\rho, \chi_\tau \rangle = 0$ *, se ρ e τ são não-isomorfas.*

(b) $\langle \chi_\rho, \chi_\tau \rangle = 1$ *, se $\rho \cong \tau$.*

Demonstração. Fixemos bases para os espaços V e W e sejam $M(g)$ e $Q(g)$ as matrizes associadas, respectivamente, a ρ_g e τ_g. Temos:

$$\langle \chi_\rho, \chi_\tau \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \cdot \overline{\chi_\tau(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \cdot \chi_\tau(g^{-1})$$

$$= \frac{1}{|G|} \sum_{g \in G} tr(M(g)) \cdot tr(Q(g^{-1}))$$

Dada a aplicação linear $\psi : V \to W$, sabemos que:

$$\psi_0 : \mathbf{v} \ \mapsto \ \frac{1}{|G|} \cdot \sum_{g \in G} (\mathbf{v})(\rho_{g^{-1}} \, \psi \, \tau_g) \text{ é um } G\text{-homomorfismo (Proposição 5.1)} \quad \text{(I)}$$

Seja $\psi(\alpha, \beta)$ uma aplicação linear cuja matriz associada $P(\alpha, \beta)$ que satisfaz:

- $(P(\alpha, \beta))_{ij} = 1$, quando $i = \alpha$ e $j = \beta$
- $(P(\alpha, \beta))_{ij} = 0$, em todas as outras entradas.

Descrevemos a seguir o efeito do produto de matrizes envolvendo $P = P(\alpha, \beta)$:

- Seja $C = M(g) \cdot P$. Tal multiplicação move a coluna α de $M(g)$ para a coluna β de C. Todas as entradas fora da coluna β serão nulas.

- Seja $D = C \cdot Q$. A multiplicação por C afeta apenas a linha β de Q. Um elemento não-nulo da linha i de C aparecerá como fator apenas na linha i de D. Um elemento $q_{\beta j}$ de Q aparecerá como fator apenas na coluna j da matriz resultante D.

Seja $\psi_0(\alpha, \beta)$ uma aplicação linear construída a partir de $\psi(\alpha, \beta)$, de forma análoga ao que fizemos em (I). Matricialmente, podemos escrever:

$$(\psi_0(\alpha,\beta))_{ij} = \frac{1}{|G|}\sum_{g\in G}(M(g)\cdot P(\alpha,\beta)\cdot Q(g^{-1}))_{ij} \ , \ \forall i,j \ .$$

Considerando o efeito da multiplicação de matrizes $P(\alpha, \beta)$, obtemos:

$$(\psi_0(\alpha,\beta))_{ij} = \frac{1}{|G|}\sum_{g\in G}(M(g)\cdot P(\alpha,\beta)\cdot Q(g^{-1}))_{ij} = \frac{1}{|G|}\sum_{g\in G}(M(g))_{i\alpha}\cdot(Q(g^{-1}))_{\beta j} \quad \text{(II)}$$

Calculemos, agora, a soma $\sum_{\alpha,\beta}(\psi_0(\alpha,\beta))_{\alpha\beta}$. Fazendo $i = \alpha$ e $j = \beta$ em (II), vem:

$$\begin{aligned}
\sum_{\alpha,\beta}(\psi_0(\alpha,\beta))_{\alpha\beta} &= \sum_{\alpha,\beta}\Big(\frac{1}{|G|}\sum_{g\in G}(M(g))_{\alpha\alpha}\cdot(Q(g^{-1}))_{\beta\beta}\Big) \\
&= \frac{1}{|G|}\sum_{g\in G}\Big(\sum_{\alpha,\beta}(M(g))_{\alpha\alpha}\cdot(Q(g^{-1}))_{\beta\beta}\Big) \\
&= \frac{1}{|G|}\sum_{g\in G}\Big(\sum_{\alpha}(M(g))_{\alpha\alpha}\Big)\cdot\Big(\sum_{\beta}(Q(g^{-1}))_{\beta\beta}\Big) \\
&= \frac{1}{|G|}\sum_{g\in G} tr((M(g))\cdot tr(Q(g^{-1})) \\
&= \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g)\cdot\chi_\tau(g^{-1}) = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g)\cdot\overline{\chi_\tau(g)} \\
&= \langle\chi_\rho,\chi_\tau\rangle \qquad \text{(III)}
\end{aligned}$$

Aplicaremos o que foi discutido até aqui à demonstração dos ítens (a) e (b).

(a) Sendo $\psi_0 : V \to W$ um G-homomorfismo e $\rho \ncong \tau$ (com ρ e τ irredutíveis), a Proposição 5.2 garante que ψ_0 é a função nula (para qualquer $\psi : V \to W$, linear). Tal resultado vale, em particular, para as aplicações lineares $\psi(\alpha, \beta)$ e $\psi_0(\alpha, \beta)$, que acabamos de analisar. Para ρ e τ não-isomorfas, temos $\psi_0(\alpha, \beta) = 0$ para quaisquer valores de α e β , de modo que a soma em (III) se anula. Daí segue:

$\langle\chi_\rho, \chi_\tau\rangle = \sum_{\alpha,\beta}(\psi_0(\alpha,\beta))_{\alpha\beta} = 0$, o que completa a prova.

(b) O caso $\rho \cong \tau$ significa que existe $f : V \to W$ que é um G-isomorfismo. Ou seja: $(\mathbf{v})(f \circ \tau_g) = (\mathbf{v})(\rho_g \circ f)$, $\forall g \in G$, $\forall \mathbf{v} \in V$, em que f é bijetiva.

Do fato $\rho_g f = f\tau_g$, decorre: $\rho_g = f\tau_g f^{-1}$ e, calculando o traço:
$tr(\rho_g) = tr(f\tau_g f^{-1}) = tr(\tau_g)$ (conforme Proposição 5.7)

Assim, o caso (b) corresponde a $\chi_\rho = \chi_\tau = \chi$ e queremos mostrar que $\langle \chi, \chi \rangle = 1$. Podemos supor, sem perda de generalidade, que $W = V$. Nessa situação específica, temos $\psi_0(\alpha, \beta) : V \to V$, em que V é irredutível e tem dimensão n .

Conforme visto no corolário 5.3 do Teorema de Schur, valem os seguintes fatos:

- $tr(\psi_0(\alpha, \beta)) = tr(\psi(\alpha, \beta))$.

- O G-endomorfismo $\psi_0(\alpha, \beta)$ é uma multiplicação por escalar:
  $(\mathbf{v})\psi_0(\alpha, \beta) = \lambda_{\alpha\beta}\, \mathbf{v}, \forall \mathbf{v} \in V$ e $\psi_0(\alpha, \beta) = \lambda_{\alpha\beta}\, id_V$, com $\lambda_{\alpha\beta} \in \mathbb{C}$

- O escalar $\lambda_{\alpha\beta}$ é dado por $\lambda_{\alpha\beta} = \dfrac{tr(\psi_0(\alpha, \beta))}{dim(V)} = \dfrac{tr(\psi_0(\alpha, \beta))}{n}$

