UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Raimundo de Araújo Bastos Júnior

Comutadores em Grupos Finitos

Fortaleza
2010

Raimundo de Araújo Bastos Júnior

Comutadores em Grupos Finitos

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática da Universidade Federal do Ceará, como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. José Robério Rogério.
Área de Concentração: Matemática.

Fortaleza

2010

.

Bastos Júnior, Raimundo de Araújo

B329c Comutadores em grupos finitos / Raimundo de Araújo Bastos Júnior - Fortaleza: 2010.

103 f.

Orientador: Prof. Dr. José Robério Rogério

Área de Concentração: Matemática

Dissertação (Mestrado) - Universidade Federal do Ceará, Departamento de Matemática, 2010.

1 - Teoria dos Grupos

CDD 512.2

A Deus

Aos avós (in memorian) Horácio, Maria, Raimundo (Preto), Chico e Mimi

AGRADECIMENTOS

Aos meus companheiros da graduação e do mestrado pela amizade e paciência, entre eles cabe destacar: Átila, Fabiano, Henrique (Topo), Gleriston, Henrique (Enrico), Kelvin, Diego Silva, Wilson, Rondinelle, Luide (Baiano), Luiz Antônio, João, Ederson, Kelton, Rodrigo, Yure, Alexandre, Gleison, João Vítor, Landerson, Vanderson, Marcelo Dário, Edinardo, Deibsom, Luis Carlos, Justino, Euclides, Max, Ernani e Luís Farias.

Agradeço ao professor José Robério Rogério por ter aceitado o convite para ser meu orientador e pelo incentivo para continuar meus estudos em nível de doutorado.

Agradeço aos meus professores que me proporcionaram uma boa formação acadêmica, em especial a José Robério, José Afonso, Gervasio Gurgel Bastos, Alexandre Fernandes, Antonio Caminha, Ricardo Bastos, Luquésio Jorge, J. Petrus van Ool, João Siqueira, Jorge Herbert, Saulo, Assis Ribeiro, Manoel Azevedo, J. Filho, José Fábio, Francisco Pimentel, Lev, Gilberto, Newton Luís, Sasaki, André Jalles e Plácido.

Aos meus amigos da UnB, Felipe Viterbo, Eudes Antônio, Tonires Sales, Francisco Enio, Luís Felipe, Ismael Lins, Robson Alves, Reinaldo pela hospitalidade e companheirismo.

Gostaria também de agradecer também aos professores José Othon e Orlando Stanley por terem aceitado o convite para participar da minha banca e pelas inúmeras sugestões apresentadas para melhorar o meu trabalho.

Não posso deixar de citar os funcionários da Matemática, Andrea, Elizeuda, D. Fernanda, D. Lúcia Helena, D. Rocilda, Sr. Erivan, Lacerda, Júnior por

todas as ajudas e, acima de tudo, pela amizade ao longo desses anos.

Aos meus parentes, minha mãe Francisca (Peta), minha vó Elza, minha sobrinha Diana, meus irmãos Ricardo e Rochele por toda a ajuda, incentivo, dedicação e muita paciência. A minha namorada Karla da Silva por ser minha companheira e, consequentemente, a inspiração dos meus estudos.

Ao CNPq pela ajuda financeira.

RESUMO

Os problemas que abordaremos estão diretamente associados à existência de elementos no subgrupo derivado que não são comutadores. Nosso objetivo será apresentar os resultados de Tim Bonner [1], que são estimativas para a razão entre o comprimento do derivado e a ordem do grupo (limitação superior e determinação do "comportamento assintótico"), culminando com uma prova da conjectura de Bardakov.

ABSTRACT

The problems which we address in this work are directly related to the existence of elements in the derived subgroup that are not commutators. Our purpose is to present the results of Tim Bonner [1]. In his paper, one finds estimates for the ratio between the commutator length and the order of group (more precisely, upper limits and the establishment of its asymptotic behavior), leading to the proof of Bardakov's Conjecture.

Sumário

Em 1902, o matemático William B. Fite [5] apresentou o primeiro exemplo de um grupo cujo derivado não coincide com o conjunto dos comutadores, esse exemplo tem ordem 256 e possui um elemento não comutador. Isso motivou a definição de **comprimento do derivado** de um grupo G, que é o menor inteiro positivo n para o qual todos os elementos de G' podem ser escrito como o produto de n comutadores, esse número será denotado por $\lambda(G)$.

Em 1911, o matemático inglês W. Burnside, em seu livro [2], propôs um critério para garantir quando um dado elemento do derivado não é um comutador (na perspectiva da teoria dos caracteres). Na década de 60, P.X. Gallagher [1] em [7] apresentou um critério bem mais robusto que o proposto por Burnside e ampliou as perspectivas dos problemas relacionados aos comutadores (Gallagher [6] e [7]). De certa forma, sua motivação foi a seguinte: "**Que limitação podemos obter para o comprimento do derivado usando como parâmetro a ordem do derivado?**"Com essa abordagem ele obteve as seguintes estimativas:

- ([6]) "Se $4^n \geq |G'|$, então $\lambda(G) \leqslant n$";
- ([7]) "Se $(n+2)!(n)! > 2|G'| - 2$, então $\lambda(G) \leqslant n$";
- ([7]) "Se G é um p - grupo, com $|G'| = p^\alpha$, e $n(n+1) > a$, então $\lambda(G) \leqslant n$".

Em [9] e [10], Robert M. Guralnick apresentou dois grupos de ordem 96,

[1]Em [6], Gallagher desenvolve resultados sobre comutadores para Grupos Finitos e Grupos (Topológicos) Compactos

com elementos do derivado que não são comutadores e provou que tais exemplos são mínimais, em relação a ordem, isto é, não existem outros grupos com ordem inferior a 96 que tenham subgrupo derivado diferente do conjunto dos comutadores (a prova da minimalidade não será feita aqui, para uma demonstração veja Guralnick [10]). Em 2006, o matemático V. G. Bardakov conjecturou em "Unsolved Problems in Group Theory - The Kourovka Notebook"[13] o seguinte problema: Seja G um grupo, finito, não abeliano. Então,

$$\frac{\lambda(G)}{|G|} \leqslant \frac{1}{6}$$

E mais, a igualdade só ocorre quando $G \simeq S_3$.

Em 2008, O "Problema de Bardakov"foi demonstrado por Tim Bonner [1]. A "Conjectura de Bardakov", juntamente com algumas das estimativas apresentadas acima são as motivações para nosso trabalho. Por uma questão de ambientação, diversos exemplos serão apresentados para motivar a teoria e, de certa forma, situar melhor os resultados. Os conceitos relativos a espaços vetoriais, anéis e grupos não serão definidos e suas propriedades elementares são usadas livremente, bem como os resultados relativos aos polinômios (sobre $\mathbb{R}$ ou $\mathbb{C}$), derivadas... Nosso trabalho, em vias gerais, terá a seguinte estrutura:

Capítulo 1: Mostraremos os resultados básicos da Teoria das Representações e dos Caracteres necessários para a leitura do trabalho. As primeiras seções são dedicadas exclusivamente à Teoria de Representação de Grupos e à Teoria dos Caracteres, culminando com as famosas relações de ortogonalidade e algumas indentidades de caracteres.

Capítulo 2: Definiremos nosso objeto de estudo que são os grupos não

abelianos que possuem elementos não comutadores e, consequentemente, o comprimento do derivado desses grupos. Nessa perspectiva vamos entender como, sob certos aspectos, a estrutura do grupo interfere no comprimento do derivado.

Para exemplificar a existência de elementos não comutadores iremos apresentar uma construção capaz de gerar grupos com comprimento do derivado maior que 1, tal processo foi descrito por Guralnick em [9] e por essa razão chamaremos tais grupos de grupos de Guralnick. E finalmente, usando algumas identidades de Caracteres, mostraremos o Critério de Burnside - Gallagher:

Lema 0.0.1 *(Gallagher [7]) Sejam G um grupo e $g \in G'$ o qual não é o produto de n comutadores. Então,*

$$\sum_{\chi \in Irr(G)} \frac{1}{\chi(1)^{2k-1}} \chi(g) = 0, \text{ para todo } 0 \leqslant k \leqslant n.$$

tal resultado relacionará a "existência"de elementos não comutadores em um grupo com uma expressão dos caracteres irredutíveis.

Capítulo 3: Nosso objetivo: analisar, para grupos finitos, o comportamento do comprimento do derivado a partir dos graus de caracteres irredutíveis e demonstrar da Conjectura de Bardakov.

Agora, além de garantir a veracidade do Problema formulado por Bardakov, podemos melhorar tal limitação para grupos cuja seja maior que 1000 e, finalmente, mostraremos um estudo do comportamento assintótico (qualitativo) para a razão do comprimento do derivado pela ordem do grupo.

Teorema 0.0.1 *(Bonner [1]) Seja G um grupo finito e não abeliano. Então,*

(a) (Conjectura de Barbakov)

$$\frac{\lambda(G)}{|G|} \leqslant \frac{1}{6}.$$

Além disso, a igualdade só se verifica quando $G \simeq S_3$.

(b) Se $|G| > 1000$*, então*

$$\frac{\lambda(G)}{|G|} \leqslant \frac{1}{250}.$$

(c) (Comportamento Assintótico)

$$\lim_{|G|\to\infty} \frac{\lambda(G)}{|G|} = 0.$$

Apêndice A Apresentaremos uma família de grupos (infinitos), devido a Phyllis J. Cassidy [3], cujo comprimento do derivado é "ilimitado".

Apêndice B Classificaremos todos os G - módulos irredutíveis de um grupo finito e mostraremos que a ordem do grupo é uma função dos graus dos seus caracteres irredutíveis, esse capítulo é um complemento do Capítulo 1.

Capítulo 1

Representações de Grupos Finitos

Nesse capítulo apresentaremos alguns resultados da Teoria de Representações e dos Caracteres em grupos Finitos que serão necessários para uma leitura do trabalho. As principais referências são G. James e M. Liebeck [11] e R. Maier [14].

1.1 Representações

1.1.1 G - módulos

Definição 1.1.1 *(G - módulos) Sejam G um grupo e $\mathbb{K}$ um corpo. Um espaço vetorial M sobre $\mathbb{K}$ chama-se um G - módulo sobre $\mathbb{K}$ se for definida uma aplicação*

$$\begin{aligned} \alpha \ : \ M \times G \ &\longrightarrow \ M \\ (m, g) \ &\longmapsto \ mg \end{aligned}$$

satisfazendo

- $(\lambda_1 m + \lambda_2 m')g = \lambda_1(mg) + \lambda_2(m'g)$;
- $m(gg') = (mg)g'$;
- $(m)1 = m$.

Para quaisquer $\lambda_1, \lambda_2 \in \mathbb{K}$, $m, m' \in M$ *e* $g, g' \in G$

Na literatura também pode aparecer G - espaço à direita sobre $\mathbb{K}$ ou "$\mathbb{K}G$ - módulo".

Definição 1.1.2 *(Homomorfismos e Isomorfismos entre G - módulos) Sejam* M *e* M' *G - módulos sobre* $\mathbb{K}$.

1. *Dizemos que uma aplicação linear* $\theta : M \to M'$ *é um G - homomorfismo se para todos* $m \in M$ *e* $g \in G$, *temos* $\theta(mg) = \theta(m)g$;
2. *Dizemos que uma aplicação* $\mu : M \to M'$ *é um G - isomorfismo de M sobre* M' *se* μ *é um G - homomorfismo e é invertível. Naturalmente,* μ^{-1} *também é G - isomorfismo de* M' *sobre* M.

Denotaremos por $Hom_{\mathbb{K}G}(M, M')$ o conjunto dos G - homomorfismos de M em M'. Tal conjunto tem uma estrutura natural de espaço vetorial (sobre $\mathbb{K}$), vejamos: dados $\varphi, \varphi' \in Hom_{\mathbb{K}G}(V, W)$ e $\lambda \in \mathbb{K}$ basta considerar:

- $(\varphi + \varphi')(v) = \varphi(v) + \varphi'(v)$

- $(\lambda\theta)(v) = \lambda\theta(v)$

para todo $v \in V$.

Definição 1.1.3 *(G - submódulo, G - módulos irredutíveis e completamente redutíveis)*

1. *Um subespaço vetorial $X \leqslant M$ é dito um G - submódulo de M, se para todo $x \in X$ e $g \in G$ tivermos $xg \in X$. Notação: $X \leqslant_G M$.*

2. *Um G - módulo M é irredutível se $M \neq \{0\}$ e os únicos G - submódulos de M são $\{0\}$ e M.*

3. *Um G - módulo M é dito completamente redutível se para todo $X \leqslant_G M$, existe um $Y \leqslant_G M$ tal que $M = X \oplus Y$.*

Exemplo 1.1.1 *Sejam V e W G - módulos sobre $\mathbb{K}$. Se $\theta : V \to W$ é um G - homomorfismo, então $Ker\ \theta \leqslant_G V$ e $Im\ \theta \leqslant_G W$. Como θ é, em particular, uma aplicação linear já temos que $Ker\ \theta$ e $Im\ \theta$ são subespaços de V, W, respectivamente.*

Dados $v \in Ker\ \theta$ e $g \in G$: $\theta(vg) = \theta(v)g = 0$, portanto $vg \in Ker\ \theta$ e $Ker\ \theta \leqslant_G V$.

Agora, dados $w \in Im\ \theta$ e $g \in G$, temos que existe $v \in V$ tal que $\theta(v) = w$. Daí, $wg = \theta(v)g = \theta(vg) \in Im\ \theta$. Logo, $Im\ \theta \leqslant_G W$.

Os dois resultados a seguir (Lema de Schur e o Teorema de Maschke) formam a base da Teoria das Representações dos grupos finitos.

Proposição 1.1.1 *(Lema de Schur) Sejam V e W G - módulos irredutíveis (sobre $\mathbb{C}$) de dimensão finita. Então,*

(i) *Se $\theta : V \to W$ é um G - homomorfismo, então θ é um G - isomorfismo ou $\theta(v) = 0$, para todo $v \in V$;*

(ii) *Se $\theta : V \to V$ é um G - isomorfismo, então $\theta = \lambda Id_V$ para algum $\lambda \in \mathbb{C}$.*

Demonstração do Item (i): *Suponhamos que $\theta(v) \neq 0$, para algum $v \in V$. Portanto, $Im\ \theta \neq \{0\}$ e $Ker\ \theta \neq V$. Como V e W são G - módulos irredutíveis, com $\{0\} \neq Im\ \theta \leqslant_G W$ e $Ker\ \theta \neq V$, temos $Ker\ \theta = \{0\}$ e $Im\ \theta = W$. Logo, θ é um G - isomorfismo.*

Demonstração do Item (ii): *Temos que a aplicação $\theta : V \to V$ tem um autovalor $\lambda \in \mathbb{C}$, ou seja, existe $v \in V$ tal que $\theta(v) = \lambda v$. Portanto, $\{0\} \neq Ker(\theta - \lambda Id_V) \leqslant_G V$, como V é irredutível, temos que $Ker(\theta - \lambda Id_V) = V$. Dessa forma, $(\theta - \lambda Id_V)(v) = 0$ para todo $v \in V$. Logo, $\theta = \lambda Id_V$.*

□

Teorema 1.1.1 *(Teorema de Maschke) Sejam G um grupo finito, $\mathbb{K} = \mathbb{R}$, ou $\mathbb{C}$. Se M é um G - módulo sobre $\mathbb{K}$, então M é um G - módulo completamente redutível.*

Demonstração: Se M é um G - módulo irredutível, então M já é completamente redutível. Com isso podemos supor que M não é irredutível, daí existe $X \leqslant_G M$ e $X \neq M$. Com isso, existe um subespaço Y de M tal que $M = X \oplus Y$. Consideremos a projeção no subespaço X, dada por

$$\begin{array}{rccc} \pi & : & X \oplus Y & \longrightarrow & X \\ & & m = x + y & \longmapsto & x \end{array}$$

Note que π está bem definida, pois cada elemento $m \in M$ admite uma única "fatoração"$m = x + y$, onde $x \in X$ e $y \in Y$. Definamos ainda a aplicação:

$$\begin{array}{rccc} \tau & : & M & \longrightarrow & M \\ & & m & \longmapsto & \tau(m) \end{array}$$

onde $\tau(m) := m - \dfrac{1}{|G|}\left(\displaystyle\sum_{g\in G} \pi(mg^{-1})g\right)$. Com isso,

- τ é um G - homomorfismo. Temos que τ é linear, pois é a combinação de aplicações lineares. Agora, dados $m \in M$ e $g \in G$,

$$\begin{array}{rcl} \tau(mg) & = & mg - \dfrac{1}{|G|}\displaystyle\sum_{h\in G} \pi(mgh^{-1})h \\ & \overset{x^{-1}=gh^{-1}}{=} & mg - \left(\dfrac{1}{|G|}\displaystyle\sum_{x\in G} \pi(mx^{-1})xg\right) \\ & = & \left(m - \dfrac{1}{|G|}\displaystyle\sum_{x\in G} \pi(mx^{-1})x\right)g \\ & = & \tau(m)g. \end{array}$$

- $X \subseteq Ker\ \tau$: Dado $x \in X$, temos $\pi(xg) = xg$, para todo $g \in G$, pois $X \leqslant_G M$. Assim,

$$\begin{array}{rcl} \pi(x) & = & x - \dfrac{1}{|G|}\displaystyle\sum_{g\in G} \pi(xg^{-1})g \\ & = & x - \dfrac{1}{|G|}\displaystyle\sum_{g\in G} (xg^{-1})g \\ & = & x - \dfrac{1}{|G|}\displaystyle\sum_{g\in G} x \\ & = & 0. \end{array}$$

- $\tau^2 = \tau$: Para todo $m \in M$, temos

$$\begin{aligned}\tau^2(m) &= \tau(\tau(m)) \\ &= \tau(m - \frac{1}{|G|}\sum_{g\in G}\pi(mg^{-1})g) \\ &= \tau(m) - \frac{1}{|G|}\sum_{g\in G}\tau(\pi(mg^{-1})g) \\ &= \tau(m),\end{aligned}$$

pois $\pi(mg^{-1})g \in X \subseteq Ker\ \tau$. Logo, $\tau^2 = \tau$.

Agora consideremos $Y^* = Im\ \tau$. Como τ é linear, Y^* é um subespaço. Além disso, para todo $y \in Y^*$ existe $m \in M$ tal que $\tau(m) = y$. Com isso, para todo $g \in G$, $yg = \tau(m)g = \tau(mg) \in Y^*$. Portanto, $Y^* \leqslant_G M$. Mais ainda, dado $m \in M$ temos $m = (m - \tau(m)) + \tau(m)$, onde $\tau(m) \in Y^*$ e $m - \tau(m) = \frac{1}{|G|}\sum_{g\in G}\tau(mg^{-1})g \in X$, pois $\pi(mg^{-1})g \in X$. Com isso, $M = X + Y^*$. Dado $x = \tau(m) \in X \cap Y^*$, temos $0 = \tau(x) = \tau(\tau(m)) = \tau^2(m) = \tau(m) = x$. Logo, $X \cap Y^* = \{0\}$ e $M = X \oplus Y^*$.

□

A versão do Teorema de Maschke apresentada não está em sua formulação mais geral, mas é suficiente para o nosso estudo [1].

Corolário 1.1.1 *Sejam G um grupo finito e $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Se $\{0\} \neq M$ é um G - módulo sobre $\mathbb{K}$ de dimensão finita, então $M = U_1 \oplus \ldots \oplus U_r$, onde os U_i são G - submódulos irredutíveis.*

[1] Veja Rudolf Maier [14]

Demonstração: Façamos indução sobre a dimensão do G - módulo M. Se M é irredutível, então M já está na forma desejada. Com isso, podemos supor que M não é irredutível e $dim_{\mathbb{K}}(M) > 1$. Assim, existe um G - submódulo próprio $\{0\} \neq X$ em M e, pelo Teorema de Maschke, existe $Y \leqslant_G M$, tal que $M = X \oplus Y$. Como $0 < dim_{\mathbb{K}}(X),\ dim_{\mathbb{K}}(Y) < dim_{\mathbb{K}}(M)$, segue por indução,

$$X = V_1 \oplus \ldots \oplus V_r \text{ e } Y = W_1 \oplus \ldots \oplus W_s,$$

onde $V_i \leqslant_G X$ é um G - módulos irredutível, $1 \leqslant i \leqslant r$ e $W_j \leqslant_G Y$ é um G - módulos irredutível, $1 \leqslant j \leqslant s$. Logo,

$$M = V_1 \oplus \ldots \oplus V_r \oplus W_1 \oplus \ldots \oplus W_s,$$

onde os fatores são G - submódulos irredutíveis.

□

1.1.2 Representações e Caracteres

Definição 1.1.4 *(Representações e G - módulos) Sejam G um grupo, M e M' espaços vetoriais sobre $\mathbb{K}$.*

1. *Uma representação (linear) do grupo G sobre um corpo $\mathbb{K}$ é um homomorfismo $\varphi : G \to GL_{\mathbb{K}}(M)$, onde $GL_{\mathbb{K}}(M)$ é o grupo das aplicações lineares invertíveis de M;*

2. *Duas representações $\varphi : G \to GL_{\mathbb{K}}(M)$, $\varphi : G \to GL_{\mathbb{K}}(M')$ de G sobre $\mathbb{K}$ são ditas equivalentes se existe uma bijeção linear $\mu : M \to M'$*

satisfazendo $\varphi'(g)(\mu(m)) = \mu(\varphi(g)(m))$ *para quaisquer* $m \in M$ *e* $g \in G$.