A matriz $n \times n$ associada a $\psi_0(\alpha, \beta)$ é escalar e, portanto, todos os elementos de sua diagonal principal são iguais a $\lambda_{\alpha\beta}$. Além disso, as entradas $\alpha\beta$ de uma matriz escalar são nulas sempre que $\alpha \neq \beta$ e a soma em (III) se reduz a uma soma em α, conforme mostrado a seguir:

$$\begin{aligned}
\sum_{\alpha,\beta} (\psi_0(\alpha, \beta))_{\alpha\beta} &= \sum_{\alpha} (\psi_0(\alpha, \alpha))_{\alpha\alpha} \\
&= \sum_{\alpha=1}^{n} \lambda_{\alpha\alpha} = \sum_{\alpha=1}^{n} \frac{1}{n} \cdot tr(\psi_0(\alpha, \alpha)) \\
&= \sum_{\alpha=1}^{n} \frac{1}{n} \cdot tr(\psi(\alpha, \alpha)) = \sum_{\alpha=1}^{n} \frac{1}{n} \cdot tr(P(\alpha, \alpha)) \\
&= \sum_{\alpha=1}^{n} \frac{1}{n} \cdot 1 = \sum_{\alpha=1}^{n} \frac{1}{n} = 1
\end{aligned}$$

Revisitando a relação obtida em (III), concluímos a demonstração:

$$\langle \chi, \chi \rangle = \langle \chi_\rho, \chi_\tau \rangle = \sum_{\alpha,\beta} (\psi_0(\alpha, \beta))_{\alpha\beta} = 1$$ □

Corolário 5.9. *O produto interno de dois caracteres complexos é um número inteiro não-negativo.*

Demonstração. Vimos na Proposição 5.7 que, em conseqüência do *Teorema de Maschke*, o caráter de uma representação é uma soma de caracteres irredutíveis. Mas, pela Proposição 5.8, sabemos que o produto interno de caracteres irredutíveis vale 0 ou 1. □

Proposição 5.10 (Teorema Fundamental sobre Caracteres Irredutíveis)**.** *Seja* $\{\chi_1, \ldots, \chi_m\} = \mathcal{B} \subseteq \mathcal{C}(G)$ *o conjunto dos caracteres irredutíveis. São válidas as seguintes propriedades:*

(a) $\mathcal{B}$ *é uma base ortonormal do espaço vetorial das funções de classe,* $\mathcal{C}(G)$.
(b) *O número de caracteres irredutíveis de* G *coincide com o número de classes de conjugação, ou seja,* $k(G) = dim(\mathcal{C}(G))$

Demonstração. (a) Provemos inicialmente que caracteres irredutíveis distintos, $\chi_1, \ldots, \chi_m$, são linearmente independentes. (Isso é uma conseqüência de serem ortonormais, conforme Proposição 5.8).

Seja $a_1 \cdot \chi_1 + \cdots + a_m \cdot \chi_m = 0$, com $a_i \in \mathbb{C}$.

Tomando o produto interno dessa soma com χ_i , $1 \leqslant i \leqslant m$, obtemos:

$$0 = \langle a_1 \cdot \chi_1 + \cdots + a_i \cdot \chi_i + \cdots + a_m \cdot \chi_m \ , \ \chi_i \rangle \ = \ a_1 \cdot \langle \chi_1, \chi_i \rangle + \cdots + a_i \cdot \langle \chi_i, \chi_i \rangle + \cdots + a_m \cdot \langle \chi_m, \chi_i \rangle = a_i$$

Seja $f \in \mathcal{C}(G)$ e denotemos $\langle f \ , \ \chi_i \rangle = a_i \ , \forall i$. Mostraremos que $f = \sum_i a_i \cdot \chi_i$

Pela definição de cada a_i, temos: $\langle f - \sum_i a_i \cdot \chi_i \, , \, \chi_j \rangle = a_j - a_j = 0$, o que significa que $f - \sum_i a_i \cdot \chi_i$ é ortogonal a todo caráter irredutível. Logo, basta mostrar que se $f \in \mathcal{C}(G)$ é ortogonal a todo $\chi \in \mathcal{B}$, então $f = 0$.

Seja $f \in \mathcal{C}(G)$ tal que $\langle f, \chi \rangle = 0$ para todo $\chi \in \mathcal{B}$. Se $\pi : G \to GL(V)$ é uma representação de G, então $\pi_f : V \to V$ definida por: $\pi_f(v) := \dfrac{1}{|G|} \sum_{g \in G} f(g)\pi_g(v)$ é um homomorfismo G-invariante. De fato:

$$\pi_x(\pi_f(v)) = \pi_x \left(\frac{1}{|G|} \sum_{g \in G} f(g)\pi_g(v) \right) = \frac{1}{|G|} \sum_{g \in G} f(g)\pi_{xg}(v)$$
$$= \frac{1}{|G|} \sum_{g \in G} f(x^{-1}gx)\pi_{x(x^{-1}gx)}(v) = \frac{1}{|G|} \sum_{g \in G} f(g)\pi_g(\pi_x(v)) = \pi_f(\pi_x(v)).$$

Assim, se π é irredutível então $\pi_f = \lambda Id_V$, com $\lambda \in \mathbb{C}$ (Proposição 5.2). Sendo $tr(\pi_f) = \lambda \cdot tr(Id_V) = \lambda n$, segue $\lambda = tr(\pi_f)/n$, em que $n = \dim_{\mathbb{C}}(V)$.

Por outro lado: $tr(\pi_f) = \dfrac{1}{|G|}\displaystyle\sum_{g\in G} f(g)tr(\pi_g) = \dfrac{1}{|G|}\sum_{g\in G} f(g)\chi_\pi(g) = \langle f, \overline{\chi_\pi}\rangle = 0$

A última igualdade é válida, pois $\overline{\chi_\pi}$ é um caráter irredutível de G sempre que χ_π é irredutível (conforme Proposição 5.7). Daí resulta $\lambda = 0$ e, portanto, $\pi_f = 0$ para todo caráter irredutível π de G. Além disso, $\pi_f = 0$ para todo caráter π de G (pois todo caráter é soma de irredutíveis). Em particular, $\rho_f = 0$, em que ρ é a representação regular $G \to GL(V)$ onde $V = \mathbb{C}^G$.

Seja $\{e_x \ : \ x \in G\}$ a base canônica de V com a ação regular de G dada por $(e_x)\rho_g = e_{xg}$. Como $\rho_f = 0$,

$$0 = \rho_f(e_1) = \frac{1}{|G|}\sum_{g\in G} f(g)\rho_g(e_1) = \frac{1}{|G|}\sum_{g\in G} f(g)e_g$$

logo $f(g) = 0$ para todo $g \in G$, pois os e_g são linearmente independentes. Isso mostra que $f = 0$.

(b) Já sabemos que as funções características, δ_j, das k classes de conjugação formam uma base do espaço $\mathcal{C}(G)$ das funções de classe. Além disso, tem-se $dim_{\mathbb{C}}(\mathcal{C}(G)) = k$, donde segue a tese. □

Proposição 5.11. *Sejam $\rho : G \to GL(V)$ uma representação do grupo finito G e φ o caráter associado. Suponha que V pode ser decomposto na seguinte soma direta de subespaços irredutíveis $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$. Sejam ρ_i a representação em cada W_i e χ_i o caráter associado. São válidos os seguintes fatos:*

(a) *O número de representações ρ_j isomorfas a ρ_i é $\langle \varphi, \chi_i\rangle = m_i$. O número m_i é chamado de multiplicidade de W_i em V ou multiplicidade de ρ_i em ρ;*

(b) $\langle \varphi, \varphi\rangle = \displaystyle\sum_{i=1}^{r} {m_i}^2$.

Demonstração. (a) Usando a hipótese, $\varphi = \chi_1 + \cdots + \chi_k$, podemos escrever:

$\langle \varphi, \chi_i\rangle = \langle \chi_1, \chi_i\rangle + \cdots + \langle \chi_k, \chi_i\rangle$

Se uma representação ρ_j que aparece na decomposição de φ é não-isomorfa a ρ_i , a Proposição 5.8 garante que $\langle \chi_i, \chi_j \rangle = 0$. Isso nos permite concluir que a expressão para φ como soma de caracteres irredutíveis contém tantos termos iguais a 1 quantos forem as ρ_j equivalentes a ρ_i .