Observação 1.1.1 *Sejam* G *um grupo e* $\mathbb{K}$ *um corpo. Então, existe uma correspondência biunívoca entre as representações lineares não equivalentes de* G *e o conjunto dos* G *- módulos não isomorfos (sobre* $\mathbb{K}$*).*

De fato, tomemos M um G - módulo sobre $\mathbb{K}$. Podemos definir $\varphi : G \to GL_{\mathbb{K}}(M)$, dada por $\varphi(g)(m) = mg$. Portanto, da definição de G - módulo, φ é uma representação linear de G sobre $\mathbb{K}$.

Agora, dado φ uma representação linear de G sobre $\mathbb{K}$, podemos definir um G - módulo M usando a representação da seguinte forma

$$\begin{array}{rccc} \alpha & : & M \times G & \longrightarrow & M \\ & & (m, g) & \longmapsto & \varphi(g)(m). \end{array}$$

Portanto, M é um G - módulo sobre $\mathbb{K}$. Assim, estudar as representações lineares de G sobre $\mathbb{K}$ é o mesmo que estudar os G - módulos sobre $\mathbb{K}$.

Sejam G um grupo, $\mathbb{K}$ um corpo, M um G - módulo, onde $\{e_1, \ldots, e_n\}$ é uma base de M. Para cada $g \in G$, temos definido $\varphi(g) : M \to M$ dada por $\varphi(g)(m) = mg$. Consideremos a matriz da aplicação $\varphi(g)$ dada por

$$T(g) = \begin{pmatrix} (\varphi(x))_{11} & \ldots & (\varphi(x))_{1n} \\ \vdots & \ldots & \vdots \\ (\varphi(x))_{n1} & \ldots & (\varphi(x))_{nn} \end{pmatrix}$$

Com isso podemos definir o caracter de um grupo.

Definição 1.1.5 *(Caracteres de um grupo [2])*

$$\begin{array}{rccl} \chi & : & G & \longrightarrow & \mathbb{C} \\ & & g & \longmapsto & tr(T(g)) = \sum_i (\varphi(g))_{ii} \end{array}$$

tal aplicação é o caracter de G relativo ao G - módulo M (ou ainda, o caracter de G associado a representação φ).

Observação 1.1.2 *O estudo dos caracteres de um grupo revela muito sobre a sua estrutura, os elementos a seguir são fundamentais no estudo dos caracteres:*

- *Chamamos $dim_{\mathbb{K}}(M) = n$ o grau do caracter χ e diremos que χ é um caracter irredutível de G se M for um G - módulo irredutível. Os carateres de grau 1 são ditos caracteres lineares.*

- *Seja G um grupo. O conjunto dos graus dos caracteres irredutíveis de G será denotado por $c.d.(G)$ [3].*

- *Seja χ um caracter. Definimos o núcleo de χ (o qual será indicado por $Ker\ \chi$) como sendo o seguinte conjunto:*

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

Proposição 1.1.2 *Sejam M e M' G - módulos, de dimensão finita, sobre $\mathbb{C}$ e χ o caracter de G relativo a M. Então,*

[2] Nessas notas os caracteres são sempre relativos a um G - módulo, de dimensão finita, sobre $\mathbb{C}$.

[3] Vem do inglês: "character degree"

(a) χ *está bem definido;*

(b) Se M *e* M' *são* G *- isomorfos, então os seus caracteres* χ, χ' *são iguais;*

(c) $\chi(x^g) = \chi(x)$ *para todos* $g, x \in G$*;*

(d) $\chi(1) = n(\in \mathbb{K})$.

Demonstração. (a): Nossa definição de caracter foi dada a partir de uma base fixada. Vamos mostrar que o caracter independende da escolha da base. Tomemos $(\alpha_{ij}(g))$ e $(\beta_{ij}(g))$ as matrizes de φ, relativo a duas bases quaiquer. Temos que existe uma matriz invertível T tal que $(\alpha_{ij}(g)) = T^{-1}(\beta_{ij}(g))T$. Portanto,

$$tr((\alpha_{ij}(g))) \;=\; tr(T^{-1}(\beta_{ij}(g))T) \;=\; tr((\beta_{ij}(g))TT^{-1}) \;=\; tr((\beta_{ij}(g))).$$

Lembre que dado A, B matrizes $n \times n$ com entradas em $\mathbb{K}$, temos $tr(AB) = tr(BA)$.

Demonstração. (b): Tomemos μ um G - isomorfismo de M sobre M', $\beta = \{e_1, \ldots, e_n\}$ uma base de M e, por linearidade, $\beta' = \{\mu(e_1, \ldots, \mu(e_n))\}$ uma base de M'. Temos que os caracteres as aplicações $\varphi : M \to M$, dada por $\varphi(g)(m) = mg$ e $\varphi' : M' \to M'$, dada por $\varphi(g)(m') = m'g$ nas bases fixadas inicialmente, são representadas pela mesma matriz. Dessa forma, $\chi = \chi'$, isto é, $\chi(g) = \chi'(g)$, para todo $g \in G$.

Demonstração. (c): Basta observar que $\varphi(x)$ e $\varphi(g^{-1}xg) = \varphi(g)^{-1}\varphi(x)\varphi(g)$ Portanto, $\chi(x) = \chi(x^g)$.

Demonstração.(d): Note que $\chi(1) = tr(\varphi(1)) = tr(Id) = n$, onde esse elemento é a soma de "$1_{\mathbb{K}}$".

Proposição 1.1.3 *Sejam G um grupo finito, M um G - módulo de dimensão finita sobre $\mathbb{C}$ e χ o caracter de G relativo a M. Então, para todo $g \in G$,*

(a) $\chi(g)$ é uma soma de raízes $|G|$ - ésimas da unidade;

(b) $\chi(g^{-1}) = \bar{\chi}(g)$;

(c) $|\chi(g)| \leqslant \chi(1)$ [4].

Demonstração. (a): Sejam $dim_{\mathbb{C}}(M)$ e $g \in G$. Tomemos uma base para M, onde a matriz de $\varphi(g)$ tenha a seguinte forma (triangular superior)

$$T(g) = \begin{pmatrix} \varepsilon_1(g) & & * \\ & \ddots & \\ 0 & & \varepsilon_n(g) \end{pmatrix}$$

Portanto, $Id_{n\times n} = T(1) = T(g^{|G|}) = \begin{pmatrix} \varepsilon_1(g)^{|G|} & & * \\ & \ddots & \\ 0 & & \varepsilon_n(g)^{|G|} \end{pmatrix}$

Logo, $\varepsilon_1(g), \ldots, \varepsilon_n(g)$ são raízes $|G|$ - ésimas da unidade.

Demonstração. (b): Usando a mesma base para M do item anterior, temos que

$\overline{\chi(g)} = \overline{\sum_{j=1}^{n} \varepsilon_j(g)} = \sum_{j=1}^{n} \overline{\varepsilon_j(g)} = \sum_{j=1}^{n} \varepsilon_j(g)^{-1} = \chi(g^{-1})$, visto que $T(g^{-1}) = T(g)^{-1}$.

Demonstração. (c): Pelo item (a), $\chi(g)$ é a soma de raízes $|G|$ - ésimas da unidade. Assim, $|\chi(g)| \leqslant |\varepsilon_1(g)| + \ldots + |\varepsilon_n(g)| = n = \chi(1)$.

□

[4] Abuso de notação, estaremos identificando $\chi(1) = f_\chi = |\chi(1)|$.

1.1.3 A - módulo e Álgebras

Definição 1.1.6 *(A - módulos) Sejam A um anel com 1 e M um grupo abeliano. Dizemos que M é um A - módulo (à esquerda) se for definida uma aplicação*

$$\begin{array}{rccc} \alpha & : & A \times M & \longrightarrow & M \\ & & (a, m) & \longmapsto & a \cdot m = am \end{array}$$

satisfazendo

- $1_A m = m$;
- $a(m + m') = am + am'$;
- $(a + a')m = am + a'm$
- $(aa')m = a(a'm)$

para quaisquer $m, m' \in M$ e $a, a' \in A$.

Definição 1.1.7 *(A - submódulos, A - módulos irredutíveis e completamente redutíveis)*

1. *Seja $X \leqslant M$. Dizemos que X é um A - submódulo de M (e indicaremos por $X \leqslant_A M$), se para cada elemento $m \in X$ e para todo $a \in A$ tivermos $am \in X$.*
2. *Um A - módulo M é dito irredutível se $M \neq \{0\}$ e se os únicos A - submódulos são $\{0\}$ e M;*
3. *Um A - módulo M é dito completamente redutível se para todo $X \leqslant_A M$, existe $Y \leqslant_A M$ tal que $M = X \oplus Y$.*

Exemplo 1.1.2

- *Sejam* $\mathbb{K}$ *um corpo,* $n \in \mathbb{N}$, $\mathbb{K}^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{K}\}$ *e* A *o anel das matrizes* $n \times n$ *com entradas em* $\mathbb{K}$. *Temos que* $\mathbb{K}^n$ *é um* A *- módulo, basta considerar a multiplicação de "vetor por matriz", i.e.,*

$$\begin{array}{rccc} \alpha \ : & A \times \mathbb{K}^n & \longrightarrow & \mathbb{K}^n \\ & (M, (x_1, \ldots, x_n)) & \longmapsto & (x_1, \ldots, x_n)M \end{array}$$

- *Seja* $M \neq \{0\}$ *um grupo abeliano. Temos que* $End\ M = \{a : M \to M \mid a$ *é um homomorfismo*$\}$ *é um anel, basta definir:*

$$(a + a')(m) = a(m) + a'(m) \ e \ (aa')(m) = a(a'(m))$$

para todo $m, m' \in M$ *e* Id_M *é a identidade de* M. *Temos que* M *é um* A *- módulo, onde* $A = End\ M$.

Definição 1.1.8 *(Homomorfismos e Isomorfismos entre* A *- módulos) Sejam* A *um anel com* 1, M, M' *dois* A *- módulos.*

1. *Dizemos que uma Homomorfismo* $\theta : (M, +) \to (M', +)$ *é um* A *- homomorfismo se para todos* $m \in M$ *e* $a \in A$, *tivermos* $\theta(ma) = \theta(m)a$.

2. *Dizemos que uma aplicação* $\mu : M \to M'$ *é um* A *- isomorfismo de* M *sobre* M' *se* μ *é um* A *- homomorfismo e é invertível. Naturalmente,* μ^{-1} *também é* A *- isomorfismo de* M' *sobre* M.

O conjunto dos A - homomorfismo de M em M' será denotado por $Hom_A(M, M')$.

Definição 1.1.9

1. *(Representações e A - módulos) Uma representação φ de um anel A com 1 sobre um grupo abeliano M é um homomorfismo de A no anel $(End\ M, +, \cdot)$*

2. *(Representações Equivalentes) Duas representações φ, φ' de A sobre os grupos abelianos M, M', respectivamante, são ditas equivalentes, se existir um isomorfismo (de grupo) $\mu : M \to M'$ tal que $\mu(\varphi(a)(m)) = \varphi'(a)(\mu(m))$, para todos os $m \in M$ e $a \in A$.*

Definição 1.1.10 *(Álgebras sobre Corpos) Seja $\mathbb{K}$ um corpo. Um anel A com 1 é uma álgebra sobre $\mathbb{K}$, se tiver definida uma aplicação:*

$$\begin{aligned} \alpha \ : \ \mathbb{K} \times A \ &\longrightarrow \ A \\ (x, a) \ &\longmapsto \ xa \end{aligned}$$

satisfazendo,

- *$(A, +)$ é um espaço vetorial sobre $\mathbb{K}$ onde "$+$"é a operação definida no anel e o produto por escalar é o apresentado por α;*

- *$\lambda(ab) = a(\lambda b) = (\lambda a)b$, $\forall\ a, b \in A$ e todo $\lambda \in \mathbb{K}$.*

Proposição 1.1.4 *Sejam $\mathbb{K}$ um corpo e A uma álgebra sobre $\mathbb{K}$. Se M é um A - módulo, então M torna-se um espaço vetorial sobre $\mathbb{K}$, onde podemos definir $\lambda m = m(\lambda \cdot 1)$.*

Demonstração: Já temos que $(M, +)$ é um grupo abeliano. Daí, resta mostrar: para todos $m, m_1 \in M$ e $\lambda_1, \lambda_2 \in \mathbb{K}$

- $1_{\mathbb{K}}m = m(1_{\mathbb{K}} \cdot 1) = m(1) = m$;
- $\lambda_1(m + m_1) = (m + m_1)(\lambda_1 \cdot 1) = m(\lambda_1 \cdot 1) + m_1(\lambda_1 \cdot 1) = \lambda_1 m + \lambda_1 m_1$;
- $(\lambda_1\lambda_2)m = m((\lambda_1\lambda_2) \cdot 1) = m(\lambda_1(\lambda_2) \cdot 1)) = m((\lambda_1 \cdot 1)(\lambda_2 \cdot 1) = m((\lambda_2 \cdot 1)(\lambda_1 \cdot 1) = (m(\lambda_2 \cdot 1))(\lambda_1 \cdot 1) = (\lambda_2 m)(\lambda_1 \cdot 1) = \lambda_1(\lambda_2 m)$;
- $(\lambda_1+\lambda_2)m = m((\lambda_1+\lambda_2)\cdot 1) = m(\lambda_1 \cdot 1+\lambda_2 \cdot 1) = m(\lambda_1 \cdot 1)+m(\lambda_2 \cdot 1) = \lambda_1 m + \lambda_2$

□

1.1.4 Álgebra de Grupo

Sejam G um grupo finito e $g_1, \ldots, g_n$ seus elementos. Vamos definir um espaço vetorial (que será denotado por $\mathbb{K}G$) onde $g_1, \ldots, g_n$ formam uma base desse espaço e os elementos são dados por:

$$\lambda_1 g_1 + \ldots + \lambda_n g_n,$$

onde $\lambda_i \in \mathbb{K}$. E dados $u = \sum_{i=1}^{n} \lambda_i g_i$, $v = \sum_{i=1}^{n} \mu_i g_i$ e $\lambda \in \mathbb{K}$, definamos:

$$u + v = \sum_{i=1}^{n} (\lambda_i + \mu_i) g_i \text{ e } \lambda u = \sum_{i=1}^{n} \lambda\lambda_i g_i.$$

Temos que $dim_{\mathbb{K}}(\mathbb{K}G) = |\{g_1, \ldots, g_n\}| = |G|$. Chamamos $\beta = \{g_1, \ldots, g_n\}$ a base natural de $\mathbb{K}G$.

O espaço vetorial $\mathbb{K}G$ tem uma estrutura natural de G - módulo sobre $\mathbb{K}$, bastando para isso considerar:

$$\begin{aligned} \alpha \ : \ \mathbb{K}G \times G \ &\longrightarrow \ \mathbb{K}G \\ (m, g) \ &\longmapsto \ mg \end{aligned}$$

onde $m = \sum_{h \in G} \mu_h h$ e $mg = \sum_{h \in G} \mu_h hg$.

Observação 1.1.3 *Seja G um grupo finito. O espaço vetorial $\mathbb{K}G$ com a "multiplicação α" é chamado de G - módulo regular.*

No espaço vetorial $\mathbb{K}G$ definimos uma multiplicação dada por:

$$\Big(\sum_{g \in G} \lambda_g g\Big)\Big(\sum_{h \in G} \mu_h h\Big) = \Big(\sum_{g,h \in G} (\lambda_g \mu_h)(gh)\Big)$$

onde $\lambda_g, \mu_g \in \mathbb{K}$.

Proposição 1.1.5 *Sejam G um grupo finito com h classes de conjugação, $\chi_1, \ldots, \chi_h$ seus caracteres irredutíveis sobre $\mathbb{C}$ e $n_1 = 1, n_2 = \chi_2(1), \ldots, n_h = \chi_h(1)$ seus respectivos graus de caracteres. Então*

$1 + n_2\chi_2(g) + \ldots + n_h\chi_h(g) = 0$ *ou* $|G|$, *se* $g \neq 1$ *ou* $g = 1$, *respectivamante.*

Para uma demonstração veja J. Gordon e M. Liebeck [11]

Definição 1.1.11 *(Álgebra de Grupo)*

1. *O espaço vetorial $\mathbb{K}G$ com essa multiplicação é chamada álgebra de grupo sobre $\mathbb{K}$ (ou simplesmente, álgebra de grupo).*

2. *Em $\mathbb{K}G$ consideremos seguinte subespaço $Z(\mathbb{K}G) = \{z \in \mathbb{K}G \ | \ zr = rz, \text{ para todo } r \in \mathbb{K}G\}$, que é chamado de centro da álgebra de grupo.*

Observação 1.1.4 *Seja G um grupo. Indicaremos por $k(G)$ o número de classes de conjugação do grupo G.*

Definição 1.1.12 *Sejam G um grupo, $l = k(G)$ e $C_1, \ldots, C_l$ as classes de conjugação de G.Definamos, para cada $1 \leqslant i \leqslant l$, os seguintes elementos na álgebra de grupo:*

$$\overline{C}_i = \sum_{g \in C_i} g.$$

Proposição 1.1.6 *Sejam G um grupo, $l = k(G)$ e $C_1, \ldots, C_l$ as classes de conjugação de G. Então $\{\overline{C}_1, \ldots, \overline{C}_l\}$ formam uma base para o centro da álgebra de grupo $Z(\mathbb{C}G)$.*

Demonstração: Faremos a demonstração em etapas:

- $\overline{C}_i \in Z(\mathbb{C}G)$, $1 \leqslant i \leqslant l$: Consideremos C_i a classe de conjugação de um dado elemento $g \in G$ com, digamos, r elementos. Dessa forma, $C_i = \{y_1^{-1} g y_1, \ldots, y_r^{-1} g y_r\}$. E $\overline{C}_i$ é escrito como:

$$\overline{C}_i = \sum_{j=1}^{r} y_j^{-1} g y_j.$$

Para cada $h \in G$,

$$h^{-1}\overline{C}_i h = \sum_{j=1}^{r} h^{-1} y_j^{-1} g y_j h = \sum_{j=1}^{r} x_j^{-1} y x_j = \overline{C}_i.$$

Com isso, $h\overline{C}_i = \overline{C}_i h$, para todo $h \in G$. Assim, para todo $r = \sum_{h \in G} \mu_h h \in \mathbb{C}G$, temos

$$\Big(\sum_{h\in G}\mu_h h\Big)\overline{C}_i = \overline{C}_i\Big(\sum_{h\in G}\mu_h h\Big).$$

Portanto, $\overline{C}_i \in Z(\mathbb{C}G)$.

- $\beta = \{\overline{C}_i \mid \ 1 \leqslant i \leqslant l\}$ é linearmente independente: Com efeito, dados $\lambda_1, \ldots, \lambda_l \in \mathbb{C}$ tais que $\sum_{i=1}^{l} \lambda_i \overline{C}_i = 0$, como as classes são disjuntas, temos que $\lambda_i \overline{C}_i = 0$, para todo $i = 1, \ldots, l$, assim $\lambda_i \sum_{g\in C_i} g = 0$ e, consequentemente, $\lambda_i = 0$. Como esse i é qualquer, segue que $\lambda_1 = \ldots = \lambda_l = 0$ e β é linearmente independente.

- $\beta = \{\overline{C}_1, \ldots, \overline{C}_l\}$ gera $Z(\mathbb{C}G)$: Tome $z = \sum_{g\in G} \lambda_g \ g \in Z(\mathbb{C}G)$. Para cada $h \in G$, temos $rh = hr$ e, conseqüentemente, $h^{-1}rh = r$. Ou ainda,

$$\sum_{g\in G} \lambda_g \ h^{-1}gh = \sum_{g\in G} \lambda_g \ g.$$

Portanto, se g e g' são elementos conjugados, então os coeficientes correspondentes são iguais ($\lambda_g = \lambda_{g'}$). Com isso, $r = \sum_{i=1}^{l} \lambda_i \overline{C}_i$, onde $\lambda_i = \lambda_{g_i}$ para algum elemento da classe de conjugação C_i.

Logo, $dim_{\mathbb{C}}\ Z(\mathbb{C}G) = k(G)$.

Proposição 1.1.7 *Sejam G um grupo com $l = k(G)$classes de conjugação $C_1, \ldots, C_l$ e V um G - módulo irredutível (sobre $\mathbb{C}$) e $z \in Z(\mathbb{C}G)$. Então, existe $\lambda \in \mathbb{C}$ tal que*

$$vz = \lambda v,$$

para todo $v \in V$.

Demonstração: Temos que $z = \sum_{i=1}^{l} \lambda_i \overline{C}_i$, onde $\lambda_i \in \mathbb{C}$. Definamos

$$\begin{array}{rccc} \theta & : & V & \longrightarrow & V \\ & & v & \longmapsto & vz \end{array}$$

onde, $vz = \sum_{i=1}^{l} \lambda_i (v\overline{C}_i)$ e $\overline{C}_i = \sum_{g \in C_i} g$.

- θ é um G - homomorfismo: De fato,

– $\theta(v_1 + \lambda v_2) = (v_1 + \lambda v_2)z = (v_1)z + \lambda(v_2)z = \theta(v_1) + \lambda\theta(v_2)$;

– $\theta(vg) = (vg)z = (v)gz \overset{z \in Z(\mathbb{C}G)}{=} (v)zg = \theta(v)g$.

Como V é irredutível e θ é um G - homomorfismo segue que θ é um G - isomorfismo e mais, existe $\lambda \in \mathbb{C}$ tal que $\theta = \lambda Id_V$ (Lema de Schur).