(b) Se um subespaço irredutível W_i aparece m_i vezes em V como um somando direto, temos:

- $V = m_1 W_1 \oplus m_2 W_2 \oplus \cdots \oplus m_r W_r$
- $\varphi = m_1 \chi_1 + m_2 \chi_2 + \cdots + m_r \chi_r$

Por outro lado:

$$\langle \varphi, \varphi \rangle = \Big\langle \sum_i m_i \chi_i \, , \, \sum_j m_j \chi_j \Big\rangle = \sum_{i,j} m_i m_j \langle \chi_i, \chi_j \rangle$$

Levando em conta que $\langle \chi_i, \chi_j \rangle = 0$ se $i \neq j$ e que $\langle \chi_i, \chi_i \rangle = 1$, segue:

$$\langle \varphi, \varphi \rangle = \sum_{i=1}^{r} {m_i}^2$$

□

Proposição 5.12. *Sendo G um grupo finito, são válidos os seguintes fatos:*

(a) *Uma representação irredutível de grau n_i de G aparece na decomposição da representação regular com multiplicidade n_i ;*

(b) *Sejam k o número de classes de conjugação de G e n_i o grau da representação irredutível ρ_i de G. Os graus n_i satisfazem a seguinte relação:*
$\sum_{i=1}^{k} {n_i}^2 = |G|$.

Demonstração. O caráter da representação regular (vide seção 7.2) é dado por:

$$\varphi(g) = \begin{cases} 0 \, , & \text{se } g \neq 1 \\ |G|, & \text{se } g = 1 \end{cases}$$

(a) Seja χ_i o caráter associado à representação irredutível ρ_i. Pela proposição 5.7, temos: $\chi_i(1) = n_i$. Usando a definição do produto interno e levando em conta que φ é o caráter da representação regular, podemos escrever:

$$m_i = \langle \varphi, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\chi_i(g)} = \frac{1}{|G|} \cdot |G| \cdot \overline{\chi_i(1)} = \chi_i(1) = n_i$$

(b) Pela proposição 5.11, temos: $\varphi = m_1 \chi_1 + m_2 \chi_2 + \cdots + m_k \chi_k$. Por outro lado, o item (a) fornece $m_i = \chi_i(1) = n_i$. Assim:

$$\varphi = \sum_{i=1}^{k} n_i \chi_i$$

Lembrando que $\varphi(1) = |G|$, podemos avaliar a última expressão em $1 \in G$:

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

□

Exemplo 5.17. *Tabela de Caracteres Irredutíveis do Grupo* S_3

Como aplicação da Proposição 5.12, podemos ver que o grupo $S_3 \cong D_3$ *possui a seguinte composição de caracteres irredutíveis (dois de grau* 1 *e um de grau* 2*):*
$|S_3| = 6 = 1^2 + 1^2 + 2^2$

Algumas informações relevantes sobre a tabela:

- *a primeira coluna da tabela traz o valor de* $\chi_i(1)$*, em que* χ_i *é o caráter associado a uma representação irredutível* ρ_i *;*
- χ_1 *é o caráter associado à representação trivial;*
- χ_2 *é o caráter associado à representação sinal;*
- *os valores de* χ_3 *foram obtidos a partir do Exemplo 5.16.*

caráter	***representante da classe***			***grau***
	Id	(123)	(23)	
χ_1	1	1	1	1
χ_2	1	1	-1	1
χ_3	2	-1	0	2
elementos na classe	1	2	3	

Talvez seja instrutivo revisitar o Exemplo 5.15, sob a luz da Proposição 5.12. Devemos ter a seguinte decomposição: $|C_4| = 4 = 1^2 + 1^2 + 1^2 + 1^2$*. Isso reforça que todas as representações irredutíveis de* C_4 *são de grau* 1*, o que é coerente com o fato de tal grupo ser abeliano (vide Corolário 5.4).*

5.4. O TEOREMA DE FROBENIUS-SCHUR.

Tendo apresentado as propriedades básicas de representações e caracteres, nosso próximo objetivo é o estudo do Teorema de Frobenius-Schur, o qual permite obter informações sobre a quantidade de involuções em um grupo de ordem par. Esse resultado será diretamente utilizado na demonstração do Teorema 6.1.

Lema 5.13. *Seja G um grupo finito. Dados $g \in G$ e $n > 0$, consideremos a função θ_n, que fornece o número de raízes n-ésimas de g em G :*

$$\begin{aligned} \theta_n : G &\to \mathbb{C} \\ g &\mapsto \theta_n(g) = |\{x \in G : x^n = g\}| \end{aligned}$$

Para a função θ_n ,assim definida, são válidos os seguintes fatos:

(a) *θ_n é uma função de classe;*

(b) $\theta_n = \sum_{\chi \in Irr(G)} \nu_n(\chi) \cdot \chi$, *em que $\nu_n(\chi) \in \mathbb{C}$ é unicamente determinado;*

(c) *Na expressão de θ_n, tem-se:* $\nu_n(\chi) = \frac{1}{|G|} \cdot \sum_{g \in G} \theta_n(g) \cdot \overline{\chi(g)} = \frac{1}{|G|} \cdot \sum_{g \in G} \chi(g^n)$.

Demonstração. (a) Vejamos que θ_n é, de fato, uma função de classe:

$$\begin{aligned} \theta_n(h^{-1}gh) &= \left|\{ x \in G : x^n = h^{-1}gh \}\right| \\ &= \left|\{ x \in G : hx^nh^{-1} = g \}\right| = \left|\{ x \in G : (hxh^{-1})^n = g\}\right| \end{aligned}$$

Mas a conjugação por um elemento fixo $h \in G$ é uma bijeção. Dessa forma, para cada y que satisfaz $y^n = g$, existe um único $x \in G$ tal que $x = h^{-1}yh$. Daí resulta:

$$\theta_n(h^{-1}gh) = \left|\{ x \in G : (hxh^{-1})^n = g \}\right| = |\{ y \in G : y^n = g \}| = \theta_n(g).$$

(b) Os caracteres irredutíveis associados a um grupo finito G formam uma base ortonormal para o espaço $\mathcal{C}(G)$ das funções de classe de G. Assim, uma função $\theta_n \in \mathcal{C}(G)$ pode ser expressa na forma:

$\theta_n = \sum_{\chi \in Irr(G)} \nu_n(\chi) \cdot \chi$, em que $\nu_n(\chi) \in \mathbb{C}$ é unicamente determinado.