Observação 1.1.5 *De modo análogo iremos definir o caracter de uma álgebra. Vejamos:*

Sejam A uma álgebra com 1 (sobre $\mathbb{C}$), M um A - módulo, onde $\{e_1, \ldots, e_n\}$ é uma base de M. Para cada $a \in G$, temos definido $\varphi(a) : M \to M$ dada por $\varphi(a)(m) = am$. Consideremos a matriz da aplicação $\varphi(a)$ dada por

$$T(a) = \begin{pmatrix} (\alpha(a))_{11} & \ldots & (\alpha(a))_{1n} \\ \vdots & \ldots & \vdots \\ (\alpha(a))_{n1} & \ldots & (\alpha(a))_{nn} \end{pmatrix}$$

Com isso, o caracter da álgebra A é dada pela seguinte aplicação:

$$\begin{array}{rccl} \chi & : & A & \longrightarrow & \mathbb{C} \\ & & a & \longmapsto & tr(T(a)) = \sum_i (\alpha(a))_{ii} \end{array}$$

tal aplicação é o caracter de A relativo ao A - módulo M (ou ainda, o caracter de G associado a representação φ).

Quando a álgebra em questão é $A = \mathbb{C}G$ o caracter da álgebra induz, de maneira natural um caracter do grupo G, dado pela restrição do caracter aos elementos do grupo.

1.2 Caracteres

1.2.1 Levantamento de Caracteres

Sejam G um grupo e $N \lhd G$. Iremos construir, de modo natural, um caracter de G a partir de um caracter de G/N.

Proposição 1.2.1 *Sejam $N \lhd G$ e $\tilde{\chi}$ um caracter de G/N. Se*

$$\begin{array}{rccl} \chi & : & G & \longrightarrow & GL(n, \mathbb{C}) \\ & & g & \longmapsto & \tilde{\chi}(gN) \end{array}$$

Então, χ é um caracter de G e os caracteres χ, $\tilde{\chi}$ tem o mesmo grau.

Demonstração: Como $\tilde{\chi}$ é um caracter de G/N, consideremos a sua representação $\tilde{\rho} : G/N \to GL(n, \mathbb{C})$. Definamos

$$\begin{array}{rccl} \rho & : & G & \longrightarrow & GL(n, \mathbb{C}) \\ & & g & \longmapsto & \tilde{\rho}(gN) \end{array}$$

Note que $\rho = \tilde{\rho} \circ \pi_N$ é um homomorfismo de G em $GL(n, \mathbb{C})$, com isso ρ é uma representação de G. E para cada $g \in G$ o caracter de ρ:

$\chi(g) = \chi_\rho(g) = tr(\rho(g)) = tr(\tilde{\rho}(gN)) = \tilde{\chi}(gN)$. Portanto, $\chi(g) = \tilde{\chi}(gN)$, para todo $g \in G$. Logo, χ e $\tilde{\chi}$ tem o mesmo grau.

□

Definição 1.2.1 *Se $N \lhd G$ e $\tilde{\chi}$ é um caracter de G/N, então o caracter χ de G o qual é dado pela Proposição 1.2.1 é chamado de o levantamento de $\tilde{\chi}$ para G.*

Teorema 1.2.1 (Correspondência de Caracteres) *Seja $N \lhd G$. Para cada caracter de G/N associaremos o seu levantamento para G, nós obtemos uma correspondência biunívoca entre o conjunto dos caracteres de G/N e o conjunto dos caracteres χ, de G, satisfazendo $N \leqslant Ker\ \chi$. Além disso, os caracteres irredutíveis de G/N correspondem, "via levantamento", aos caracteres irredutíveis de G para os quais N está no seu núcleo.*

Demonstração: Tomemos $\tilde{\chi}$ um caracter de G/N e consideremos o seu levantamento, então para cada $n \in N$, $\chi(n) = \tilde{\chi}(nN) = \tilde{\chi}(N) = \chi(1)$. Assim, $N \leqslant Ker\ \chi$.

Por outro lado, dado χ um caracter de G com $N \leqslant Ker\ \chi$ e a sua representação ρ de G. Dados $g_1, g_2 \in G$ tais que $g_1N = g_2N$, portanto $g_2^{-1}g_1 \in N$ e $\rho(g_2^{-1}g_1) = I$. Assim, podemos definir (e estará bem definido)

$$\begin{array}{rccc} \tilde{\rho} & : & G/N & \longrightarrow & GL(n, \mathbb{C}) \\ & & gN & \longmapsto & \rho(g) \end{array}$$

– $\tilde{\rho}$ é uma representação de G/N: $\tilde{\rho}(g_1Ng_2N) = \tilde{\rho}(g_1g_2N) = \rho(g_1g_2) = \rho(g_1)\rho(g_2) = \tilde{\rho}(g_1N)\tilde{\rho}(g_2N)$.

– O caracter $\tilde{\chi}$ de $\tilde{\rho}$ é um levantamento de χ para G: $\tilde{\chi}(gN) = tr(\tilde{\rho}(gN)) = tr(\rho(g)) = \chi(g)$.

Agora resta mostrar que caracteres irredutíveis de G/N corresponde aos caracteres irredutíveis de G com $N \leqslant Ker\chi$. Para isso basta observar que um subespaço U de $\mathbb{C}^N$ é um $\mathbb{C}G$ - submódulo de $\mathbb{C}^n$ se, e somente se U é um $\mathbb{C}(G/N)$ - submódulo, pois $\rho(g)(u) \in U$ para todo $u \in U$ se, e somente se $\rho(gN)(u) \in U$ para todo $u \in U$. Daí, a representação ρ é irredutível é equivalente a ρ ser irredutível e, consequentemente, χ é irredutível se, e somente se, $\bar{\chi}$ é irredutível.

□

Proposição 1.2.2 *Se χ é um caracter linear de G, então $G' = \langle a^{-1}b^{-1}ab \mid a, b \in G\rangle \leqslant Ker\ \chi$*

Demonstração: Consideremos a representação $\rho : G \to \mathbb{C}^*$, cujo caracter associado seja χ. Como ρ é um homomorfismo e $(\mathbb{C}^*, .)$ é abeliano, dados $g, h \in G$, temos $\rho(g^{-1}h^{-1}gh) = 1$. Assim, para qualquer elemento $\alpha \in G'$, $\rho(\alpha) = 1$. Logo, $G' \leqslant Ker\chi$.

Como veremos a seguir, a quantidade de caracteres lineares de um grupo é dado pelo índice do subgrupo derivado.

Teorema 1.2.2 *Os caracteres lineares de G são precisamente os levantamentos dos caracteres irredutíveis de G/G'. Em particular, o número de caracteres lineares distintos de G é igual $|G : G'|$.*

Demonstração: Consideremos $m = |G : G'|$. Como G/G' é abeliano temos que o número de caracteres irredutíveis é $|G : G'|$ (que é o número de classes de conjugação de G/G'). Chamemos $\tilde{\chi}_1, \ldots, \tilde{\chi}_m$ os levantamentos de $\chi_1, \ldots, \chi_m$, respectivamente.

Pelo Teorema 1.2.1, os levantamentos dos caracteres irredutíveis de G/G' são caracteres irredutíveis de G e como $G' \leqslant Ker\ \chi$, pela Proposição 1.2.2 temos que $\tilde{\chi}_1, \ldots, \tilde{\chi}_m$ são os únicos caracteres lineares de G.

1.2.2 Identidades de Caracteres e Aplicações

Nessa seção vamos apresentar identidades dos caracteres, entre elas cabe ressaltar as relações de ortogonalidade e as "relações aritméticas"dos caracteres irredutíveis.

Lema 1.2.1 (Lema de Schur para A - módulos) *Sejam A um anel com 1, M e N A - módulos irredutíveis. Então:*

(a) *Se $M \ncong_A N$, então $Hom_A(M, N) = \{0\}$;*

(b) *Se $M = N$, então $Hom_A(M, N) = End_A(M)$ é um anel de divisão;*

(c) *Se $A = \mathbb{C}G$ para algum grupo finito G, então $End_{\mathbb{C}G}(M) \cong \mathbb{C}$.*

Demonstração. (a): Dado $\rho \in Hom_A(M, N)$, temos que $Ker\ \rho$ e $\rho(M)$ são A - submódulos de M e N, respectivamente. Suponhamos que

exista $\rho \in Hom_A(M,N)$, com $\rho \neq 0$, portanto $Ker\ \rho \neq M$ e $\rho(M) \neq N$. Mas M, N são A - módulos irredutíveis, assim $Ker\ \rho = \{0\}$ e $\rho(M) = n$. Logo, $M \simeq_A N$. Absurdo. Daí, $Hom_A(M,N) = \{0\}$.

Demonstração. (b): Como M é um A - módulo irredutível, temos que $M \neq \{0\}$. Já sabemos que $Hom_A(M,M) = End_A(M)$ e, mais, $Id_M \in End_A(M)$. Agora tomemos $0 \neq \rho \in End_A(M)$, portanto, $Ker\ \rho \neq M$ e $\{0\} \neq \rho(M) \leqslant_A M$. Mas M é um A - módulo irredutível, assim, $Ker\ \rho = \{0\}$ e $\rho(M) = M$. Logo, ρ é uma bijeção de M em M. Daí, existe $\varphi \in End_A(M)$ tal que $\rho\varphi = \varphi\rho = Id_M$.

Demonstração. (c): Vamos apresentar um isomorfismo (de anéis) entre $End_{\mathbb{C}G}M$ e $\mathbb{C}$. Definamos:

$$\begin{array}{rccc} \rho & : & \mathbb{C} & \longrightarrow & End_{\mathbb{C}G}(M) \\ & & \lambda & \longmapsto & \rho_\lambda \end{array}$$

onde $\rho_\lambda(m) = \lambda m$, para todo $m \in M$. Dados $\lambda_1, \lambda_2 \in \mathbb{C}$ e $m \in M$, temos

- $\rho_1(m) = 1m = m$;
- $\rho_{\lambda_1+\lambda_2}(m) = (\lambda_1 + \lambda_2)m = \rho_{\lambda_1}(m) + \rho_{\lambda_2}(m)$;
- $\rho_{\lambda_1\lambda_2}(m) = (\lambda_1\lambda_2)m = \lambda_1(\rho_{\lambda_2}(m)) = \rho_{\lambda_1}(\rho_{\lambda_2}(m))$.

Agora vamos mostrar que ρ é sobre. Seja $\mu \in End_A(M)$, como $\mathbb{C}G$ é uma álgebra podemos pensar M como um espaço vetorial sobre $\mathbb{C}$, bastando para isso considerar a multiplicação por escalar $\lambda m = m(\lambda \cdot 1)$.

Consideremos $P_\lambda = \mu - \lambda Id_M$, com $\lambda \in \mathbb{C}$. Como $\mathbb{C}$ é algebricamente fechado e o determinante da matriz de P_λ é um polinômio de tem grau, temos que existe um $\lambda_1 \in \mathbb{C}$ tal que P_{λ_1} não é invertivel. Ou seja, existe $m_0 \in M$ tal que $\mu(m_0) = \lambda m_0$.

Note que $0 \neq m_0A \leqslant_A M$ e como M é irredutível, portanto $m_0A = M$. Assim, dado $m \in M$ existe $a \in A$ tal que $m = m_0a$ e

$$\mu(m) = \mu(m_0a) = \mu(m_0)a = (\lambda_1 m_0)a = \lambda_1 m.$$

Como é m é arbitrário, $\mu = \lambda_1 Id$. Logo, ρ é sobre e, consequentemente, $End_{\mathbb{C}G}(M) \simeq \mathbb{C}$.

A proposição a seguir é, de certa forma, uma maneira de reescrever o **Lema de Schur** numa perspectiva "pontual", isto é, possibilita entender como as entradas da matriz do operador ("de entrelaçamento") se comportam.

Proposição 1.2.3 *Sejam G um grupo finito, M e N $\mathbb{C}G$ - módulos irredutíveis de dimensões m e n, respectivamente. Sejam φ, ψ as representações correspondentes e $x \in G$. Se $(\alpha_{ij}(x)) \in M(m, \mathbb{C})$ e $(\beta_{ij}(x)) \in M(n, \mathbb{C})$ são as matrizes das aplicações $\varphi(x)$ e $\psi(x)$ com respeito a bases, fixadas, de M e N, então*

(a) *Se $M \ncong_{\mathbb{C}G} N$, então $\sum_{x\in G} \alpha_{ij}(x)\beta_{kl}(x^{-1}) = 0$, para quaisquer $1 \leqslant i, j \leqslant m$ e $1 \leqslant k, l \leqslant n$.*

(b) *Se $M = N$, então $\sum_{x\in G} \alpha_{ij}(x)\alpha_{kl}(x^{-1}) = \frac{\delta_{jk}\delta_{il}|G|}{m}$, para todo $i, j, k, l \in \{1, \ldots, m\}$.*

Observação 1.2.1 *Para cada aplicação linear $u : M \to N$, associaremos $T_u : M \to N$, dada por $\sum_{x\in G} \varphi(x)u\psi(x^{-1})$. Como T_u é a soma de aplicações de lineares, temos que ela é linear. Além disso para cada $y \in G$*

$$\begin{aligned}\varphi(y)T_u &= \sum_{x\in G}\varphi(yx)u\psi(x^{-1}) = \sum_{x\in G}\varphi(yx)u\psi(x^{-1}y^{-1})\psi(y)\\ &\overset{z=yx}{=} \left(\sum_{z\in G}\varphi(z)u\psi(z^{-1})\right)\psi(y) = T_u\psi(y).\end{aligned}$$

Demonstração. (a): Como $M \not\cong_A N$, pelo Lema de Schur, $T_u = 0$ qualquer que seja a aplicação linear u escolhida. Fixemos $\{e_1, \ldots, e_m\}$ base de M e $\{f_1, \ldots, f_m\}$ base de N. Dado (γ_{ij}) uma matriz de uma aplicação linear u na base acima. Temos que

$$0 = (T_u)_{il} = \sum_{x\in G}\sum_{s=1}^{m}\sum_{r=1}^{n}\alpha_{is}(x)\gamma_{sr}\beta_{rl}(x^{-1})$$

Escolha a seguinte aplicação linear $u_{sr} : M \to N$, com $e_k \mapsto \delta_{rk}f_s$. E sua matriz $(u_{sr}) = (\delta_{sj}\delta_{rk})_{s,r}$, com $1 \leqslant j \leqslant m$ e $1 \leqslant k \leqslant n$. Portanto,

$$\begin{aligned}0 &= (T_u)_{il} = \sum_{x\in G}\sum_{s=1}^{m}\sum_{r=1}^{n}\alpha_{is}(x)\delta_{sj}\delta_{rk}\beta_{rl}(x^{-1})\\ &= \sum_{x\in G}\alpha_{ij}(x)\beta_{kl}(x^{-1})\end{aligned}$$

para quaisquer escolhas de $1 \leqslant i, j \leqslant m$ e $1 \leqslant k, l \leqslant n$.

Demonstração. (b): Se $M = N$, então, pelo Lema de Schur - $End_{\mathbb{C}G}$, para cada aplicação linear u, T_u é um múltiplo da identidade, i.e., existe $\lambda \in \mathbb{C}$ tal que $T_u = \lambda\, Id_M$. Assim, para cada $i, l = 1, \ldots, m$ temos

$$\lambda\delta_{il} = (T_u)_{il} = \sum_{x\in G}\alpha_{is}(x)\gamma_{sr}\beta_{rl}(x^{-1}) \tag{1.1}$$

Como o traço é aditivo,

$$tr(T_u) = tr(\sum_{x\in G} \varphi(x)(u)\psi(x^{-1})) = \sum_{x\in G} tr(\varphi(x)u\psi(x^{-1})) = |G|tr((u)).$$

Ainda para (γ_{sr}) (definido no item **(a)**), temos $tr((\gamma_{sr})) = \sum_{l=1}^{m}(\gamma_{sr})_{ll} = \sum_{l=1}^{m}\delta_{lj}\delta_{lk} = \delta_{kj}$. Por outro lado, $tr(T_u) = \lambda m$. Daí,

$$\lambda = \frac{\delta_{jk}|G|}{m} \text{ e } \sum_{x\in G}\alpha_{ij}(x)\alpha_{kl}(x^{-1}) = \frac{|G|\delta_{jk}\delta_{il}}{m}.$$

Teorema 1.2.3 *Sejam G um grupo, $y \in G$ e $k(G) = h$. Se $\chi_1, \ldots, \chi_h$ são os caracteres irredutíveis de G, então,*

(a) *para qualquer $h \in G$:*

$$\sum_{x\in G}\chi_m(g)\chi_n(x^{-1}y) = \begin{cases} \dfrac{\chi_n(y)}{f_{\chi_n}}|G|, & m = n \\ 0, & m \neq n \end{cases}$$

(b) $\sum_{\tau\in G}\chi([\sigma,\tau]) = \dfrac{|G|}{f_\chi}\bar{\chi}(\sigma)\chi(\sigma)$, *onde χ é um caracter irredutível de G.*

Demonstração do Teorema 1.2.3 :

Demonstração. (a): Caso $m \neq n$: tome ρ, ρ' as representações de G, que tem como caracteres χ, χ', respectivamente. Dado $h \in G$, pela Proposição 1.2.3 (a): Para quaisquer $1 \leqslant i, j \leqslant m$ e $1 \leqslant k, l \leqslant n$, temos $\sum_{x\in G}(\rho(x))_{ij}(\rho'(x^{-1}))_{kl} = 0$ e, consequentemente,

$$\sum_{x\in G}(\rho(x))_{ij}\left[(\rho'(x^{-1}))_{kl}(\rho'(y))_{lk}\right] = 0.$$

Portanto,

$$0 = \sum_{l}\sum_{x\in G}(\rho(x))_{ij}(\rho'(x^{-1}))_{kl}(\rho'(y))_{lk} \quad (1.2)$$

$$= \sum_{x\in G}(\rho(x))_{ij}(\rho'(x^{-1}y))_{kk}. \quad (1.3)$$

Como a expressão da proposição anterior (item (a)) é válida para quaisquer $1 \leqslant i, j \leqslant n$. Tomemos $i = j$ em (1.2),

$$\sum_{x\in G}(\rho(x))_{ii}(\rho'(x^{-1}y))_{kk} = 0.$$

Assim,

$$0 = \sum_{i,k}\sum_{x\in G}(\rho(x))_{ii}(\rho'(x^{-1}y))_{kk}$$

$$= \sum_{x\in G}\chi_m(x)\chi_n(x^{-1}y).$$

Caso $m = n$: tomemos ρ uma representação cujo caracter é $\chi_m = \chi_n = \chi$ e $y \in G$. Pela Proposição 1.2.3 (item (b)), temos

$$\frac{1}{|G|}\sum_{x\in G}(\rho(x))_{ij}(\rho(x^{-1}))_{kl}(\rho(y))_{lk} = \frac{\delta_{il}\delta_{jk}(\rho(y))_{lk}}{f_\chi}$$

Assim,

$$\frac{1}{|G|}\sum_{l}\sum_{x\in G}(\rho(x))_{ij}(\rho(x^{-1}))_{kl}(\rho(y))_{lk} = \frac{\delta_{jk}(\rho(y))_{ik}}{f_\chi}$$

Para $i = j$:

$$\frac{1}{|G|}\sum_{l}\sum_{x\in G}(\rho(x))_{ii}(\rho(x^{-1}y))_{kk} = \frac{\delta_{ik}(\rho(y))_{ik}}{f_\chi}.$$

Logo,

$$\begin{aligned}\frac{1}{|G|}\sum_{i,k,l}\sum_{x\in G}(\rho(x))_{ii}(\rho(x^{-1}y))_{kk} &= \sum_{i,k}\frac{\delta_{ik}(\rho(y))_{ik}}{f_\chi}\\ \frac{1}{|G|}\sum_{x\in G}\chi(x)\chi(x^{-1}y) &= \sum_{k}\sum_{i}\frac{\delta_{ik}(\rho(y))_{ik}}{f_\chi}\\ &= \sum_{k}\frac{(\rho(y))_{kk}}{f_\chi}\\ &= \frac{\chi(y)}{f_\chi}.\end{aligned}$$

Prova. (b): Sejam ρ e χ o seu caracter. De modo análogo ao resultado anterior, considere a proposição 1.2.3, temos $\frac{1}{|G|}\sum_{x\in G}(\rho(x))_{ij}(\rho(x^{-1}))_{kl}(\rho(y))_{lk} = \frac{\delta_{il}\delta_{jk}(\rho(y))_{lk}}{f_\chi}$. Dessa forma,

$$\frac{1}{|G|}\sum_{x\in G}(\rho(y^{-1}))_{li}(\rho(x))_{ij}(\rho(y))_{jk}(\rho(x^{-1}))_{kl} = \frac{\delta_{il}\delta_{jk}(\rho(y^{-1}))_{li}(\rho(y))_{jk}}{f_\chi}$$

Somando as expressões em i e j, obtemos:

$$\begin{aligned}\frac{1}{|G|}\sum_{x\in G}(\rho((x^{-1})^y))_{lk}(\rho(x))_{kl} &= \frac{(\rho(y^{-1}))_{ll}(\rho(y))_{kk}|G|}{f_\chi}\\ \sum_{k,l}\frac{1}{|G|}\sum_{x\in G}(\rho((x^y)^{-1}))_{lk}(\rho(x))_{kl} &= \frac{\chi(y^{-1})\chi(y)}{f_\chi}.\end{aligned}$$

Com isso temos o resultado.

Corolário 1.2.1 *(Relações de Ortogonalidade) Sejam G um grupo finito e $\chi_1,\ldots,\chi_m$ os caracteres irredutíveis de G sobre $\mathbb{C}$. Se χ_i,χ_j são caracteres, então*

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

Demonstração: Basta considerar o Teorema 1.2.3 item **(a)** fazer $h = 1$ e analisar os casos.

Corolário 1.2.2 *Seja G um grupo. Se χ é um caracter irredutível de G e definamos*

$$d_\chi := \frac{1}{|G|^2}\sum_{\sigma_1,\sigma_2}\bar{\chi}([\sigma_1,\sigma_2]),$$

então $d_\chi = f_\chi^{-1}$.