(c) Sendo χ e θ_n duas funções de classe, podemos recorrer ao produto interno:

$$\theta_n = \sum_{\chi \in Irr(G)} \nu_n(\chi) \cdot \chi \;\Rightarrow\; \nu_n(\chi) = \langle \theta_n, \chi \rangle = \frac{1}{|G|} \cdot \sum_{g \in G} \theta_n(g) \cdot \overline{\chi(g)}$$

Dado que θ_n é um número de raízes, podemos removê-lo do somando $\theta_n(g) \cdot \overline{\chi(g)}$:

$$\theta_n(g) \cdot \overline{\chi(g)} = \sum_{h \in G,\, h^n = g} \overline{\chi(h^n)}$$

Obtemos, então, uma série de expressões equivalentes para o coeficiente $\nu_n(\chi)$:

$$\nu_n(\chi) = \frac{1}{|G|} \sum_{g \in G} \theta_n(g) \cdot \overline{\chi(g)} = \frac{1}{|G|} \sum_{h \in G} \overline{\chi(h^n)} = \frac{1}{|G|} \sum_{h \in G} \chi((h^{-1})^n) = \frac{1}{|G|} \sum_{g \in G} \chi(g^n)$$

□

Proposição 5.14 (Teorema de Frobenius-Schur)**.** *Consideremos a representação $\rho : G \to GL(V)$, de grau $\underline{n}$, do grupo finito G. Sendo $\chi \in Irr(G)$ um caráter irredutível associado a tal representação, valem os seguintes fatos:*

(a) *Sendo φ uma função de classe de G e $n > 0$ um inteiro, a função $\varphi^{(n)}$ definida por $\varphi^{(n)}(g) = \varphi(g^n)$ é uma função de classe.*
(b) *$\chi^{(2)}(g) = \chi(g^2)$ é uma diferença de caracteres.*
(c) *Os valores possíveis para $\nu_2(\chi)$ são 1, -1 ou 0. Tal função é conhecida como o indicador de Frobenius-Schur.*
(d) *$\nu_2(\chi) \neq 0$ se, e somente se, χ é uma função com valores reais.*

Demonstração. (a) Temos que $\varphi(h^{-1}gh) = \varphi(g)$, pois, por hipótese, φ é uma função de classe.

$$\varphi^{(n)}(h^{-1}gh) = \varphi((h^{-1}gh)^n) = \varphi(h^{-1}g^nh) = \varphi(g^n) = \varphi^{(n)}(g)$$

Com essa notação, o coeficiente $\nu_n(\chi)$ definido no Lema 5.13 se escreve:

$$\nu_n(\chi) = \frac{1}{|G|} \cdot \sum_{g \in G} \chi(g^n) = \frac{1}{|G|} \cdot \sum_{g \in G} \chi^{(n)}(g) = \langle\, \chi^{(n)}, 1 \,\rangle \text{ , para } \chi \in Irr(G).$$

(b) (I) Sejam V um $\mathbb{C}G$-módulo e χ o caráter associado. Seja $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ uma base para V. Os elementos da forma $v_i \otimes v_j$, em que $1 \leqslant i, j \leqslant n$, constituem uma base (de dimensão n^2) para o produto tensorial $W = V \otimes V$.

Definamos agora a transformação linear "$*$" para elementos de uma base de W. (A partir daí, usando linearidade, a definição poderá ser estendida a um elemento genérico de W):

$$\begin{array}{rccc} * : & W & \to & W \\ & (v_i \otimes v_j) & \mapsto & (v_i \otimes v_j)^* = (v_j \otimes v_i) \end{array}$$

Consideremos os seguintes subespaços de W:

$$W_S = \{w \in W \mid w^* = w\} \text{ e } W_A = \{w \in W \mid w^* = -w\}$$

Dado $w \in W$, temos:

- $(w + w^*)^* = w^* + w = w + w^* \ \therefore \ w + w^* \in W_S$
- $(w - w^*)^* = w^* - (w^*)^* = w^* - w = -(w - w^*) \ \therefore \ w - w^* \in W_A$

Para um qualquer $w \in W$, podemos escrever: $w = \dfrac{w + w^*}{2} + \dfrac{w - w^*}{2}$, ou seja, $W = W_S + W_A$.

Um elemento $w \in W_S \cap W_A$, deve satisfazer $w = w^* = -w$, o que só ocorre quando $w = 0$. Conclui-se que $W_S \cap W_A = \{0\}$ e resulta: $W = W_S \oplus W_A$.

Agora que sabemos que W é expresso como uma soma direta, podemos buscar bases para os subespaços W_S e W_A. Notemos que:

A) os elementos da forma $v_i \otimes v_i$ pertencem a W_S. Há n desses elementos;
B) os elementos $v_i \otimes v_j + v_j \otimes v_i$ pertencem a W_S ;
C) os elementos $v_i \otimes v_j - v_j \otimes v_i$ pertencem a W_A ;
D) há $\binom{n}{2}$ elementos do tipo (B) em W_S e $\binom{n}{2}$ do tipo (C) em W_A ;
E) $n^2 = n + \binom{n}{2} + \binom{n}{2}$.

Usaremos essa base de W_A no item (V).

(II) Dados $x, y \in V$, vale, de forma geral: $(x \otimes y)^* = y \otimes x$.

$$\Big(\Big(\sum_i a_i v_i\Big) \otimes \Big(\sum_j b_j v_j\Big)\Big)^* = \Big(\sum_{i,j} a_i b_j v_i \otimes v_j\Big)^* = \sum_{i,j} a_i b_j (v_i \otimes v_j)^* =$$

$$= \sum_{i,j} a_i b_j (v_j \otimes v_i) = \Big(\sum_j b_j v_j\Big) \otimes \Big(\sum_i a_i v_i\Big)$$

(III) Dados $g \in G$ e $v_i, v_j \in V$, definamos uma ação de G sobre $W = V \otimes V$ para elementos de uma base de W:

$$\begin{array}{rccc} \mu: & W \times G & \to & W \\ & (v_i \otimes v_j \ , \ g) & \mapsto & v_i g \otimes v_j g \end{array}$$

Tal ação fornece uma representação $\rho_W : G \to GL(W)$. Temos ainda que o resultado em (II) vale, especificamente, para $x = v_i g$ e $y = v_j g$:

$$(v_i g \otimes v_j g)^* = (v_j g \otimes v_i g)$$

(IV) Sejam agora $w \in W$ e $g \in G$. Temos:

$$w = \sum_{i,j} a_{ij}(v_i \otimes v_j) \therefore wg = \sum_{i,j} a_{ij}(v_i g \otimes v_j g)$$

$$\therefore (wg)^* = \sum_{i,j} a_{ij}(v_i g \otimes v_j g)^* = \sum_{i,j} a_{ij}(v_j g \otimes v_i g) = \sum_{i,j} a_{ij}(v_j \otimes v_i)g = w^* g$$

Isso significa que "$*$" é G-invariante. Além disso, os subespaços W_S e W_A são G-invariantes:

- Se $w \in W_S$, então $w^* = w$. Assim, $(wg)^* = w^* g = wg \ \therefore \ wg \in W_S$.
- Se $w \in W_A$, então $w^* = -w$. Daí, $(wg)^* = w^* g = -wg \ \therefore \ wg \in W_A$.

Sendo $W = W_S \oplus W_A$, temos $\chi_W = \chi_S + \chi_A$, em que χ_W, χ_S e χ_A são os caracteres associados às representações W, W_S e W_A, respectivamente.

Sejam P e Q as matrizes associadas, respectivamente, às representações V e W. Recorrendo à definição de caráter e lembrando que $tr(A \otimes B) = tr(A) \cdot tr(B)$ (Proposição 7.1), podemos escrever:

$$\chi_W = tr(P) = tr(Q \otimes Q) = tr(Q) \cdot tr(Q) = (tr(Q))^2 = \chi^2$$

Resulta: $\chi^2 = \chi_S + \chi_A$.

(V) Para calcular $\chi_A(g)$, usaremos a base $w_{ij} = v_i \otimes v_j - v_j \otimes v_i$, em que $i < j$, para o subespaço W_A. (Veja a discussão sobre as bases dos subespaços em (I)).