Demonstração: Do Teorema 1.2.3 (itens (a) e (b)), temos

$$\begin{aligned}
d_\chi &\overset{def.}{=} \frac{1}{|G|^2}\sum_{\sigma_1}\sum_{\sigma_2}\bar{\chi}([\sigma_1,\sigma_2]) \\
&= \frac{1}{|G|^2}\sum_{\sigma_2}\Big(\sum_{\sigma_1}\chi(\sigma_2^{-1}\sigma_1^{-1}\sigma_2\sigma_1)\Big) \\
&\overset{(b)}{=} \frac{1}{|G|^2}\sum_{\sigma_2}|G|f_\chi^{-1}\bar{\chi}(\sigma_2)\chi(\sigma_2) \\
&= \frac{f_\chi^{-1}}{|G|}\sum_{\sigma_2}\chi(1\cdot\sigma_2^{-1})\chi(\sigma_2) \\
&\overset{(a)}{=} f_\chi^{-1}.
\end{aligned}$$

1.2.3 Uma Base para as Funções de Classe

Definição 1.2.2 *Uma função de classe de um grupo G é uma função $\psi : G \to \mathbb{C}$ que assume valores constantes nas classes de conjugação, ou seja, se x e y são elementos conjugados em G, então $\psi(x) = \psi(y)$. O conjunto*

das funções de classe de G (será indicado por $CL(G)$), tem uma estrutura natural de espaço vetorial sobre $\mathbb{C}$.

Observação 1.2.2

- *Sejam G um grupo, com $C_1, \ldots, C_{k(G)}$ suas classes de conjugação e $CL(G)$ o espaço das funções de classe de G. Para cada $1 \leqslant i \leqslant k(G)$, consideremos f_i de G em $\mathbb{C}$, onde f_i é constante e igual a 1 na classe de conjugação C_i e 0 para os demais valores. Com isso, $dim_{\mathbb{C}(CL(G))} = k(G)$.*

- *Definamos o seguinte produto interno (Hermitiano) em $CL(G)$:*

$$\begin{array}{rccc} \langle .,. \rangle & : & CL(G) \times CL(G) & \longrightarrow & \mathbb{C} \\ & & (f,g) & \longmapsto & \displaystyle\sum_{x \in G} f(x)\overline{g(x)} \end{array}$$

  com isso podemos reescrever as relações de ortogonalidade da seguinte forma: os caracteres irredutíveis de G é um conjunto l.i. em $CL(G)$. Mais ainda, o resultado a seguir vai mostrar que os caracteres irredutíveis forma uma base ortonormal para $CL(G)$.

Teorema 1.2.4 *Os caracteres irredutíveis de G formam uma base ortonormal para $CL(G)$.*

Demonstração: Sejam $\chi_1, \ldots, \chi_h$ os caracteres irredutíveis, não equivalentes, de G. Pelas relações de ortogonalidade, $\chi_1, \ldots, \chi_h$ são linearmente independentes (" em $< .,. >_G$"). Portanto, $h \leqslant k(G)$. Mostraremos que $k(G) \leqslant h$. Consideremos o G - módulo regular e $V_1, \ldots, V_h$ um sistema completo de G - módulos irredutíveis não isomorfos (dado no Apêndice B), então

$$\mathbb{C}G = W_1 \oplus \ldots \oplus W_h,$$

onde para cada i, W_i é isomorfo a uma soma direta de cópias de V_i. Como $\mathbb{C}G$ contém um elemento identidade 1, nós podemos escrever $1 = f_1 + \ldots + f_h$, com $f_i \in W_i$ para $1 \leqslant i \leqslant h$.

Tomemos $z \in Z(\mathbb{C}G)$. Pela Proposição 1.1.7, para cada i existe $\lambda_i \in \mathbb{C}$ tal que $vz = \lambda_i v$, para todo $v \in V_i$. Portanto, $wz = \lambda_i w$ para todo $w \in W_i$. Em particular, $f_i z = \lambda_i f_i$ para cada $1 \leqslant i \leqslant h$. Daí,

$z = 1z = (f_1 + \ldots + f_h) = f_1 z + \ldots + f_h z = \lambda_1 f_1 + \ldots + \lambda_h f_h$.

Assim, $f_1, \ldots, f_h$ gera $Z(\mathbb{C}G)$, ou seja, $k(G) = dim_{\mathbb{C}} Z(\mathbb{C}G) \leqslant h$.

□

Corolário 1.2.3 *Os caracteres irredutíveis formam uma base do espaço das funções de classe sobre G. Mais ainda, se ψ é uma função de classe sobre G, então*

$$\psi = \sum_{i=1}^{k} \lambda_i \chi_i.$$

onde $\lambda_i = \langle \psi, \chi_i \rangle_G$ para $1 \leqslant i \leqslant k$.

Demonstração: Os caracteres $\chi_1, \ldots, \chi_k$ são linearmente independentes e geram um $CL(G)$, cuja dimensão é k. Sabemos que $dim_{\mathbb{C}} CL(G) = l$ e pelo teorema anterior, $k = l$. Logo, $\chi_1, \ldots, \chi_k$ forma uma base para $CL(G)$.

Dado $\psi \in CL(G)$, temos que $\psi = \sum_{i=1}^{k} \lambda_i \chi_i$. Portanto,

$$\langle \psi, \chi_j \rangle = \left\langle \sum_{i=1}^{k} \lambda_i \chi_i, \chi_j \right\rangle = \lambda_j.$$

Capítulo 2

Elementos não Comutadores

Apresentaremos propriedades elementares sobre os comutadores, subgrupos derivados e grupos com elementos no derivado que não são comutadores. Nosso interesse é estudar como a existência de elementos não comutadores interfere na estrutura do grupo (tais como, a ordem do próprio grupo e do subgrupo derivado) e reciprocamente, como a estrutura do grupo (especialmente os caracteres irredutíveis) "limitam"o comprimento do derivado.

2.1 Definições e Propriedades

Definição 2.1.1 (Comutadores e o Subgrupo Derivado) *Seja G um grupo.*

1. *Sejam $x, y \in G$. Definimos o comutador de x e y como sendo o elemento dado por $x^{-1}y^{-1}xy$, o qual é escrito como $[x, y]$.*

2. *O derivado de G é o subgrupo gerado pelos comutadores de G e será denotado por G'.*

Lema 2.1.1 *Sejam G um grupo, $x, y, z \in G$ e $j \in \mathbb{Z}$. Então,*

(i) $[x,y]^z = [x^z, y^z]$;

(ii) $[x,y]^{-1} = [y,x]$;

(iii) $[x,yz] = [x,z]\,[x,y]^z$;

(iv) $[xy,z] = [x,z]^y\,[y,z]$;

(v) Se x comuta com $[x,y]$, então $[x^j,y] = [x,y]^j$;

(vi) Se y comuta com $[x,y]$, então $[x,y^j] = [x,y]^j$;

(vii) Se $|G : Z(G)| = n$, então $[x,y]^{n+1} = [x,y^2]\,[x^y,y]^{n-1}$.

Demonstração do item (i): De fato,

$$[x,y]^z = z^{-1}(x^{-1}y^{-1}xy)z = (x^z)^{-1}(y^z)^{-1}x^zy^z = [x^z,y^z]\,;$$

Demonstração do item (ii): Temos $(x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y,x]$. Portanto, todo elemento do derivado pode ser escrito como o produto de comutadores.

Demonstração do item (iii):

$$\begin{aligned}
[x,yz] &= x^{-1}z^{-1}y^{-1}xyz \\
&= x^{-1}z^{-1}(xzz^{-1}x^{-1})y^{-1}xyz \\
&= x^{-1}z^{-1}xz(z^{-1}\,[x,y]\,z) \\
&= [x,z]\,[x,y]^z\,.
\end{aligned}$$

Demonstração do item (iv):

$$\begin{aligned}
[xy, z] &= y^{-1}x^{-1}z^{-1}xyz \\
&= y^{-1}x^{-1}z^{-1}x(zyy^{-1}z^{-1})yz \\
&= (y^{-1}\,[x, z]\,y)y^{-1}z^{-1}yz \\
&= [x, z]^{y}\,[y, z]\,.
\end{aligned}$$

Demonstrações dos itens (v) e (vi): Consideremos inicialmente o item (v), façamos indução sobre j, com $j \geqslant 0$. Quando $j = 0$ ou 1, o resultado já é verdadeiro. Note que se x comuta com $[x, y]$, então x^{-1} também comuta com $[x, y]$. Agora, consideremos que o resultado é válido para $j \in \mathbb{N}$, portanto

$$\begin{aligned}
[x, y]^{j+1} &= [x, y]^{j}\,[x, y] \\
&\overset{hip.}{=} x^{-1}\,[x, y]^{j}\,y^{-1}xy \\
&\overset{ind.}{=} x^{-1}\left[x^{j}, y\right]y^{-1}xy \\
&= x^{-1}x^{-j}y^{-1}x^{j}yy^{-1}xy \\
&= \left[x^{j+1}, y\right].
\end{aligned}$$

Por hipótese, $x\,[x, y] = [x, y]\,x$, assim $[y, x^{-1}] = [x, y]$, $[x, y]^{-1} = [x^{-1}, y]$ e x^{-1} comuta com $[x^{-1}, y]$. Com isso, para $j \leqslant 0$:

$$[x, y]^{j} = [x^{-1}, y]^{-j} = [x^{j}, y].$$

Para o item (vi):

$$[x, y]^{j} = ([x, y]^{-1})^{-j} = [y, x]^{-j} \overset{(iv)}{=} [y^{j}, x]^{-1} = [x, y^{j}].$$

Demonstração do item (vii): Podemos supor, sem perda de generalidade, que G não é abeliano, senão "$[.,.] \equiv 1$". Como $[x,y]^n \in Z(G)$, temos:

$$\begin{aligned}
[x,y]^{n+1} &= x^{-1}y^{-1}x\,[x,y]^n\,y \\
&= x^{-1}y^{-1}x(x^{-1}y^{-1}xy)\,[x,y]^{n-1}\,y \\
&= x^{-1}y^{-2}xy(yy^{-1})\,[x,y]^{n-1}\,y \\
&= x^{-1}y^{-2}xy^2([x,y]^{n-1})^y \\
&= \left[x,y^2\right][x^y,y]^{n-1}\,.
\end{aligned}$$

□

Proposição 2.1.1 *Seja G um grupo. Então*

(i) $G' \lhd G$;

(ii) Se $N \lhd G$, então $G' \leqslant N$ se, e somente se, o grupo quociente G/N é abeliano. Em particular, G/G' é abeliano.

Demonstração do item (i): Temos $[x,y]^z = [x^z, y^z] \in G'$, para quaisquer $x, y, z \in G$. Mas G' é o subgrupo gerado pelos comutadores, daí $G' \lhd G$.

Demonstração do item (ii): Suponhamos que $G' \subseteq N$, consequentemente $[x,y] \in G' \subseteq N$, para quaisquer $x, y \in G$. Assim, $[x,y]\,N = N$, i.e., $xyN = xNyN = yNxN = yxN$ e G/N é abeliano. E tomando $N = G'$, obtemos que $G/G' = G/N$ é abeliano.

Reciprocamente, dados $x, y \in G$, por hipótese temos $xNyN = yNxN$. Portanto, $[x,y]\,N = N$, isto é, $[x,y] \in N$, para todos $x, y \in G$. Logo, $G' \subseteq N$.

Observação: Na Definição 2.1.1 temos que o subgrupo derivado é o subgrupo gerado pelos comutadores que é, em geral, diferente do conjunto dos comutadores (veja os Grupos de Guralnick - seção 2.2). Isso sugere a introdução das seguintes terminologias:

Definição 2.1.2 *(Elementos não comutadores e o Comprimento do Derivado) Seja G um grupo.*

1. *Dizemos que $g \in G$ é um elemento não comutador (ou simplesmente, não comutador), se $g \in G'$ e não existem $a, b \in G$ tais que $g = [a, b]$;*

2. *O menor inteiro positivo n tal que todos os elementos de G' podem ser escritos como o produto de n comutadores é o comprimento do derivado de G. O comprimento do derivado do grupo G será denotado por $\lambda(G)$.*

Inferências da Definição 2.1.2:

- Se G é um grupo finito, então "$\lambda(G) < \infty$". Basta observar que cada elemento do derivado é o produto de uma quantidade finita de comutadores e $|G'| \leqslant |G| < \infty$, daí $\lambda(G)$ (existe e) é finito.

- É equivalente afirmar que um grupo G possui elementos não comutadores e escrever $\lambda(G) > 1$. Quando G é um grupo infinito, pode ocorrer que não exista um menor inteiro positivo n para o qual todos os elementos do derivado sejam escritos como o produto de n comutadores. Se G é um grupo que tem comprimento derivado ilimitado, então adotaremos a seguinte notação: $\lambda(G) = \infty$. No Apêndice A, vamos mostrar que de fato existem grupos (infinitos) com comprimento derivado "infinito".

Para simplificar o enunciado dos nossos resultados adotaremos as seguintes notações:

- $\Gamma G = \{[x, y] \mid x, y \in G\}$.

- $K_n(G)$ o conjunto dos elementos (de G') que podem ser expressos como o produto de n comutadores. Note que $K_1(G) = \Gamma G$.

2.1.1 Exemplos de Grupos com $\lambda(G) = 1$

Nosso objetivo aqui será exibir alguns exemplos de grupos, não abelianos, cujo comprimento do derivado seja igual a 1 (grupos com $\lambda(G) = 1$ - abuso de notação).

Proposição 2.1.2 *Sejam G, H grupos. Se $\lambda(G) = 1 = \lambda(H)$, então*

$$\lambda(G \times H) = 1.$$

Demonstração: Temos $(G \times H)' = G' \times H'$. Consideremos $g \in G' = \Gamma G$ e $h \in H' = \Gamma H$, portanto, $g = [a, b]$ e $h = [c, d]$, onde $a, b \in G$ e $c, d \in H$. Finalmente, tomemos $(a, c), (b, d) \in G \times H$, cujo comutador é:

$$[(a, c), (b, d)] = \Big([a, b], [b, d]\Big) = (g, h) \in \Gamma(G \times H).$$

Logo, $\lambda(G \times H) = 1$.

□

Lema 2.1.2 *Seja G um grupo. Se $|G'| \leqslant 3$, então $\lambda(G) = 1$.*

Demonstração: Já podemos supor que $|G'| > 1$, senão G é abeliano (e $\lambda(G) = 1$). Agora consideremos as demais possibilidades: Caso $|G'| = 2$: Existem $a, b \in G$ tais que $[a, b] \neq 1$ (senão $G' = \{1\}$). Com isso, $G' = \{1, [a, b]\} = \Gamma G$. Assim, $\lambda(G) = 1$;

Caso $|G'| = 3$: Mais uma vez, temos assegurado a existência de elementos $a, b \in G$ tais que $[a, b] \neq 1$. Mas $\mathtt{o}([a, b]) = 3$, pois $|G'| = 3$ e $[a, b] \neq 1$. Assim, $[a, b]^{-1} \neq [a, b]$ e $G' = \{1, [a, b], [a, b]^{-1} = [b, a]\} = \Gamma G$. Logo, $\lambda(G) = 1$.

□

Proposição 2.1.3 *Sejam G um grupo e p um número primo. Se $|G'| = p$, então $\lambda(G) = 1$.*

Demonstração: No Lema 2.1.2 já mostramos os casos $p = 2$ e 3. Daí, podemos supor $p \geqslant 5$. Dividiremos a demonstração em dois casos:

Caso $G' \not\subseteq Z(G)$: Consideremos $1 \neq a \in G'$ e $b \in G$ tais que $ab \neq ba$. Daí, existe $1 \leqslant n \leqslant p - 2$ de modo que $[a, b] = a^n$, pois $a^{-1}b^{-1}ab = [a, b] \neq a^{p-1}$ e $ab \neq ba$. Portanto, $b^{-1}ab = a^{n+1}$.

Afirmação: $|\{[a^j, b] \mid 1 \leqslant j \leqslant p\}| = |G'| = p$ (i.e., $\Gamma G = G'$).

Demonstração da Afirmação: Tomemos $i, j \in \{1, \ldots, m\}$ com $i \leqslant j$ tais que $[a^j, b] = [a^i, b]$. Dessa forma,

$$\begin{aligned}
\left[a^j, b\right] \;=\; \left[a^i, b\right] \quad &\Rightarrow \quad a^{-j}b^{-1}a^jb \;=\; a^{-i}b^{-1}a^ib \\
&\Rightarrow \quad (b^{-1}ab)^j \;=\; a^{j-i}(b^{-1}ab)^i \\
&\overset{a^b = a^{n+1}}{\Rightarrow} \quad a^{(n+1)j} \;=\; a^{j-i}a^{(n+1)i} \\
&\Rightarrow \quad a^{n(j-i)} \;=\; 1.
\end{aligned}$$

Temos $\mathsf{o}(a) = p$ (primo), portanto $p \mid n$ ou $p \mid j - i$. Mas $p \nmid n$, pois $1 \leqslant n \leqslant p-2$. Daí, $p \mid j-i$ e como $0 \leqslant j-i \leqslant p-1$, obtemos $i = j$. Assim, $\lambda(G) = 1$.

Caso $G' \subseteq Z(G)$: Temos que existe $c, d \in G$ tal que $[c,d] \neq 1$, senão $G' = 1$. Como $|G'| = p$ primo, $G' = \langle [c,d] \rangle \subseteq Z(G)$ e c comuta com $[c,d]$. Dessa forma, $[c^j, d] = [c,d]^j$. Assim,

$$G' = \{[c,d]^j = [c^j, d] \mid \ 1 \leqslant j \leqslant p\} = \Gamma G.$$

Logo, $\lambda(G) = 1$.

□

Observação 2.1.1

- *Em 1982, Guralnick [10] demonstrou um resultado bem mais geral do que o exposto acima, que é: "Sejam G um grupo e $p_1, \ldots, p_k$ os primos que comparecem na fatoração de $|G|$. Se $|G'| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ e $\alpha_1 + \ldots + \alpha_k \leqslant 3$, então $\lambda(G) = 1$".*

- *A proposição acima nos dá uma condição suficiente para que um grupo não possua elementos não comutadores. Entretanto, tal condição não é necessária como veremos na proposição a seguir.*

Proposição 2.1.4 *Sejam $n \geqslant 3$ e $D_n = \langle \sigma, \tau \mid \sigma^n = 1 = \tau^2$ e $\tau\sigma\tau = \sigma^{-1} \rangle$ ($\simeq C_n \rtimes C_2$). Então, $\lambda(D_n) = 1$.*

Demonstração: Temos $D_n' \subseteq \langle \sigma \rangle$ e $D_n = \langle \sigma \rangle \langle \tau \rangle$, pois $\langle \sigma \rangle \overset{2}{\lhd} D_n$. Dados $a, b \in D_n$ (portanto, $a = \sigma^i \tau^r$ e $b = \sigma^j \tau^s$) temos a seguinte expressão para o

comutador de a e b:

$$\begin{aligned}
\textbf{(I)} \quad [a,b] &= \left[\sigma^i\tau^r, \sigma^j\tau^s\right] \\
&= \tau^r\sigma^{-i}\tau^s\sigma^{-j}\sigma^i\tau^r\sigma^j\tau^s \\
&= \begin{cases} 1, & \text{se } r \text{ e } s \text{ são pares;} \\ \sigma^{-2i}, & \text{se } r \text{ é par e } s \text{ é ímpar;} \\ \sigma^{2j}, & \text{se } r \text{ é ímpar e } s \text{ é par;} \\ \sigma^{2j}, & \text{se } r \text{ e } s \text{ são ímpares.} \end{cases}
\end{aligned}$$

Dessa forma, $D'_n = \langle [a,b] \mid a,b \in D_n \rangle \subseteq \langle \sigma^2 \rangle$. Vamos analisar os seguintes casos:

- D_n, n **ímpar**: Por **(I)**, $\left[\tau, \sigma^{\frac{n+1}{2}}\right] = \sigma$. Portanto, $D'_n = \langle\sigma\rangle$. Por outro lado, dado $1 \leqslant j \leqslant n$:

  - Se j é par, então $\left[\tau, \sigma^{\frac{j}{2}}\right] = \sigma^j$;
  - Se j é ímpar, então $\left[\tau, \sigma^{\frac{j+n}{2}}\right] = \sigma^j$.

  Assim, $D'_n = \{\sigma^j \mid 1 \leqslant j \leqslant n\} = \Gamma D_n$ (isto é, $\lambda(D_n) = 1$).

- D_n, n **par**: Por **(I)**, $[\tau, \sigma^j] = \sigma^{2j}$, $1 \leqslant j \leqslant \frac{n}{2}$. Com isso, $\langle\sigma^2\rangle \subseteq D'_n$. Portanto, $D'_n = \langle\sigma^2\rangle = \{[\tau, \sigma^j] \mid 1 \leqslant j \leqslant \frac{n}{2}\}$ e $\lambda(D_n) = 1$.

- **Diedral Infinito** - D_∞: De modo análogo, vamos definir

$$D_\infty = \langle \sigma, \tau \mid \ \mathtt{o}(\sigma) = \infty,\ \mathtt{o}(\tau) = 2 \text{ e } \tau\sigma\tau = \sigma^{-1} \rangle.$$

  A expressão **(I)** continua válida para D_∞. Daí, para cada $j \in \mathbb{Z}$, temos $\sigma^{2j} = [\tau, \sigma^j]$ e $\langle\sigma^2\rangle \subseteq D'_\infty$. Daí, $D'_\infty = \langle\sigma^2\rangle = \{[\tau, \sigma^j] \mid j \in \mathbb{Z}\}$. Logo, $\lambda(D_\infty) = 1$.

2.1.2 Relações entre $\lambda(G)$ e $|G'|$

Nessa seção iremos estudar como, sob certas condições, $\lambda(G)$ interfere na finitude de G'. Mesmo que o comprimento do derivado de um grupo seja finito isso não garante que o subgrupo derivado seja finito (por exemplo, $\lambda(D_\infty) = 1$ e $|D_\infty| = \infty$).

Proposição 2.1.5 *Seja G um grupo com centro Z. Se $|G : Z| = n$, então*

(i) $|\Gamma G| \leqslant n^2$;

(ii) $\lambda(G) \leqslant n^3$;

(iii) *(Lema de Schur [1])* $|G'| \leqslant n^{2n^3} < \infty$.

Demonstração do item (i): Seja $\tau = \{t_1, \ldots, t_n\}$ um transversal de Z em G, ou seja, G se escreve como a união disjunta das classes laterais t_iZ 's (G $= \bigcup_{i=1}^{n} t_iZ$). Com isso, dados $x, y \in G$, existem $z_1, z_2 \in Z$ e $i, j \in \{1, \ldots, n\}$ tais que $x = t_iz_1$ e $y = t_jz_2$. Portanto, $[x, y] = [t_iz_1, t_jz_2] = [t_i, t_j]$. Como os elementos $x, y \in G$ são arbitrários, temos:

$\Gamma G = \{[x, y] \mid x, y \in G\} = \{[t_i, t_j] \mid 1 \leqslant i, j \leqslant n\}$. Logo, $|\Gamma G| \leqslant n^2$.

Demonstração do item (ii): Mostraremos que para cada elemento do derivado pode ser escrito como o produto de n^3 comutadores. Sem perda de generalidade podemos supor que $\lambda(G) > 1$, senão o resultado seria direto. Com isso, podemos escolher um $u \in G'$ tal que $m = min\{t \in \mathbb{N} \mid u \in K_t(G)\} > 1$. Daí, existem $x_1, \ldots, x_m, y_1, \ldots, y_m \in G$ tais que

$$u = \prod_{j=1}^{m} c_j \tag{2.1}$$

[1] Na sua versão completa teríamos também $exp(G) \mid n$.

onde $c_j = [x_j, y_j]$. Para cada $i \in \{1, \ldots, m\}$, $C_i := \{i \mid c_j = c_i\}$.

Afirmação: $|C_j| \leqslant n$, $1 \leqslant j \leqslant m$.

Demonstração da Afirmação: Suponhamos que existe $j \in \{1, \ldots, m\}$ tal que $|C_j| > n$, i.e., $c_j = [x_j, y_j]$ comparece mais que n vezes na fatoração de u dada acima. Como $G' \lhd G$, podemos reescrever $u = [x_j, y_j]^{n+1} c'_{n+2} \ldots c'_m$, onde cada c'_k é um conjugado de algum comutador de (2.1), portanto cada c'_k, em questão, é ainda um comutador. Assim, pelo Lema 2.1.1, temos

$$u = [x_j, y_j]^{n+1} c'_{n+2} \ldots c'_m \overset{(vi)}{=} [x_j, y_j^2][x_j^{y_j}, y_j]^{n-1} c'_{n+2} \ldots c'_m$$

Portanto, $u \in K_{m-1}(G)$ o que contradiz a minimalidade de m. Com isso mostramos a afirmação.

Voltando à demonstração do item (ii): Dado $u \in G'$ e $m = min\{t \in \mathbb{N} \mid u \in K_t(G)\}$, temos:

$$u = \prod_{j=1}^{m} [x_j, y_j], \text{ onde } x_j, y_j \in G.$$

Do item (i), sabemos que $|\Gamma G| \leqslant n^2$ e pela Afirmação mostrada acima cada comutador ($[x_j, y_j]$) "não pode comparecer"mais que n vezes nessa fatoração. Daí, $m \leqslant n^3$. Como $u \in G'$ é arbitrário, temos que $min\{t \in \mathbb{N} \mid u \in K_t(G)\} \leqslant n^3$, para todo $u \in G'$. Logo, $\lambda(G) \leqslant n^3$.

Demonstração do item (iii): Estimaremos (superiormente) o número de elementos do derivado, para isso observemos que qualquer elemento de G' pode ser escrito como o produto de, no máximo, n^3 comutadores ($\lambda(G) \leqslant n^3$), por outro lado o número de comutadores de G é finito (mais precisamente, $|\Gamma G| \leqslant n^2$). Daí, G' é finito e mais podemos limitar sua ordem da seguinte forma:

$$|G'| \leqslant \underbrace{n^2 \cdot n^2 \cdot \ldots \cdot n^2}_{n^3 \text{ vezes}} = n^{2n^3}.$$

Observação 2.1.2 *Seja G um grupo finito e não abeliano. No Capítulo 3, estudaremos como, sob certos aspectos, $\lambda(G)$ interfere na estrutura de G e, reciprocamente, como a estrutura do grupo (por exemplo, os graus dos caracteres irredutíveis de G) limitam a ordem de G' e o comprimento do derivado de G. Tal análise permitirá estudar a razão $\frac{\lambda(G)}{|G|}$, obtendo estimativas de natureza global ("estimativa de Bardakov") e assintótica (isto é, quando $|G| \to \infty$).*

2.2 Grupos de Guralnick

Nesta seção, que é baseada em Guralnick [9], apresentaremos uma família de grupos finitos, cujo comprimento do derivado é maior que 1. Além de "justificar"a definição de elementos não comutadores, esses exemplos tem importância teórica, pois o exemplo de menor ordem obtido é minimal entre os grupos com $G' \neq \Gamma G$, tal grupo tem ordem 96 (veja Guralnick [9]).

Lema 2.2.1 *Sejam G um grupo com subgrupo H tal que $G' \subseteq H$ e $G = \langle H, x\rangle$. Se w é um comutador de G, então $w = [x^j a, b]$ para algum $j \in \mathbb{Z}$ e $a, b \in H$.*

Demonstração: Temos $G = \langle H, x\rangle = \langle x\rangle H$, pois $H \lhd G$ e podemos escrever cada $g \in G$ como $g = x^m h$, onde $h \in H$ e $m \in \mathbb{Z}$. Daí, os comutadores de G são da forma $w = [g_1, g_2]$, onde $g_1 = x^s h_1$ e $g_2 = x^t h_2$. Caso $t = 0$, estamos com o comutador na forma desejada e para $s = 0$, pelo Lema 2.1.1, reescrevemos w como:

$$[h_1, x^t h_2] \overset{(iii)}{=} \left[\left(x^t h_2\right) h_1, x^t h_2\right] \overset{(ii)}{=} \left[x^t h_2 h_1, \left(x^t h_2 h_1\right)^{-1} x^t h_2\right] = \left[x^t h_3, h_1^{-1}\right]$$

o qual está na forma pedida. A conclusão da prova segue por indução sobre $k = min\{|s|, |t|\}$. Já temos a base de indução, pois o caso $k = 0$ já foi verificado acima. Consideremos $w = [x^s h_1, x^t h_2]$, com $k > 0$ e, suponhamos que o resultado é válido para todos os $0 \leqslant k' < k$. Podemos supor $|s| \geqslant |t|$ (o caso, $|t| > |s|$ é inteiramente análogo), pelo Algoritmo da Divisão, $s = tq + r$, com $0 \leqslant r < |t|$. Daí, vamos reescrever o comutador da seguinte forma:

$$w = [x^s h_1, x^t h_2] \overset{(iii)}{=} \left[\left(x^t h_2\right)^{-q} x^s h_1, x^t h_2\right] \overset{H \lhd G}{=} [x^{s-qt} h_3, x^t h_2].$$

Mas $k' = min\{|s - qt|, |t|\} < k = min\{|s|, |t|\}$. E por indução, temos que existe $\tilde{h}_1, \tilde{h}_2 \in H$ e $j \in \mathbb{Z}$ tal que $w = \left[x^j \tilde{h}_1, \tilde{h}_2\right]$. Com isso os comutadores do grupo G podem ser reescritos na forma desejada.

□

Agora consideremos um grupo G_1 ($\simeq Q_8 \rtimes C_3$) com a seguinte apresentação:

$$\left\langle a,\ b,\ x,\ \mid a^4 = b^4 = x^3 = 1,\ a^{x^{-1}} = b,\ b^{x^{-1}} = ab,\ a^2 = b^2,\ b^{a^{-1}} = b^{-1} \right\rangle.$$

Chamemos $H_1 = \langle a, b \rangle$, daí $H_1 \simeq Q_8$. Temos que $G_1' \simeq H_1$.

- "$\subseteq$": Como $H_1 \overset{3}{\lhd} G_1$, $G_1' \subseteq H_1$;
- "$\supseteq$": Temos que $xax^{-1} = b$ e $xbx^{-1} = ab$. Portanto, $a = [x^{-1}, b^{-1}]$, $ba^{-1} = [x^{-1}, a^{-1}] \in G_1'$. Assim, $\langle a, b^{-1} \rangle \subseteq G_1'$. Logo, $G_1' = H_1$.

Lema 2.2.2 *Se $u, v \in H_1$ e $[x^j u, v] = a^2$, então $3 \mid j$.*

Demonstração: Se $3 \nmid j$, então $\mathtt{o}([x^j, v]) = 4$ ou $v = a^2$. Temos que $[x^j, v] \in H_1 \simeq Q_8$, portanto, $\mathtt{o}([x^j, v]) = 1, 2$ ou 4. Como $3 \nmid j$ e $\mathtt{o}(x) = 3$ é suficiente considerar os expoentes $j = 1, 2$.

Suponhamos que $\mathtt{o}([x^j, v]) < 4$ (portanto, $\mathtt{o}([x^j, v]) = 1$ ou 2), vamos mostrar que devemos ter $v \in \langle a^2 \rangle$. A demonstração do Lema será dividida em alguns casos:

Caso $j = 1$ e $\mathtt{o}([x, v]) = 1$: Teremos $xv = vx$, daí

- se $v = a^i$ (para algum $0 \leqslant i \leqslant 3$), então

$$\begin{aligned} xa^i = a^i x &\Rightarrow xa^i x^{-1} = a^i \\ &\Rightarrow b^i = a^i \\ &\Rightarrow v \in \left\langle a^2 \right\rangle \end{aligned}$$

- se $v = a^i b$ (para algum $0 \leqslant i \leqslant 3$), então

$$\begin{aligned} xa^i b = a^i bx &\Rightarrow xa^i bx^{-1} = a^i b \\ &\Rightarrow b^i ab = a^i b \\ &\Rightarrow b^i = a^{i-1}. \end{aligned}$$

Absurdo, pois $a^i = b^j \in \langle a^2 \rangle$, então i, j são pares e $i \equiv j \pmod 4$.

Caso $j = 1$ e $\mathtt{o}([x, v]) = 2$: Como $[x, v] \in H_1$ tem ordem 2, obtemos $[x, v] = a^2$. Daí,

- Se $v = a^i$ (para algum $0 \leqslant i \leqslant 3$), então

$$\begin{aligned} x^{-1}a^{-i}xa^i = a^2 &\Rightarrow a^{-i}xa^i x^{-1} = xa^2 x^{-1} = a^2 \\ &\Rightarrow a^{-i}b^i = a^2 \\ &\Rightarrow b^i = a^{i+2}. \end{aligned}$$

Absurdo, pois $i \not\equiv i + 2 \pmod 4$.

- Se $v = a^i b$ (para algum $0 \leqslant i \leqslant 3$), então

$$\begin{aligned} x^{-1}b^{-1}a^{-i}xa^ib = a^2 &\Rightarrow b^{-1}a^{-i}xa^ibx^{-1} = xa^2x^{-1} = a^2 \\ &\Rightarrow b^{-1}a^{-i}b^iab = a^2 \\ &\Rightarrow a^{-i}b^ia = a^2 \\ &\Rightarrow b^i = a^{i+1}. \end{aligned}$$

Absurdo, pois $i \not\equiv i+1 \pmod 4$.

Os demais casos, $j = 2$ e $\mathtt{o}([x, v]) = 1$ ou 2, a verificação é análoga.

Se $\mathtt{o}([x^j, v]) = 4$, então $a^2 = [x^j u, v] = u\,[x^j, v]\,u^{-1}\,[u, v] = [x^j, v]\,[u, v]$ (lembre que $H_1' = Z(H_1)$). Por outro lado, $\mathtt{o}([x^j, v]) = \mathtt{o}([u, v])\mathtt{o}([x^j, v]) = 4$. Absurdo, pois $[x^j, v] = a^2$ que tem ordem 2.

Assim, $v \in \langle a^2 \rangle$. Portanto, $[ux^j, a^2] = a^2$ o que nos garante que $a = 1$. Absurdo, logo $j \equiv 0 \pmod 3$.

□

Construção dos Grupos de Guralnick: Sejam G_1 o grupo descrito acima e G_2 um grupo não abeliano que tenha um subgrupo normal abeliano H_2 de índice 3 (portanto, $G_2' \subseteq H_2$). Dado $y \in G_2 \setminus H_2$, temos $G_2 = H_2\,\langle y \rangle$. Finalmente, consideremos o grupo dado por $G = \langle H_1 \times H_2, (x, y) \rangle = (H_1 \times H_2)\,\langle (x, y) \rangle$, pois $G' \subseteq G_1' \times G_2' \subseteq H_1 \times H_2$.

Teorema 2.2.1 *(a)* $G' = G_1' \times G_2'$;

(b) $|G| = 24|H_2|$;

(c) $\lambda(G) > 1$.

Demonstração do Item (a): Temos $G' \subseteq G'_1 \times G'_2$, pois $G \leqslant G_1 \times G_2$. Por outro lado, dado $\gamma_1 \in \Gamma G_1$ (pelo Lema 2.2.1, podemos escrever $\gamma_1 = [x^m h, h_1]$, onde $h, h_1 \in H_1$ e $m \in \mathbb{Z}$). Dessa forma,

$$(\gamma_1, 1_{G_2}) = [(x^m h, y^m), (h_1, 1)] \in G'.$$

De modo análogo, dado $\gamma_2 \in \Gamma G'_2$ temos $(1_{G_1}, \gamma_2) \in G'$. Assim,

$$G'_1 \times G'_2 \;=\; \langle\, (\gamma_1, 1_{G_2}), (1_{G_1}, \gamma_2) \mid \gamma_i \in \Gamma G_i, i = 1, 2 \rangle \;\subseteq\; G'.$$

Logo, $G' = G'_1 \times G'_2$.

Demonstração do Item (b): Como $y \notin H_2$ e $H_2 \overset{3}{\lhd} G_2$, temos que $y^3 \in H_2$. Com isso, $(H_1 \times H_2) \cap \langle (x, y) \rangle = \langle (x, y)^3 \rangle = \langle (1, y^3) \rangle$ e $|\, \langle (x, y) \rangle : \langle (1, y^3) \rangle \,| = 3$. Portanto,

$$|G| = \frac{|H_1 \times H_2|\,|\, \langle (x, y) \rangle \,|}{|(H_1 \times H_2) \cap \langle (x, y) \rangle \,|} = \frac{8|H_2|\,|\, \langle (x, y) \rangle \,|}{|\, \langle (1, y^3) \rangle \,|} = 24|H_2|.$$

Demonstração do item (c): Tomemos $c \in G'_2 \setminus \{1\}$ (G_2 foi escolhido não abeliano) e $w = (a^2, c)$. Mostraremos que $w \notin \Gamma G$. Suponhamos que w é um comutador e consideremos $H = H_1 \times H_2$, daí $G = \langle H, (x, y) \rangle = H\, \langle (x, y) \rangle$. Pelo Lema 2.2.1: existem (h_1, h_2), $(h_1, h_2) \in H$ e $j \in \mathbb{Z}$ tais que

$$(a^2, c) = [(x^j, y^j)(h_1, h_2), (k_1, k_2)], \text{ i.e., } a^2 = [x^j h_1, k_1] \text{ e } c = [y^j h_2, k_2].$$

Pelo Lema 2.2.2, temos que $3 \mid j$. Como $\mathtt{o}(x) = 3$ e $|G_2 : H_2| = 3$, temos que $a^2 = [h_1, k_1]$ e $y^j \in H_2$. Portanto, $c = [h_2 y^j, k_2] \in H'_2 = \{1\}$. Absurdo, pois $c \neq 1$.

Conclusão: Seja dado G_2 um grupo não abeliano com subgrupo normal abeliano H_2 de índice 3, pelo processo descrito acima, temos associado um grupo G de ordem $24|H_2|$, com $\lambda(G) > 1$ e $G' \simeq Q_8 \times G_2'$. Vejamos alguns exemplos:

Exemplo 2.2.1

(i) *(Exemplo Minimal - Guralnick [10]) Façamos* $G_2 = A_4$. *Como* $A_4' = V \overset{3}{\lhd} A_4$, *onde* V *é o grupo de Klein. Obtemos um grupo* G *com ordem* 96, $G' \simeq Q_8 \times V$ *e* $G' \neq \Gamma G$.

(ii) *Tomemos* G_2 *um* 3 *- grupo não abeliano de ordem* 27 *e* $H_2 \overset{3}{\lhd} G_2$, *onde* $|H_2| = 9$. *Note que,* $|G_2'| = 3$, *pois* G_2 *não é abeliano. Portanto, temos associado um grupo* G *de ordem* 216, $G' \simeq Q_8 \times C_3$ *e* $\lambda(G) > 1$.

(iii) *Sejam* C_3 *um grupo cíclico de ordem* 3, N *um grupo com ordem* p, p *primo e* $p \equiv 1$ *(mod* 3*). Dessa forma, podemos definir o produto semidireto de* N *por* C_3, $G_2 = N \rtimes C_3$. *Portanto,* G_2 *é um grupo não abeliano com subgrupo normal abeliano* H_2 $(\simeq N)$ *de índice* 3. *Daí, temos associado um grupo* G *de ordem* $24p$, $G' \simeq Q_8 \times N$ *e* $\lambda(G) \neq 1$.

2.3 Critério de Burnside - Gallagher

Apresentaremos um critério devido a P.X. Gallagher [7] para decidir quando $g \in G' \setminus K_n(G)$, o qual é uma generalização de um problema proposto por W. Burnside em [2]. Tal critério será de suma importância para o desenvolvimento do próximo capítulo, pois relaciona a existência de elementos

não comutadores com os caracteres irredutíveis do grupo. Para isso, motivaremos nosso estudo pela seguinte pergunta: "dado $n \in \mathbb{N}$, de quantas maneiras podemos escrever um dado elemento de G como o produto de n comutadores".

Definição 2.3.1 *Sejam $\sigma \in G$ e $n \in \mathbb{N}$. Chamemos:*

1. $C_n(\sigma) = \left\{ \big((a_1, b_1), \ldots, (a_n, b_n)\big) \mid \ (a_i, b_i) \in G \times G \text{ e } \sigma = \prod_{i=1}^{n} [a_i, b_i] \right\}$;
2. *Consideremos a função ϕ_n de G em $\mathbb{C}$, dado por $\phi_n(\sigma) = |C_n(\sigma)|$. A grosso modo, $\phi_n(\sigma)$ "conta"o número de maneiras distintas que σ pode ser escrito como o produto de n comutadores.*

Fato: Se $g \notin K_n(G)$, então $C_n(\sigma) = \emptyset$ e $\phi_n(\sigma) = 0$.

Lema 2.3.1 *A função ϕ_n admite a seguinte expressão "indutiva":*

$$\phi_{n+1}(\sigma) = \sum_{\tau} \phi_n(\sigma\tau^{-1})\phi_1(\tau).$$

Demonstração: Seja $\sigma \in G$. Então, $C_n(\sigma\tau^{-1}) \times C_1(\tau) \subseteq C_{n+1}(\sigma)$ para cada $\tau \in G$ (abuso de notação). Portanto,

$$\bigcup_{\tau \in G} C_n(\sigma\tau^{-1}) \times C_1(\tau) \subseteq C_{n+1}(\sigma). \tag{2.2}$$

Observe que, se $\tau, \tau_1 \in G$ são distintos, então $C_1(\tau) \cap C_1(\tau_1) = \emptyset = C_n(\sigma\tau^{-1}) \cap C_n(\sigma\tau_1^{-1})$. Basta observar que, se $C_1(\tau) \cap C_1(\tau_1) \neq \emptyset$ ou $C_n(\sigma\tau^{-1}) \cap C_n(\sigma\tau_1^{-1}) \neq \emptyset$, então existiriam $(a, b) \in C_1(\tau) \cap C_1(\tau_1)$ ou $\big((a_i, b_i)\big)_{i=1}^{n} \in C_n(\sigma\tau^{-1}) \cap C_n(\sigma\tau_1^{-1})$ tais que

- $\tau = [a, b] = \tau_1$;

- $\sigma\tau^{-1} = \prod_{i=1}^{n} [a_i, b_i] = \sigma\tau_1^{-1}$.

Em ambos os casos, teríamos $\tau = \tau_1$. Absurdo. Portanto, a união (2.2) é disjunta.