Supondo $v_i \cdot g = \sum_r a_{ir} v_r$ e $v_j \cdot g = \sum_s a_{js} v_s$, vem:

$$\begin{aligned} w_{ij} \cdot g &= v_i \cdot g \otimes v_j \cdot g - v_j \cdot g \otimes v_i \cdot g = \\ &= \Big(\sum_r a_{ir} v_r\Big) \otimes \Big(\sum_s a_{js} v_s\Big) - \Big(\sum_r a_{jr} v_r\Big) \otimes \Big(\sum_s a_{is} v_s\Big) \\ &= \Big(\sum_{r,s} a_{ir} a_{js} \cdot (v_r \otimes v_s)\Big) - \Big(\sum_{r,s} a_{jr} a_{is} \cdot (v_r \otimes v_s)\Big) \\ &= \Big(\sum_{r,s} (a_{ir} a_{js} - a_{jr} a_{is}) \cdot (v_r \otimes v_s)\Big) \end{aligned}$$

Na última soma, temos r e s variando de 1 a n, em que n é o número de elementos da base de V. Ao desenvolver tal somatório, devemos notar que:

- quando $r = s$, ocorre um cancelamento de termos: $a_{ir}a_{js} - a_{jr}a_{is} = a_{ir}a_{jr} - a_{jr}a_{ir} = 0$
- se $r = k$ e $s = l$ e $k < l$, podemos promover o seguinte agrupamento: $(a_{ik}a_{jl} - a_{jk}a_{il}) \cdot (v_k \otimes v_l) + (a_{il}a_{jk} - a_{jl}a_{ik}) \cdot (v_l \otimes v_k) = (a_{ik}a_{jl} - a_{jk}a_{il}) \cdot (v_k \otimes v_l - v_l \otimes v_k)$

Com base no exposto acima, tem-se:

$$w_{ij} \cdot g = \Big(\sum_{r,s} (a_{ir}a_{js} - a_{jr}a_{is}) \cdot (v_r \otimes v_s) \Big) = \Big(\sum_{r<s} (a_{ir}a_{js} - a_{jr}a_{is}) \cdot w_{rs} \Big).$$

Por definição, o caráter de uma representação é calculado a partir do traço da matriz associada a um elemento de G. Assim, na expressão acima, para obter o valor de χ_A, devemos impor $i = r$ e $j = s$ e efetuar a soma. Temos:

$$\chi_A(g) = \sum_{i<j} (a_{ii}a_{jj} - a_{ji}a_{ij}) = \sum_{i<j} b_{ij}, \text{ em que } b_{ij} = (a_{ii}a_{jj} - a_{ji}a_{ij}).$$

Reescrevendo b_{ij}, obtemos: $b_{ij} = (a_{jj}a_{ii} - a_{ij}a_{ji}) = b_{ji}$.

Notando que no caso $i = j$ tem-se $b_{ij} = 0$, segue: $\sum_{i \neq j} b_{ij} = \sum_{i,j} b_{ij}$

Podemos resumir o que foi exposto acima, escrevendo:

$$\begin{aligned} 2 \cdot \chi_A(g) &= \sum_{i<j} b_{ij} + \sum_{i<j} b_{ij} = \sum_{i<j} b_{ij} + \sum_{i>j} b_{ji} = \sum_{i \neq j} b_{ij} = \sum_{i,j} (a_{ii}a_{jj} - a_{ji}a_{ij}) \\ &= \sum_{i,j} a_{ii}a_{jj} - \sum_{i,j} a_{ji}a_{ij} = \Big(\sum_{i} a_{ii} \Big) \cdot \Big(\sum_{j} a_{jj} \Big) - \sum_{i,j} a_{ji}a_{ij} \end{aligned}$$

Resulta: $2 \cdot \chi_A(g) = \chi(g)^2 - \chi(g^2) \ \therefore \ \chi^{(2)}(g) = \chi(g)^2 - 2 \cdot \chi_A(g)$

Usando o fato que $\chi^2 = \chi_S + \chi_A$ (demonstrado no item IV), obtemos:

$\chi^{(2)}(g) = \chi_S - \chi_A$ (evidenciando que $\chi^{(2)}(g)$ é uma diferença de caracteres).

(c) Aplicando a definição de θ_n para $n = 2$, escrevemos: $\theta_2(g) = \big| \{ x \in G : x^2 = g \} \big|$

$\theta_2 = \sum_{\chi \in Irr(G)} \nu_2(\chi) \cdot \chi$, com $\nu_2(\chi) = \dfrac{1}{|G|} \cdot \sum_{g \in G} \chi(g^2)$, conforme Lema 5.13.

Além disso, usando a notação do item (a), obtemos:

$$\nu_2(\chi) = \langle \chi^{(2)}, 1 \rangle = \langle \chi^2 - 2 \cdot \chi_A \, , \, 1 \rangle = \langle \chi^2 \, , \, 1 \rangle - 2 \cdot \langle \chi_A \, , \, 1 \rangle$$

Temos, pela Proposição 5.7, que se χ é irredutível, $\overline{\chi}$ também o é. Sabemos ainda que dois caracteres irredutíveis α e β são ortogonais e que o produto interno $\langle \alpha, \beta \rangle$ assume os valores 0 ou 1, para os casos $\alpha \ncong \beta$ e $\alpha \cong \beta$, respectivamente.

Existem dois casos a analisar:

Caso 1: $\langle\, \chi, \overline{\chi}\, \rangle = 0$

Numa tal situação, tem-se $\chi \neq \overline{\chi}$ e, portanto, χ não é função real. Além disso:

$$0 = \langle\, \chi, \overline{\chi}\, \rangle = \frac{1}{|G|} \cdot \sum_{g \in G} \chi(g) \cdot \overline{\overline{\chi(g)}} = \frac{1}{|G|} \cdot \sum_{g \in G} \chi(g)^2 \cdot \overline{1} = \langle\, \chi^2, 1\, \rangle$$

Lembrando que $\chi^2 = \chi_S + \chi_A$ e usando corolário 5.9 vem:

$$0 = \langle\, \chi_S, 1\, \rangle + \langle\, \chi_A, 1\, \rangle \;\therefore\; \langle\, \chi_S, 1\, \rangle = \langle\, \chi_A, 1\, \rangle = 0 \;\therefore\; \langle\, \chi^{(2)}, 1\, \rangle = 0 \;\therefore\; \nu_2(\chi) = 0$$

Caso 2: $\langle\, \chi, \overline{\chi}\, \rangle = 1$

$$1 = \langle\, \chi^2, 1\, \rangle = \langle\, \chi_S + \chi_A, 1\, \rangle = \langle\, \chi_S, 1\, \rangle + \langle\, \chi_A, 1\, \rangle$$

Há duas combinações possíveis para os produtos internos envolvidos na última equação:

(A) $\langle\, \chi_S, 1\, \rangle = 1$ e $\langle\, \chi_A, 1\, \rangle = 0$

(B) $\langle\, \chi_S, 1\, \rangle = 0$ e $\langle\, \chi_A, 1\, \rangle = 1$

Lembrando que: $\nu_2(\chi) = \langle\, \chi^{(2)}, 1\, \rangle = \langle\, \chi^2\, ,\; 1\, \rangle - 2 \cdot \langle\, \chi_A\, ,\; 1\, \rangle$, temos:

- No caso (A), $\langle\, \chi_A, 1\, \rangle = 0$ e $\nu_2(\chi) = 1 - 2 \cdot (0) = 1$.
- Já para o caso (B), $\langle\, \chi_A, 1\, \rangle = 1$ e $\nu_2(\chi) = 1 - 2 \cdot (1) = -1$

(d) Conforme já demonstrado em (c), quando $\nu_2(\chi) = 0$, a função χ não assume valores reais. $\square$

6. DEMONSTRAÇÃO DO SEGUNDO TEOREMA

Teorema 6.1. ([5] - *Theorem 14*)
(a) Para qualquer grupo finito G é válida a seguinte desigualdade:

$$cp(G) \geqslant \Big(\frac{1}{|G|} \cdot \sum_{\chi \in Irr(G)} \chi(1)\Big)^2$$

(b) Se G é um grupo finito de ordem par e com centro trivial, então:

$|G| < |C_G(x)|^3$, *para algum* $x \in G - \{1\}$.