Agora dado $\Big((a_i, b_i)\Big)_{i=1}^{n+1} \in C_{n+1}(\sigma)$, chamemos $\tau = [a_{n+1}, b_{n+1}]$ e obtemos $\Big((a_i, b_i)\Big)_{i=1}^{n} \in C_n(\sigma\tau^{-1})$ e $\tau = [a_{n+1}, b_{n+1}]$. Dessa forma, $\Big((a_1, b_1), \ldots, (a_{n+1}, b_{n+1})\Big) \in C_n(\sigma\tau^{-1}) \times C_1(\tau)$ (abuso de notação). Com isso,

$$\bigcup_{\tau \in G} C_n(\sigma\tau^{-1}) \times C_1(\tau) = C_{n+1}(\sigma)$$

Portanto,

$$\begin{aligned} \phi_{n+1}(\sigma) = |C_{n+1}(\sigma)| &= |\dot{\bigcup_{\tau \in G}} C_n(\sigma\tau^{-1}) \times C_1(\tau)| \\ &= \sum_{\tau \in G} |C_n(\sigma\tau^{-1})||C_1(\tau)| \\ &= \sum_{\tau \in G} \phi_n(\sigma\tau^{-1})\phi_1(\tau). \end{aligned}$$

□

Teorema 2.3.1 *(Critério de Burnside - Gallagher) Sejam G um grupo e $g \in G' \setminus K_n(G)$. Então,*

$$\sum_{\chi \in Irr(G)} \frac{1}{\chi(1)^{2k-1}} \chi(g) = 0, \text{ para todo } 0 \leqslant k \leqslant n.$$

Demonstração: Dado χ um caracter irredutível de G, já definimos

$$d_\chi = \frac{1}{|G|^2} \sum_{\sigma_1, \sigma_2 \in G} \bar{\chi}([\sigma_1, \sigma_2]).$$

Temos que ϕ_1 é uma função de classe sobre G e como tal pode ser escrita como combinação linear dos caracteres irredutíveis de G, isto é,

$$\phi_1 = \sum_{\chi \in Irr(G)} c_\chi \ \chi, \text{ onde } c_\chi = \langle \chi, \phi_1 \rangle_G.$$

E mais, podemos reescrever c_χ da seguinte forma:

$$c_\chi \ = \ \frac{1}{|G|} \sum_{x \in G} \bar{\chi}(x)\phi_1(x) \ = \ \frac{1}{|G|} \sum_{\sigma_1, \sigma_2 \in G} \bar{\chi}([\sigma_1, \sigma_2]) \ = \ |G| d_\chi.$$

Portanto, $\phi_1(\sigma) = |G| \sum_{\chi \in Irr(G)} d_\chi \ \chi(\sigma)$.

Afirmação: Seja $n \in \mathbb{N}$. Então,

$$\phi_n(\sigma) = |G|^{2n-1} \sum_{\chi \in Irr(G)} \left(\frac{d_\chi}{f_\chi}\right)^n f_\chi \ \chi(\sigma).$$

Demonstração da Afirmação: Façamos indução sobre n. A base de indução no Lema 2.3.1. Agora, suponhamos que o resultado é válido para um $n \in \mathbb{N}$. Assim,

$$\phi_{n+1}(\sigma) = \sum_\tau \phi_n(\sigma\tau^{-1})\phi_1(\tau)$$

.

Daí,

$$\begin{aligned}
\phi_{n+1}(\sigma) &= \sum_{\tau} \phi_n(\sigma\tau^{-1})\phi_1(\tau) \\
&\overset{Hip.}{=} \sum_{\tau}\left(|G|^{2n-1}\sum_{\chi}\left(\frac{d_\chi}{f_\chi}\right)^n f_\chi\ \chi(\sigma\tau^{-1})\right)\phi_1(\tau) \\
&= \sum_{\tau}\left(|G|^{2n-1}\sum_{\chi}\left(\frac{d_\chi}{f_\chi}\right)^n f_\chi\ \chi(\sigma\tau^{-1})\right)\left(|G|\sum_{\chi} d_\chi\ \chi(\tau)\right) \\
&= \sum_{\tau}|G|^{2n}\left(\sum_{\chi,\chi'}\left(\frac{d_\chi}{f_\chi}\right)^n f_\chi d_{\chi'}\ \chi(\sigma\tau^{-1})\chi'(\tau)\right) \\
&= |G|^{2n}\left(\sum_{\tau}\sum_{\chi,\chi'}\left(\frac{d_\chi}{f_\chi}\right)^n f_\chi d_{\chi'}\ \chi(\sigma\tau^{-1})\chi'(\tau)\right) \\
&= |G|^{2n}\sum_{\chi,\chi'}\left(\frac{d_\chi}{f_\chi}\right)^n f_\chi d_{\chi'}\left(\sum_{\tau}\chi(\sigma\tau^{-1})\chi'(\tau)\right) \\
&= |G|^{2n}\sum_{\chi}\left(\frac{d_\chi}{f_\chi}\right)^n f_\chi d_\chi\left(\frac{|G|}{f_\chi}\chi(\sigma)\right), \text{ pelo Teorema 1.2.3 (a)} \\
&= |G|^{2n+1}\sum_{\chi}\left(\frac{d_\chi}{f_\chi}\right)^{n+1} f_\chi\ \chi(\sigma).
\end{aligned}$$

Com isso mostramos que a afirmação é verdadeira. E voltemos à demonstração do Teorema. Consideremos $\sigma \notin K_n(G)$, daí,

- $\phi_m(\sigma) = 0$ para $1 \leqslant m \leqslant n$.
- Pela Proposição 1.1.5,

$$\sum_{\chi\in Irr(G)} f_\chi\ \chi(\sigma) = 0,$$

pois $\sigma \neq 1$ (lembre que $\sigma \notin K_n(G)$).

Conclusão: Para $\sigma \notin K_n(G)$ temos

$$\sum_{\chi \in Irr(G)} \left(\frac{d_\chi}{f_\chi}\right)^m f_\chi \ \chi(\sigma) \ = \ 0, \text{ para } 0 \leqslant m \leqslant n \tag{2.3}$$

Do Corolário 1.2.2, sabemos que $d_\chi = f_\chi^{-1}$. Com isso,

$$\sum_{\chi \in Irr(G)} \frac{1}{\chi(1)^{2m-1}} \chi(g) \ = \ \sum_{\chi \in Irr(G)} \left(\frac{d_\chi}{f_\chi}\right)^m f_\chi \ \chi(\sigma) = 0, \text{ para } 0 \leqslant m \leqslant n.$$

□

Capítulo 3

Conjectura de Bardakov

Nesse mostraremos que o problema formulado por Bardakov em [13] é verdadeiro, e mais melhoraremos sua estimativa para grupos de ordem maior que 1000 e estudaremos o comportamento de $\lambda(G)$ quando $|G| \to \infty$ (comportamento assintótico de $\lambda(G)$). Aqui salvo menção em contrário, todos os grupos considerados são finitos e não abelianos. Com isso, dado um grupo G fixaremos as seguintes notações:

$$c.d.(G) = \{1 = f_0 < f_1 < \ldots < f_r\} \text{ e } \lambda_i = \frac{1}{f_i^2},\ i = 0, \ldots, r.$$

3.1 Estimativas para $\lambda(G)$

Nessa seção vamos verificar que o comprimento do derivado e a quantidade de graus de caracteres irredutíveis do grupo estão relacionados, da seguinte maneira: $\lambda(G) < |c.d.(G)|$.

Teorema 3.1.1 *Sejam G um grupo e $1 \leqslant n \leqslant r$. Se $p(x)$ é um polinômio com coeficientes em $\mathbb{C}$ de grau n e*

$$m_p := \min_{1 \leqslant i \leqslant r} \left\{ \left| \frac{p(1)}{p(\lambda_i)} \right| \right\} \geqslant |G'|,$$

então $\lambda(G) \leqslant n$.

Demonstração: Suponhamos que a afirmação acima não é válida e tomemos o menor inteiro positivo n onde o resultado não vale. Daí, existem $p(x) \in \mathbb{C}[x]$, com $\partial p = n$, $m_p \geqslant |G'|$ e $\lambda(G) > n$. Mais ainda, existe um elemento não comutador g que não pertence a $K_n(G)$ e, pelo Critério de Burnside - Gallagher,

$$\sum_{\chi \in \ Irr(G)} \frac{1}{\chi(1)^{2m-1}} \chi(g) = 0, \text{para } 0 \leqslant m \leqslant n. \tag{3.1}$$

Para cada $i \in \{0, \ldots, r\}$, chamemos

$$a_i = \frac{|G'|}{|G|} \sum_{\substack{\chi \in \ Irr(G) \\ \chi(1) = f_i}} \chi(1)\chi(g).$$

Temos que $a_0 = 1$: Como χ é um caracter linear, pela Proposição 1.2.2, $G' \leqslant Ker\ \chi = \{g \in G \mid \chi(g) = \chi(1) = 1\}$ e, pelo Teorema 1.2.2, o número de caracteres lineares de G é igual ao índice de G' em G. Assim,

$$a_0 \ = \ \frac{|G'|}{|G|} \sum_{\substack{\chi \in \ Irr(G) \\ \chi(1) = f_0}} \chi(1)\chi(g) \ = \ \frac{|G'|}{|G|} \sum_{\substack{\chi \in \ Irr(G) \\ \chi(1) = 1}} 1 \ = \ \frac{|G'|}{|G|} |G : G'| \ = \ 1.$$

Para cada $0 \leqslant m \leqslant n$, podemos reescrever (3.1):

$$0 = \frac{|G'|}{|G|} \sum_{\chi \in \ Irr(G)} \frac{1}{\chi(1)^{2m-1}} \chi(g) = \sum_{i=0}^{r} \lambda_i^m \frac{|G'|}{|G|} \sum_{\substack{\chi \in \ Irr(G) \\ \chi(1) = f_i}} \chi(1)\chi(g) = \sum_{i=0}^{r} \lambda_i^m a_i.$$

Observação 3.1.1 *Dado* $q(x) = \beta_0 + \beta_1 x + \ldots + \beta_s x^s \in \mathbb{C}[x]$ *com* $s = \partial q \leqslant n$. *Obtemos:*

$$\sum_{i=0}^{r} a_i q(\lambda_i) = \sum_{i=0}^{r} a_i(\beta_0 + \beta_1\lambda_i + \ldots + \beta_s\lambda_i^s) = \sum_{j=0}^{s}(\beta_j \sum_{i=0}^{r} a_i\lambda_i^j) = 0,$$

pois $\sum_{i=0}^{r} a_i\lambda_i^m = 0$ para cada $0 \leqslant m \leqslant n$.

Afirmação: $\partial p = n < r$.

Demonstração da Afirmação: Suponhamos que $n \geqslant r$ e tomemos $q(x) = \prod_{j=1}^{r}(x - \lambda_j)$. Dessa forma, os números $\lambda_1, \ldots, \lambda_r$ são raízes distintas do polinômio $q(x)$, onde $\lambda_r < \ldots < \lambda_1 < 1$ e como $\partial q = n$, teremos $q(1) = q(\lambda_0) \neq 0$. Daí,

$$0 = \sum_{i=0}^{r} a_i q(\lambda_i) = a_0 q(1) + \sum_{i=1}^{r} a_i q(\lambda_i) = a_0 q_1 = q(1) \neq 0.$$

Absurdo. Logo $n < r$.

Conclusões da Afirmação: Temos $\partial p = n < r$ e $M_p := \max_{1 \leqslant j \leqslant r}\{|p(\lambda_i)|\} > 0$, pois p tem no máximo n raízes. Mais ainda,

$$\left|\sum_{i=1}^{r} a_i p(\lambda_i)\right| = \left|\sum_{i=0}^{r} a_i p(\lambda_i) - a_0 p(1)\right| = |p(1)|$$

e, consequentemente,

$$|p(1)| \leqslant \sum_{i=1}^{r} |a_i p(\lambda_i)|. \tag{3.2}$$

Voltando à demonstração do Teorema: Pela Proposição 1.1.3, item (c), temos $|\chi(g)| \leqslant \chi(1)$. Com isso,

$$\sum_{\chi \in\ Irr(G)} |\chi(1)\chi(g)| \leqslant \sum_{\chi \in\ Irr(G)} \chi(1)^2$$

e mais pelo Teorema B.0.4 B, temos que $\sum_{\chi\in\ Irr(G)} \chi(1)^2 = |G|$.

Portanto,

$$\begin{aligned}
\sum_{\substack{\chi\in\ Irr(G)\\ \chi(1)>1}} |\chi(1)\chi(g)| &= \sum_{\chi\in\ Irr(G)} |\chi(1)\chi(g)| - \sum_{\substack{\chi\in\ Irr(G)\\ \chi(1)=1}} |\chi(1)\chi(g)| \\
&\leqslant \sum_{\chi\in\ Irr(G)} \chi(1)^2 - \sum_{\substack{\chi\in\ Irr(G)\\ \chi(1)=1}} |\chi(1)\chi(g)| \\
&= |G| - |G:G'| \\
&= |G:G'|(|G'|-1) \\
&< |G:G'|\ m_p.
\end{aligned}$$

Por outro lado, $|a_i| \leqslant \dfrac{|G'|}{|G|} \sum_{\substack{\chi\in Irr(G)\\ \chi(1)=f_i}} |\chi(1)\chi(g)|$, onde $1 \leqslant i \leqslant r$. Dessa forma,

$$\begin{aligned}
\sum_{\substack{\chi\in\ Irr(G)\\ \chi(1)>1}} |\chi(1)\chi(g)| &\geqslant |G:G'| \sum_{i=1}^{r} |a_i| \\
&\geqslant |G:G'| \sum_{i=1}^{r} \Big|\frac{a_i p(\lambda_i)}{M_p}\Big| \\
&\geqslant |G:G'| \sum_{i=1}^{r} \Big|\frac{p(1)}{M_p}\Big|, \text{ por (3.2)} \\
&= |G:G'|\ m_p
\end{aligned}$$

Absurdo. Logo, $\lambda(G) \leqslant n$.

□

O resultado a seguir nos dá uma relação entre as "propriedades" dos caracteres e os elementos do subgrupo derivado. Mais especificamente, obtemos que o comprimento do derivado é limitado superiormente pelo número de graus de caracteres irredutíveis do grupo.

Corolário 3.1.1 (Limitação para $\lambda(G)$) *Seja G um grupo. Então $\lambda(G) < |c.d.(G)|$.*

Demonstração: Temos $c.d.(G) = \{1 = f_0 < f_1 < \ldots < f_r\}$ e $\lambda_i = \dfrac{1}{f_i^2}$, daí, $|c.d.(G)| = r+1$. Consideremos $q(x) = \prod_{j=1}^{r}(x-\lambda_j)$ e $c = |G'|^{-1}$. Como $\lambda_r < \ldots < \lambda_1 < 1$ são raízes distintas de q, segue que $q(1) \neq 0$ e podemos definir:

$$p(x) = c + (1-c)\frac{q(x)}{q(1)}.$$

Dessa forma, $p(1) = 1$ e $p(\lambda_j) = c$, $1 \leqslant j \leqslant r$. Assim,

$$\min_{1\leqslant j\leqslant r}\left\{\left|\frac{p(1)}{p(\lambda_j)}\right|\right\} = \frac{1}{c} = |G'| \geqslant |G'|.$$

Logo, pelo Teorema 3.1.1, $\lambda(G) \leqslant r < r+1 = |c.d.(G)|$.

□

Lema 3.1.1 *Sejam $(f_i)_{i=0}^{r}$ uma lista de inteiros, onde $1 = f_0 < f_1 < \ldots < f_r$, $\lambda_i = \dfrac{1}{f_i^2}$ e $1 \leqslant n \leqslant r$. Então existe $p(x) \in \mathbb{R}[x]$ de grau n tal que*

$$\left|\frac{p(1)}{p(\lambda_j)}\right| \geqslant 2\prod_{i=1}^{n}(f_i^2-1) - 1 \text{ para } j = 1, 2, \ldots, r.$$

Demonstração: Consideremos o polinômio $p(x) = c+(1-c)\dfrac{q(x)}{q(1)}$, onde

$$q(x) \;=\; \prod_{i=1}^{n}(x-\lambda_i) \;\text{ e }\; c = \frac{(-1)^{n+1}}{2\prod_{i=1}^{n}(f_i^2-1) + (-1)^{n+1}}. \tag{3.3}$$

Afirmação: O polinômio $p(x)$ como descrito acima tem as propriedades em questão.

Demonstração da Afirmação: Temos que $p(\lambda_j) = c$, $1 \leqslant j \leqslant n$. Desse modo, para todo $j \in \{1, \ldots, n\}$,

$$\begin{aligned}\left|\frac{p(1)}{p(\lambda_j)}\right| &= \frac{1}{|c|} = 2\prod_{i=1}^{n}(f_i^2 - 1) + (-1)^{n+1} \\ &\geqslant 2\prod_{i=1}^{n}(f_i^2 - 1) - 1.\end{aligned}$$

Se $p(\lambda_j) = 0$, para algum $n < j \leqslant r$, então convencionaremos que o resultado é válido para aquele λ_j. Assim, resta mostrar que o resultado é válido para os índices $j \in \{n+1, \ldots, r\}$ (portanto, $0 < \lambda_j < \lambda_n$) com $p(\lambda_j) \neq 0$.

Observe que $\partial\, p = n$ e $p(\lambda_j) = c$, para todo $j \in \{1, \ldots, n\}$. Pelo Teorema de Rolle, existem $\xi_i \in (\lambda_{i+1}, \lambda_i)$, $i = 1, \ldots, n-1$, tais que $p'(\xi_i) = 0$ para todo i. E como $\xi_1, \ldots, \xi_{n-1}$ são raízes distintas do polinômio $p'(x)$ temos que $p'(x) \neq 0$ para $x \in \mathbb{R} \setminus \{\xi_1, \ldots, \xi_{n-1}\}$. Como $\xi_1, \ldots, \xi_{n-1} \in (\lambda_n, \lambda_1)$, temos que $p(x)$ restrito ao intervalo $(-\infty, \lambda_n)$ é estritamente crescente ou decrescente, pois $p'(x)$ não pode mudar de sinal fora do intervalo (λ_n, λ_1) (Teorema do Valor Intermediário). Com isso,

$$p(\lambda_n) < p(\lambda_j) < p(0) \qquad \text{ou} \qquad p(0) < p(\lambda_j) < p(\lambda_n).$$

Consequentemente, $|p(\lambda_j)| < \ max\ \{|p(0)|, |p(\lambda_n)|\}$ para $n < j \leqslant r$ e para os $p(\lambda_j) \neq 0$. Pela expressão anterior,

$$\left|\frac{p(1)}{p(\lambda_j)}\right| > \ \min\ \left\{\left|\frac{p(1)}{p(0)}\right|,\ \left|\frac{p(1)}{p(\lambda_n)}\right|\right\}.$$

Mostraremos que $|p(0)| = |c|$. Inicialmente considere,

$$\frac{q(1)}{q(0)} = \frac{\prod_{i=1}^{n}(1-\lambda_i)}{\prod_{i=1}^{n}(-\lambda_i)} = (-1)^n \prod_{i=1}^{n}\left(\frac{1}{\lambda_i} - 1\right) = (-1)^n \prod_{i=1}^{n}(f_i^2 - 1).$$

Da expressão (3.3), obtemos $\prod_{i=1}^{n}(f_i^2 - 1) = (-1)^n \frac{c-1}{2c}$.

Portanto,

$$\begin{aligned} p(0) &= c + (1-c)\frac{q(0)}{q(1)} \\ &= c + (1-c)(-1)^n \left(\prod_{i=1}^{n}(f_i^2 - 1)\right)^{-1} \\ &= c - (1-c)\frac{2c}{c-1} \\ &= -c. \end{aligned}$$

Assim, $|p(0)| = |c|$ e para os $j \in \{n+1, \ldots, r\}$, com $p(\lambda_j) \neq 0$, temos:

$$\begin{aligned} \left|\frac{p(1)}{p(\lambda_j)}\right| &> \frac{1}{|c|} \\ &= 2\prod_{i=1}^{n}(f_i^2 - 1) + (-1)^{n+1} \\ &\geqslant 2\prod_{i=1}^{n}(f_i^2 - 1) - 1. \end{aligned}$$

Logo, $p(x)$ é o polinômio procurado.

□

Corolário 3.1.2 *Sejam G um grupo e $1 \leqslant n \leqslant r$. Se*

$$2\prod_{i=1}^{n}(f_i^2-1)-1 \geqslant |G'|,$$

então $\lambda(G) \leqslant n$.

Demonstração: Consideremos $p(x) \in \mathbb{R}[x]$ o polinômio de grau n obtido no Lema 3.1.1, portanto,

$$\left|\frac{p(1)}{p(\lambda_j)}\right| \geqslant 2\prod_{i=1}^{n}(f_i^2-1)-1 \text{ para } \ j=1,2,\ldots,r.$$

Por hipótese já temos que $|G'| \leqslant 2\prod_{i=1}^{n}(f_i^2-1)-1$ e pelo Teorema 3.1.1, $\lambda(G) \leqslant \partial p = n$.

□

Corolário 3.1.3 *Sejam G um grupo e $1 \leqslant n < r$. Se $\prod_{i=1}^{n} f_i^2 \geqslant |G'|$, então $\lambda(G) \leqslant n$.*

Demonstração: Como $c.d.(G) = \{1 = f_0 < f_1 < \ldots < f_r\}$, temos que $i < f_i$. Daí,

$$\begin{aligned}
\frac{\prod_{i=1}^{n}(f_i^2-1)}{\prod_{i=1}^{n} f_i^2} &= \prod_{i=1}^{n}\left(1-\frac{1}{f_i^2}\right) \\
&\geqslant \prod_{i=2}^{n+1}\left(1-\frac{1}{i^2}\right) \\
&= \prod_{i=2}^{n+1}\left(\frac{i-1}{i}\right)\left(\frac{i+1}{i}\right) \\
&= \frac{n+2}{2(n+1)}.
\end{aligned}$$

Assim,

$$2\prod_{i=1}^{n}(f_i^2-1) \geqslant \frac{n+2}{n+1}\prod_{i=1}^{n} f_i^2 = \Big(1+\frac{1}{n+1}\Big)\Big(\prod_{i=1}^{n} f_i^2\Big) > \prod_{i=1}^{n} f_i^2 \geqslant |G'|.$$

Portanto, $2\prod_{i=1}^{n}(f_i^2-1)-1 \geqslant |G'|$. Pelo Corolário 3.1.2, temos $\lambda(G) \leqslant n$.

□

3.2 Estimativas para $|G'|$

Essa seção é motivada pela seguinte pergunta: "Dado um valor para $\lambda(G)$, que estimativa (inferior) podemos dar para $|G'|$?"No intuito de responder essa pergunta, obtemos uma limitação inferior para a ordem dos derivados dos grupos que possuem elementos não comutadores, tal resultado será de fundamental importância na demonstração do Problema de Bardakov.

Lema 3.2.1 *(Bonner [1]) Seja G um grupo. Se $n = \lambda(G) > 1$, então $|G'| \geqslant (n+1)!(n-1)!$.*

Demonstração: Pelo Corolário 3.1.1, temos $1 < n = \lambda(G) < |c.d.(G)|$, dessa forma, $|c.d.(G)| \geqslant n+1$. Como $n-1 < \lambda(G)$, o Corolário 3.1.2 nos dá a seguinte limitação para a ordem do subgrupo derivado:

$$|G'| > 2\prod_{i=1}^{n-1}(f_i^2-1) - 1.$$

Como $f_i > i$, $i = \{1, \ldots, n\}$, obtemos

$$\begin{aligned} |G'| &> 2\prod_{i=1}^{n-1}(f_i^2 - 1) - 1 \\ &\geqslant 2\prod_{i=2}^{n}(i^2 - 1) - 1 \\ &= \Big(\prod_{i=2}^{n}(i-1)\Big)\Big(2\prod_{i=2}^{n}(i+1)\Big) - 1 \\ &= (n+1)!(n-1)! - 1. \end{aligned}$$

Logo, $|G'| \geqslant (n-1)!(n+1)!$.

□

Observação 3.2.1 *Se G é um grupo com $|G'| < 6$, então $\lambda(G) = 1$. Do Lema 3.2.1 temos que se $\lambda(G) \geqslant 2$, então $|G'| \geqslant (\lambda(G)+1)!(\lambda(G)-1)! \geqslant 6$. Com isso, os grupos cuja ordem seja menor ou igual a 12 tem comprimento do derivado igual a 1, pois seus subgrupos derivados tem ordem menor que 6.*

Proposição 3.2.1 *Seja G um p - grupo. Se $|G'| = p^a$ e $n = \lambda(G) > 1$, então $a > n(n-1)$.*

Demonstração: Pelo Corolário 3.1.1, temos que $n = \lambda(G) < |c.d.(G)|$. Assim, $|c.d.(G)| \geqslant n + 1$. E como G é um p - grupo, todos os f_i's são potências de p, pois dado $\chi \in Irr(G)$, temos $\chi(1)\Big||G|$. Mais ainda, cada $f_i > p^i$, pois são potências de p em ordem crescente e $1 = f_0 < f_1 < \ldots < f_r$. Por outro lado, como $\lambda(G) > n - 1$ temos a seguinte limitação para a ordem do derivado (Corolário 3.1.3):

$$|G'| > \prod_{i=1}^{n-1} f_i^2.$$

Assim,

$$p^a = |G'| > \prod_{i=1}^{n-1}(f_i^2) \geqslant \prod_{i=1}^{n-1}(p^i)^2 = \prod_{i=1}^{n-1}(p^{2i}) = p^{n(n-1)}.$$

Logo, $a > n(n-1)$.

□

Lema 3.2.2 *Seja G um grupo com graus de caracteres $1 < f_1 < f_2$. Então $\lambda(G) \leqslant 2$. Além disso, se $\lambda(G) = 2$, então $|G'| > \dfrac{2f_1^2 f_2^2 - f_1^2 - f_2^2}{f_2^2 - f_1^2}$.*

Demonstração: Pelo Corolário 3.1.1, $\lambda(G) \leqslant 2$. Agora suponhamos que $\lambda(G) = 2$ e tomemos o polinômio $p(x) = ax + b$, onde

$a = \dfrac{-2}{\lambda_1 + \lambda_2 - 2}$ e $b = \dfrac{\lambda_1 + \lambda_2}{\lambda_1 + \lambda_2 - 2}$.

Temos que $p(0) = 1$ e $0 \neq p(\lambda_1) = -p(\lambda_2) = \dfrac{\lambda_2 - \lambda_1}{\lambda_1 + \lambda_2 - 2}$, pois $0 < \lambda_2 < \lambda_1 < 1$. Como $\lambda_2 - \lambda_1 < 0$ e $\lambda_1 + \lambda_2 - 2 < 0$. Portanto,

$$\left|\frac{p(1)}{p(\lambda_1)}\right| = \left|\frac{p(1)}{p(\lambda_2)}\right| = \frac{\lambda_2 + \lambda_1 - 2}{\lambda_2 - \lambda_1} = \frac{2f_1^2 f_2^2 - f_1^2 - f_2^2}{f_2^2 - f_1^2}.$$

Se $|G'| \leqslant \left|\dfrac{p(1)}{p(\lambda_1)}\right| = \left|\dfrac{p(1)}{p(\lambda_2)}\right|$, então $\lambda(G) \leqslant \partial p = 1$ (Teorema 3.1.1). Absurdo, pois $\lambda(G) = 2$. Daí, segue o resultado.

□

Exemplo 3.1 *Se* $|G| = 2^5$*, então* $\lambda(G) = 1$*. Suponhamos que existe um* 2 *- grupo* G *de ordem* 2^5 *com* $\lambda(G) > 1$*. Como* G *tem ordem* 32 *(portanto,* $|G'| \leqslant 8$*). Temos que c.d.*$(G) \subseteq \{1, 2, 2^2\}$*, pois dado* $\chi' \in Irr(G)$ *(Teoremas B.0.4 e B.0.3, respectivamente):*

$$\chi'(1)^2 < \sum_{\chi \in Irr(G)} \chi(1)^2 = |G| \text{ e } \chi'(1)\Big||G|.$$

Mais ainda, se $|c.d.(G)| < 3$*, então* $\lambda(G) = 1$ *(Corolário 3.1.1). Assim, podemos supor que c.d.*$(G) = \{1, 2, 2^2\}$ *e como* $\lambda(G) = 2$*, temos:*

$$|G'| > \frac{2(2^2)(4^2) - 2^2 - 4^2}{4^2 - (2^2)} = 9.$$

Absurdo, pois $|G'| \leqslant 8$*.*

3.3 Conjectura de Bardakov

A partir das limitações apresentadas nas seções anteriores (para "$\lambda(G)$"e "$|G'|$") vamos verificar a Conjectura de Bardakov. Nessa seção iremos adotar a seguinte convenção: grupos com $\lambda(G) = n$ entendemos como sendo a família dos grupos finitos, não abelianos, cujo comprimento do derivado é igual a n.

Proposição 3.3.1 *(Comportamento Assintótico de* $\lambda(G)$ *- Bonner [1])*

$$\lim_{|G| \to \infty} \frac{\lambda(G)}{|G|} = 0.$$

Demonstração: Seja G um grupo, com $c.d.(G) = \{1 = f_0 < f_1 < \ldots < f_r\}$. Pelo Corolário 3.1.1, temos que $\lambda(G) < |c.d.(G)|$. Tomemos $\chi' \in Irr(G)$ cujo grau seja f_r, daí $\chi'(1) = f_r \geqslant r + 1 = |c.d.(G)|$. Por outro lado,

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

Portanto, $|c.d.(G)| \leqslant \sqrt{|G|}$. Assim,

$$\frac{\lambda(G)}{|G|} < \frac{|c.d.(G)|}{|G|} \leqslant \frac{\sqrt{|G|}}{|G|} = \frac{1}{\sqrt{|G|}}.$$

Logo,

$$\lim_{|G|\to\infty} \frac{\lambda(G)}{|G|} = \lim_{|G|\to\infty} \frac{1}{\sqrt{|G|}} = 0.$$

□

Teorema 3.3.1 *(Bonner [1]) Seja G um grupo. Então $\dfrac{\lambda(G)}{|G|} \leqslant \dfrac{1}{6}$ e a igualdade só se verifica quando $G \simeq S_3$.*

Demonstração: Seja G um grupo. Pelo Lema 3.2.1, se $\lambda(G) > 1$, então $|G'| \geqslant (\lambda(G) + 1)!(\lambda(G) - 1)!$ Daí,

$$\textbf{(I)} \quad \frac{\lambda(G)}{|G|} \leqslant \frac{\lambda(G)}{|G'|} \leqslant \frac{\lambda(G)}{(\lambda(G)+1)!(\lambda(G)-1)!} = \frac{1}{(\lambda(G)+1)\left[(\lambda(G)-1)!\right]^2}.$$

Agora vamos verificar a Conjectura de Bardakov, dividindo os grupos nas famílias de Grupos com $\lambda(G) = n$.

Grupos com $\lambda(G) = 1$:

- Se $\lambda(G) = 1$ e $|G| = 6$, então $G \simeq S_3$ e

$$\frac{\lambda(G)}{|G|} = \frac{1}{6}.$$

- Se $\lambda(G) = 1$ e $|G| > 6$, então

$$\frac{\lambda(G)}{|G|} < \frac{1}{6}.$$

Grupos com $\lambda(G) = 2$: Se $\lambda(G) = 2$, então $|G| > 12$ (Observação 3.2.1) e

$$\frac{\lambda(G)}{|G|} = \frac{2}{|G|} < \frac{1}{6}.$$

Grupos com $\lambda(G) \geqslant 3$: Por **(I)**,

$$\frac{\lambda(G)}{|G|} \leqslant \frac{1}{(\lambda(G)+1)[(\lambda(G)-1)!]^2} \leqslant \frac{1}{16} < \frac{1}{6}.$$

□

Observação 3.3.1 *No trabalho de Kappe - Morse em [10] afirma que todos os grupos de ordem menor ou igual a* 1000*, tem comprimento do derivado no máximo* 2 *(usando resultados de Gallagher e implementando em GAP). Usando o Corolário 3.1.1 melhoramos a estimativa conjecturada por Bardakov para grupos de ordem* > 1000 *e temos*

Corolário 3.3.1 *(Bonner [1]) Seja G um grupo. Se $|G| > 1000$, então* $\frac{\lambda(G)}{|G|} \leqslant \frac{1}{250}$.

Demonstração: Suponhamos que o resultado é falso, com isso existe um grupo G tal que

$$|G| > 1000 \text{ e } \frac{\lambda(G)}{|G|} > \frac{1}{250}.$$

Assim, $\lambda(G) > 4$ e por **(I)**:

$$\frac{1}{250} < \frac{\lambda(G)}{|G|} \leqslant \frac{1}{6 \cdot (4!)^2}$$

.

Absurdo. Com isso o resultado é verdadeiro.

□

Pergunta: A Observação 3.3.1 nos propõe, indiretamente, o seguinte problema: "Qual é o grupo G, de ordem mínima, tal que $\lambda(G) = 3$"? E mais geral, qual o exemplo minimal para o qual $\lambda(G) = n$? Mesmo para $\lambda(G) = 3$ esse problema está em aberto, para esse e outros problemas relacionados aos comutadores veja Kappe - Morse [10].

Apêndice A

Grupos com $\lambda(G) = \infty$

Objetivo: Para cada corpo $\mathbb{K}$, apresentaremos um grupo $G_{\mathbb{K}}$ cujo comprimento do derivado é infinito, isto é, dado $n \in \mathbb{N}$, existe $g_n \in G'_{\mathbb{K}}$ o qual não pode ser expresso como o produto de n comutadores. Essa família de exemplos foi dado por P.J. CASSIDY [3] em 1979.

Seja $\mathbb{K}$ um corpo. Denotaremos por $\mathbb{K}[x, y]$ o anel dos polinômios em duas variáveis sobre o corpo $\mathbb{K}$. Em $\mathbb{K}[x, y]$, vamos denotar por $\mathbb{K}[x]$ e $\mathbb{K}[y]$ os subanéis dos polinômios nas variáveis x e y, respectivamente. Podemos ainda considerar, se necessário, $\mathbb{K}[x, y]$ como um $\mathbb{K}$ - espaço vetorial e os subanéis $\mathbb{K}[x], \mathbb{K}[y]$ são $\mathbb{K}$ - subespaços vetoriais de $\mathbb{K}[x, y]$. Definiremos $G_{\mathbb{K}}$ o conjunto das matrizes da forma

$$\begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix}$$

onde $f \in \mathbb{K}[x]$, $g \in \mathbb{K}[y]$ e $h \in \mathbb{K}[x, y]$. De maneira reduzida denotaremos as matrizes apresentadas acima, simplesmente, por $m(f, g, h)$. Tal identificação

é muito útil, pois o produto de matrizes se expressa de maneira simplificada nessa "notação", conforme veremos abaixo.

Proposição A.0.2 *(Propriedades de $G_{\mathbb{K}}$)*

(a) *O conjunto $G_{\mathbb{K}}$ tem uma estrutura natural de grupo, com a operação "herdada"do produto de matrizes;*

(b) $G'_{\mathbb{K}} = Z(G_{\mathbb{K}}) = \{m(0,0,h) \mid h \in \mathbb{K}[x,y]\}$;

(c) $\lambda(G_{\mathbb{K}}) = \infty$.

Demonstração do item (a): Basta observar que dados $f, f_1 \in \mathbb{K}[x]$, $g, g_1 \in \mathbb{K}[y]$, $h, h_1 \in \mathbb{K}[x,y]$

$$\begin{aligned} m(f,g,h)m(f_1,g_1,h_1) &= \begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & f_1 & h_1 \\ 0 & 1 & g_1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & f+f_1 & h+h_1+fg_1 \\ 0 & 1 & g+g_1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= m(f+f_1, g+g_1, h+h_1+fg_1) \end{aligned}$$

Com isso, a multiplicação de matrizes restrita ao conjunto acima é de fato uma operação. Temos que $1_{G_{\mathbb{K}}} = m(0,0,0)$, a expressão do produto de dois elementos dado acima nos dá $m(f,g,h)^{-1} = m(-f,-g,fg-h)$ e a associatividade é herdada do anel de matrizes (com entradas em $\mathbb{K}[x,y]$ - que é um anel comutativo com 1). Daí, $G_{\mathbb{K}}$ é um grupo.

Demonstração do item (b): Chamemos $H = \{m(0,0,h) \ : \ h \in \mathbb{K}[x,y]\}$ e para simplificar a demonstração desse item vamos dividi-la em duas afirmações, onde vamos comparar o subgrupo derivado e o centro do grupo (com H).

Afirmação (1): $H = Z(G_{\mathbb{K}})$.

Demonstração da Afirmação (1): Dados $m(f,g,h)$ e $m(0,0,h_1) \in G_{\mathbb{K}}$, temos $m(f,g,h)m(0,0,h_1) = m(f,g,h+h_1) = m(0,0,h_1)m(f,g,h)$. Portanto, $H \leqslant Z(G_{\mathbb{K}})$. Por outro lado, seja $m(f_0,g_0,h_0) \in Z(G_{\mathbb{K}})$, temos para todo $m(f,g,h)$: $m(f,g,h)m(f_0,g_0,h_0) = m(f_0,g_0,h_0)m(f,g,h)$, ou seja,

$$m(f+f_0, g+g_0, fg_0+h+h_0) = m(f_0+f, g_0+g, f_0g+h+h_0).$$

Assim, $fg_0 = f_0g$ para qualquer $f \in \mathbb{K}[x]$ e $g \in \mathbb{K}[y]$. Vamos mostrar que $f_0 = 0 = g_0$.

Suponhamos que $f_0 \neq 0$ e tomemos $g \neq 0$ e $f = 0$, com isso $0 \neq fg_0 = f_0g = 0$. Absurdo, dessa forma, $f_0 = 0$. De modo análogo, $g_0 = 0$. Assim, $H = Z(G_{\mathbb{K}})$.

Afirmação (2): $H = G'_{\mathbb{K}}$.

Demonstração da Afirmação (2): Vamos mostrar que: $G'_{\mathbb{K}} \leqslant H$. O comutador de dois elementos é dado por:

$$\begin{aligned}
[m(f,g,h), m(f_1,g_1,h_1)] &= [m(f,g,0)m(0,0,h), m(f_1,g_1,0)m(0,0,h_1)] \\
&= [m(f,g,0), m(f_1,g_1,0)], \text{ pois } Z(G_{\mathbb{K}}) = H \\
&= m(f,g,0)^{-1}m(f_1,g_1,0)^{-1}m(f,g,0)m(f_1,g_1,0) \\
&= m(-f,-g,0)m(-f_1,-g_1,0)m(f,g,0)m(f_1,g_1,0) \\
&= m(0,0,fg_1-gf_1).
\end{aligned}$$

Assim,

$$\begin{aligned} G'_{\mathbb{K}} &\overset{def.}{=} \langle [m(f,g,h), m(f_1,g_1,h_1)] \mid m(f,g,h), m(f_1,g_1,h_1) \in G_{\mathbb{K}} \rangle \\ &= \langle [m(f,g,0), m(f_1,g_1,0)] \mid m(f,g,0), m(f_1,g_1,0) \in G_{\mathbb{K}} \rangle \\ &= \langle [m(0,0,fg_1 - f_1g)] \rangle \\ &\leqslant H \end{aligned}$$

A outra inclusão é garantida pelo seguinte, se $h = \sum_{i,j} a_{ij}x^iy^j$, então

$$\begin{aligned} m(0,0,h) &= m(0,0,\sum_{i,j} a_{ij}x^iy^j) \\ &= \prod_{i,j} m(0,0,a_{ij}x^iy^j) \\ &= \prod_{i,j} \left[m(a_{ij}x^i,0,0), m(0,y^j,0) \right]. \end{aligned}$$

Logo, $H = G'_{\mathbb{K}}$.

Dem.(c): Seja $n \in \mathbb{N}$. Consideremos $h = \sum_{i=0}^{2n} x^iy^{2n-i}$ e $m(0,0,h) \in G'_{\mathbb{K}}$. Vamos mostrar que $m(0,0,h)$ não pode ser escrito como o produto de n comutadores.

Suponhamos que $m(0,0,h) \in K_n(G_{\mathbb{K}})$. Sem perda de generalidade, pois $H = Z(G)$, existem $s_j(x), u_j(x) \in \mathbb{K}[x]$ e $t_j(y), v_j(y) \in \mathbb{K}[y]$, com $1 \leqslant j \leqslant n$, tais que

$$\begin{aligned} m(0,0,h) &= \prod_{j=1}^{n} [m(s_j(x), t_j(y), 0), m(u_j(x), v_j(y), 0)] \\ &= \prod_{j=1}^{n} m(0,0, s_j(x)v_j(y) - t_j(y)u_j(x)) \\ &= m(0,0, \sum_{j=1}^{n} \big(s_j(x)v_j(y) - t_j(y)u_j(x)\big)). \end{aligned}$$

Portanto, $h = \sum_{j=1}^{n} \big(s_j(x)v_j(y) - t_j(y)u_j(x)\big)$. Chamemos $s_j(x) = \sum_i a_{ij}x^i$, $t_j(x) = \sum_i b_{ij}x^i$, onde $a_{ij}, b_{ij} \in \mathbb{K}$ e $1 \leqslant j \leqslant n$. Por outro lado,

$$\begin{aligned} \sum_{i=0}^{2n} x^i y^{2n-i} &= \sum_{j=1}^{n} \Big(\Big(\sum_i a_{ij}x^i \Big) v_j(y) - \Big(\sum_i b_{ij}x^i \Big) u_j(y) \Big) \\ &= \sum_{j=1}^{n} \sum_i \Big(a_{ij}v_j(y) - b_{ij}t_j(y) \Big) x^i \\ &= \sum_i \Big(\sum_{j=1}^{n} a_{ij}v_j(y) - b_{ij}t_j(y) \Big) x^i \end{aligned}$$

Com isso, $y^{2n-i} = \sum_{j=1}^{n} \big(a_{ij}v_j(y) - b_{ij}t_j(y)\big)$, para cada $0 \leqslant i \leqslant 2n$.

Dessa forma, o subespaço V gerado pelos polinômios $1, y, \ldots, y^{2n}$ está contido no subespaço W gerado por $\{t_1(y), \ldots, t_n(y), v_1(y), \ldots, v_n(y)\}$. Absurdo, pois teríamos $2n + 1 = dim_{\mathbb{K}}(V) \leqslant dim_{\mathbb{K}}(W) = 2n$.

Assim, para todo $n \in \mathbb{N}$ existe $g_n = m(0,0, \sum_{i=0}^{2n} x^i y^{2n-i}) \notin K_n(G_{\mathbb{K}})$. Logo, $\lambda(G) = \infty$.

□

Apêndice B

G - módulos Irredutíveis

B.0.1 Classificação dos G - módulos Irredutíveis

Seja G um grupo finito. Como consequência do Teorema de Maschke, o $\mathbb{C}G$ módulo regular é completamente redutível e, portanto admite uma fatoração da forma:

$$\mathbb{C}G = U_1 \oplus \ldots \oplus U_s,$$

sendo cada U_i um G - submódulo irredutível de $\mathbb{C}G$. Nessa seção vamos mostrar que: "Se M é um G - módulo irredutível, então existe $i \in \{1, \ldots, s\}$ tal que $M \simeq_G U_i$". Dessa forma estamos classificando todos os G - módulos irredutíveis, a menos de G - isomorfismo, como sendo os G - submódulos irredutíveis de $\mathbb{C}G$.

Proposição B.0.3 *(Teorema dos Homomorfismos para G - módulos [1]) Sejam V e W G - módulos. Se $\theta : V \to W$ é um G - homomorfismo, então existe $U \leqslant_G V$ tal que $V = U \oplus Ker\ \theta$ e $U \simeq_G Im\ \theta$.*

[1] Teorema do Núcleo e da Imagem para G - módulos

Demonstração: Já temos que $Ker\ \theta \leqslant_G V$ e pelo Teorema de Maschke, existe $U \leqslant_G V$ tal que $V = U \oplus Ker\ \theta$. Resta mostrar que $U \simeq_G Im\ \theta$, para isso definamos

$$\begin{array}{rccc} \bar{\theta} & : & U & \longrightarrow & Im\ \theta \\ & & u & \longmapsto & \theta(u) \end{array}$$

- $\bar{\theta}$ é um G - isomorfismo: De fato, $\bar{\theta}$ é um G - homomorfismo, pois θ o é. Com isso, resta mostrar que $\bar{\theta}$ é uma bijeção.