Demonstração. (a) (I) A desigualdade de Cauchy-Schwarz se escreve:

$$\Big(\sum_{k=1}^{n} a_k \cdot b_k\Big)^2 \leqslant \Big(\sum_{k=1}^{n} {a_k}^2\Big) \cdot \Big(\sum_{k=1}^{n} {b_k}^2\Big)$$

(II) Recordemos dois fatos importantes:

- $|G| = \sum_{i=1}^{k} \chi_i(1)^2$ (proposição 5.12);
- o número de caracteres irredutíveis coincide com $k(G)$ (proposição 5.10).

Podemos aplicar (I) à soma dos caracteres irredutíveis:

$$\Big(\sum_{\chi \in Irr(G)} \chi(1) \cdot 1\Big)^2 \leqslant \Big(\sum_{\chi \in Irr(G)} \chi(1)^2\Big) \cdot \Big(\sum_{\chi \in Irr(G)} 1^2\Big) = |G| \cdot k(G) = |G|^2 \cdot cp(G)$$

Daí segue: $cp(G) \geqslant \Big(\frac{1}{|G|} \cdot \sum_{\chi \in Irr(G)} \chi(1)\Big)^2$

(b) (I) Dados $g \in G$ e $n > 0$, consideremos a função θ_n , definida no Lema 5.13, a qual fornece o número de raízes n-ésimas de g em G.

$$\theta_n : G \to \mathbb{C}$$
$$g \mapsto \theta_n(g) = |\{\, x \in G : x^n = g \,\}|$$

Vimos, nesse lema, que a função de classe θ_n pode ser expressa na forma:

$\theta_n = \sum_{\chi \in Irr(G)} \nu_n(\chi) \cdot \chi$, em que $\nu_n(\chi) \in \mathbb{C}$ é unicamente determinado.

$$\nu_n(\chi) = \frac{1}{|G|} \cdot \sum_{g \in G} \chi(g^n) = \frac{1}{|G|} \cdot \sum_{g \in G} \chi^{(n)}(g) = \langle\, \chi^{(n)}, 1_G \,\rangle\,,$$

em que χ é um caráter irredutível (Proposição 5.14).

(II) Consideremos o caso particular $n = 2$, ou seja, a função que fornece o número de soluções da equação $x^2 = 1$ em G. Podemos escrever:

$$\big|\{\, x \in G : x^2 = 1 \,\}\big| = \theta_2(1) = \sum_{\chi \in Irr(G)} \nu_2(\chi) \cdot \chi(1)$$

Seja t um elemento de ordem 2 do grupo G, o qual existe, pois, por hipótese, G é um grupo de ordem par. Sabemos que todos os conjugados de t possuem ordem 2 e pertencem a uma mesma classe de conjugação (órbita). Assim:

$[G : C_G(t)] = |Cl(t)| \leqslant \theta_2(1)$

A identidade, 1_G , satisfaz $x^2 = 1_G$ mas não pertence a $Cl(t)$. Logo:

$\theta_2(1) > [G : C_G(t)] \;\therefore\; \theta_2(1)^2 > [G : C_G(t)]^2$

Por outro lado, a Proposição 5.14 garante que $\nu_2(\chi) \in \{0, 1, -1\}$. Assim:

$$\theta_2(1)^2 = \Big(\sum_{\chi \in Irr(G)} \nu_2(\chi) \cdot \chi(1) \Big)^2 \leqslant \Big(\sum_{\chi \in Irr(G)} \nu_2(\chi)^2 \Big) \cdot \Big(\sum_{\chi \in Irr(G)} \chi(1)^2 \Big)$$

$$\leqslant \Big(\sum_{\chi \in Irr(G)} 1^2 \Big) \cdot \Big(\sum_{\chi \in Irr(G)} \chi(1)^2 \Big) \leqslant k(G) \cdot |G|$$

$$\therefore\; [G : C_G(t)]^2 < \theta_2(1)^2 \leqslant k(G) \cdot |G| \;\therefore\; |G| < k(G) \cdot |C_G(t)|^2$$

(III) Pelo Lema 2.8, sabemos que, se $\mathrm{Z}(G) = 1$, então $k(G) \leqslant \max |C_G(y)|$ para algum y em $G - \{1\}$. Unindo tal fato ao resultado obtido em (II), resulta:

$|G| < |C_G(x)|^3$ para algum $x \in G - \{1\}$.

□

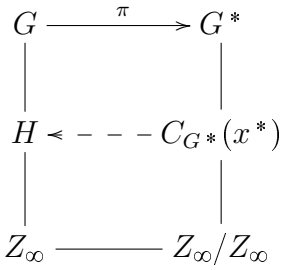
Corolário 6.2 ([5] - Corollary 15)**.** *Seja G um grupo finito cuja ordem é par e maior que 2. Então G possui um subgrupo próprio H tal que $|G| < |H|^3$.*

Demonstração. Iniciaremos a análise, tratando os casos em que o grupo G tem ordem par, mas não é um 2-grupo.

Representemos por $Z_\infty(G) = Z_\infty$ o último termo da série central ascendente do grupo G e por G^* o quociente G/Z_∞ . Com essas definições, o centro de G^* é trivial e podemos aplicar o Teorema 6.1. Há dois casos a analisar.

Caso 1: $|G^*|$ é par.

O Teorema 6.1 assegura que existe $x^* \in G^*$ tal que $|G^*| < |C_{G^*}(x^*)|^3$
Seja H a imagem inversa em G de $C_{G^*}(x^*) = H/Z_\infty(G)$



Podemos escrever:

$$|C_{G^*}(x^*)|^3 > |G^*| \therefore |H/Z_\infty|^3 > |G/Z_\infty| \therefore |H|^3 > |G| \cdot |Z_\infty|^2 \geqslant |G|$$

Caso 2: $|G^*|$ é ímpar.

$|G| = |G^*| \cdot 2^\alpha$ e Z_∞ contém um 2-subgrupo de Sylow de G, o qual denotaremos por P. A série $1 = Z_0 \leqslant Z_1 = Z(G) \leqslant \cdots \leqslant Z_\infty$ é uma série central para Z_∞, construída a partir da série central ascendente de G, o que assegura que Z_∞ é nilpotente. Pela Proposição 3.3, temos que o subgrupo P, que também é um 2-Sylow em Z_∞, é tal que $P \trianglelefteq Z_\infty$. Mas um Sylow que é normal é também característico. Unindo tal informação ao fato que $Z_\infty \trianglelefteq G$, decorre $P \trianglelefteq G$.

Dado que G contém um 2-subgrupo de Sylow normal, o *Teorema de Schur-Zassenhaus* (vide 7.4) estabelece que G possui um $2'$-subgrupo de Hall (digamos K). Tal K é próprio em G, pois é um $2'$-subgrupo em um grupo de ordem par.

Se ocorrer $|P| \leqslant |K|$, temos $|G| = |P| \cdot |K| \leqslant |K|^2 < |K|^3$. Nesse caso, K é o subgrupo próprio procurado.

Por outro lado, se tivermos $|K| \leqslant |P|$, segue $|G| = |P| \cdot |K| \leqslant |P|^2 < |P|^3$. Notando que K é não-trivial (pois estamos tratando o cenário em que G não é um 2-grupo), vemos que P é uma escolha natural para o subgrupo próprio que estamos buscando.

Isso conclui a demonstração para o caso em que G não é um 2-grupo.