  – $Im\ \bar{\theta} = Im\ \theta$: Por definição, $Im\ \bar{\theta} \subseteq Im\ \theta$. Agora vamos mostrar a inclusão oposta, dado $w \in Im\ \theta$, existe $v \in V$ tal que $\theta(v) = w$. Mas, $V = U \oplus Ker\ \theta$ temos que $v = v_1 + v_2$, onde $v_1 \in U$ e $v_2 \in Ker\ \theta$, portanto $w = \theta(v) = \theta(v_1 + v_2) = \theta(v_1) + \theta(v_2) = \theta(v_1) = \bar{\theta}(v_1)$. aí, $w \in Im\ \bar{\theta}$ e, como w é arbitrário, temos $Im\ \theta \subseteq Im\ \bar{\theta}$.

  – $Ker\ \theta = \{0\}$: Vejamos,

$$\begin{aligned} Ker\ \bar{\theta} &= \{u \in U \mid \bar{\theta}(u) = 0\} \\ &= \{u \in U \mid \theta(u) = 0\} \\ &= U \cap Ker\ \theta \\ &= \{0\}. \end{aligned}$$

  Logo, $\bar{\theta}$ é um G - isomorfismo e $U \simeq_G Im\ \theta$.

□

A proposição a seguir vai nos garantir que independente da fatoração que tomarmos para um dado G - módulo ("por G - submódulos irredutíveis"), ela

irá conter, a menos de G - isomorfismos, todos os G - submódulos irredutíveis do G - módulo em questão.

Proposição B.0.4 *Sejam V um G - módulo, U um G - módulo irredutível e $V = U_1 \oplus \ldots \oplus U_s$. Se $U_1, \ldots, U_s$ são irredutíveis, então existe $i \in \{1, \ldots, s\}$ tal que $U \simeq_G U_i$.*

Demonstração: Para cada $u \in U$, podemos escrever (de modo único) $u = u_1 + \ldots + u_s$, onde $u_i \in U_i$. Com isso podemos definir (e estará bem definido) as projeções sobre os G - submódulos:

$$\begin{aligned} \pi_i \ : \ U &\longrightarrow U_i \\ u &\longmapsto u_i \end{aligned}$$

Temos que existe $i \in \{1, \ldots, s\}$ tal que $Im\ \pi_i(U) \neq \{0\}$. Caso contrário, teríamos $U = \{0\}$, o que não pode ocorrer, visto que U é um G - módulo irredutível. Já temos que π_i é um G - homomorfismo e pelo Lema de Schur, π_i é um G - isomorfismo de U sobre U_i, visto que U, U_i são G - módulos irredutíveis e $Im\ \pi_i \neq \{0\}$.

□

Teorema B.0.2 *(Classificação dos G - módulos Irredutíveis) Sejam $\mathbb{C}G$ o G - módulo regular e $\mathbb{C}G = U_1 \oplus \ldots \oplus U_r$, uma fatoração de $\mathbb{C}G$ por G - submódulos irredutíveis. Se W um G - módulo irredutível, então $W \simeq_G U_i$ para algum $i \in \{1, \ldots, r\}$.*

Demonstração: Consideremos $0 \neq w \in W$ e definamos

$$\begin{aligned} \theta \ : \ \mathbb{C}G &\longrightarrow W \\ r &\longmapsto wr \end{aligned}$$

- θ é um G - submódulo: dados $r, s \in \mathbb{C}G$ e $\lambda \in \mathbb{C}$, temos
  - $\theta(r + \lambda s) = w(r + \lambda s) = (wr) + \lambda(ws) = \theta(r) + \lambda(s)$;
  - $\theta(rs) = (w)rs = (wr)s = \theta(r)s$.

Pelo Teorema do Núcleo e da Imagem, existe $U \leqslant_G \mathbb{C}G$ tal que $\mathbb{C}G = U \oplus Ker\ \theta$ e $U \simeq_G Im\ \theta = W$. Assim, U é um G - módulo irredutível e pela Proposição anterior, existe $i \in \{1, \ldots, r\}$ tal que $U \simeq_G U_i$. Logo, $W \simeq_G U_i$.

□

Corolário B.0.2 *e G é um grupo finito, então existem um número finito de G - módulos irredutíveis não isomorfos.*

Demonstração: Sejam W um G - módulo irredutível e $\mathbb{C}G$ o G - módulo regular. Como consequência do Teorema de Maschke,

$$(*) \qquad \mathbb{C}G \ = \ U_1 \oplus \ldots \oplus U_r$$

onde $U_i \leqslant_G \mathbb{C}G$, $i = 1, \ldots r$. Como W é um G - módulo irredutível, pelo Teorema de Classificação dos G - módulos irredutíveis, existe $i \in \{1, \ldots, r\}$ tal que $W \simeq_G U_i$. Logo, o número de G - módulos irredutíveis é igual ao número de G - submódulos não isormofos da fatoração $(*)$[2].

□

[2]Ou qualquer outra fatoração de $\mathbb{C}G$ por G - submódulos irredutíveis.

B.0.2 G - módulos e a ordem do grupo G

Nessa seção estudaremos como a aritmética de $|G|$ está relacionada com os G - módulos (sobre $\mathbb{C}$).

Teorema B.0.3 *Sejam G um grupo com h classes de conjugação e $\chi_1, \ldots, \chi_h$ os caracteres irredutíveis de G. Os graus $n_1, \ldots n_h$ dos caracteres irredutíveis de G sobre $\mathbb{C}$ dividem $|G|$.*

Para uma demonstração desse resultado veja G. James e M. Liebeck [11], página 249.

Definição B.0.1 *Dizemos que os G - módulos $V_1, \ldots, V_k$ formam um sistema completo de G - módulos irredutíveis se $V_i \not\simeq_G V_j$, para $i \neq j$ e dado um G - módulo irredutível, digamos U, temos que $V_i \simeq_G U$, para algum $i \in \{1, \ldots, k\}$. Como consequência do Teorema de Classificação dos G - módulos irredutíveis, para todo grupo finito G existe um sistema completo de G - módulos irredutíveis.*

Proposição B.0.5 *Sejam V e W G - módulos irredutíveis. Então*

$$dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V,W)) = \begin{cases} 1, & se \quad V \simeq_G W \\ 0, & se \quad V \not\simeq_G W \end{cases}$$

Demonstração: *Se $V \not\simeq_G W$, então o Lema de Schur garante que o único G - homomorfismos de V em W possível é o trivial. Portanto, $Hom_{\mathbb{C}G}(V,W) = \{0\}$ e $dim_{\mathbb{C}G}(Hom_{\mathbb{C}G}(V,W)) = 0$. Agora suponhamos que $V \simeq_G W$ e tomemos $\theta : V \to W$ um G - isomorfismo.*

- *$Hom_{\mathbb{C}G}(V,W) = \{\lambda\theta \mid \lambda \in \mathbb{C}\}$ (ou seja, $dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V,W)) = 1$).*

Dado $\varphi \in Hom_{\mathbb{C}G}(V,W)$, temos que $\theta^{-1}\varphi : V \to V$ é um G - isomorfismo de V sobre V. Pelo Lema de Schur, existe $\lambda \in \mathbb{C}$ tal que $\theta^{-1}\varphi = \lambda Id_V$ e $\varphi = \lambda\theta$. Portanto, θ gera $Hom_{\mathbb{C}G}(V,W)$ e $dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V,W)) = 1$.

□

Proposição B.0.6 *Sejam V, W, V_1, W_1, V_2 e W_2 G - módulos. Então,*

(a) $dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V, W_1 \oplus W_2)) = \sum_{i=1}^{2} dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V, W_i))$;

(b) $dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)) = \sum_{i=1}^{2} dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V_i, W))$.

Demonstração do item (a): *Consideremos as projeções $\pi_i : W_1 \oplus W_2 \to W_i$, com $i = 1, 2$ e*

$$\begin{array}{rccc} f & : & Hom_{\mathbb{C}G}(V, W_1 \oplus W_2) & \longrightarrow & Hom_{\mathbb{C}G}(V, W_1) \oplus Hom_{\mathbb{C}G}(V, W_2) \\ & & \theta & \longmapsto & (\pi_1 \circ \theta, \pi_2 \circ \theta) \end{array}$$

Note que f está bem definida, pois $\pi_i \circ \theta$, com $i = 1, 2$, são G - homomorfismo de V em W_i.

Afirmação: *f é um isomorfismo linear.*

Demonstração da Afirmação: *A aplicação f é linear, pois $\pi_i \circ \theta$ é a composta de aplicações lineares. Agora mostremos que f é bijeção,*

- *f é sobre: dados $\phi_i \in Hom_{\mathbb{C}G}(V, W_i)$, definamos:*

$$\begin{array}{rccc} \phi & : & V & \longrightarrow & W_1 \oplus W_2 \\ & & v & \longmapsto & (\phi_1(v), \phi_2(v)) \end{array}$$

dessa forma ϕ é um G - homomorfismo e

$$f(\phi) = (\pi_1 \circ \phi, \pi_2 \circ \phi) = (\phi_1, \phi_2).$$

Logo, f é sobre.

- *f é $1-1$: dado $\theta \in Ker\ f$, daí, $\pi_i(\theta(v)) = 0$, para $i = 1, 2$. Logo, $\theta \equiv 0$.*

Conclusão: *os espaços $Hom_{\mathbb{C}G}(V, W_1 \oplus W_2)$ e $Hom_{\mathbb{C}G}(V, W_1) \oplus Hom_{\mathbb{C}G}(V, W_2)$ são isomorfos ("no sentido linear"), logo tem mesma dimensão.*

Demonstração do item (b): *Dado $\theta \in Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)$, consideremos as restrições*

$$\begin{array}{rccc} \theta_i := \theta_{|_{V_i}} & : & V_i & \longrightarrow & W \\ & & v_i & \longmapsto & \theta(v_i) \end{array}$$

com isso, $\theta_i \in Hom_{\mathbb{C}G}(V_i, W)$ e consideremos:

$$\begin{array}{rccc} h & : & Hom_{\mathbb{C}G}(V_1 \oplus V_2, W) & \longrightarrow & Hom_{\mathbb{C}G}(V_1, W) \oplus Hom_{\mathbb{C}G}(V_2, W) \\ & & \theta & \longmapsto & (\theta_1, \theta_2) \end{array}$$

Temos que h é uma aplicação linear, pois é a restrição de aplicações lineares a seus subespaços e mais:

- *h é injetora: dados $\theta, \psi \in Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)$ tais que $h(\theta) = h(\psi)$. Assim, $\theta_1 = \psi_1$, $\theta_2 = \psi_2$ e consequentemente, $\theta = \psi$.*

- *h é sobre: dados $\theta_i \in Hom_{\mathbb{C}G}(V_i, W)$, para $i = 1, 2$. Consideremos $\bar{\theta} \in Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)$, onde $\bar{\theta}(v_1, v_2) = \theta_1(v_1) + \theta_2(v_2)$. Portanto, $h(\bar{\theta}) = (\theta_1, \theta_2)$.*

Logo, os espaços $Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)$ e $Hom_{\mathbb{C}G}(V_1, W) \oplus Hom_{\mathbb{C}G}(V_2, W)$ tem mesma dimensão.

Observação B.0.2 *Sejam $V, W, V_1, \ldots, V_r, W_1, \ldots, W_s$ G - módulos. Então,*

(a') $dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V_1 \oplus \ldots \oplus V_r, V)) = \sum_{j=1} r dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V_i, V))$;

(b') $dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(W, W_1 \oplus \ldots \oplus W_s)) = \sum_{j=1} s dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V, W_j))$.

Para o item (a'), façamos indução sobre r, o caso $r = 2$ (base da indução) foi feito na Proposição B.0.6. Suponhamos que o resultado é válido para $n \in \mathbb{N}$ e tomemos o "caso" $n+1$: tomemos $U = V_1 \oplus \ldots \oplus V_n$ e V_{n+1}. Daí, pelo item (a) e indução, segue o item (a') da Proposição B.0.6. O item (b') é análogo.

□

Corolário B.0.3 *Sejam W um G - módulo irredutível e V um G - módulo com $V = U_1 \oplus U_s$. Se cada U_i é um G - módulos irredutíveis, então*

$$dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V, W)) = Hom_{\mathbb{C}G}(W, V) = |\{i \mid 1 \leqslant i \leqslant s \text{ e } U_i \simeq W\}|.$$

Demonstração: *Pelo Lema de Schur: se W é um G - módulo irredutívelo, então*

$$dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(U_i, W)) = dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(W, U_i)) = \begin{cases} 1, & se \quad U_i \simeq_G W \\ 0, & se \quad U_i \not\simeq_G W \end{cases}.$$

Assim,

$$\begin{aligned} dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V,W)) &= dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(U_1 \oplus \ldots \oplus U_s, W)) \\ &= \sum_{i=1}^{s} dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(U_i, W)) \\ &= \sum_{i=1}^{s} dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(W, U_i)) \\ &= dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(W, U_1 \oplus \ldots \oplus U_s)) \\ &= dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(W,V)). \end{aligned}$$

Finalmente,

$$\begin{aligned} dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V,W)) &= \sum_{i=1}^{s} dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(U_i, W)) \\ &= |\{i \mid 1 \leqslant i \leqslant s \ e \ U_i \simeq W\}|. \end{aligned}$$

□

Proposição B.0.7 *Se U é um G - módulo, então*

$$dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(\mathbb{C}G, U)) = dim_{\mathbb{C}}(U).$$

Demonstração: *Escolhamos $\beta = \{u_1, \ldots, u_d\}$ uma base para U, onde $d = dim_{\mathbb{C}}(U)$. Definamos para cada $1 \leqslant i \leqslant d$:*

$$\begin{aligned} \phi_i \ : \ \mathbb{C}G &\longrightarrow U \\ r &\longmapsto u_i r \end{aligned}$$

note que $\phi_i \in Hom_{\mathbb{C}G}(\mathbb{C}G, U)$, $i = 1, \ldots, d$. Mostraremos que $\phi_1, \ldots, \phi_d$ forma uma base para $Hom_{\mathbb{C}G}(\mathbb{C}G, U)$.

– *Temos* $\phi(1) \in U$, *assim* $\phi(1) = \lambda_1 u_1 + \ldots + \lambda_d u_d$, *onde* $\lambda_i \in \mathbb{C}$. *Como* ϕ *é um* G *- homomorfismo, dado* $r \in \mathbb{C}G$, *temos:*

$$\phi(r) = \phi(1)r = \left(\sum_{i=1} d\lambda_i u_i\right) r = \sum_{i=1} d\lambda_i (u_i r) = \sum_{i=1} d\lambda_i \phi_i.$$

Portanto, $\phi_1, \ldots, \phi_d$ *geram* $Hom_{\mathbb{C}G}(\mathbb{C}G, U)$.

– $\phi_1, \ldots, \phi_d$ *é linearmente independente: dados* $\mu_1, \ldots, \mu_d \in \mathbb{C}$, *tais que* $\sum_{i=1}^{d} \mu_i \phi_i = 0$, *assim*

$$0 = (\sum_{i=1}^{d} \mu_i \phi_i)(1) = \sum_{i=1}^{d} \mu_i \phi_i(1) = \sum_{i=1}^{d} \mu_i (u_i 1) = \sum_{i=1}^{d} \mu_i u_i.$$

Mas $u_1, \ldots, u_d$ *forma uma base para* U. *Logo,*

$$dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(\mathbb{C}G, U)) = d = dim_{\mathbb{C}}(U).$$

□

Lema B.0.1 *Suponhamos que* $\mathbb{C}G = U_1 \oplus \ldots \oplus U_r$, *onde* U_i *são* G *- submódulos irredutíveis. Se* U *é um* G *- módulo irredutível, então*

$$|\{i \mid 1 \leqslant i \leqslant r \text{ e } U_i \simeq U\}| = dim_{\mathbb{C}}(U).$$

Demonstração: *Pela Proposição B.0.7,* $dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(\mathbb{C}G, U))$ *o qual é justamente o número de* U_i *que são* G *- isomorfos a* U.

□

Teorema B.0.4 *Sejam $V_1, \ldots, V_k$ um sistema completo de G - módulos irredutíveis não isomorfos. Então:*

$$\sum_{i=1}^{k} \Big(dim_{\mathbb{C}}(V_i) \Big)^2 = |G|.$$

Demonstração: *Consideremos $\mathbb{C}G$ o G - módulo regular com fatoração $\mathbb{C}G = U_1 \oplus \ldots \oplus U_r$, onde U_i são G - módulos irredutíveis. Chamemos $d_i = dim_{\mathbb{C}}(U_i)$. Pelo Lema B.0.1 $|\{j \mid 1 \leqslant j \leqslant r \text{ e } U_j \simeq_G V_i\}| = d_i$. Daí,*

$$\begin{aligned} |G| &= dim_{\mathbb{C}}(\mathbb{C}G) = dim_{\mathbb{C}}(U_1) + \ldots + dim_{\mathbb{C}}(U_r) \\ &= \sum_{i=1}^{k} d_i (dim_{\mathbb{C}}(V_i) \\ &= \sum_{i=1}^{k} \Big(dim_{\mathbb{C}}(V_i) \Big)^2. \end{aligned}$$

□

Notações

x^y	$y^{-1}xy$;
$[x, y]$	$x^{-1}y^{-1}xy$;
$\|S\|$	Cardinalidade do conjunto S;
$H \leqslant G$	H é subgrupo de G;
$H \trianglelefteq G$ *ou* $H \triangleleft G$	H é subgrupo normal de G;
$G \simeq K$	G é isomorfo a K;
$W \simeq_G V$	W é G - isomorfo a V;
$\|G : H\|$	Índice do subgrupo H no grupo G;
$\langle X \rangle$	O subgrupo gerado por X;
$[A, B]$	subgrupo $\langle [a, b] \mid a \in A$ e $y \in B \rangle$;
G'	$[G, G]$;
$\lambda(G)$	comprimento do derivado de G;
ΓG	conjunto dos comutadores de G;
G/N	Grupo quociente de G por (um subgrupo normal) N;
$G_1 \times \ldots \times G_k$	produto direto dos grupos $G_1, \ldots, G_k$;
$H \rtimes N$	produto semidireto de N por H;

$dim_{\mathbb{K}}(V)$	dimensão do $\mathbb{K}$ - espaço vetorial V;
$W \leqslant_G V$	W é G - submódulo de V;
$GL(n, F)$	conjunto das matrizes $n \times n$ invertíveis, onde $n \in \mathbb{N}$ e $F = \mathbb{R}$ ou $\mathbb{C}$;
$Z(G)$	centro de G;
V	grupo de Klein e $V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;
S_n	grupo das permutações de n letras;
A_n	grupo das permutações pares de n letras;
D_n	grupo diedral de ordem $2n$;
$Irr(G)$	conjunto dos caracteres irredutíveis de G;
$c.d.(G)$	conjunto dos graus dos caracteres irredutíveis de G;
f_χ	grau do caracter χ;
$k(G)$	número de classes de conjugação de G.
∂p	grau do polinômio p;
$Hom_{\mathbb{C}G}(V, W)$	conjunto dos G - homomorfismos de V em W.

Referências Bibliográficas

[1] BONNER, T. Products of commutators and the order of a finite group. **Journal of Algebra**, v. 320, p. 3165-3171, 2008.

[2] BURNISDE, W. **Theory of groups of finite order.** Cambridge, Cambridge University Press, 1911.

[3] CASSIDY, P.J. Products of Commutators are Not Always Commutators: An Example. **The American Mathematical Monthly**, v. 86, n. 9, p. 772, novembro, 1979.

[4] DIXON, J.D. **Problems in group theory.** New York, Dover, 2007.

[5] FITE, B. W. On metabelian groups. **Transactions of the American Mathematical Society**, v. 3, n. 3, p. 331-353, julho, 1902.

[6] GALLAGHER, P.X. Group characters and commutators. **Mathematische Zeitschrift**, v. 79, p. 122-126, 1962.

[7] GALLAGHER, P.X. The Generation of the Lower Central Series. **Canadian Journal of Mathematics**, v. 17, p. 405-410, 1965.

[8] GORENSTEIN, D. **Finite Groups.** New York, Harper Row, 1968. 527 p.

[9] GURALNICK, R.M. Expressing Group Elements as Commutators. **Rocky Moutain Journal of Mathematics**, v. 10, n. 3, 1980

[10] GURALNICK, R.M. Commutators and Commutator Subgroups. **Advances in Mathematics**, v. 45, p. 319-330, 1982.

[11] JAMES, G., LIEBECK, M. **Representations and characters of groups**, Cambridge, Cambridge University Press, 2002.

[12] KAPPE, L.-C., MORSE, R.F. On Commutators in groups. In: **Groups St Andrews 2005**, Cambridge: Cambridge University Press, 2007.

[13] KHUKHRO, E.I., MAZUROV, V.D. (eds), ***Unsolved Problems in Group Theory***, The Kourovka Notebook Notebook, No. 16, Russian Academy of Sciences Siberian Division, Institute of Mathematics, Novosibirsk, 2006

[14] MAIER, R. R., **Introdução à Teoria das Representações dos Grupos Finitos - Texto de Aula**, Brasília, 2002, 70 p.

[15] ROBINSON, D. J. S., ***A Course in the Theory Group***, 2° ed., New York (Graduate Texts in Mathematics, 80), Springer-Verlag, 1996.

[16] SIMON, B., ***Representations of Finite and Compact Groups***, American Mathematical Society, Providence (Graduate Studies in Mathematics, 10), 1996.