Para finalizar, consideremos a situação em que $|G| = 2^\alpha$, com $\alpha \geqslant 2$. Seja $L \leqslant G$ um subgrupo de índice 2. Temos $|L| = 1/2 \cdot |G|$, com $|G| > 2$ e, portanto, $|L| \geqslant 2$. Finalmente:

$|G| = 2 \cdot |L| \leqslant |L| \cdot |L| < |L|^3$, concluindo a prova. □

Exemplo 6.1. *Análise do número de involuções em um Grupo de Ordem Par.*

Sabemos, do Teorema 6.1, que o número de soluções de $x^2 = 1$ *em* G *é tal que:*

$$|\{ x \in G : x^2 = 1 \}| = \theta_2(1) = \sum_{\chi \in Irr(G)} \nu_2(\chi) \cdot \chi(1) \, .$$

Vimos também que: $\theta_2(1)^2 \leqslant k(G) \cdot |G|$.

Denotando por $\mathcal{I}$ *o número de involuções no grupo em análise, podemos escrever:*

$$\mathcal{I}^2 < \theta_2(1)^2 \leqslant k(G) \cdot |G| \, .$$

Podemos agora pensar na proporção de involuções em G*:*

$$\left(\frac{\mathcal{I}}{|G|} \right)^2 < \frac{k(G)}{|G|} = cp(G) \, .$$

Essa última expressão permite estabelecer uma cota inferior para a probabilidade de comutar em função da proporção de involuções em G*. Assim, por exemplo:*

$$\left(\frac{\mathcal{I}}{|G|} \right) \geqslant 1/3 \Rightarrow cp(G) > \frac{1}{9} \, .$$

Exemplo 6.2. *Uso conjunto dos dois teoremas*

Considerando, novamente, a proporção de involuções em um grupo de ordem par, podemos usar os Teoremas 4.1 e 6.1 em conjunto:

$$\left(\frac{\mathcal{I}}{|G|} \right)^2 < \frac{k(G)}{|G|} = cp(G) \leqslant [G : sol(G)]^{-\frac{1}{2}}$$

Dessa forma, por exemplo, temos:

$$\left(\frac{\mathcal{I}}{|G|} \right) \geqslant 1/2 \Rightarrow [G : sol(G)] < 16 \, .$$

Ou seja, a partir da análise do número de involuções, foi possível tirar conclusões sobre o índice de $sol(G)$*. O que permitiu tal conexão foi, justamente, o estudo que desenvolvemos sobre a probabilidade de comutar,* $cp(G)$*. Tal exemplo ainda sugere que um grupo com grande incidência de involuções se aproxima de ser solúvel.*

7. APÊNDICE

7.1. PROPRIEDADES DO TRAÇO DE UMA MATRIZ.

O traço de uma matriz quadrada $A = (a_{ij}) \in M_n(\mathbb{C})$ é definido como a soma dos elementos da sua diagonal principal, ou seja:

$$tr(A) = \sum_{k=1}^{n} a_{kk} \ .$$

O traço de um operador linear $f : V \to V$, em um espaço vetorial de dimensão finita, V, é o traço de uma matriz que representa o operador. Tal definição não depende da base escolhida para V, pois, bases distintas dão origem a matrizes semelhantes (as quais possuem o mesmo traço).

Proposição 7.1. *Propriedades do Traço*

(a) $tr(A + B) = tr(A) + tr(B)$
(b) $tr(A \oplus B) = tr(A) + tr(B)$
(c) $tr(cA) = c \cdot tr(A)$, *em que* $c \in \mathbb{C}$
(d) $tr(AB) = tr(BA)$
(e) $tr(A \otimes B) = tr(A) \cdot tr(B)$

Demonstração. (a) Sejam $A = (a_{ij})$ e $B = (b_{ij})$, com $A, B \in M_n(\mathbb{C})$.

$$tr(A + B) = \sum_{i=1}^{n} a_{ii} + b_{ii} = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = tr(A) + tr(B)$$

(b) Sejam $A = (a_{ij}) \in M_n(\mathbb{C})$ e $B = (b_{ij}) \in M_m(\mathbb{C})$.
Seja $M = (m_{ij}) \in M_{n+m}(\mathbb{C})$ a matriz que representa a soma direta de A e B.
A matriz $M = A \oplus B$ tem o seguinte formato:

$$M = \left[\begin{array}{c|c} A_{n\times n} & 0 \\ \hline 0 & B_{m\times m} \end{array}\right]$$

Usando a definição de traço, escrevemos:

$$tr(A \oplus B) = tr(M) = \sum_{i=1}^{n+m} m_{ii} = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{m} b_{ii} = tr(A) + tr(B)$$

(c) Sendo $cA := (c \cdot a_{ij})$ uma matriz em $M_n(\mathbb{C})$, temos:

$$tr(cA) = \sum_{i=1}^{n} c \cdot a_{ii} = c \cdot \sum_{i=1}^{n} a_{ii} = c \cdot tr(A)$$

(d) Dadas as matrizes $A = (a_{ij})_{m\times n}$ e $B = (b_{jk})_{n\times m}$, o produtos AB e BA são matrizes quadradas $AB = C = (c_{ik})_{m\times m}$ e $BA = D = (d_{jk})_{n\times n}$, em que:

$$c_{ik} = \sum_{j=1}^{n} a_{ij}\cdot b_{jk} \quad \text{e} \quad d_{jk} = \sum_{i=1}^{m} b_{ji}\cdot a_{ik}$$

Manipulando os somatórios, conforme a seguir, obtemos a tese:

$$tr(AB) = tr(C) = \sum_{i=1}^{m} c_{ii} = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n} a_{ij}\cdot b_{ji}\Big) = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n} b_{ji}\cdot a_{ij}\Big)$$
$$= \sum_{i=1}^{m}\Big(b_{1i}\cdot a_{i1} + \cdots + b_{ni}\cdot a_{in}\Big) = \sum_{i=1}^{m} b_{1i}\cdot a_{i1} + \cdots + \sum_{i=1}^{m} b_{ni}\cdot a_{in}$$
$$= \sum_{j=1}^{n}\Big(\sum_{i=1}^{m} b_{ji}\cdot a_{ij}\Big) = \sum_{j=1}^{n} d_{jj} = tr(D) = tr(BA)$$

(e) Seja $\mathcal{B} = \{\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n}\}$ uma base para o espaço vetorial, de dimensão finita, V. Os elementos da forma $\mathbf{v_i} \otimes \mathbf{v_j}$, em que $1 \leqslant i\,,\, j \leqslant n$, constituem uma base para o produto tensorial $W = V \otimes V$.

Consideremos as transformações lineares $\alpha : V \to V$ e $\beta : V \to V$, tais que:

$$\alpha(\mathbf{v_i}) = \sum_{r} a_{ir}\mathbf{v_r} \quad \text{e } \beta(\mathbf{v_j}) = \sum_{s} a_{js}\mathbf{v_s}\ \text{, com } i, j \in \{1, 2, \ldots, n\}\ .$$

Definamos $\alpha \otimes \beta = f : W \to W$, para elementos de uma base de W :

$$f : W \ \to \ W$$
$$\mathbf{v_i} \otimes \mathbf{v_j} \mapsto f(\mathbf{v_i} \otimes \mathbf{v_j}) = \alpha(\mathbf{v_i}) \otimes \beta(\mathbf{v_j})$$

Fazendo $w_i = \mathbf{v_i} \otimes \mathbf{v_j}$, temos:

$$f(\mathbf{v_i} \otimes \mathbf{v_j}) = \Big(\sum_{r} a_{ir}\mathbf{v_r}\Big) \otimes \Big(\sum_{s} a_{js}\mathbf{v_s}\Big) = \sum_{r,s} a_{ir}a_{js}(\mathbf{v_r} \otimes \mathbf{v_s})$$

Pela definição de traço de um operador linear:

$$tr(f) = \sum_{i,j} a_{ii}b_{jj} = \sum_{i} a_{ii}\cdot\sum_{j} b_{jj} = tr(A)\cdot tr(B)$$

□

7.2. CARÁTER DE PERMUTAÇÃO.

Definição 7.1. *Consideremos a ação de um grupo finito G sobre um conjunto finito Ω ($G \curvearrowright \Omega$). Definimos o caráter de permutação (associado à ação) por:*

$\chi(g) = |\{\ \alpha \in \Omega \mid \alpha^g = \alpha\ \}|$

Estamos interessados em saber quantos são os elementos $\alpha \in \Omega$ que permanecem fixos sob ação desse $g \in G$. Vejamos dois exemplos básicos.

No caso da ação regular $G \curvearrowright G$ ($\Omega = G$), o caráter de permutação é dado por:

$$\chi(g) = \begin{cases} 0, & \text{se } g \neq 1 \\ |G|\,, & \text{se } g = 1 \end{cases}$$

Já a ação por conjugação $G \curvearrowright G$ ($\Omega = G$), tem como caráter de permutação:

$\chi(g) = |\{\alpha \in \Omega \mid \alpha^g = \alpha\}| = |\{\alpha \in \Omega \mid g^{-1}\alpha g = \alpha\}| = |\, C_G(g)\,|$

Em particular, temos, nesse caso, $\chi(1) = |\Omega|$.

Proposição 7.2 (Teorema de Cauchy-Frobenius)**.** *Sendo G um grupo finito que age sobre um conjunto finito Ω, o número total, $\underline{n}$, de órbitas da ação é dado por:*

$$n = \frac{1}{|G|} \cdot \sum_{g \in G} \chi(g) = \frac{1}{|G|} \cdot \sum_{\alpha \in \Omega} |G_\alpha|$$

Demonstração. Seja S o conjunto dos elementos α fixados sob ação de algum $g \in G$:

$S = \{\ (\alpha, g) \mid \alpha^g = \alpha,\ \alpha \in \Omega,\ g \in G\ \}$

(I) Seja $\alpha \in \Omega$ (fixo). Quantos são os elementos $g \in G$ que fixam tal α ?
Precisamente os elementos de G que estabilizam α, ou seja, $|G_\alpha|$.
Assim: $|G_\alpha|$ = número de elementos $g \in G$ tais que $(\alpha, g) \in$ S.

$$\therefore \quad |S| = \sum_{\alpha \in \Omega} |G_\alpha|$$

(II) Por outro lado, para cada $g \in G$, o número de elementos $\alpha \in \Omega$ que permanecem fixos sob ação desse g é $\chi(g)$.

$$\therefore \quad |S| = \sum_{g \in G} \chi(g)$$

(III) $$\frac{|S|}{|G|} = \frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{\alpha\in\Omega}|G_\alpha|$$

(IV) Além disso, o FCP (*Fundamental Counting Principle*) fornece:

$$|G| = |G_\alpha| \cdot |\mathcal{O}(\alpha)|$$

(V) Por (III) e (IV), segue:

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{\alpha\in\Omega}|G_\alpha| = \sum_{\alpha\in\Omega}\frac{1}{|\mathcal{O}(\alpha)|}$$

Observemos que a soma $1/|\mathcal{O}(\alpha)|$ é tomada tantas vezes quantos forem os elementos de tal órbita (e, portanto, seu valor é igual a 1 em cada órbita). Pelo fato de existirem $\underline{n}$ órbitas, resulta:

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{\alpha\in\Omega}|G_\alpha| = \sum_{\alpha\in\Omega}\frac{1}{|\mathcal{O}(\alpha)|} = n \qquad \square$$

O Teorema de Cauchy-Frobenius afirma que o número de órbitas é igual ao valor médio do caráter de permutação χ.

Proposição 7.3 (Conseqüência do Teorema de Cauchy-Frobenius)**.** *O número $k(G)$ de classes de conjugação de um grupo finito G é dado por:*

$$k(G) = \frac{1}{|G|}\sum_{g\in G}|C_G(g)| \ .$$

Demonstração. Basta usar o Teorema de Cauchy-Frobenius, lembrando que:

- na ação por conjugação cada órbita coincide com uma classe de conjugação
- na ação por conjugação o estabilizador de um $x \in G$ é o centralizador $C_G(x)$

$\square$

7.3. O TEOREMA DE SCHUR-ZASSENHAUS.

Dado um subgrupo $N \lhd G$, um subgrupo $H \leqslant G$ é dito um *complemento* para N em G se $NH = G$ e $N \cap H = 1$.

Proposição 7.4 (Teorema de Schur-Zassenhaus)**.** *Sejam G um grupo finito e um subgrupo $N \trianglelefteq G$ tal que $|N|$ e $[G : N]$ são coprimos. Então N possui um complemento H em G.*

Demonstração. Para uma discussão desse importante teorema, vide [9] seção 3A. $\square$

Referências

[1] CURTIS, C.W.; REINER, I.; Representation Theory of Finite Groups and Associative Algebras, AMS Chelsea Publishing, Rhode Island, 1962.

[2] FULMAN, J.; GURALNICK, R.M.; Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, Trans. AMS 364 (2012), 3023 - 3070.

[3] GALLAGHER, P. X.; The number of conjugacy classes in a finite group, Math. Z. 118 (1970), 175 - 179.

[4] GARONZI, M.; MARÓTI, A.; On the number of conjugacy classes of a permutation group. Journal of Combinatorial Theory. Series A (Print), v. 133 (2015), 251 - 260.

[5] GURALNICK, R.M.; ROBINSON, G. R.; On the commuting probability in finite groups; J. Algebra 300 (2006), 509 - 528.

[6] GUSTAFSON, W.H.; What is the probability that two group elements commute ?, Amer. Math. Monthly 80 (1973), 1031 - 1034.

[7] HOFMANN, K. H.; RUSSO, F. G.; The probability that x and y commute in a compact group. Math. Proc. Cambridge Philos. Soc.153 no. 3 (2012), 557 - 571.

[8] ISAACS, I. M.; Character Theory of Finite Groups, Dover Publications Inc, New York, 1994.

[9] ISAACS, I. M.; Finite Group Theory, American Mathematical Society, Rhode Island, 2008.

[10] KOVÁCS, L.G.; ROBINSON, G.R.; On The Number of Conjugacy Classes of a Finite Group, J. Algebra 160 (1993), 441 - 460.

[11] KURZWEIL, H.; STELLMACHER, B.; The Theory of Finite Groups - An Introduction, Springer-Verlag, New York, 2004.

[12] MACHÌ, A.; An Introduction to Ideas and Methods of the Theory of Groups, Springer-Verlag Italia, Milan, 2012.

[13] MARÓTI, A.; Bounding the number of conjugacy classes of a permutation group, J. Group Theory 8 (2005), 97 - 111.

[14] ROBINSON, D.J.S.; A Course in the Theory of Groups 2nd ed, Springer-Verlag, New York, 1996.

[15] ROSE, J. S.; A Course on Group Theory, Dover Publications Inc, New York, 1994.

[16] ROTMAN, J.J.; An Introduction to the Theory of Groups 4th ed, Springer-Verlag, New York, 1995.

[17] SAGAN, B.E.; The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions 2nd ed, Springer-Verlag, New York, 2001.

[18] SERRE, J.; Représentations Linéaires des Groupes Finis 5ème ed, Hermann, Paris, 1998.